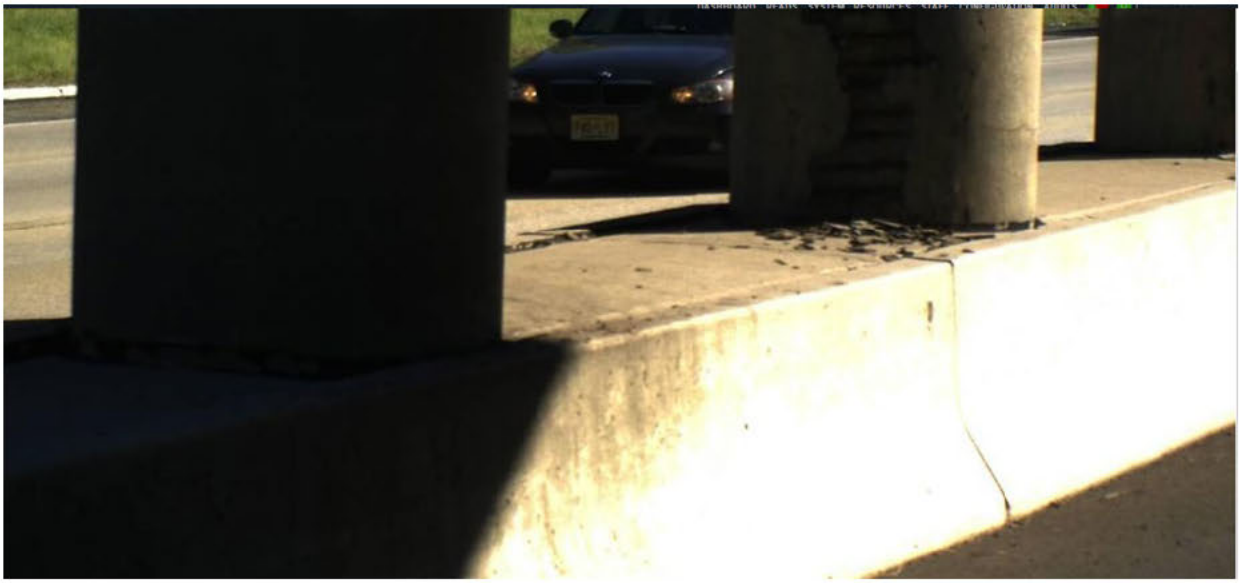
From: John Tedona
To: Egnitz, Brian (POL)
Subject: ALPR Cameras
Date: Wednesday, June 10, 2020 6:12:06 PM
Attachments: image001.png
image003.png
image009.png
image010.png
Mobile P720 Brochure.pdf

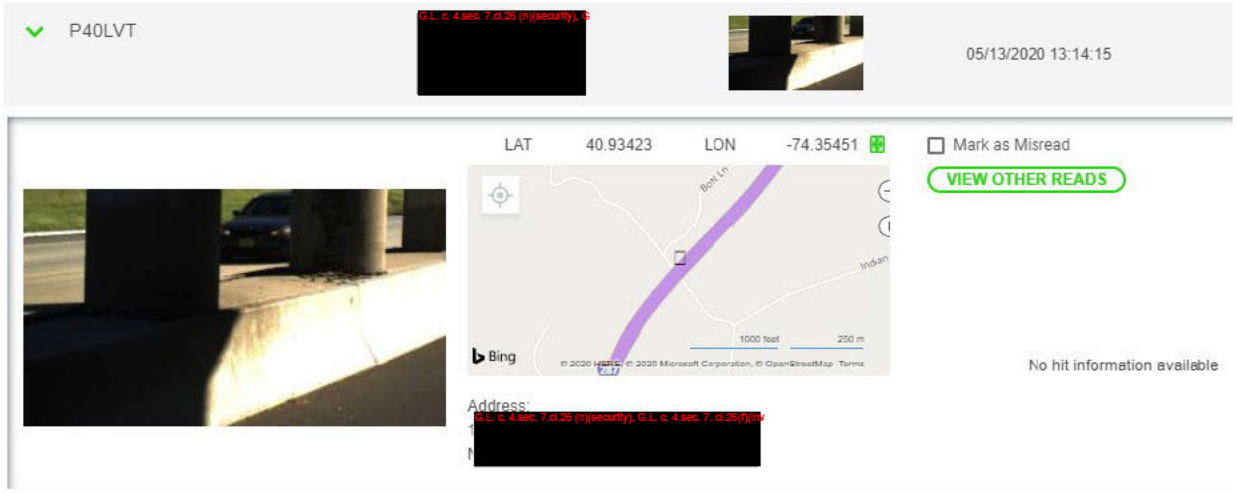
CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Brian,

I learned that we are working to deploy a fixed version of a P720 mobile camera -minus the processor- to augment the IRIS camera. The below is a screen shot of a plate I read the other week. Combined speed was 140mph and the on coming vehicle was five lane widths away. Not to mention it was read in a very tight window between two bridge supports. The camera is 60 FPS so at 140mph it was most likely captured in only one frame.

You have the credentials to log into BOSS now and I should be able to mail the demo mobile system out to you this Friday. You'll have plenty to play with now Where do I send the mobile system....470 Worcester Rd?







A NEOLOGY Business

John Tedona
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: Terrey, Susan (EPS)
To: Collins, Kerry (EPS); Staples, Jennifer (POL); Koulouris, Agapi (CHS); Lord, Spencer (EPS); McGarry, Matthew (CHS); Mullaney, Arielle (EPS); Wark, Jake (EPS)
Subject: ALPR eopss 122220 swt NDB
Date: Tuesday, December 22, 2020 11:31:16 AM
Attachments: ALPR eopss 122220 swt NDB.docx

See the last two small changes if we can live with it let me know

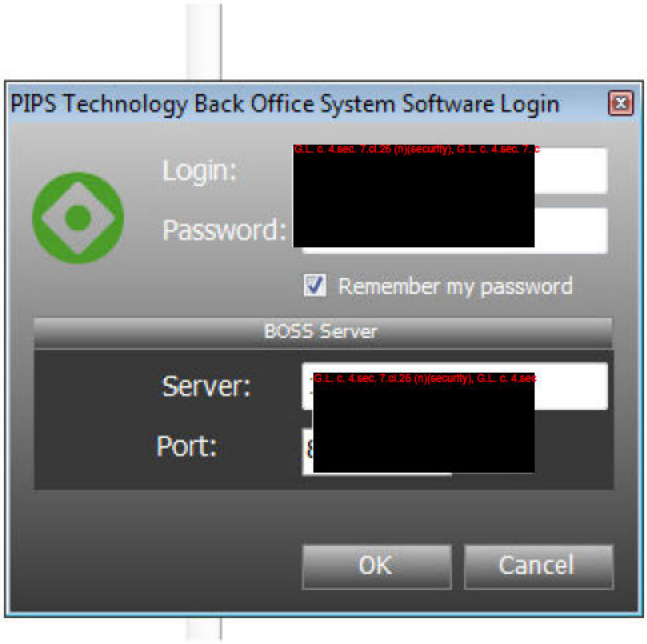
From: Gallagher, David (POL)
To: Connolly, Steven (AGO)
Subject: ALPR information
Date: Sunday, July 26, 2020 1:49:32 PM
Attachments: pastedImagebase640.png
BOSS 3.6 USER MANUAL Rev2.pdf

Steve,

To download the software cut and paste the following into your browser http[redacted].htm once loaded you will need to configure the port and perhaps the IP address. Click on the "Boss server" which will open the box below and make sure you have the correct server/port info. Once you connect to the server you won't have to do it again.

Your login would be msp2719 and the password I sent you would obviously go in the password section

Could you please forward this info as well as the login information to the other accounts I set up.



David M. Gallagher
Captain, Massachusetts State Police
Special Operations
508-988-7442
David.Gallagher3@MassMail.state.ma.us

From: Gallagher, David (POL)
To: Snow, Corrine (POL)
Subject: ALPR User Guide
Date: Tuesday, April 28, 2020 9:05:15 AM
Attachments: BOSS 3.6 USER MANUAL Rev2.pdf

Corrine,

Please see attached.

Thank you,

David M. Gallagher
Captain, Massachusetts State Police
Special Operations
508-988-7442
David.Gallagher3@MassMail.state.ma.us

From: Gallagher, David (POL)
To: Berberena, Jorell (POL)
Subject: ALPR User Guide
Date: Saturday, November 7, 2020 11:17:35 AM
Attachments: BOSS 3.6 USER MANUAL Rev2.pdf

Please see attached.

David M. Gallagher
Major, Massachusetts State Police
Special Operations
508-820-2162
David.Gallagher3@MassMail.state.ma.us

From: Gallagher, David (POL)
To: Tirella, Orlando (AGO)
Subject: ALPR
Date: Friday, August 7, 2020 1:55:56 PM
Attachments: pastedImagebase640.png
BOSS 3.6 USER MANUAL Rev2.pdf

Sergeant,

MAKE SURE YOU ARE USING INTERNET EXPLORER 11

To download the software cut and paste the following into your browser http://[redacted]9988/publish.htm once loaded you will need to configure the port and perhaps the IP address. Click on the “Boss server” which will open the box below and make sure you have the correct server/port info. Once you connect to the server you won’t have to do it again.

Your login would be [redacted] and your password is [redacted]
You can change it after you logon.

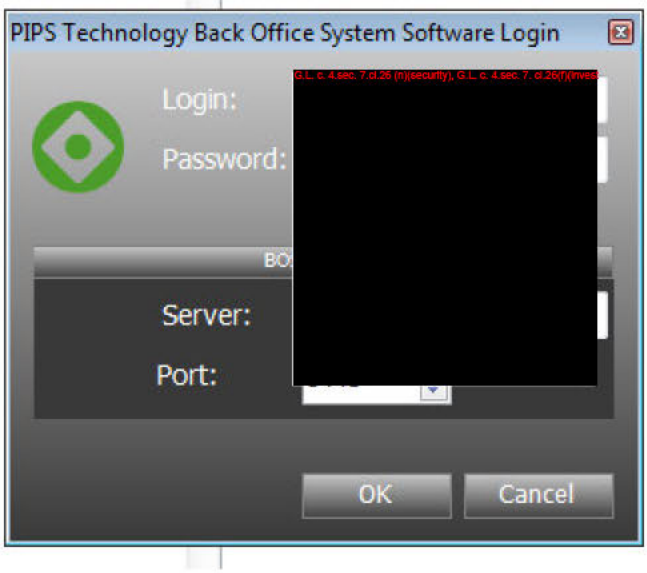
You have Advanced User status which means you can create hot lists. It also means you can change other information in other users lists so please be careful.

User guide is attached. I'll send you a separate email with some helpful shortcuts.

If there is anyone else in your office that could benefit from having an account, please forward me their information and I'll be happy to set it up.

Please reach out to me with any issues, sometimes the first attempt to login in isn't always successful .

Thank you,



David M. Gallagher
Major, Massachusetts State Police
Special Operations
508-820-2162
David.Gallagher3@MassMail.state.ma.us

From: Egnitz, Brian (POL)
To: Quinn, Dermot (POL)
Subject: ALPR
Date: Tuesday, March 3, 2020 9:48:00 AM
Attachments: image001.png
RE SLA breach warning for INC0318850 - 100.01%.msg
RE MassPort ALPR.msg
RE BOSS LPR DB Server Memory Increase.msg
RE BOSS LPR DB Server Memory Increase.msg
BOSS 4.0 Meeting.msg
RE BOSS 4.0 Pricing.msg
Re Boss and LPR.msg
FW MassPort LPR Cameras.msg

TKT0048098 Closed Complete Request for review and implementation of Mantis for BOSS (RITM0071508 Work in Progress Server Consulting, see below image)

TKT0048084 Closed Complete Request for LPR Storage (RITM0071489 Work in Progress Server Consulting, see Re: BOSS LPR DB Server Memory Increase)

INC0318850 Assigned Request for hosting (see email attached)

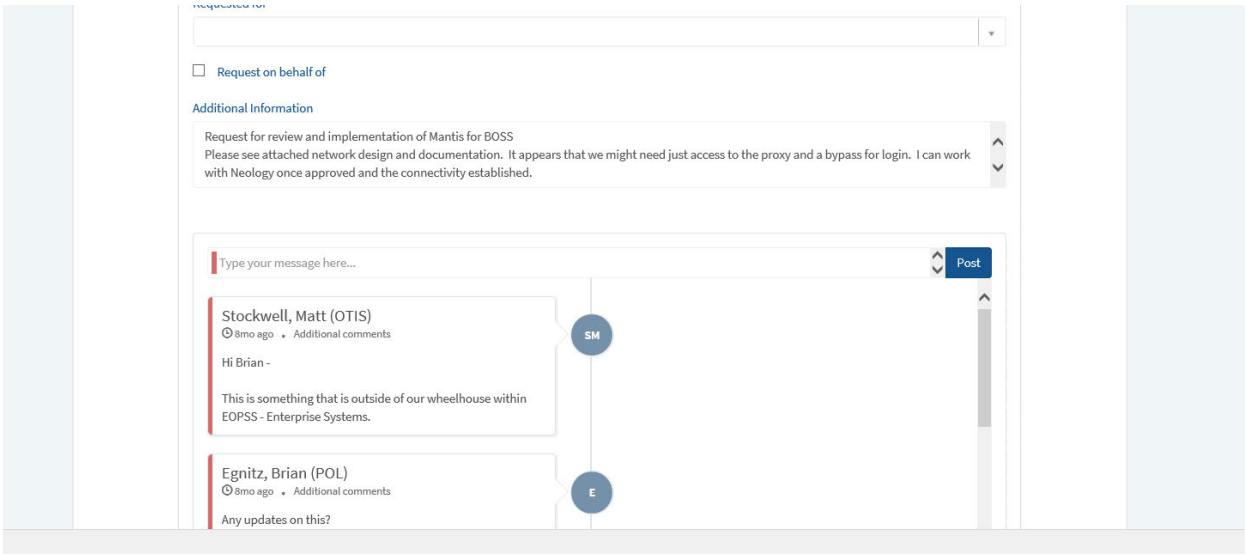
Massport request (see RE:Massport ALPR)

Seprate Massport request thread (fw: MassPort LPR Cameras)

Boss 4.0 meeting request for discussion (see Re: BOSS LPR DB Server Memory Increase 64kb, Boss 4.0 meeting web link)

Boss 4.0 pricing sent to Slater (fwd:Boss 4.0 Pricing)

Boss 4.0 sent per request to Slater (Re: Boss and LPR)



Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
Phone: 978-451-3710 (Maynard) 508-988-7302 (GHQ)
Email: Brian.Egnitz@massmail.state.ma.us
Monday - Friday, 8 to 4

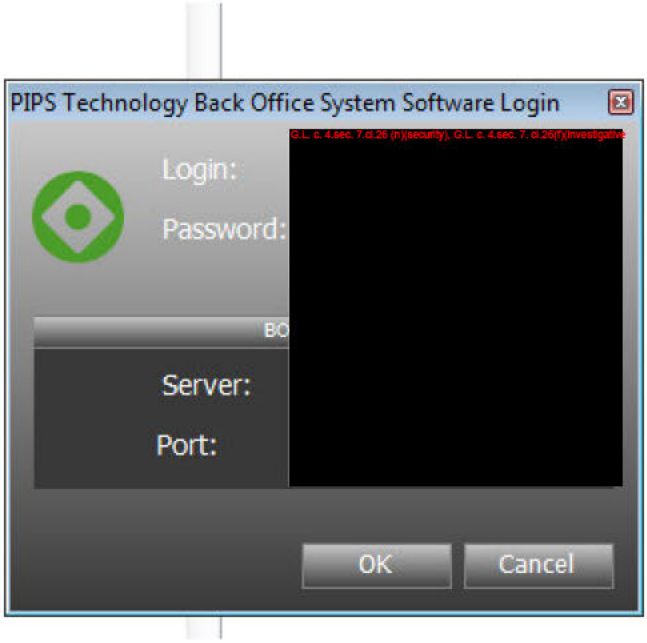
CONFIDENTIALITY NOTICE: *The information contained in this email and any attachment is privileged and confidential law enforcement information. If you have received this email in error, please call 978-451-3700 immediately. Thank you.*

From: Gallagher, David (POL)
To: McSweeney, William (POL)
Subject: ALPR
Date: Monday, October 19, 2020 12:47:18 PM
Attachments: pastedImagebase640.png
BOSS_3.2x_User_Manual_final.pdf

Billy,

To download the software cut and paste the following into your browser http://[redacted]9988/publish.htm once loaded you will need to configure the port and perhaps the IP address. Click on the "Boss server" which will open the box below and make sure you have the correct server/port info. Once you connect to the server you won't have to do it again.

Your login would be msp3317 and the password I will send you would obviously go in the password section



David M. Gallagher
Major, Massachusetts State Police
Special Operations
508-820-2162
David.Gallagher3@MassMail.state.ma.us

From: Porter, Bradford (POL)
To: Bulman, Paul (NOR)
Subject: Automatic License Plate Reader SJC Decision
Date: Thursday, April 16, 2020 2:00:00 PM
Attachments: APLR Decision.pdf

Capt. –

For your perusal.

Respectfully,

Sgt. Brad Porter #3166
Massachusetts State Police Detectives
Cape & Islands District
(508) 790-5799

From: John Tedona
To: Egnitz, Brian (POL)
Subject: BOSS4 Requirements
Date: Thursday, March 5, 2020 6:02:19 PM
Attachments: image001.png
image003.png
PIPS BOSS4 Specifications.pdf
BOSS4 Questionnaire Form.pdf

Brian -Here's the On-Prem "Only" spec requirements for BOSS4 plus a questionnaire we send out to assist with growth.

A NEOLOGY Business

John Tedona
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: Rudolph, Jessica (NAU)
To: Dalton, Jim (NAU); Gallagher, Andrew (NAU); Kazakewich, Alyssa (NAU); Kerrison, Kelly (NAU); Pelland, Kirk (NAU); Sawtelle, Mary (NAU)
Subject: Case Law Update: Win for Bourne/Sagamore Bridges via a search
Date: Tuesday, April 21, 2020 11:14:45 PM
Attachments: Case Update Graphic.png

Case Law update.

Win for the good guys. Defense tried to mirror the Connolly case and suggest a S/W needed to check ALPRs. Court said no. But this could change if a case relied more heavily on ALPR info. Interesting read.

-rudy

RESPECTFULLY
LIEUTENANT JAMES R. RUDD, PH #2786
NORFOLK DISTRICT ATTORNEY'S OFFICE
45 SHAWMUT ROAD, CANTON, MA 02021
339-830-2173

From: Grant Marguerite (NFK) <Marguerite.Grant@MassMail.State.MA.US>
Sent: Friday, April 17, 2020 5:33 PM



Chiefs
Commonwealth v. McCarthy (SJC-12750) ← click on that link to see the case
In this case the SJC ruled that police tracking D's car using 4 automatic license plate readers (ALPRs) at both ends of the Bourne and Sagamore Bridges was too limited to amount to a constitutional "search." The SJC declined to say exactly how detailed digital surveillance would have to be to constitute a search leaving that issue for future cases.

State Po ice maintain ALPRs including ones at both ends of the Bourne and Sagamore Bridges. (p.3) The ALPRs photograph vehicles' license plates; that data along with the date and time of the sighting is retained by EOPPS for a year. (p.3-4) Authorized users including police may put a license plate number on a "hot list " and receive an alert if that plate is sighted; reasons to put someone on the "hot list" include not only criminal investigations but also Amber alerts missing persons and BOLO alerts. (p. 3 25 n.13)

Through surveillance controlled buys and information from 4 Civ Barnstable police suspected that the co-D was selling heroin out of his house in Barnstable. (p.4) Police saw a black Hyundai driven by D visit there briefly so they suspected that D was the co-D's supplier. Police put the Hyundai's license plate number on the State Police ALPR "hot list " so that they'd be notified whenever the Hyundai crossed one of the bridges. (p.5) After getting an alert that the Hyundai had crossed onto the Cape police followed both the Hyundai and the co-D to the buy location on a quiet residential street where D and co-D met for about 30 seconds but police could not see a physical exchange. (p.5) From the ALPR data police generated a spreadsheet showing that in mid-winter the Hyundai had crossed the bridges dozens of times sometimes more than once a day adding to police suspicion that D was the heroin supplier. (p.5-6) When police got a second alert that the Hyundai had crossed onto the Cape they again followed D and co-D to the buy location and saw a 30-second meeting but could not see any exchange. This time police stopped both cars handcuffed both co-D and D and read them Miranda. On co-D police found heroin; on D police found 2 cell phones and cash. (p.6-7) At the station police repeatedly told D he was "not under arrest " and D made statements.

D moved to suppress the ALPR data his statements and evidence obtained from the stop. A Superior Court judge found that the moment of arrest was when D and co-D were handcuffed at the scene of the traffic stop but denied the motion to suppress. (p.33) The SJC upheld the denial.

ALPRs and expectation of privacy in digital surveillance At some length the SJC discussed the constitutional issues raised by digital surveillance. (p.7-29) Police conduct amounts to a search if: (1) it intrudes on a D's expectation of privacy and (2) society is willing to recognize the expectation of privacy as reasonable. Here the SJC ruled D did have an expectation of privacy because D and co-D chose a buy location in a quiet residential area. (p.8 n.5) As to what expectation of privacy society recognizes as reasonable with regard to digital surveillance the SJC was guided by historical understandings of what was an unreasonable search and seizure when the U.S. and Mass. Constitutions were adopted in the late 1700s In reaction to redcoats' rummaging without restraint through colonists' homes. (p.8-10) New technologies like ALPRs raise difficult legal issues because they are easier and less expensive for police than traditional surveillance can be done secretly and permit police to search back in time for a vehicle's movements even before police suspicion arose. (p.12-14) Society does not recognize as reasonable an expectation of privacy in what someone "knowingly exposes" to public view like a license plate – which by statute must be "displayed conspicuously." (p.15-16 & n.8) In older cases involving less advanced technology courts have held that a D did not have an expectation of privacy in contents of a phone conversation in a phone booth or a radio beeper" tracking a single journey. (p14-17) But technology like ALPRs GPS and CSLI are different because they may give police a **mosaic** of information where each piece may be public but when viewed together they create a picture that implicates someone's privacy interests like their political religious or sexual associations. (p.17-21) The SJC was concerned that with enough ALPRs police could track someone's location everywhere which would be "creepy." (p.25) Exigent circumstances would likely justify using an ALPR in a situation involving an Amber alert or missing person. (p.25 n.13) The D urged the SJC to consider not just these four ALPRs on the Bourne and Sagamore Bridges but the hundreds of ALPRs across Massachusetts; the SJC declined to do so because that evidence is not in the record of this case. (p.26) The **limited number of cameras** here and their placements on the bridges was not enough to give D an expectation of privacy that society would recognize as reasonable. (p.28) The SJC declined to say how much digital surveillance would give such an expectation and admitted that its unwillingness to do so "**may bring some interim confusion**" until further cases develop the law on this issue. (p.28 n.15) Chief Justice Gants wrote a separate concurrence suggesting that one thing the SJC could do is to require police who want to search a vast amount of digital data to apply for a court order supported by an affidavit showing reasonable suspicion to do so. (concurrence p.3) This would be like a SW but with a lower standard than PC.

Written policy The SJC rejected D's argument that Barnstable PD should have had a written policy about ALPRs and the MSP policy on which Barnstable relied was not specific enough. (p.30) Written policies are required to justify certain exceptions to the SW requirement (like inventory searches and sobriety checkpoints) – they do not apply to the threshold question whether a search occurred in the first place. (p.31)

Miranda review At the station police repeatedly told D that D was "not under arrest." But the motion judge found that the moment of arrest was when police handcuffed D at the traffic stop. (p.33) D argued that his statements should be suppressed because police telling him he was not under arrest amounted to "deceit or trickery" to get D to confess. The motion judge and the SJC rejected that argument saying that even if telling D he was not under arrest amounted to deceit or trickery it was just one factor to be used in determining voluntariness.

Bottom line: Police use of ALPRs at limited locations is not a constitutional search – but we don't know how many locations it'd have to be to amount to one. Using an ALPR in **exigent circumstances** like an Amber Alert is likely OK. Local police don't need a written policy to use ALPRs maintained by MSP. After a D has been handcuffed police should not tell D that D is "not under arrest" – police will likely be accused later of deceit and trickery.

A thought: There are news stories online that cell phones may be used to do contact tracing for people exposed to COVID-19. If lots of people willingly agree to let their cell phone data be used to track their whereabouts would that ever change courts' view of what society recognizes as a reasonable expectation of privacy? At some point if members of the pub ic come to expect that they're being tracked should police be allowed to use that evidence too? Or at the very least should there be a jury instruction explaining that police have less access to the data than other entities (like software companies or public health agencies)?

As always email me with any questions. Wash your hands!

Marguerite

Marguerite T. Grant
General Counsel • Director of Training
Office of Norfolk District Attorney Michael W. Morrissey
45 Shawmut Road
Canton, MA 02021
781-830-4819

From: Thibeault, Sharon (CPI)
To: Mason, Christopher (POL)
Subject: Commonwealth v McCarthy - SJC Decision (the Sagamore bridge cam case)
Date: Thursday, April 16, 2020 10:23:20 AM
Attachments: e12750.pdf
ATT00001.txt

---

https://www.mass.gov/files/documents/2020/04/16/e12750.pdf

Good morning Colonel,

It is nice to share some good news for a change.
I know the Bridge cam case has wide State Police implications. Thought you would like to give it a read.
Another win for the Cape!
Stay healthy.

Sharon Thibeault

From: Thibeault, Sharon (CPI)
To: Mawn, John (POL)
Subject: Commonwealth v McCarthy SJC Decision - (the Sagamore bridge cam case)
Date: Thursday, April 16, 2020 10:57:11 AM
Attachments: e12750.pdf
ATT00001.txt

---

https://www.mass.gov/files/documents/2020/04/16/e12750.pdf

Good morning Jack,

The SJC decision in the bridge cam case came out today.
I know you were interested in the case.
Another win for the Cape!
Thought you might like to give it a read.
Hope you are staying safe! Nothing like starting a new job and a pandemic hits!

Sharon

From: Nardone, Andrea (DAA)
To: DAA-DL-ADA"s; DAA-DL-Case Summaries; DAA-DL-DA&EXEC.ASST
Subject: Court Decision - April 16, 2020
Date: Thursday, April 16, 2020 11:15:06 AM
Attachments: image001.png
Commonwealth v. McCarthy - opinion.pdf

SUPPORTING MASSACHUSETTS PROSECUTORS

MDAA

Massachusetts District Attorneys Association

Commonwealth v. McCarthy

Supreme Judicial Court, April 16, 2020
(Search and Seizure/Automatic License Plate Readers)

The use of four automatic license plate reader cameras, placed at two fixed locations on the ends of the Bourne and Sagamore bridges and used to "hit" on the defendant's license when he drove over either bridge,, does not constitute a search within the meaning of either art. 14 or the Fourth Amendment.

"While we recognize that the widespread use of ALPRs in the Commonwealth could implicate constitutional protections against unreasonable searches, the limited use of the technology in this case does not."

Note:
The Court did not find error in the fact that the Bourne Police Department did not have a separate policy, apart from State Police TRF-11, regarding ALPRs.

Additionally, the Court ruled that the government's use of ALPR data is not subject to the Stored Communication Act nor the Electronic Communications Privacy Act

See attached opinion.

For other recent case law decisions, go to the MDAA website at www.mass.gov/mdaa

From: Sue Roy
To: Baker, Michael (POL)
Subject: CTS
Date: Thursday, June 25, 2020 2:41:01 PM
Attachments: image001.png
image003.png
image004.png
image005.png
image006.png
image007.png
LE-Catalog-2020_bleed web.pdf
Safeware_CatalogPriceList_CombinedSystems_2020.3.1_v2.xlsx

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Hi Mike,
I have attached the entire CTS file. This is all State contract pricing.
I have also attached the law enforcement catalog.
Thanks
Sue

Sue Roy, QSSP
Sr. Territory Manager

Cell: 203-[redacted]
Fax: 301-683-1200
sue.roy@safewareinc.com
18 Evanwood Drive
Wallingford, Ct. 06492

Safeware Inc.
Cell: 203.800.6298
After Hours Emergency Number: 844-880-7029







www.safewareinc.com

This e-mail is intended only for the person or entity to which it is addressed and may contain information that is privileged, confidential or otherwise protected from disclosure. Dissemination, distribution or copying of this e-mail or the information herein by anyone other than the intended recipient, or an employee or agent responsible for delivering the message to the intended recipient, is prohibited. If you have received this e-mail by mistake, please delete it from your system immediately and notify the sender.

From: Fecteau, Robert
To: Egnitz, Brian (POL)
Subject: Draft Narrative
Date: Tuesday, July 28, 2020 7:52:13 AM
Attachments: image001.png
image002.png
image003.png
image004.png
Genetec Deployment Overview REV1 07282020.pdf

Brian,
As a follow up to our discussion of last week, attached is a draft version of the narrative system overview that we discussed.

Please take a few minutes to review, and let me know if you think it accurately outlines the need for an assigned administrator, and accurately outlines the need for further operational/use discussions.

I'll be leaving the house at 8:30 to head to a meeting in Cambridge and will be in the car until about 10a (if you'd like to discuss).

I have consolidated a bunch of the badge/ID information, and will send that over to you later today.

Regards,
Bob

COMFORT SYSTEMS USA
BCM Controls Corporation

BOB FECTEAU
VICE PRESIDENT - STRATEGIC BUSINESS
(781) 897-5152 DIRECT
(781) 879-9554 MOBILE

From: Connolly, Steven (AGO)
To: Telford, Erik (POL); Nunes, Daniel (AGO); Walczak, Ryan (POL); Towle, Peter (POL); Walczak, Ryan (POL); Johnson, Stephen (POL)
Subject: FW: ALPR information
Date: Monday, July 27, 2020 9:44:28 AM
Attachments: pastedImagebase640.png
BOSS 3.6 USER MANUAL Rev2.pdf

Lieutenant Steven Connolly #2719
Massachusetts State Police
Office of the Attorney General

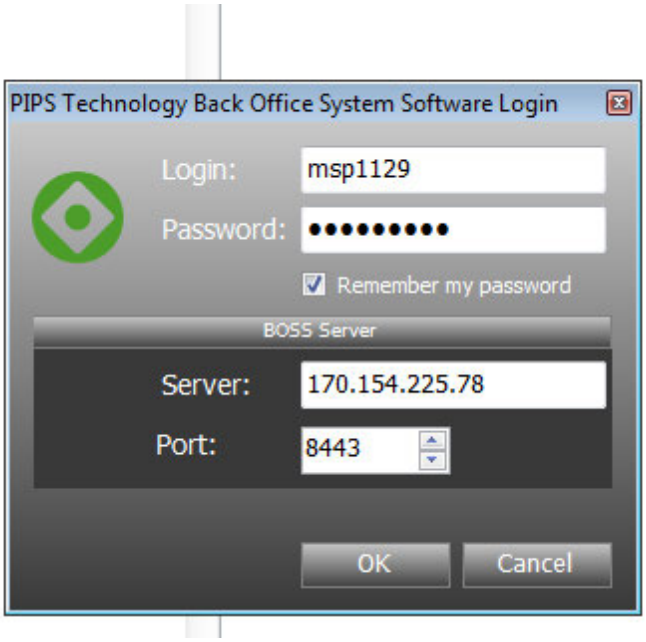
From: Gallagher, David (POL) <david.gallagher3@MassMail.State.MA.US>
Sent: Sunday, July 26, 2020 1:50 PM
To: Connolly, Steven (AGO) <Steven.B.Connolly@mass.gov>
Subject: ALPR information

Steve,

To download the software cut and paste the following into your browser h[redacted] once loaded you will need to configure the port and perhaps the IP address. Click on the “Boss server” which will open the box below and make sure you have the correct server/port info. Once you connect to the server you won’t have to do it again.

Your login would be msp2719 and the password I sent you would obviously go in the password section

Could you please forward this info as well as the login information to the other accounts I set up.



David M. Gallagher

Captain, Massachusetts State Police

Special Operations

508-988-7442

David.Gallagher3@MassMail.state.ma.us

From: Berberena, Jorell (POL)
To: Gallagher, David (POL)
Subject: Fw: ALPR User Guide
Date: Monday, November 9, 2020 10:44:23 AM
Attachments: BOSS 3.6 USER MANUAL Rev2.pdf

Thank you it is much appreciated sir. The software that is on my current cruiser laptop is the 3M License Plate Capture Software. Would the login info you've provided grant me access to this software?

Thank you very much

Trooper Jorell B. Berberena #4430
A-4 Medford
781-215-4096

From: Gallagher, David (POL) <david.gallagher3@MassMail.State.MA.US>
Sent: Saturday, November 7, 2020 11:17 AM
To: Berberena, Jorell (POL) <Jorell.B.Berberena@pol.state.ma.us>
Subject: ALPR User Guide

Please see attached.

David M. Gallagher
Major, Massachusetts State Police
Special Operations
508-820-2162
David.Gallagher3@MassMail.state.ma.us

To: Slater, James (CHS)
Cc: Quinn, Dermot (POL)
Subject: FW: BOSS update
Date: Tuesday, March 3, 2020 4:11:37 PM
Attachments: BOSS4 Specifications 20191015.pdf
image001.png

Specs attached

From: Peter Crary [mailto:pcrary@neology.net]
Sent: Tuesday, January 14, 2020 1:34 PM
To: Egnitz, Brian (POL); John Tedona
Subject: RE: BOSS update

No, attached are the current server specs.

-Peter Crary
Global R&D Director, ANPR/ALPR
(858) 391-0260 x1153 (d)
(865) 386-3821 (m)

The information contained in this communication is confidential and intended only for the use of the recipient named and may also be legally privileged. If you are not the intended recipient (named addressee), you are hereby notified that any dissemination, distribution, copying or making use of this communication, or any of its contents, is strictly prohibited. Please notify the sender immediately by email and delete the original message and any copy of it from your computer system. The integrity, security of and absence of viruses in this message cannot be guaranteed on the internet. The sender therefore does not accept liability for any errors or omissions in the contents of this message, nor any damage caused, which arise as a result of e-mail transmission.

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Tuesday, 14 January, 2020 05:07
To: Peter Crary <pcrary@neology.net>; John Tedona <jtedona@neology.net>
Subject: FW: BOSS update

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Are this still current for Boss 4.0?

From: Egnitz, Brian (POL)
Sent: Tuesday, March 12, 2019 4:14 PM
To: Stockwell, Matt (EPS); Mitchell, Timothy (EPS)
Subject: RE: BOSS update

From: Stockwell, Matt (EPS)
Sent: Tuesday, March 12, 2019 4:14 PM
To: Egnitz, Brian (POL); Mitchell, Timothy (EPS)
Subject: RE: BOSS update

Hi Brian –

If there was an attachment or additional details on the sizing they did not come through via e-mail.

Matt

From: Egnitz, Brian (POL)
Sent: Tuesday, March 12, 2019 3:04 PM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Stockwell, Matt (EPS) <matt.stockwell@mass.gov>
Subject: FW: BOSS update

FYI

From: John Tedona [mailto:jtedona@neology.net]
Sent: Tuesday, March 12, 2019 11:00 AM
To: Egnitz, Brian (POL)
Cc: Michael Roth
Subject: RE: BOSS update

Brian,

Here's the recommended sizing criteria for the application and database servers. With more fixed cameras pushing data to BOSS it's highly recommended you keep this sizing criteria in mind.

John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237

Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Tuesday, March 12, 2019 10:49 AM
To: Michael Roth <mroth@neology.net>
Cc: Peter Crary <pcrary@neology.net>; Israel Padilla <ipadilla@neology.mx>; Michell Itallekzi Garcia Garcia <colaborador6@neopartners.mx>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; John Tedona <jtedona@neology.net>; PIPS Technology Support <support@pipstechnology.com>; Quinn, Dermot (POL) <dermot.quinn@state.ma.us>; Clarke, Shannon (EPS) <shannon.clarke@state.ma.us>
Subject: RE: BOSS update

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Thanks Mike, Ive sent that to the tech. here is the license key. I saw the 5 concurrent number in the boss log folder

---

From: Michael Roth [mailto:mroth@neology.net]
Sent: Tuesday, March 12, 2019 10:33 AM
To: Egnitz, Brian (POL); Peter Crary; Israel Padilla; Michell Itallekzi Garcia Garcia; Mitchell, Timothy (EPS); John Tedona; PIPS Technology Support; Quinn, Dermot (POL); Clarke, Shannon (EPS)
Subject: RE: BOSS update

Can you send me screen shoot of the licenses.

That error occurs when using other browser than IE.

1. Prerequisites needed to successful install of BossUI client, the below settings pertain to OS where client is being installed.
    a. "Active Scripting" needs to be enabled in Windows "Internet Options"- "Security"- "Internet"- "Custom level". (This setting is for Bing maps to function).
    b. Can you add http:// address to "Local Intranet" in Intranet Zones Sites. (This can be taken out after installation as it is only needed for deployment).

2. Internet Explorer must be use.

Michael B. Roth
ALPR Technician
O: 858.391.0260 Ext. 1234
C: 513.767.7610
mroth@neology.net
A Business
www.pipstechnology.com

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Tuesday, March 12, 2019 7:06 AM
To: Peter Crary <pcrary@neology.net>; Michael Roth <mroth@neology.net>; Israel Padilla <ipadilla@neology.mx>; Michell Itallekzi Garcia Garcia <colaborador6@neopartners.mx>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; John Tedona <jtedona@neology.net>; PIPS Technology Support <support@pipstechnology.com>; Quinn, Dermot (POL) <dermot.quinn@state.ma.us>; Clarke, Shannon (EPS) <shannon.clarke@state.ma.us>
Subject: RE: BOSS update

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

I addition, I believe we may need a new license file. The logs say "5 concurrent" licenses available.

From: Egnitz, Brian (POL)
Sent: Tuesday, March 12, 2019 6:43 AM
To: Peter Crary; Michael Roth; Israel Padilla; Michell Itallekzi Garcia Garcia; Mitchell, Timothy (EPS); John Tedona; PIPS Technology Support; Quinn, Dermot (POL); Clarke, Shannon (EPS)
Subject: Fwd: BOSS update

Hi guys,

Is there an updated client? This on appears to be calling the Spanish version of dot net, it's also not using the updated version already installed. Do you have one that is properly signed too???

Begin forwarded message:

From: "Ghasemi, Kiarash (POL)" <Kiarash.Ghasemi@pol.state.ma.us>
Date: March 11, 2019 at 10:35:38 PM EDT
To: "Egnitz, Brian (POL)" <brian.egnitz@pol.state.ma.us>, "Sullivan, Margaret (POL)" <Margaret.Sullivan@pol.state.ma.us>
Cc: "Quinn, Dermot (POL)" <dermot.quinn@pol.state.ma.us>, "Kelly, Edward (POL)" <Edward.Kelly@pol.state.ma.us>, "Hernandez, Oscar (POL)" <Oscar.Hernandez@pol.state.ma.us>, "Weldon, Stephen (POL)" <Stephen.Weldon@pol.State.MA.US>, "Griffin, Daniel (POL)" <daniel.griffin@MassMail.State.MA.US>
Subject: RE: BOSS update

Hi Brian,

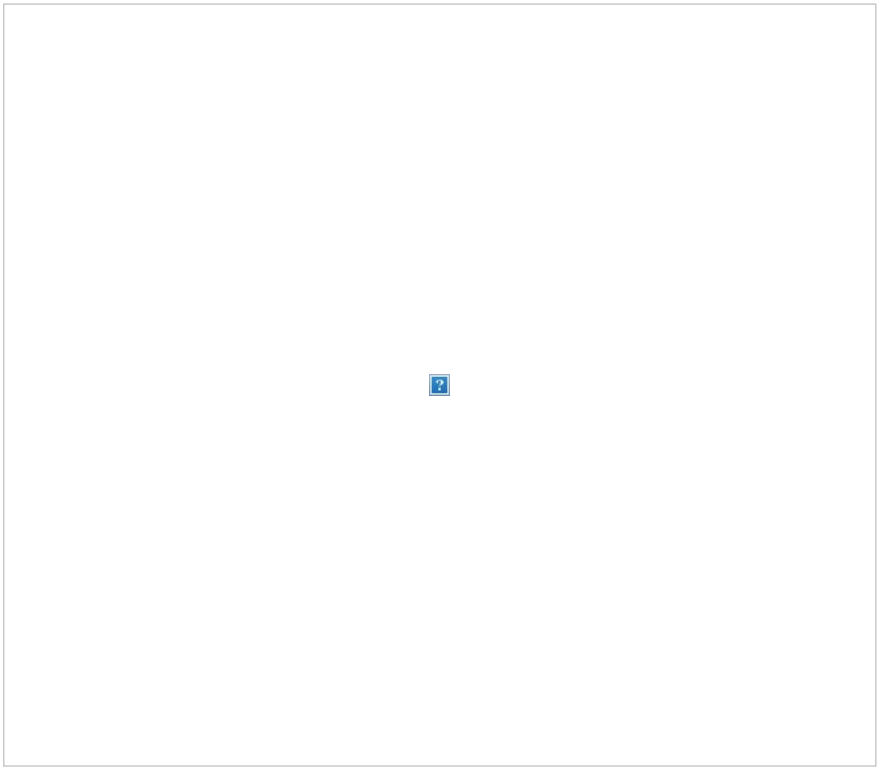
Before this update, On computers that needed access to LPR reporting, we have a copied a folder called “SA Client” and “SA.UI” within that folder, we create a shortcut to that file and that eliminated installation of any program.

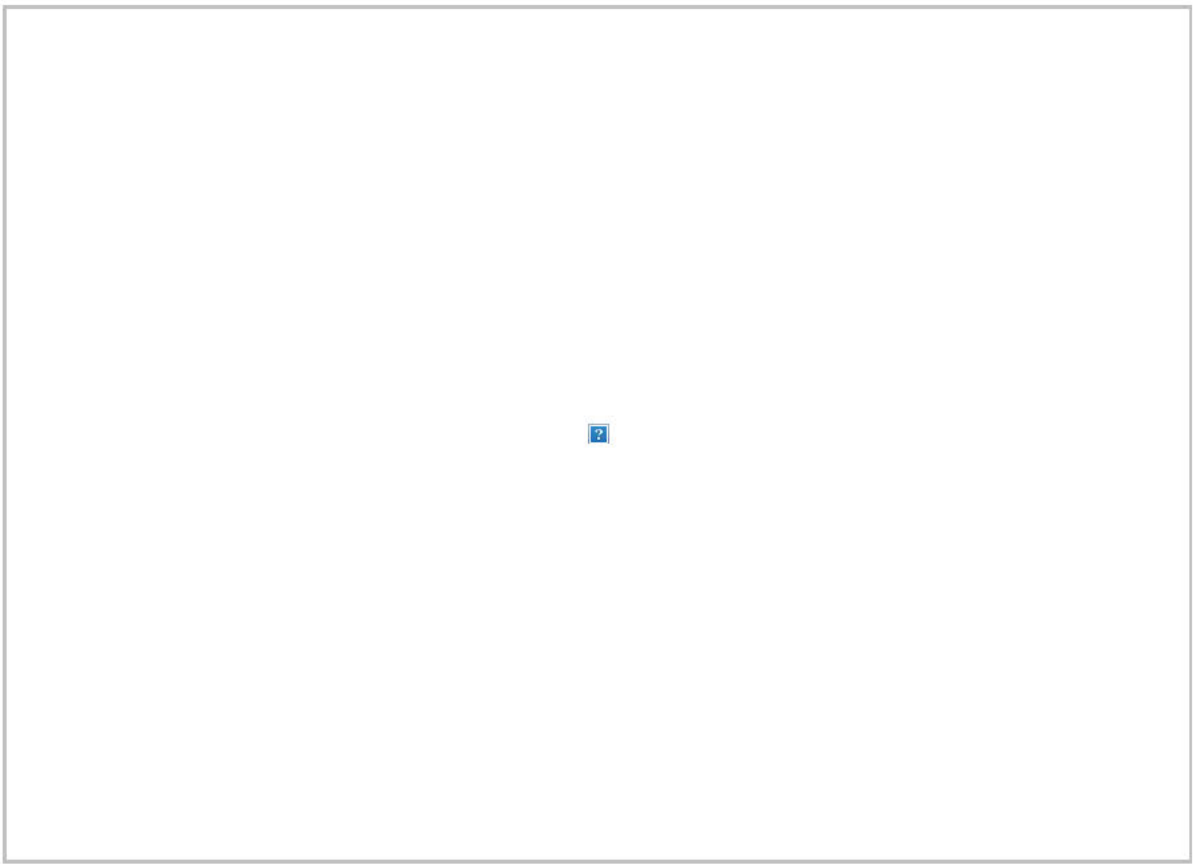
But I have tried the link that you have provided us and I’m getting an error message in Spanish during the installation! (Please see below) What I get from it, it need .Net. 4.5.2 but my computer already has 4.7 installed on it. I also tried to install it on Watchcenter computers and I got the same error message in Spanish and .Net 4.5.2 wont install on top of the current version of 4.7

Also translation of other part of the error message is that:

"The Microsoft .NET Framework 4.5.2 installation is not supported on this operating system. Please contact the administrator."

I have CC Lt. Griffin on this email, since he has done many installation of the old one too and all his stations are also effected too.





Error de comprobación de los requisitos previos del componente del sistema Microsoft .NET Framework 4.5.2 (x86 y x64) con el siguiente mensaje: "La instalación de Microsoft .NET Framework 4.5.2 no se admite en este sistema operativo. Póngase en contacto con el administrador."

Vea el archivo de registro de la instalación que se encuentra en 'C:\Users\MJACKS~1\AppData\Local\Temp\VSD1947.tmp\install.log' para obtener más información.

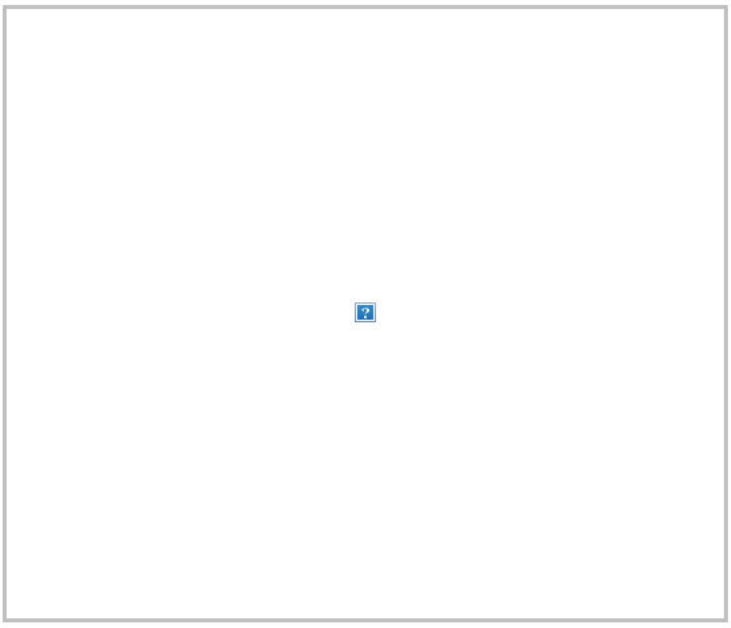
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Monday, March 11, 2019 9:58 PM
To: Sullivan, Margaret (POL) <Margaret.Sullivan@pol.state.ma.us>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Kelly, Edward (POL) <Edward.Kelly@pol.state.ma.us>; Hernandez, Oscar (POL) <Oscar.Hernandez@pol.state.ma.us>; Weldon, Stephen (POL) <Stephen.Weldon@pol.State.MA.US>; Ghasemi, Kiarash (POL) <Kiarash.Ghasemi@pol.state.ma.us>
Subject: BOSS update

Hi Peg,

The BOSS ALPR application has been updated in case you get some calls regarding ALPR. The client can be updated using the url below if it doesn't do it automatically. Configure IP and port as below.

-Brian

http:/[redacted]



Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
Phone: 978-451-3710 (Maynard) 508-988-7302 (GHQ)
Email: Brian.Egnitz@massmail.state.ma.us
Monday - Friday, 8 to 4

CONFIDENTIALITY NOTICE: *The information contained in this email and any attachment is privileged and confidential law enforcement information. If you have received this email in error, please call 978-451-3700 immediately. Thank you.*

From:	Egnitz, Brian (POL)
To:	pcrary@neology.net; John Tedona (jtedona@neology.net)
Subject:	FW: BOSS update
Date:	Tuesday, January 14, 2020 8:06:00 AM
Attachments:	PIPS Boss Specifications 06222018.pdf image002.png

Are this still current for Boss 4.0?

From: Egnitz, Brian (POL)
Sent: Tuesday, March 12, 2019 4:14 PM
To: Stockwell, Matt (EPS); Mitchell, Timothy (EPS)
Subject: RE: BOSS update

From: Stockwell, Matt (EPS)
Sent: Tuesday, March 12, 2019 4:14 PM
To: Egnitz, Brian (POL); Mitchell, Timothy (EPS)
Subject: RE: BOSS update

Hi Brian –

If there was an attachment or additional details on the sizing they did not come through via e-mail.

Matt

From: Egnitz, Brian (POL)
Sent: Tuesday, March 12, 2019 3:04 PM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Stockwell, Matt (EPS) <matt.stockwell@mass.gov>
Subject: FW: BOSS update

FYI

From: John Tedona [mailto:jtedona@neology.net]
Sent: Tuesday, March 12, 2019 11:00 AM
To: Egnitz, Brian (POL)
Cc: Michael Roth
Subject: RE: BOSS update

Brian,

Here's the recommended sizing criteria for the application and database servers. With more fixed cameras pushing data to BOSS it's highly recommended you keep this sizing criteria in mind.

John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Tuesday, March 12, 2019 10:49 AM
To: Michael Roth <mroth@neology.net>
Cc: Peter Crary <pcrary@neology.net>; Israel Padilla <ipadilla@neology.mx>; Michell Itallekzi Garcia Garcia <colaborador6@neopartners.mx>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; John Tedona <jtedona@neology.net>; PIPS Technology Support <support@pipstechnology.com>; Quinn, Dermot (POL) <dermot.quinn@state.ma.us>; Clarke, Shannon (EPS) <shannon.clarke@state.ma.us>
Subject: RE: BOSS update

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Thanks Mike, Ive sent that to the tech. here is the license key. I saw the 5 concurrent number in the boss log folder

From: Michael Roth [mailto:mroth@neology.net]
Sent: Tuesday, March 12, 2019 10:33 AM
To: Egnitz, Brian (POL); Peter Crary; Israel Padilla; Michell Itallekzi Garcia Garcia; Mitchell, Timothy (EPS); John Tedona; PIPS Technology Support; Quinn, Dermot (POL); Clarke, Shannon (EPS)
Subject: RE: BOSS update

Can you send me screen shoot of the licenses.

That error occurs when using other browser than IE.

1. Prerequisites needed to successful install of BossUI client, the below settings pertain to OS where client is being installed.
   a. "Active Scripting" needs to be enabled in Windows "Internet Options"- "Security"- "Internet"- "Custom level". (This setting is for Bing maps to function).
   b. Can you add http:// address to "Local Intranet" in Intranet Zones Sites. (This can be taken out after installation as it is only needed for deployment).

2. Internet Explorer must be use.

Michael B. Roth
ALPR Technician
O: 858.391.0260 Ext. 1234
C: 513.767.7610
mroth@neology.net
A Business
www.pipstechnology.com

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Tuesday, March 12, 2019 7:06 AM
To: Peter Crary <pcrary@neology.net>; Michael Roth <mroth@neology.net>; Israel Padilla <ipadilla@neology.mx>; Michell Itallekzi Garcia Garcia <colaborador6@neopartners.mx>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; John Tedona <jtedona@neology.net>; PIPS Technology Support <support@pipstechnology.com>; Quinn, Dermot (POL) <dermot.quinn@state.ma.us>; Clarke, Shannon (EPS) <shannon.clarke@state.ma.us>
Subject: RE: BOSS update

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

I addition, I believe we may need a new license file. The logs say "5 concurrent" licenses available.

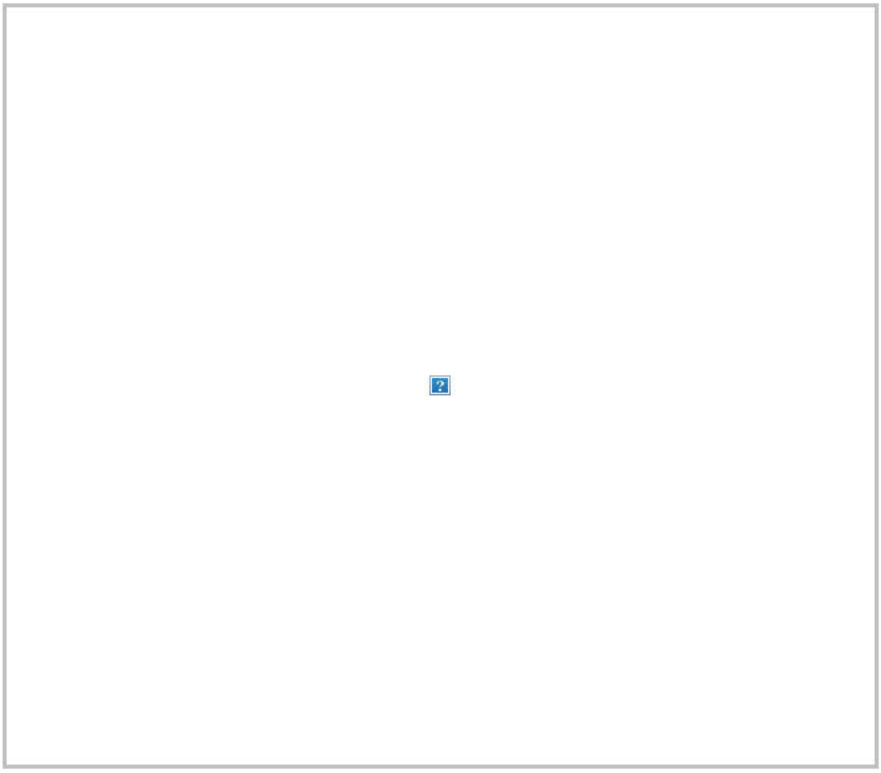
From: Egnitz, Brian (POL)
Sent: Tuesday, March 12, 2019 6:43 AM
To: Peter Crary; Michael Roth; Israel Padilla; Michell Itallekzi Garcia Garcia; Mitchell, Timothy (EPS); John Tedona; PIPS Technology Support; Quinn, Dermot (POL); Clarke, Shannon (EPS)
Subject: Fwd: BOSS update

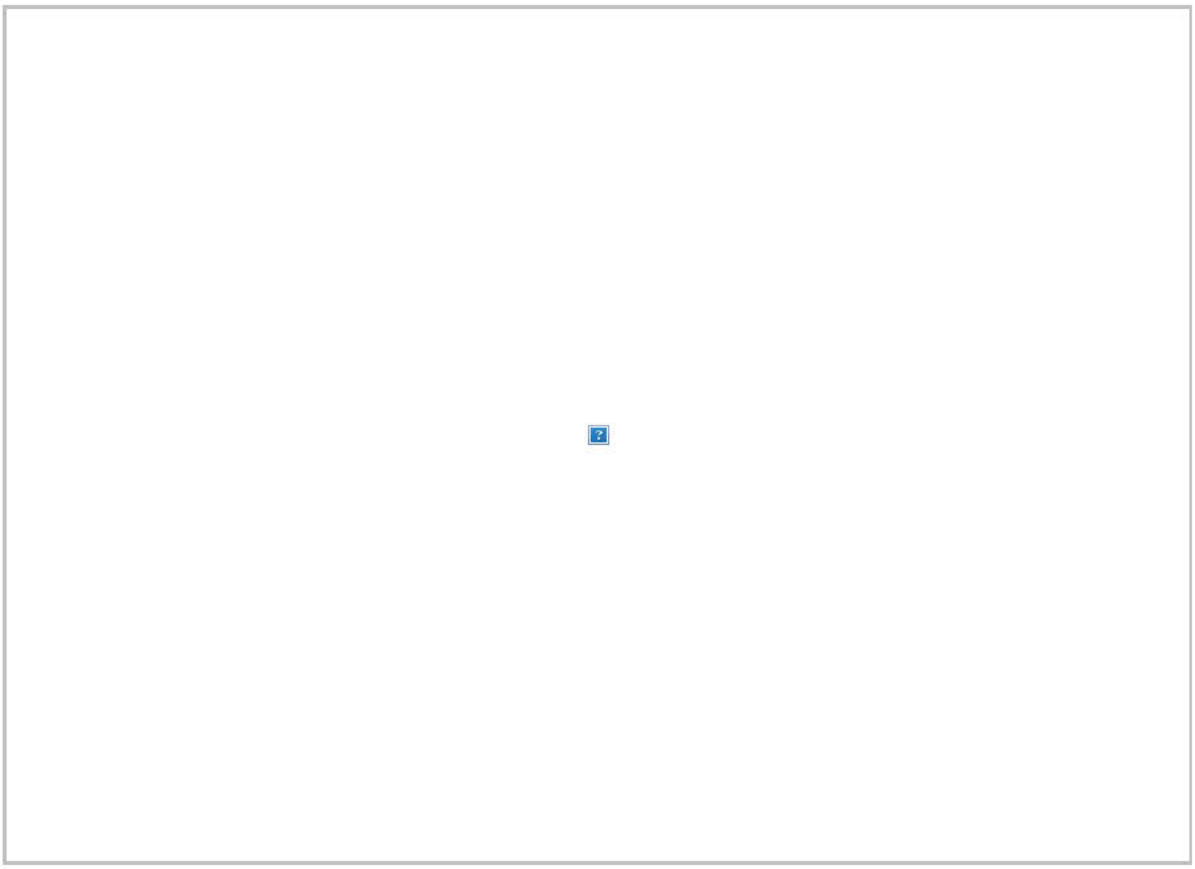
Hi guys,

Is there an updated client? This on appears to be calling the Spanish version of dot net, it's also not using the updated version already installed. Do you have one that is properly signed too???

Begin forwarded message:

> **From:** "Ghasemi, Kiarash (POL)" <Kiarash.Ghasemi@pol.state.ma.us>
> **Date:** March 11, 2019 at 10:35:38 PM EDT
> **To:** "Egnitz, Brian (POL)" <brian.egnitz@pol.state.ma.us>, "Sullivan, Margaret (POL)" <Margaret.Sullivan@pol.state.ma.us>
> **Cc:** "Quinn, Dermot (POL)" <dermot.quinn@pol.state.ma.us>, "Kelly, Edward (POL)" <Edward.Kelly@pol.state.ma.us>, "Hernandez, Oscar (POL)" <Oscar.Hernandez@pol.state.ma.us>, "Weldon, Stephen (POL)" <Stephen.Weldon@pol.State.MA.US>, "Griffin, Daniel (POL)" <daniel.griffin@MassMail.State.MA.US>
> **Subject: RE: BOSS update**
>
> Hi Brian,
>
> Before this update, On computers that needed access to LPR reporting, we have a copied a folder called "SA Client" and "SA.UI" within that folder, we create a shortcut to that file and that eliminated installation of any program.
>
> But I have tried the link that you have provided us and I'm getting an error message in Spanish during the installation! (Please see below) What I get from it, it need .Net. 4.5.2 but my computer already has 4.7 installed on it. I also tried to install it on Watchcenter computers and I got the same error message in Spanish and .Net 4.5.2 wont install on top of the current version of 4.7
>
> Also translation of other part of the error message is that:
>
> "The Microsoft .NET Framework 4.5.2 installation is not supported on this operating system. Please contact the administrator."
>
> I have CC Lt. Griffin on this email, since he has done many installation of the old one too and all his stations are also effected too.





Error de comprobación de los requisitos previos del componente del sistema Microsoft .NET Framework 4.5.2 (x86 y x64) con el siguiente mensaje: "La instalación de Microsoft .NET Framework 4.5.2 no se admite en este sistema operativo. Póngase en contacto con el administrador."

Vea el archivo de registro de la instalación que se encuentra en 'C:\Users\MJACKS~1\AppData\Local\Temp\VSD1947.tmp\install.log' para obtener más información.

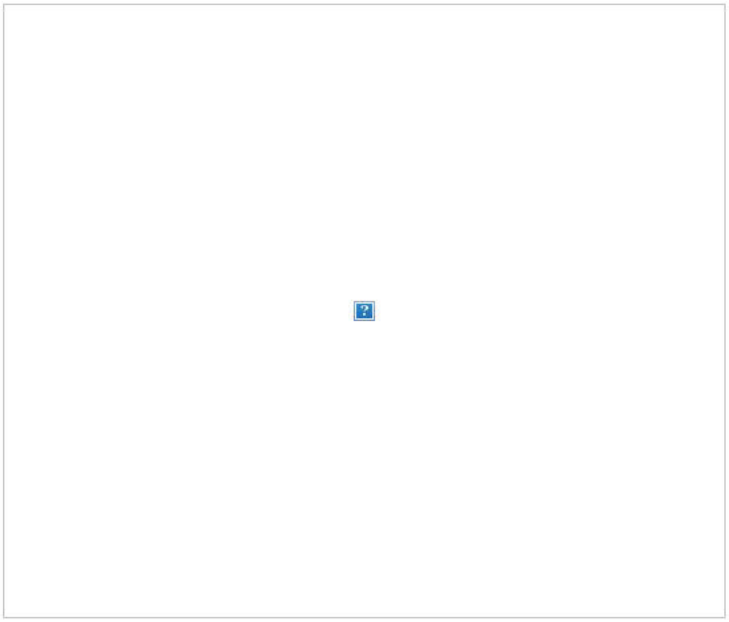
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Monday, March 11, 2019 9:58 PM
To: Sullivan, Margaret (POL) <Margaret.Sullivan@pol.state.ma.us>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Kelly, Edward (POL) <Edward.Kelly@pol.state.ma.us>; Hernandez, Oscar (POL) <Oscar.Hernandez@pol.state.ma.us>; Weldon, Stephen (POL) <Stephen.Weldon@pol.State.MA.US>; Ghasemi, Kiarash (POL) <Kiarash.Ghasemi@pol.state.ma.us>
Subject: BOSS update

Hi Peg,

The BOSS ALPR application has been updated in case you get some calls regarding ALPR. The client can be updated using the url below if it doesn't do it automatically. Configure IP and port as below.

-Brian

http://[redacted]

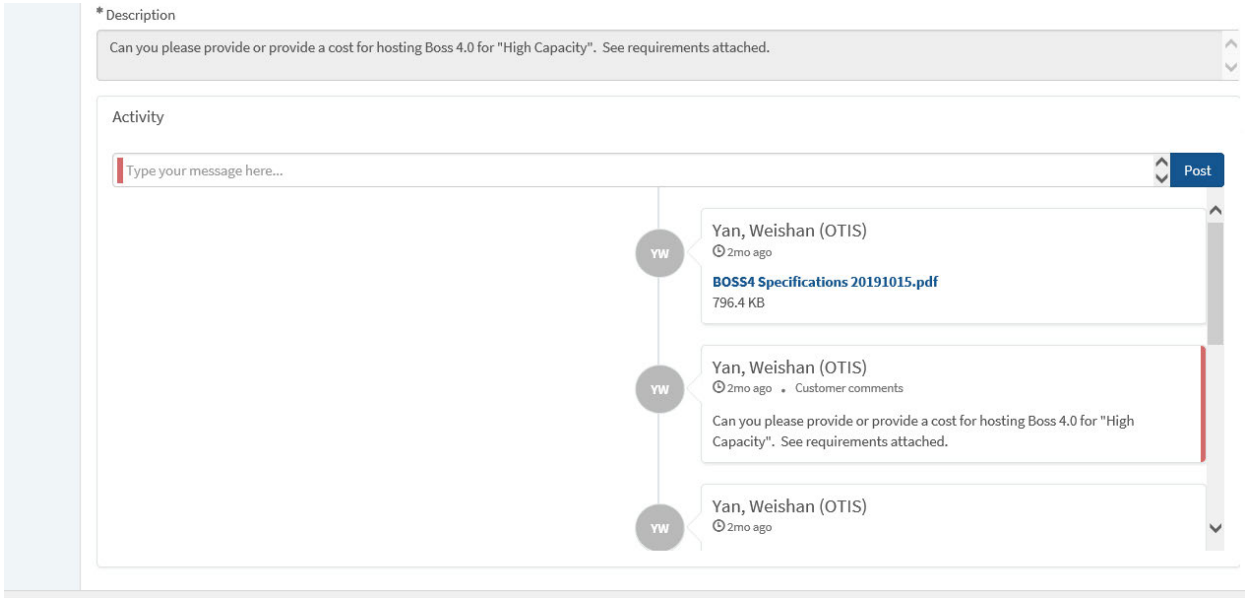


Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
Phone: 978-451-3710 (Maynard) 508-988-7302 (GHQ)
Email: Brian.Egnitz@massmail.state.ma.us
Monday - Friday, 8 to 4

CONFIDENTIALITY NOTICE: *The information contained in this email and any attachment is privileged and confidential law enforcement information. If you have received this email in error, please call 978-451-3700 immediately. Thank you.*

From: Egnitz, Brian (POL)
To: Slater, James (CHS)
Cc: Quinn, Dermot (POL)
Subject: FW: BOSS update
Date: Tuesday, March 3, 2020 4:14:00 PM
Attachments: BOSS4 Specifications 20191015.pdf
image002.png
image003.png

Specs attached. See ticket INC0318850



From: Peter Crary [mailto:pcrary@neology.net]
Sent: Tuesday, January 14, 2020 1:34 PM
To: Egnitz, Brian (POL); John Tedona
Subject: RE: BOSS update

No, attached are the current server specs.

-Peter Crary
Global R&D Director, ANPR/ALPR
(858) 391-0260 x1153 (d)
(865) 386-3821 (m)

The information contained in this communication is confidential and intended only for the use of the recipient named and may also be legally privileged. If you are not the intended recipient (named addressee), you are hereby notified that any dissemination, distribution, copying or making use of this communication, or any of its contents, is strictly prohibited. Please notify the sender immediately by email and delete the original message and any copy of it from your computer system. The integrity, security of and absence of viruses in this message cannot be guaranteed on the internet. The sender therefore does not accept liability for any errors or omissions in the contents of this message, nor any damage caused, which arise as a result of e-mail transmission.

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Tuesday, 14 January, 2020 05:07
To: Peter Crary <pcrary@neology.net>; John Tedona <jtedona@neology.net>
Subject: FW: BOSS update

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Are this still current for Boss 4.0?

From: Egnitz, Brian (POL)
Sent: Tuesday, March 12, 2019 4:14 PM
To: Stockwell, Matt (EPS); Mitchell, Timothy (EPS)
Subject: RE: BOSS update

From: Stockwell, Matt (EPS)
Sent: Tuesday, March 12, 2019 4:14 PM
To: Egnitz, Brian (POL); Mitchell, Timothy (EPS)
Subject: RE: BOSS update

Hi Brian –

If there was an attachment or additional details on the sizing they did not come through via e-mail.

Matt

From: Egnitz, Brian (POL)
Sent: Tuesday, March 12, 2019 3:04 PM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Stockwell, Matt (EPS) <matt.stockwell@mass.gov>
Subject: FW: BOSS update

FYI

From: John Tedona [mailto:jtedona@neology.net]
Sent: Tuesday, March 12, 2019 11:00 AM
To: Egnitz, Brian (POL)
Cc: Michael Roth
Subject: RE: BOSS update

Brian,

Here's the recommended sizing criteria for the application and database servers. With more fixed cameras pushing data to BOSS it's highly recommended you keep this sizing criteria in mind.

John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Tuesday, March 12, 2019 10:49 AM
To: Michael Roth <mroth@neology.net>
Cc: Peter Crary <pcrary@neology.net>; Israel Padilla <ipadilla@neology.mx>; Michell Itallekzi Garcia Garcia <colaborador6@neopartners.mx>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; John Tedona <jtedona@neology.net>; PIPS Technology Support <support@pipstechnology.com>; Quinn, Dermot (POL) <dermot.quinn@state.ma.us>; Clarke, Shannon (EPS) <shannon.clarke@state.ma.us>
Subject: RE: BOSS update

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Thanks Mike, Ive sent that to the tech. here is the license key. I saw the 5 concurrent number in the boss log folder

---

From: Michael Roth [mailto:mroth@neology.net]
Sent: Tuesday, March 12, 2019 10:33 AM
To: Egnitz, Brian (POL); Peter Crary; Israel Padilla; Michell Itallekzi Garcia Garcia; Mitchell, Timothy (EPS); John Tedona; PIPS Technology Support; Quinn, Dermot (POL); Clarke, Shannon (EPS)
Subject: RE: BOSS update

Can you send me screen shoot of the licenses.

That error occurs when using other browser than IE.

1. Prerequisites needed to successful install of BossUI client, the below settings pertain to OS where client is being installed.
   a. "Active Scripting" needs to be enabled in Windows "Internet Options"- "Security"- "Internet"- "Custom level". (This setting is for Bing maps to function).
   b. Can you add http:// address to "Local Intranet" in Intranet Zones Sites. (This can be taken out after installation as it is only needed for deployment).

2. Internet Explorer must be use.

Michael B. Roth
ALPR Technician
O: 858.391.0260 Ext. 1234
C: 513.767.7610
mroth@neology.net
A Business
www.pipstechnology.com

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Tuesday, March 12, 2019 7:06 AM
To: Peter Crary <pcrary@neology.net>; Michael Roth <mroth@neology.net>; Israel Padilla <ipadilla@neology.mx>; Michell Itallekzi Garcia Garcia <colaborador6@neopartners.mx>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; John Tedona <jtedona@neology.net>; PIPS Technology Support <support@pipstechnology.com>; Quinn, Dermot (POL) <dermot.quinn@state.ma.us>; Clarke, Shannon (EPS) <shannon.clarke@state.ma.us>
Subject: RE: BOSS update

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

I addition, I believe we may need a new license file. The logs say "5 concurrent" licenses available.

From: Egnitz, Brian (POL)
Sent: Tuesday, March 12, 2019 6:43 AM
To: Peter Crary; Michael Roth; Israel Padilla; Michell Itallekzi Garcia Garcia; Mitchell, Timothy (EPS); John Tedona; PIPS Technology Support; Quinn, Dermot (POL); Clarke, Shannon (EPS)
Subject: Fwd: BOSS update

Hi guys,

Is there an updated client? This on appears to be calling the Spanish version of dot net, it's also not using the updated version already installed. Do you have one that is properly signed too???

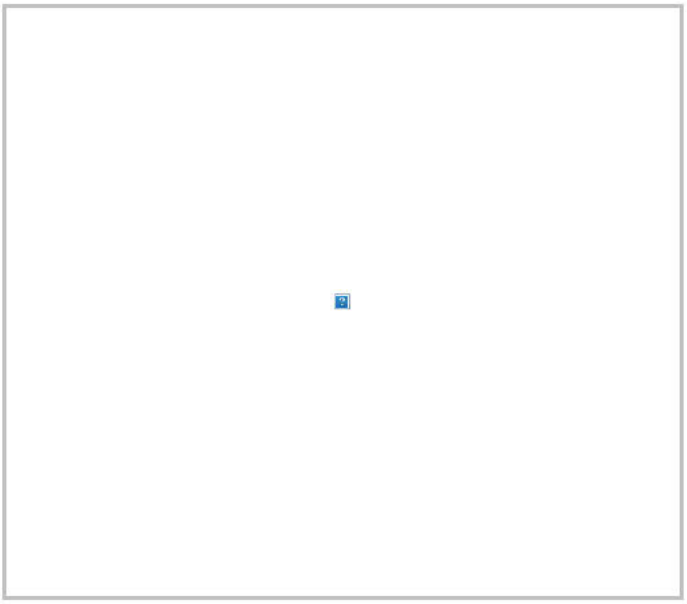
Begin forwarded message:

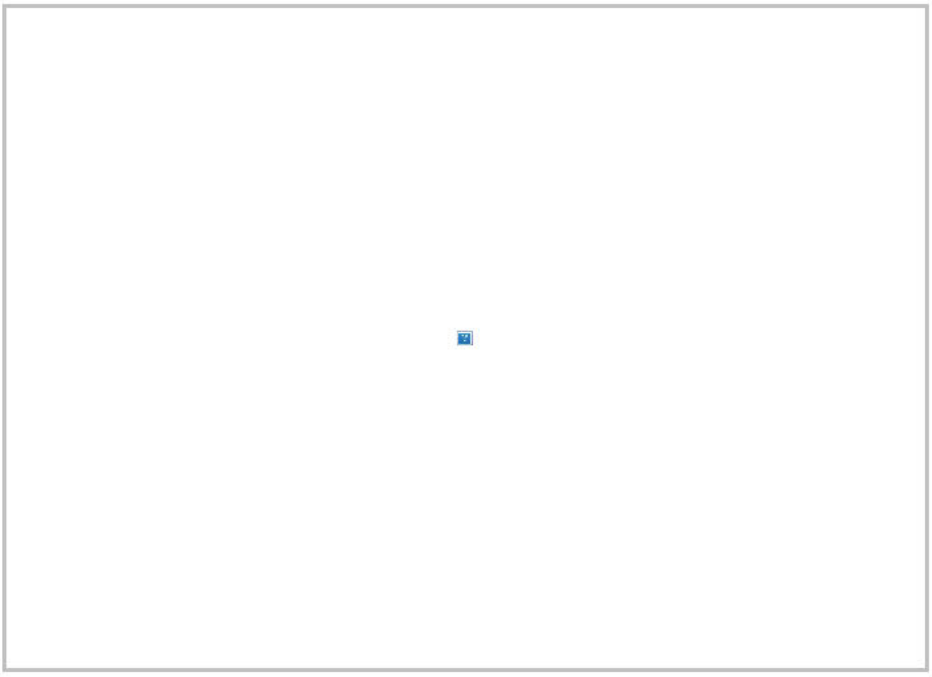
> **From:** "Ghasemi, Kiarash (POL)" <Kiarash.Ghasemi@pol.state.ma.us>
> **Date:** March 11, 2019 at 10:35:38 PM EDT
> **To:** "Egnitz, Brian (POL)" <brian.egnitz@pol.state.ma.us>, "Sullivan, Margaret (POL)" <Margaret.Sullivan@pol.state.ma.us>
> **Cc:** "Quinn, Dermot (POL)" <dermot.quinn@pol.state.ma.us>, "Kelly, Edward (POL)" <Edward.Kelly@pol.state.ma.us>, "Hernandez, Oscar (POL)" <Oscar.Hernandez@pol.state.ma.us>, "Weldon, Stephen (POL)" <Stephen.Weldon@pol.State.MA.US>, "Griffin, Daniel (POL)" <daniel.griffin@MassMail.State.MA.US>
> **Subject: RE: BOSS update**
>
> Hi Brian,
>
> Before this update, On computers that needed access to LPR reporting, we have a copied a folder called "SA Client" and "SA.UI" within that folder, we create a shortcut to that file and that eliminated installation of any program.
>
> But I have tried the link that you have provided us and I'm getting an error message in Spanish during the installation! (Please see below) What I get from it, it need .Net. 4.5.2 but my computer already has 4.7 installed on it. I also tried to install it on Watchcenter computers and I got the same error message in Spanish and .Net 4.5.2 wont install on top of the current version of 4.7

Also translation of other part of the error message is that:

"The Microsoft .NET Framework 4.5.2 installation is not supported on this operating system. Please contact the administrator."

I have CC Lt. Griffin on this email, since he has done many installation of the old one too and all his stations are also effected too.





Error de comprobación de los requisitos previos del componente del sistema Microsoft .NET Framework 4.5.2 (x86 y x64) con el siguiente mensaje:
"La instalación de Microsoft .NET Framework 4.5.2 no se admite en este sistema operativo. Póngase en contacto con el administrador."

Vea el archivo de registro de la instalación que se encuentra en 'C:\Users\MJACKS~1\AppData\Local\Temp\VSD1947.tmp\install.log' para obtener más información.

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Monday, March 11, 2019 9:58 PM
To: Sullivan, Margaret (POL) <Margaret.Sullivan@pol.state.ma.us>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Kelly, Edward (POL) <Edward.Kelly@pol.state.ma.us>; Hernandez, Oscar (POL) <Oscar.Hernandez@pol.state.ma.us>; Weldon, Stephen (POL) <Stephen.Weldon@pol.State.MA.US>; Ghasemi, Kiarash (POL) <Kiarash.Ghasemi@pol.state.ma.us>
Subject: BOSS update

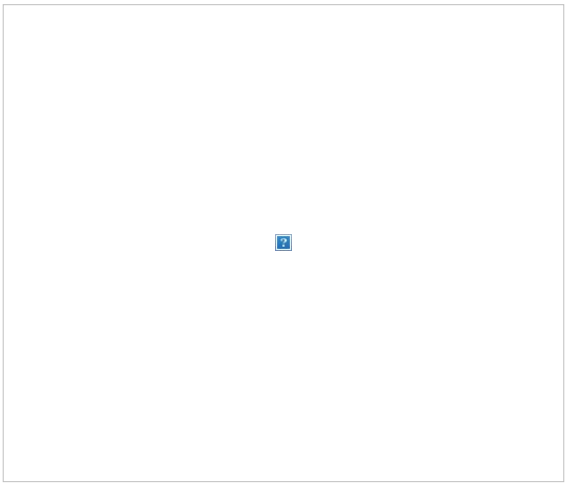
Hi Peg,

The BOSS ALPR application has been updated in case you get some calls regarding ALPR. The client can be updated using the url below if it doesn't do it automatically. Configure IP and port as

below.

-Brian

ht G.L. c. 4, sec. 7.cl. 26 (c)(privacy)



Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
Phone: 978-451-3710 (Maynard) 508-988-7302 (GHQ)
Email: Brian.Egnitz@massmail.state.ma.us
Monday - Friday, 8 to 4

CONFIDENTIALITY NOTICE: *The information contained in this email and any attachment is privileged and confidential law enforcement information. If you have received this email in error, please call 978-451-3700 immediately. Thank you.*

From: Slater, James (CHS)
To: McCarthy, Steven (POL); Venkatachalam, Krishna (EPS)
Subject: FW: BWC PO
Date: Thursday, July 23, 2020 11:08:28 AM
Attachments: Body Worn Camera Pricing 7.6.20 (003).xlsx

Good morning, gentlemen…happy Thursday!

The attached is just an FYI and are not intended for general circulation.

Thanks.

Jim

From: Joy, Emi (EPS) <Emi.Joy1@mass.gov>
Sent: Tuesday, July 21, 2020 14:00
To: Slater, James (CHS) <james.slater@mass.gov>; Collins, Kerry (EPS) <Kerry.Collins@mass.gov>
Cc: Michalski, Maria (EPS) <maria.michalski@mass.gov>; Goetz, Kelsey (EPS) <Kelsey.Goetz@mass.gov>
Subject: RE: BWC PO

To help us talk about the costs, I broke them down a little more – see attached.

We are only looking for $6.7 M in capital. I was asking about payment timing because I was wondering whether we could wait a couple of weeks for the pending bond bill to pass, which carries new EOPSS general authorization. Unless - would it be accurate to say that Secretary Heffernan committed A&F capital funds in the meeting with Chief Lepore last week? If so, I will mention that in a request to A&F for an ISA of their general equipment funds, as opposed to my default of assuming we will need to use our own funds.

The remaining $2.2 M ($1.7 M to WatchGuard, $500 K for Records Mgmt Office) in FY21 costs will need to be paid for out of MSP's operating budget. Kerry – I am going to start a thread with you and Michelle to confirm her plan to pay for that.

Emi L. Joy
Chief Financial Officer
Executive Office of Public Safety & Security
One Ashburton Place - Room 2133
Boston, MA 02108
Cell: 617-733-1158

From: Slater, James (CHS) <james.slater@mass.gov>
Sent: Tuesday, July 21, 2020 1:23 PM
To: Collins, Kerry (EPS) <Kerry.Collins@mass.gov>; Joy, Emi (EPS) <Emi.Joy1@mass.gov>
Cc: Michalski, Maria (EPS) <maria.michalski@mass.gov>
Subject: RE: BWC PO

Hi, folks!

I neglected to attach the expected payouts over the life of the contract.

Please let me know if you have any questions.

Jim

From: Collins, Kerry (EPS) <Kerry.Collins@mass.gov>
Sent: Tuesday, July 21, 2020 12:28
To: Joy, Emi (EPS) <Emi.Joy1@mass.gov>
Cc: Slater, James (CHS) <james.slater@mass.gov>; Michalski, Maria (EPS) <maria.michalski@mass.gov>
Subject: RE: BWC PO

Jim- it will all be up front, is that correct?
Thanks
Kerry

Kerry A. Collins
Undersecretary for Forensic Science and Technology
Executive Office of Public Safety and Security
1 Ashburton Place
Boston, MA 02108
Cell [redacted]
kerry.collins@mass.gov

From: Joy, Emi (EPS) <Emi.Joy1@mass.gov>
Sent: Tuesday, July 21, 2020 12:27 PM
To: Collins, Kerry (EPS) <Kerry.Collins@mass.gov>
Cc: Slater, James (CHS) <james.slater@mass.gov>; Michalski, Maria (EPS) <maria.michalski@mass.gov>
Subject: RE: BWC PO

Thank you for being on top of the finance side in advance – I will confirm the correct account and get back to you. Do you have any sense for the cashflow – as in, will we essentially need to pay the full capital cost upfront, or will we be paying the total with monthly or quarterly installments? I'll assume upfront unless I hear otherwise.

Emi L. Joy
Chief Financial Officer
Executive Office of Public Safety & Security
One Ashburton Place - Room 2133
Boston, MA 02108

Cell: 617-733-1158

From: Collins, Kerry (EPS) <Kerry.Collins@mass.gov>
Sent: Tuesday, July 21, 2020 12:19 PM
To: Joy, Emi (EPS) <Emi.Joy1@mass.gov>
Cc: Slater, James (CHS) <james.slater@mass.gov>; Michalski, Maria (EPS) <maria.michalski@mass.gov>
Subject: BWC PO

Hi Emi,
We are working on getting the BWC SOW signed this week. I'm reaching out to you now though because we will need to know out of what account we will be cutting the PO. I wanted to flag this for you now so when the SOW is signed we have the PO ready to go.
Thanks
Kerry

Kerry A. Collins
Undersecretary for Forensic Science and Technology
Executive Office of Public Safety and Security
1 Ashburton Place
Boston, MA 02108
Cell [redacted: c.L. c. 4.sec. 7.cl.26 (n)(security)]
kerry.collins@mass.gov

From: Mason, Christopher (POL)
To: Quinn, Dermot (POL); Range, Scott (POL); Egnitz, Brian (POL)
Cc: Warmington, Scott (POL)
Subject: FW: Commonwealth v McCarthy - SJC Decision (the Sagamore bridge cam case)
Date: Thursday, April 16, 2020 10:53:25 AM
Attachments: e12750.pdf
ATT00001.txt

FYI

-----Original Message-----
From: Thibeault, Sharon (CPI)
Sent: Thursday, April 16, 2020 10:23 AM
To: Mason, Christopher (POL) <Chris.Mason@pol.state.ma.us>
Subject: Commonwealth v McCarthy - SJC Decision (the Sagamore bridge cam case)

https://www.mass.gov/files/documents/2020/04/16/e12750.pdf

Good morning Colonel,

It is nice to share some good news for a change.
I know the Bridge cam case has wide State Police implications. Thought you would like to give it a read.
Another win for the Cape!
Stay healthy.

Sharon Thibeault

From: Mason, Christopher (POL)
To: Halpin, Michael (POL)
Subject: FW: Commonwealth v McCarthy - SJC Decision (the Sagamore bridge cam case)
Date: Thursday, April 16, 2020 10:53:00 AM
Attachments: e12750.pdf
ATT00001.txt

FYI

-----Original Message-----
From: Thibeault, Sharon (CPI)
Sent: Thursday, April 16, 2020 10:23 AM
To: Mason, Christopher (POL) <Chris.Mason@pol.state.ma.us>
Subject: Commonwealth v McCarthy - SJC Decision (the Sagamore bridge cam case)

https://www.mass.gov/files/documents/2020/04/16/e12750.pdf

Good morning Colonel,

It is nice to share some good news for a change.
I know the Bridge cam case has wide State Police implications. Thought you would like to give it a read.
Another win for the Cape!
Stay healthy.

Sharon Thibeault

From: Halpin, Michael (POL)
To: Eng, Brian (POL)
Subject: FW: Commonwealth v McCarthy - SJC Decision (the Sagamore bridge cam case)
Date: Friday, April 17, 2020 1:44:10 PM
Attachments: e12750.pdf
ATT00001.txt

From:	Cosgrove, Richard (CPI)
To:	Barnard, Diana (CPI); Chatigny, Anthony B (POL); Cosgrove, Richard (CPI); Diotte, Jeffrey (POL); Dunphy, David (POL); Fries, Joshua (POL); Furtado, Gregory (POL); Hatchell, Shawn (POL); Hanafin, John (CPI); Macdonald, Paul (POL); Lavoie, Matt (CPI); McCabe, Scott (CPI); Perkins, Taylor (CPI); Porter, Bradford (POL); Powell, Marc S (POL); Shaw, Dustin (POL); Walczak, David J (POL); Waskiewicz, Justin J (POL)
Subject:	FW: Commonwealth v McCarthy - SJC Decision - (the Sagamore bridge cam case)
Date:	Thursday, April 16, 2020 10:53:04 AM
Attachments:	e12750.pdf ATT00001.txt

-----Original Message-----
From: Thibeault, Sharon (CPI)
Sent: Thursday, April 16, 2020 10:26 AM
To: Cosgrove, Richard (CPI); McCabe, Scott (CPI)
Subject: FW: Commonwealth v McCarthy - SJC Decision - (the Sagamore bridge cam case)

https://www.mass.gov/files/documents/2020/04/16/e12750.pdf

Good morning Rich and Scott,

The SJC decision on the bridge cams came out this morning.
I am forwarding it along in case you want to take a look.
Another win for the Cape!

Hope you are staying safe!

Sharon

From: Silva, Kyra (POL)
To: Miller, Dianne (POL)
Subject: FW: FFY 2016 ISAs for purchase of ALPR & LiDAR/Radar Equipment
Date: Wednesday, September 30, 2020 5:05:00 PM
Attachments: FFY16 ALPR MSP ISA $50,000 6.30.16.doc
FFY16 LIDAR MSP ISA $210,000 6.30.2016.doc
FFY 16 EOPSS Proposal LIDAR 82nd RTT.DOC
FFY 2016 ALPR Funding Proposal.pdf

From: Firlit, Deborah (OGR)
Sent: Monday, February 01, 2016 3:20 PM
To: Comeau, Melissa (POL); Broderick, Deborah (POL)
Cc: Griffin, Daniel (POL)
Subject: FFY 2016 ISAs for purchase of ALPR & LiDAR/Radar Equipment
Importance: High

Good afternoon,

Attached are ISAs for the purchase of an ALPR system and LiDAR/Radar units. Please review, sign and return ASAP. The end date is June 30, 2016 and being as it can be a lengthy process to get the money into MMARS, I ask for your immediate attention to this matter.

I have also attached the Funding Proposals for your information.

That's it for now. Thanks again for your help and I look forward to your reply.

Deb

Deborah Firlit
Program Coordinator
EOPSS/Highway Safety Division
Ten Park Plaza, Suite 3720
Boston, MA 02116
T: 617-725-3356 F: 617-725-0260
U Drive, U Text, U Pay

From: Firlit, Deborah (OGR)
To: Sonia, Michael (POL)
Subject: FW: FFY 2021 Traffic Safety Grant Program for State Agencies - Massachusetts State Police
Date: Thursday, April 2, 2020 9:55:50 AM
Attachments: MSP Funding Proposal FFY2021.pdf
Distracted Driving Budget Work Sheet.xls
DRE Budget Work Sheet.xls
FFY21 LEL Budget Work Sheet (Autosaved).xls
FFY21 YDE Budget Work Sheet.xls
Occupant Protection Budget Work Sheet.xls
Sobriety Budget Work Sheet.xls
Speed and Aggressive Driving Budget Work Sheet.xls
STEP Budget Work Sheet.xls

Looks like you were not cc'd on this email.

From: Tapis, Stephen C (POL) <Stephen.C.Tapis@pol.state.ma.us>
Sent: Tuesday, March 31, 2020 1:13 PM
To: Brownell, Jeffrey (OGR) <jeffrey.brownell@mass.gov>
Cc: England, Kara (POL) <kara.england@pol.state.ma.us>; Taylor, Rita (POL) <Rita.Taylor@pol.state.ma.us>; Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Subject: FFY 2021 Traffic Safety Grant Program for State Agencies - Massachusetts State Police

Good day-

Please find attached the unsigned electronic copy of the application and budget for the FY2021 Traffic Safety Grant Program for State Agencies. Per the AGF, the signed original and one copy, including the budget detail spreadsheets have been mailed via USPS in your attention to the address provided in the AGF.

Please let me know if you have any questions.

Respectfully-
Stephen

Trooper Stephen Tapis #3888
Massachusetts State Police
Strategic Planning Section
470 Worcester Road
Framingham, MA 01702
(508) 820-2309

The information transmitted is intended only for the person or entity to which it is addressed and may contain confidential and/or privileged material. Any review, retransmission, dissemination or other use of, or taking of any action in reliance upon, this information by persons or entities other than the intended recipient is prohibited

From: Carney, Joanne (POL)
To: Serra, Anthony F (POL)
Subject: FW: FOIA REQUEST Inventory of DHS DIS and DFS 11.6.20.xlsx
Date: Monday, November 9, 2020 12:32:23 PM
Attachments: FOIA REQUEST Inventory of DHS DIS and DFS 11.6.20.xlsx

---

The complete inventories that we spoke of.

Joanne S. Carney
Massachusetts State Police
470 Worcester Road
Framingham MA 01702
508-820-2342

From: McKenna, Patricia (POL) <Patricia.McKenna@pol.state.ma.us>
Sent: Monday, November 9, 2020 12:19 PM
To: Carney, Joanne (POL) <joanne.carney@pol.state.ma.us>
Cc: Rivera Morgan, Awilda (POL) <Awilda.RiveraMorgan@pol.state.ma.us>
Subject: FOIA REQUEST Inventory of DHS DIS and DFS 11.6.20.xlsx

Joanne,

Attached are the current inventories of DHS, DIS AND DFS.

Trish

From: John Tedona
To: Egnitz, Brian (POL)
Subject: FW: Good News -Court Decision
Date: Friday, April 17, 2020 10:23:16 AM
Attachments: image001.png
image003.png

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Maybe I said Yeah too soon.

https://www.capecodtimes.com/news/20200416/court-backs-limited-use-of-license-plate-readers?utm_source=SFMC&utm_medium=email&utm_campaign=The%20Cape%20Cod%20Times%20daily%202020-04-17&utm_content=GTDT_CCT&utm_term=041720

John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: John Tedona
Sent: Thursday, April 16, 2020 7:22 PM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: Good News -Court Decision

Yeah!

Commonwealth v. McCarthy
Supreme Judicial Court, April 16, 2020
(Search and Seizure/Automatic License Plate Readers)

The use of four automatic license plate reader cameras, placed at two fixed locations on the ends of the Bourne and Sagamore bridges and used to "hit" on the defendant's license when he drove over either bridge,, does not constitute a search within the meaning of either art. 14 or the Fourth Amendment.

"While we recognize that the widespread use of ALPRs in the Commonwealth could implicate constitutional protections against unreasonable searches, the limited use of the technology in this case does not."

Note:
The Court did not find error in the fact that the Bourne Police Department did not have a separate policy, apart from State Police TRF-11, regarding ALPRs.

Additionally, the Court ruled that the government's use of ALPR data is not subject to the Stored Communication Act nor the Electronic Communications Privacy Act

See attached opinion.

For other recent case law decisions, go to the MDAA website at www.mass.gov/mdaa



A NEOLOGY Business

John Tedona
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

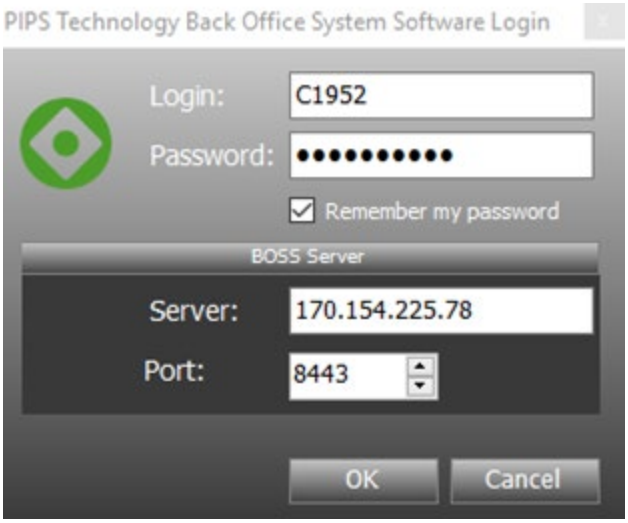
Subject: FW: LPR & Coplink Accounts
Date: Wednesday, March 25, 2020 1:37:37 PM
Attachments: _CFC WFG.PDF
image004.png
image001.png

From: Lenti, Jeffrey (POL) <[redacted]pol.state.ma.us>
Sent: Wednesday, March 25, 2020 1:37 PM
To: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Subject: FW: LPR & Coplink Accounts

From: Chandler, Brittany (POL) <Brittany.Chandler@pol.state.ma.us>
Sent: Wednesday, March 25, 2020 1:31 PM
To: Lenti, Jeffrey (POL) <[redacted]pol.state.ma.us>
Subject: RE: LPR & Coplink Accounts

Do you have the correct "Server" and "Port"? Below is the correct information. Unfortunately, it doesn't autofill with the correct information.

I've attached the CFC's Workflow guide I put together, too. There's a section on how to use the LPR that may useful.



-Brittany

From: Lenti, Jeffrey (POL)
Sent: Wednesday, March 25, 2020 1:26 PM
To: Chandler, Brittany (POL) <Brittany.Chandler@pol.state.ma.us>
Subject: RE: LPR & Coplink Accounts

Ok, now I'm having trouble logging into the LPR app. I've downloaded the latest version but still no luck using the original login you gave me or what I changed the CopLink to

---

From: Chandler, Brittany (POL) <Brittany.Chandler@pol.state.ma.us>
Sent: Wednesday, March 25, 2020 12:59 PM
To: Lenti, Jeffrey (POL) <[redacted]pol.state.ma.us>
Subject: RE: LPR & Coplink Accounts

Jeff,

That may have been it. I unsuspended your account and created a temporary password: [redacted] Once you've logged in with the temporary password, it should prompt you to create a new password. Let me know if that doesn't work.

-Brittany

Respectfully,

Brittany Chandler
Intelligence Analyst II
Massachusetts State Police | Commonwealth Fusion Center
470 Worcester Road, Framingham, MA 01702
Phone: (508) 820-2233
brittany.chandler@mass.gov

CONFIDENTIALITY NOTICE: The information contained in this email and any attachment is privileged and confidential law enforcement information. If you are not the intended recipient, you are hereby notified that any disclosure, dissemination, or copying of this communication is strictly prohibited. If you have received this email in error, call (978) 451-3700 immediately.

From: Lenti, Jeffrey (POL)
Sent: Wednesday, March 25, 2020 12:55 PM
To: Chandler, Brittany (POL) <Brittany.Chandler@pol.state.ma.us>
Cc: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Subject: RE: LPR & Coplink Accounts

Brittany,

It is saying that my Coplink account is "suspended". I had an account prior so I'm not sure if that is

the issue.

Thanks,
Jeff

From: Chandler, Brittany (POL) <Brittany.Chandler@pol.state.ma.us>
Sent: Wednesday, March 25, 2020 12:33 PM
To: Lenti, Jeffrey (POL) <[redacted]pol.state.ma.us>
Cc: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Subject: LPR & Coplink Accounts

Good Afternoon,

Please find below the information for your LPR and Coplink accounts. Let me know if you have any questions or issues.

LPR:
Login name: [redacted]
Display name: [redacted]
Password: [redacted]

In regards to Coplink, it looks like you have an existing account that is up to date. If you need to reset the password or a refresher, let me know.

Respectfully,

Brittany Chandler
Intelligence Analyst II
Massachusetts State Police | Commonwealth Fusion Center
470 Worcester Road, Framingham, MA 01702
Phone: (508) 820-2233
brittany.chandler@mass.gov

CONFIDENTIALITY NOTICE: The information contained in this email and any attachment is privileged and confidential law enforcement information. If you are not the intended recipient, you are hereby notified that any disclosure, dissemination, or copying of this communication is strictly prohibited. If you have received this email in error, call (978) 451-3700 immediately.

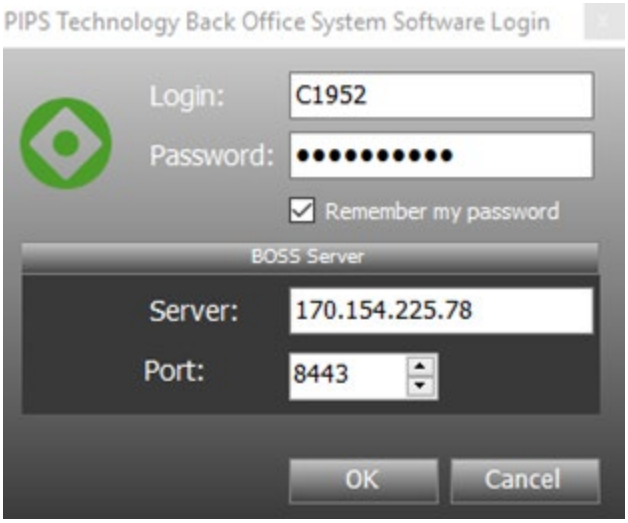
Subject: FW: LPR & Coplink Accounts
Date: Wednesday, March 25, 2020 1:37:37 PM
Attachments: _CFC WFG.PDF
image004.png
image001.png

From: Lenti, Jeffrey (POL) <[redacted]pol.state.ma.us>
Sent: Wednesday, March 25, 2020 1:37 PM
To: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Subject: FW: LPR & Coplink Accounts

From: Chandler, Brittany (POL) <Brittany.Chandler@pol.state.ma.us>
Sent: Wednesday, March 25, 2020 1:31 PM
To: Lenti, Jeffrey (POL) <[redacted]pol.state.ma.us>
Subject: RE: LPR & Coplink Accounts

Do you have the correct "Server" and "Port"? Below is the correct information. Unfortunately, it doesn't autofill with the correct information.

I've attached the CFC's Workflow guide I put together, too. There's a section on how to use the LPR that may useful.



-Brittany

From: Lenti, Jeffrey (POL)
Sent: Wednesday, March 25, 2020 1:26 PM
To: Chandler, Brittany (POL) <Brittany.Chandler@pol.state.ma.us>
Subject: RE: LPR & Coplink Accounts

Ok, now I'm having trouble logging into the LPR app. I've downloaded the latest version but still no luck using the original login you gave me or what I changed the CopLink to

---

From: Chandler, Brittany (POL) <Brittany.Chandler@pol.state.ma.us>
Sent: Wednesday, March 25, 2020 12:59 PM
To: Lenti, Jeffrey (POL) <[redacted]pol.state.ma.us>
Subject: RE: LPR & Coplink Accounts

Jeff,

That may have been it. I unsuspended your account and created a temporary password: [redacted] Once you've logged in with the temporary password, it should prompt you to create a new password. Let me know if that doesn't work.

-Brittany

Respectfully,

Brittany Chandler
Intelligence Analyst II
Massachusetts State Police | Commonwealth Fusion Center
470 Worcester Road, Framingham, MA 01702
Phone: (508) 820-2233
brittany.chandler@mass.gov

CONFIDENTIALITY NOTICE: The information contained in this email and any attachment is privileged and confidential law enforcement information. If you are not the intended recipient, you are hereby notified that any disclosure, dissemination, or copying of this communication is strictly prohibited. If you have received this email in error, call (978) 451-3700 immediately.

From: Lenti, Jeffrey (POL)
Sent: Wednesday, March 25, 2020 12:55 PM
To: Chandler, Brittany (POL) <Brittany.Chandler@pol.state.ma.us>
Cc: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Subject: RE: LPR & Coplink Accounts

Brittany,

It is saying that my Coplink account is "suspended". I had an account prior so I'm not sure if that is

the issue.

Thanks,
Jeff

From: Chandler, Brittany (POL) <Brittany.Chandler@pol.state.ma.us>
Sent: Wednesday, March 25, 2020 12:33 PM
To: Lenti, Jeffrey (POL) <[redacted]pol.state.ma.us>
Cc: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Subject: LPR & Coplink Accounts

Good Afternoon,

Please find below the information for your LPR and Coplink accounts. Let me know if you have any questions or issues.

LPR:
Login name: [redacted]
Display name: [redacted]
Password: [redacted]

In regards to Coplink, it looks like you have an existing account that is up to date. If you need to reset the password or a refresher, let me know.

Respectfully,

Brittany Chandler
Intelligence Analyst II
Massachusetts State Police | Commonwealth Fusion Center
470 Worcester Road, Framingham, MA 01702
Phone: (508) 820-2233
brittany.chandler@mass.gov

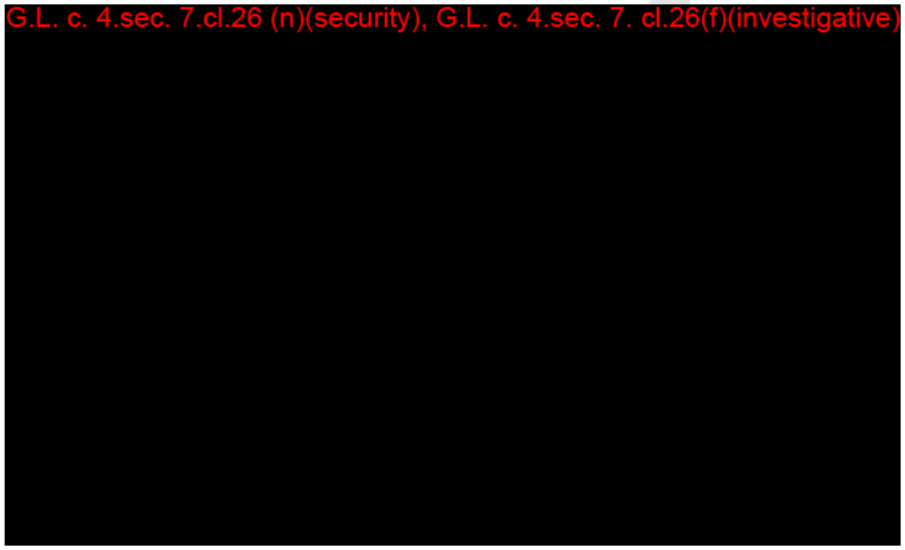
CONFIDENTIALITY NOTICE: The information contained in this email and any attachment is privileged and confidential law enforcement information. If you are not the intended recipient, you are hereby notified that any disclosure, dissemination, or copying of this communication is strictly prohibited. If you have received this email in error, call (978) 451-3700 immediately.

From: Lenti, Jeffrey (POL)
To: Brooks, Brian (POL)
Subject: FW: LPR & Coplink Accounts
Date: Wednesday, March 25, 2020 1:37:16 PM
Attachments: _CFC WFG.PDF
image004.png
image001.png

From: Chandler, Brittany (POL) <Brittany.Chandler@pol.state.ma.us>
Sent: Wednesday, March 25, 2020 1:31 PM
To: Lenti, Jeffrey (POL) <[redacted]pol.state.ma.us>
Subject: RE: LPR & Coplink Accounts

Do you have the correct "Server" and "Port"? Below is the correct information. Unfortunately, it doesn't autofill with the correct information.

I've attached the CFC's Workflow guide I put together, too. There's a section on how to use the LPR that may useful.



-Brittany

From: Lenti, Jeffrey (POL)
Sent: Wednesday, March 25, 2020 1:26 PM
To: Chandler, Brittany (POL) <Brittany.Chandler@pol.state.ma.us>
Subject: RE: LPR & Coplink Accounts

Ok, now I'm having trouble logging into the LPR app. I've downloaded the latest version but still no luck using the original login you gave me or what I changed the CopLink to

---

From: Chandler, Brittany (POL) <Brittany.Chandler@pol.state.ma.us>

Sent: Wednesday, March 25, 2020 12:59 PM
To: Lenti, Jeffrey (POL) <[redacted]pol.state.ma.us>
Subject: RE: LPR & Coplink Accounts

Jeff,

That may have been it. I unsuspended your account and created a temporary password: [redacted] Once you've logged in with the temporary password, it should prompt you to create a new password. Let me know if that doesn't work.

-Brittany

Respectfully,

Brittany Chandler
Intelligence Analyst II
Massachusetts State Police | Commonwealth Fusion Center
470 Worcester Road, Framingham, MA 01702
Phone: (508) 820-2233
brittany.chandler@mass.gov

CONFIDENTIALITY NOTICE: The information contained in this email and any attachment is privileged and confidential law enforcement information. If you are not the intended recipient, you are hereby notified that any disclosure, dissemination, or copying of this communication is strictly prohibited. If you have received this email in error, call (978) 451-3700 immediately.

From: Lenti, Jeffrey (POL)
Sent: Wednesday, March 25, 2020 12:55 PM
To: Chandler, Brittany (POL) <Brittany.Chandler@pol.state.ma.us>
Cc: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Subject: RE: LPR & Coplink Accounts

Brittany,

It is saying that my Coplink account is "suspended". I had an account prior so I'm not sure if that is the issue.

Thanks,
Jeff

From: Chandler, Brittany (POL) <Brittany.Chandler@pol.state.ma.us>
Sent: Wednesday, March 25, 2020 12:33 PM
To: Lenti, Jeffrey (POL) <Jeffrey.Lenti@pol.state.ma.us>
Cc: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Subject: LPR & Coplink Accounts

Good Afternoon,

Please find below the information for your LPR and Coplink accounts. Let me know if you have any questions or issues.

LPR:
Login name: [redacted]
Display name: [redacted]
Password: [redacted]

In regards to Coplink, it looks like you have an existing account that is up to date. If you need to reset the password or a refresher, let me know.

Respectfully,

Brittany Chandler
Intelligence Analyst II
Massachusetts State Police | Commonwealth Fusion Center
470 Worcester Road, Framingham, MA 01702
Phone: (508) 820-2233
brittany.chandler@mass.gov

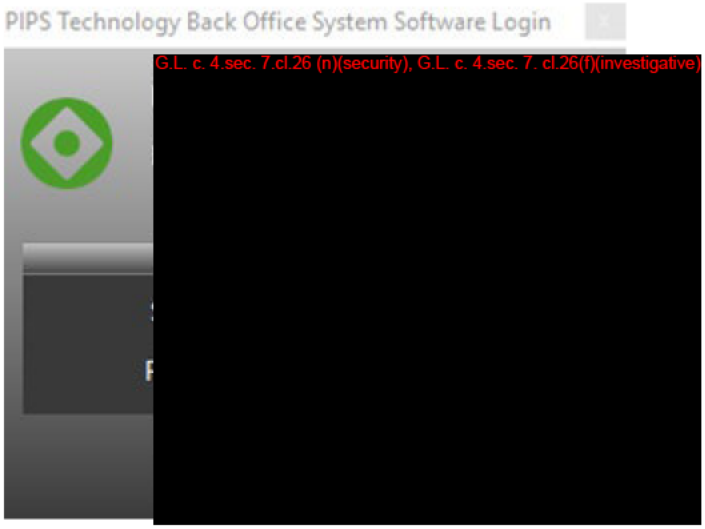
CONFIDENTIALITY NOTICE: The information contained in this email and any attachment is privileged and confidential law enforcement information. If you are not the intended recipient, you are hereby notified that any disclosure, dissemination, or copying of this communication is strictly prohibited. If you have received this email in error, call (978) 451-3700 immediately.

Subject: FW: LPR & Coplink Accounts
Date: Wednesday, March 25, 2020 1:36:47 PM
Attachments: _CFC WFG.PDF
image004.png
image001.png

From: Chandler, Brittany (POL) <Brittany.Chandler@pol.state.ma.us>
Sent: Wednesday, March 25, 2020 1:31 PM
To: Lenti, Jeffrey (POL) <[redacted]pol.state.ma.us>
Subject: RE: LPR & Coplink Accounts

Do you have the correct "Server" and "Port"? Below is the correct information. Unfortunately, it doesn't autofill with the correct information.

I've attached the CFC's Workflow guide I put together, too. There's a section on how to use the LPR that may useful.



-Brittany

From: Lenti, Jeffrey (POL)
Sent: Wednesday, March 25, 2020 1:26 PM
To: Chandler, Brittany (POL) <Brittany.Chandler@pol.state.ma.us>
Subject: RE: LPR & Coplink Accounts

Ok, now I'm having trouble logging into the LPR app. I've downloaded the latest version but still no luck using the original login you gave me or what I changed the CopLink to

---

From: Chandler, Brittany (POL) <Brittany.Chandler@pol.state.ma.us>
Sent: Wednesday, March 25, 2020 12:59 PM
To: Lenti, Jeffrey (POL) <[redacted]pol.state.ma.us>

Subject: RE: LPR & Coplink Accounts

Jeff,

That may have been it. I unsuspended your account and created a temporary password: [redacted] Once you've logged in with the temporary password, it should prompt you to create a new password. Let me know if that doesn't work.

-Brittany

Respectfully,

Brittany Chandler
Intelligence Analyst II
Massachusetts State Police | Commonwealth Fusion Center
470 Worcester Road, Framingham, MA 01702
Phone: (508) 820-2233
brittany.chandler@mass.gov

CONFIDENTIALITY NOTICE: The information contained in this email and any attachment is privileged and confidential law enforcement information. If you are not the intended recipient, you are hereby notified that any disclosure, dissemination, or copying of this communication is strictly prohibited. If you have received this email in error, call (978) 451-3700 immediately.

From: Lenti, Jeffrey (POL)
Sent: Wednesday, March 25, 2020 12:55 PM
To: Chandler, Brittany (POL) <Brittany.Chandler@pol.state.ma.us>
Cc: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Subject: RE: LPR & Coplink Accounts

Brittany,

It is saying that my Coplink account is "suspended". I had an account prior so I'm not sure if that is the issue.

Thanks,
Jeff

From: Chandler, Brittany (POL) <Brittany.Chandler@pol.state.ma.us>
Sent: Wednesday, March 25, 2020 12:33 PM

To: Lenti, Jeffrey (POL) <Jeffrey.Lenti@pol.state.ma.us>
Cc: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Subject: LPR & Coplink Accounts

Good Afternoon,

Please find below the information for your LPR and Coplink accounts. Let me know if you have any questions or issues.

LPR:
Login name: [redacted]
Display name: [redacted]
Password: [redacted]

In regards to Coplink, it looks like you have an existing account that is up to date. If you need to reset the password or a refresher, let me know.

Respectfully,

Brittany Chandler
Intelligence Analyst II
Massachusetts State Police | Commonwealth Fusion Center
470 Worcester Road, Framingham, MA 01702
Phone: (508) 820-2233
brittany.chandler@mass.gov

CONFIDENTIALITY NOTICE: The information contained in this email and any attachment is privileged and confidential law enforcement information. If you are not the intended recipient, you are hereby notified that any disclosure, dissemination, or copying of this communication is strictly prohibited. If you have received this email in error, call (978) 451-3700 immediately.

From: Brooks, Brian (POL)
To: Robles, Francis Jr. (POL); Berrios, Jorge (POL); Scott, William (POL)
Cc: O"Hara, Edward (POL)
Subject: FW: LPR & Coplink Accounts
Date: Wednesday, March 25, 2020 1:38:00 PM
Attachments: _CFC WFG.PDF
image004.png
image001.png

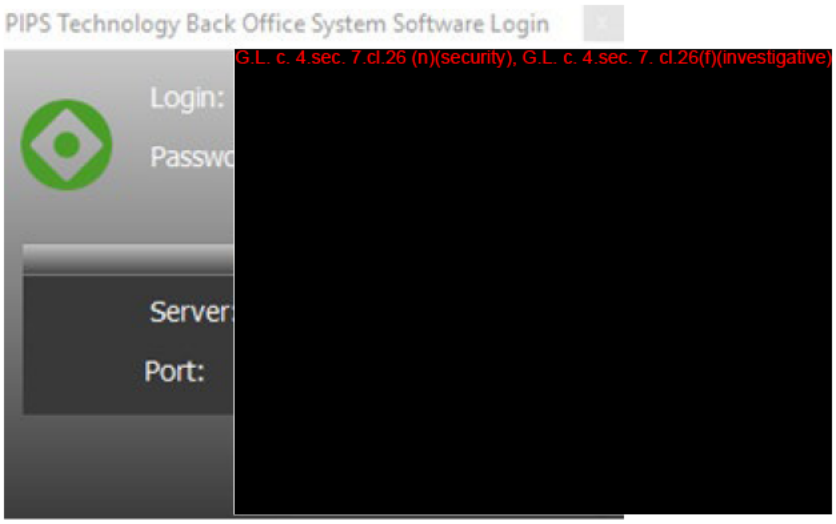
FYI please see below

From: Lenti, Jeffrey (POL) <Jeffrey.Lenti@pol.state.ma.us>
Sent: Wednesday, March 25, 2020 1:37 PM
To: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Subject: FW: LPR & Coplink Accounts

From: Chandler, Brittany (POL) <Brittany.Chandler@pol.state.ma.us>
Sent: Wednesday, March 25, 2020 1:31 PM
To: Lenti, Jeffrey (POL) <Jeffrey.Lenti@pol.state.ma.us>
Subject: RE: LPR & Coplink Accounts

Do you have the correct "Server" and "Port"? Below is the correct information. Unfortunately, it doesn't autofill with the correct information.

I've attached the CFC's Workflow guide I put together, too. There's a section on how to use the LPR that may useful.



-Brittany

From: Lenti, Jeffrey (POL)
Sent: Wednesday, March 25, 2020 1:26 PM

To: Chandler, Brittany (POL) <Brittany.Chandler@pol.state.ma.us>
Subject: RE: LPR & Coplink Accounts

Ok, now I'm having trouble logging into the LPR app. I've downloaded the latest version but still no luck using the original login you gave me or what I changed the CopLink to

---

From: Chandler, Brittany (POL) <Brittany.Chandler@pol.state.ma.us>
Sent: Wednesday, March 25, 2020 12:59 PM
To: Lenti, Jeffrey (POL) <Jeffrey.Lenti@pol.state.ma.us>
Subject: RE: LPR & Coplink Accounts

Jeff,

That may have been it. I unsuspended your account and created a temporary password: [redacted] Once you've logged in with the temporary password, it should prompt you to create a new password. Let me know if that doesn't work.

-Brittany

Respectfully,

Brittany Chandler
Intelligence Analyst II
Massachusetts State Police | Commonwealth Fusion Center
470 Worcester Road, Framingham, MA 01702
Phone: (508) 820-2233
brittany.chandler@mass.gov

CONFIDENTIALITY NOTICE: The information contained in this email and any attachment is privileged and confidential law enforcement information. If you are not the intended recipient, you are hereby notified that any disclosure, dissemination, or copying of this communication is strictly prohibited. If you have received this email in error, call (978) 451-3700 immediately.

From: Lenti, Jeffrey (POL)
Sent: Wednesday, March 25, 2020 12:55 PM
To: Chandler, Brittany (POL) <Brittany.Chandler@pol.state.ma.us>
Cc: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Subject: RE: LPR & Coplink Accounts

Brittany,

It is saying that my Coplink account is “suspended”. I had an account prior so I’m not sure if that is the issue.

Thanks,
Jeff

From: Chandler, Brittany (POL) <Brittany.Chandler@pol.state.ma.us>
Sent: Wednesday, March 25, 2020 12:33 PM
To: Lenti, Jeffrey (POL) <Jeffrey.Lenti@pol.state.ma.us>
Cc: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Subject: LPR & Coplink Accounts

Good Afternoon,

Please find below the information for your LPR and Coplink accounts. Let me know if you have any questions or issues.

LPR:
Login name: [redacted]
Display name: [redacted]
Password: [redacted]

In regards to Coplink, it looks like you have an existing account that is up to date. If you need to reset the password or a refresher, let me know.

Respectfully,

Brittany Chandler
Intelligence Analyst II
Massachusetts State Police | Commonwealth Fusion Center
470 Worcester Road, Framingham, MA 01702
Phone: (508) 820-2233
brittany.chandler@mass.gov

CONFIDENTIALITY NOTICE: The information contained in this email and any attachment is privileged and confidential law enforcement information. If you are not the intended recipient, you are hereby notified that any disclosure, dissemination, or copying of this communication is strictly prohibited. If you have received this email in error, call (978) 451-3700 immediately.

From: Bender, Sean (POL)
To: Chandler, Brittany (POL)
Subject: Fw: LPR
Date: Friday, January 24, 2020 8:47:12 AM
Attachments: Commonwealth Fusion Center - Weekly Activity Report - 17 January 2020 - 23 January 2020.docx

---

Disregard the previous version. This version has been updated by Lt. Brooks.

Sean Bender
Intelligence Analyst
Massachusetts State Police | Commonwealth Fusion Center
470 Worcester Road | Framingham | MA 01702
508-820-2233

From: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Sent: Friday, January 24, 2020 8:45 AM
To: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Subject: LPR

Lieutenant Brian Brooks #2601
Massachusetts State Police
Division of Homeland Security and Preparedness
Commonwealth Fusion Center
470 Worcester Road
Framingham, MA 01702
(W) 508-820-2233
(F) 508-988-7121

From: Commonwealth Fusion Center (POL)
To: New York State Police
Cc: Haywood, Antwan (POL)
Subject: Fw: LPR/ Toll Information Inquiry 2020-0C6-004160
Date: Friday, May 22, 2020 9:04:45 AM
Attachments: RFI_NY.pdf

Good Morning, NYSIC -

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

[redacted]

If you have any questions or require any additional information, please let us know. I have copied the original requester, Massachusetts State Police Trooper Antwan Haywood, on this exchange.

As always, thank you for your assistance!

Respectfully,

Sean Bender
Intelligence Analyst
Massachusetts State Police | Commonwealth Fusion Center
470 Worcester Road | Framingham, MA 01702
Phone: (508) 820-2233

CONFIDENTIALITY NOTICE: The information contained in this email and any attachment is privileged and confidential law enforcement information. If you are not the intended recipient, you are hereby notified that any disclosure, dissemination, or copying of this communication is strictly prohibited. If you have received this email in error, please call (978) 451-3700 immediately.

From: Haywood, Antwan (POL) <Antwan.Haywood@pol.state.ma.us>

Sent: Friday, May 22, 2020 8:56 AM
To: Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>
Subject: Re: [redacted]

The month of May 2020 would be extremely helpful.

Very Respectfully,

Tpr. Antwan Haywood #3967
Massachusetts State Police
State Police Holden, C-6
612 Main St.
Holden, MA 01520
Ph: (508) 829-4431
Fax: (508) 829-8425

From: Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>
Sent: Friday, May 22, 2020 8:53 AM
To: Haywood, Antwan (POL) <Antwan.Haywood@pol.state.ma.us>
Subject: Re: LPR/ Toll Information Inquiry 2020-0C6-004160

Good Morning, Trooper -

[redacted]

Respectfully,

Sean Bender

Intelligence Analyst
Massachusetts State Police | Commonwealth Fusion Center
470 Worcester Road | Framingham, MA 01702
Phone: (508) 820-2233

CONFIDENTIALITY NOTICE: The information contained in this email and any attachment is privileged and confidential law enforcement information. If you are not the intended recipient, you are hereby notified that any disclosure, dissemination, or copying of this communication is strictly prohibited. If you have received this email in error, please call (978) 451-3700 immediately.

From: Haywood, Antwan (POL) <Antwan.Haywood@pol.state.ma.us>
Sent: Friday, May 22, 2020 8:44 AM
To: Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>
Subject: LPR/ Toll Information Inquiry 2020-0C6-004160

Good Morning,



Tpr. Antwan Haywood #3967
Massachusetts State Police
State Police Holden, C-6
612 Main St.
Holden, MA 01520
Ph: (508) 829-4431
Fax: (508) 829-8425

From: Commonwealth Fusion Center (POL)
To: Haywood, Antwan (POL)
Subject: Fw: LPR/ Toll Information Inquiry 2020-0C6-004160
Date: Friday, May 22, 2020 2:29:06 PM
Attachments: 1.pdf
2.pdf
3.pdf
4.pdf

Good Afternoon,

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative) [redacted]

Respectfully,

Sean Bender
Intelligence Analyst
Massachusetts State Police | Commonwealth Fusion Center
470 Worcester Road | Framingham, MA 01702
Phone: (508) 820-2233

CONFIDENTIALITY NOTICE: The information contained in this email and any attachment is privileged and confidential law enforcement information. If you are not the intended recipient, you are hereby notified that any disclosure, dissemination, or copying of this communication is strictly prohibited. If you have received this email in error, please call (978) 451-3700 immediately.

From: troopers.sm.criminal.intelligence.unit <ciu@nysic.ny.gov>
Sent: Friday, May 22, 2020 2:23 PM
To: Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>
Subject: RE: LPR/ Toll Information Inquiry 2020-0C6-004160

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Please see attached.

Matthew S. Wilski
Investigator, NYS Intelligence Center
Criminal Intelligence Unit
(518)786-9399 - desk

New York State Police
31 Tech Valley Drive, Second Floor
East Greenbush, NY 12061
(518)786-2100 – main / (518)786-9398 – fax

Matthew.Wilski@troopers.ny.gov

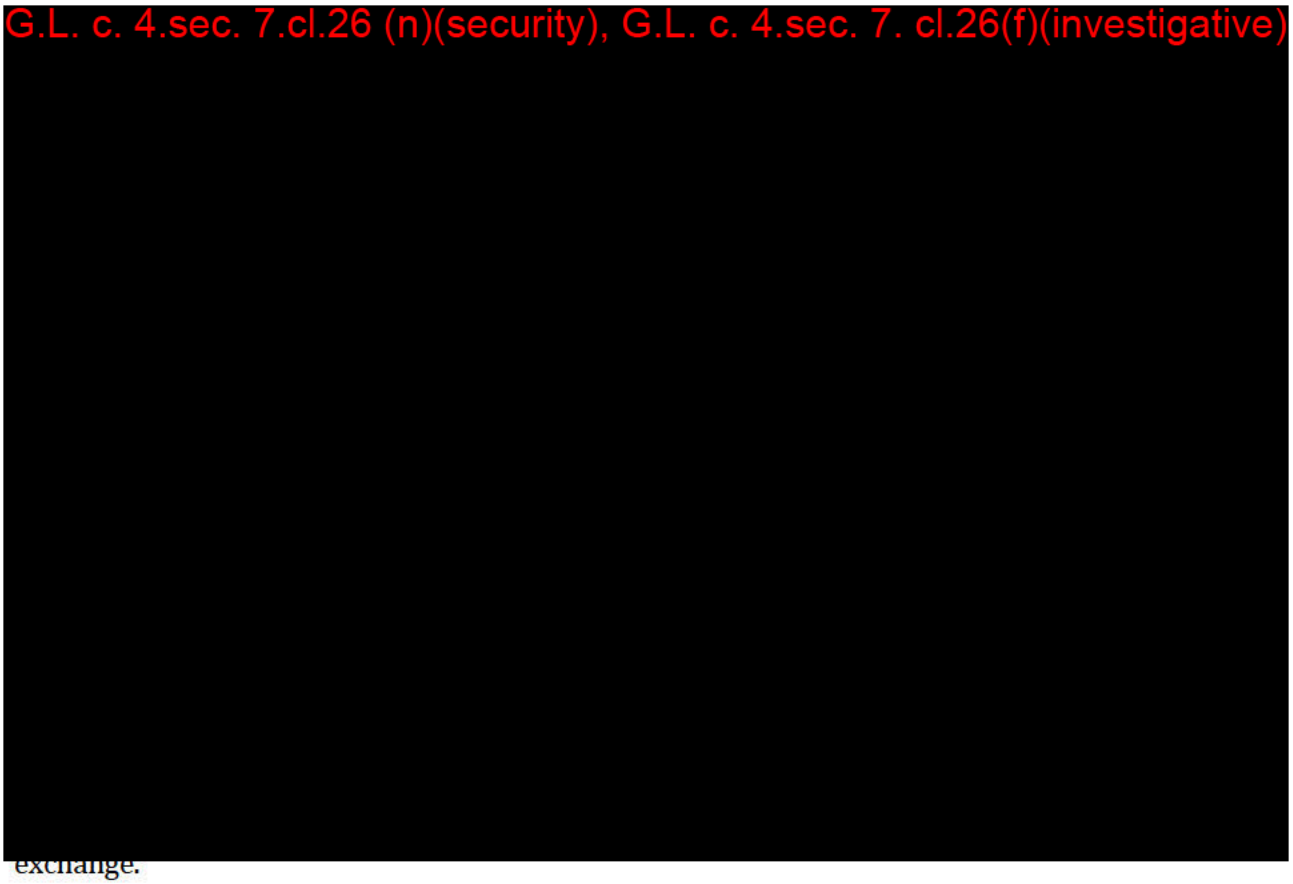
www.troopers.ny.gov

Important Information: *This e-mail and all attachments contained within should be retained in your original case file in order to fulfill any legal obligations. NYSIC does not retain copies of these records for purposes of discovery compliance.*

From: Fusion (POL) [mailto:fusion@state.ma.us]
Sent: Friday, May 22, 2020 9:05 AM
To: troopers.sm.criminal.intelligence.unit <ciu@nysic.ny.gov>
Cc: Haywood, Antwan (POL) <antwan.haywood@state.ma.us>
Subject: Fw: LPR/ Toll Information Inquiry 2020-0C6-004160

ATTENTION: This email came from an external source. Do not open attachments or click on links from unknown senders or unexpected emails.

Good Morning, NYSIC -



exchange.

As always, thank you for your assistance!

Respectfully,

Sean Bender
Intelligence Analyst
Massachusetts State Police | Commonwealth Fusion Center
470 Worcester Road | Framingham, MA 01702
Phone: (508) 820-2233

CONFIDENTIALITY NOTICE: The information contained in this email and any attachment is privileged and confidential law enforcement information. If you are not the intended recipient, you are hereby notified that any disclosure, dissemination, or copying of this communication is strictly prohibited. If you have received this email in error, please call (978) 451-3700 immediately.

From: Haywood, Antwan (POL) <Antwan.Haywood@pol.state.ma.us>
Sent: Friday, May 22, 2020 8:56 AM
To: Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>
Subject: Re: LPR/ Toll Information Inquiry 2020-0C6-004160

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

Very Respectfully,

Tpr. Antwan Haywood #3967
Massachusetts State Police
State Police Holden, C-6
612 Main St.
Holden, MA 01520
Ph: (508) 829-4431
Fax: (508) 829-8425

From: Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>
Sent: Friday, May 22, 2020 8:53 AM
To: Haywood, Antwan (POL) <Antwan.Haywood@pol.state.ma.us>
Subject: Re: LPR/ Toll Information Inquiry 2020-0C6-004160

Good Morning, Trooper -



G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

Respectfully,

Sean Bender
Intelligence Analyst
Massachusetts State Police | Commonwealth Fusion Center
470 Worcester Road | Framingham, MA 01702
Phone: (508) 820-2233

CONFIDENTIALITY NOTICE: The information contained in this email and any attachment is privileged and confidential law enforcement information. If you are not the intended recipient, you are hereby notified that any disclosure, dissemination, or copying of this communication is strictly prohibited. If you have received this email in error, please call (978) 451-3700 immediately.

From: Haywood, Antwan (POL) <Antwan.Haywood@pol.state.ma.us>
Sent: Friday, May 22, 2020 8:44 AM
To: Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>
Subject: LPR/ Toll Information Inquiry 2020-0C6-004160

Good Morning,

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

Tpr. Antwan Haywood #3967
Massachusetts State Police
State Police Holden, C-6
612 Main St.

Holden, MA 01520
Ph: (508) 829-4431
Fax: (508) 829-8425

CONFIDENTIALITY NOTICE: This e-mail, including any attachments, may contain highly sensitive and confidential information. It is intended only for the individual(s) named. If you received this e-mail in error or from someone who was not authorized to send it to you, do not disseminate, copy or otherwise use this e-mail or its attachments. Please notify the sender immediately by reply e-mail and delete the e-mail from your system.

From: Brian Kruger
To: Egnitz, Brian (POL)
Subject: FW: LRP network ideas?
Date: Wednesday, January 29, 2020 3:31:29 PM
Attachments: EF0DEC0A353447659867A42DD71164CC.png

Brian,
This is the latest thread on the broker, just an FYI.

Regards,

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Samson Dunatunga <mdunatunga@forensiclogic.com>
Sent: Wednesday, January 29, 2020 8:42 AM
To: Brian Kruger <bkruger@forensiclogic.com>; Ouellette, John (EPS) <john.ouellette@state.ma.us>
Subject: RE: LRP network ideas?

Hmm, for whatever reason I didn't get John's reply that is in the thread history from Brian.
Anyway, the XML request was compiled to match the sample in the dev package. I will go back and compare the XML sent with the dev package content.

-Samson

From: Brian Kruger
Sent: Tuesday, January 28, 2020 3:23 PM
To: Ouellette, John (EPS); Samson Dunatunga
Subject: RE: LRP network ideas?

Samson,
Did you get what you needed?

Regards,

Brian Kruger
Operations and Support Manager

Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Thursday, January 23, 2020 9:25 AM
To: Samson Dunatunga <mdunatunga@forensiclogic.com>
Cc: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hi Samson,

Do you have the dev package? There are example xml documents in there.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Samson Dunatunga <mdunatunga@forensiclogic.com>
Sent: Thursday, January 23, 2020 11:00 AM
To: Brian Kruger <bkruger@forensiclogic.com>; Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
Here is the XML sent from our server to retrieve relevant data. The CJISMessageKey is set to R1. The response we got indicates the XML sent is invalid. Can you point me to what is not valid in the XML? By the way, I checked the XML syntax with an online XML validation tool which indicates the syntax is good.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns1:CJISRequestTransaction xmlns:ns2="http://www.it.ojp.gov/jxdm/3.0"
xmlns:ns1="http://www.xfact.com/schemas/chsb/cjis/2.0">
   <ns1:CJISRequestHeader>
      <ns1:UUID>[redacted]487fc738-d2fa-4b4f-8841-067b2d85e636</ns1:UUID>
      <ns1:CreateDateTime>2020-01-22T10:47:23.216-05:00</ns1:CreateDateTime>
      <ns1:TransactionSource>COPLINK</ns1:TransactionSource>
      <ns1:UserID>TEST</ns1:UserID>
```

```
      <ns2:OrganizationORIID>
        <ns2:ID>MAMSP0000</ns2:ID>
      </ns2:OrganizationORIID>
      <ns1:TimeToLive>unlimited</ns1:TimeToLive>
      <ns1:SchemaVersion>2.0</ns1:SchemaVersion>
      <ns1:ApplicationVersion>2.0</ns1:ApplicationVersion>
      <ns1:ResponseMechanism>Wait</ns1:ResponseMechanism>
      <ns1:RespondTo>http://[redacted]6060/CHSBReceiver/CHSBService</ns1:RespondTo>
      <ns1:CJISUserID>
        <ns2:ID>TEST</ns2:ID>
      </ns1:CJISUserID>
      <ns1:CJISUserPassword>password</ns1:CJISUserPassword>
      <ns1:CJISQueryAuthorizer>
        <ns2:PersonFullName>Joe Authorizer</ns2:PersonFullName>
      </ns1:CJISQueryAuthorizer>
      <ns1:CJISQueryOperator>
        <ns2:PersonFullName>Jane Authorizer</ns2:PersonFullName>
      </ns1:CJISQueryOperator>
      <ns1:CJISQueryRequester>
        <ns2:PersonFullName>Jane Requester</ns2:PersonFullName>
      </ns1:CJISQueryRequester>
      <ns1:CJISQueryPurposeCode>C</ns1:CJISQueryPurposeCode>
    </ns1:CJISRequestHeader>
    <ns1:CJISRequestBody>
      <ns1:R1QueryInput>
        <ns1:CJISMessageKey>R1</ns1:CJISMessageKey>
        <ns2:DriverAuthorization xsi:type="ns1:DriverAuthorizationType" ns2:id="S32935254"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"/>
      </ns1:R1QueryInput>
    </ns1:CJISRequestBody>
</ns1:CJISRequestTransaction>
```


Thank you,
-Samson

From: Brian Kruger
Sent: Wednesday, January 22, 2020 1:39 PM
To: Ouellette, John (EPS); Samson Dunatunga
Subject: RE: LRP network ideas?

John,
I am adding Samson on this thread.

Regards,

Brian Kruger
Operations and Support Manager



Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Wednesday, January 22, 2020 1:35 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hi Brian,

The only namespaces I can find are:
xmlns:dcjis="http://www.xfact.com/schemas/eopss/dcjis/1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:cjx="http://www.xfact.com/schemas/eopss/dcjis/cjx/3.0"
xmlns:j="http://www.it.ojp.gov/jxdm/3.0">

Which message key are you trying to run?

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Wednesday, January 22, 2020 2:57 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
I have been putting out new versions of our Broker on this build Samson noticed that we are using xml namespace 2.0 which doesn't work. Do you know what version we should be running.

From: Samson Dunatunga <mdunatunga@forensiclogic.com>
Sent: Wednesday, January 22, 2020 11:28 AM
To: Brian Kruger <bkruger@forensiclogic.com>

Subject: RE:

Looks like the XML namespace xmlns:ns1="http://www.xfact.com/schemas/chsb/cjis/2.0"
is no longer available. Can you find out what we are supposed to use?

Thanks,
-Samson

From: Brian Kruger
Sent: Wednesday, January 22, 2020 8:56 AM
To: Samson Dunatunga
Subject:

2020-01-22 10:43:39 Commons Daemon procrun stderr initialized
22-Jan-2020 10:43:42.362 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Server version name: Apache Tomcat/9.0.14
22-Jan-2020 10:43:42.362 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Server built: Dec 6 2018 21:13:53 UTC
22-Jan-2020 10:43:42.362 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Server version number: 9.0.14.0
22-Jan-2020 10:43:42.362 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log OS Name: Windows Server 2008
22-Jan-2020 10:43:42.362 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log OS Version: 6.0
22-Jan-2020 10:43:42.362 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Architecture: amd64
22-Jan-2020 10:43:42.362 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Java Home: C:\Program Files\Java\jdk1.8.0_131\jre
22-Jan-2020 10:43:42.362 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log JVM Version: 1.8.0_131-b11
22-Jan-2020 10:43:42.362 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log JVM Vendor: Oracle Corporation
22-Jan-2020 10:43:42.362 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log CATALINA_BASE: D:\coplink\apache-tomcat-9.0.14
22-Jan-2020 10:43:42.362 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log CATALINA_HOME: D:\coplink\apache-tomcat-9.0.14
22-Jan-2020 10:43:42.362 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Dcatalina.home=D:\coplink\apache-tomcat-9.0.14
22-Jan-2020 10:43:42.362 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Dcatalina.base=D:\coplink\apache-tomcat-9.0.14
22-Jan-2020 10:43:42.362 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Dignore.endorsed.dirs=D:\coplink\apache-tomcat-9.0.14\endorsed
22-Jan-2020 10:43:42.362 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Djava.io.tmpdir=D:\coplink\apache-tomcat-9.0.14\temp
22-Jan-2020 10:43:42.362 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command

line argument: -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager
22-Jan-2020 10:43:42.362 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Djava.util.logging.config.file=D:\coplink\apache-tomcat-9.0.14\conf\logging.properties
22-Jan-2020 10:43:42.362 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: exit
22-Jan-2020 10:43:42.362 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: abort
22-Jan-2020 10:43:42.362 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Xms128m
22-Jan-2020 10:43:42.362 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Xmx1024m
22-Jan-2020 10:43:42.362 INFO [main] org.apache.catalina.core.AprLifecycleListener.lifecycleEvent Loaded APR based Apache Tomcat Native library [1.2.19] using APR version [1.6.5].
22-Jan-2020 10:43:42.362 INFO [main] org.apache.catalina.core.AprLifecycleListener.lifecycleEvent APR capabilities: IPv6 [true], sendfile [true], accept filters [false], random [true].
22-Jan-2020 10:43:42.362 INFO [main] org.apache.catalina.core.AprLifecycleListener.lifecycleEvent APR/OpenSSL configuration: useAprConnector [false], useOpenSSL [true]
22-Jan-2020 10:43:42.377 INFO [main] org.apache.catalina.core.AprLifecycleListener.initializeSSL OpenSSL successfully initialized [OpenSSL 1.1.1a 20 Nov 2018]
22-Jan-2020 10:43:43.032 INFO [main] org.apache.coyote.AbstractProtocol.init Initializing ProtocolHandler ["http-nio-6060"]
22-Jan-2020 10:43:43.235 INFO [main] org.apache.coyote.AbstractProtocol.init Initializing ProtocolHandler ["ajp-nio-8009"]
22-Jan-2020 10:43:43.235 INFO [main] org.apache.catalina.startup.Catalina.load Server initialization in [2,108] milliseconds
22-Jan-2020 10:43:43.329 INFO [main] org.apache.catalina.core.StandardService.startInternal Starting service [Catalina]
22-Jan-2020 10:43:43.329 INFO [main] org.apache.catalina.core.StandardEngine.startInternal Starting Servlet engine: [Apache Tomcat/9.0.14]
22-Jan-2020 10:43:43.376 INFO [main] org.apache.catalina.startup.HostConfig.deployWAR Deploying web application archive [D:\coplink\apache-tomcat-9.0.14\webapps\CHSBReceiver.war]
22-Jan-2020 10:43:57.681 INFO [main] com.sun.xml.ws.transport.http.servlet.WSServletDelegate.<init> WSSERVLET14: JAX-WS servlet initializing
22-Jan-2020 10:43:57.790 INFO [main] org.apache.jasper.servlet.TldScanner.scanJars At least one JAR was scanned for TLDs yet contained no TLDs. Enable debug logging for this logger for a complete list of JARs that were scanned but no TLDs were found in them. Skipping unneeded JARs during scanning can improve startup time and JSP compilation time.
22-Jan-2020 10:43:57.837 INFO [main] com.sun.xml.ws.transport.http.servlet.WSServletContextListener.contextInitialized WSSERVLET12: JAX-WS context listener initializing
22-Jan-2020 10:43:57.868 INFO [main] org.apache.catalina.startup.HostConfig.deployWAR Deployment of web application archive [D:\coplink\apache-tomcat-9.0.14\webapps\CHSBReceiver.war] has finished in [14,492] ms
22-Jan-2020 10:43:57.884 INFO [main] org.apache.catalina.startup.HostConfig.deployWAR Deploying web application archive [D:\coplink\apache-tomcat-9.0.14\webapps\ImageApplet.war]
22-Jan-2020 10:43:58.289 INFO [main] org.apache.jasper.servlet.TldScanner.scanJars At least one JAR was scanned for TLDs yet contained no TLDs. Enable debug logging for this logger for a complete list of JARs that were scanned but no TLDs were found in them. Skipping unneeded JARs during scanning can improve

startup time and JSP compilation time.
22-Jan-2020 10:44:00.582 INFO [main] org.apache.catalina.startup.HostConfig.deployWAR Deployment of web application archive [D:\coplink\apache-tomcat-9.0.14\webapps\ImageApplet.war] has finished in [2,698] ms
22-Jan-2020 10:44:00.582 INFO [main] org.apache.catalina.startup.HostConfig.deployDirectory Deploying web application directory [D:\coplink\apache-tomcat-9.0.14\webapps\docs]
22-Jan-2020 10:44:00.848 INFO [main] org.apache.jasper.servlet.TldScanner.scanJars At least one JAR was scanned for TLDs yet contained no TLDs. Enable debug logging for this logger for a complete list of JARs that were scanned but no TLDs were found in them. Skipping unneeded JARs during scanning can improve startup time and JSP compilation time.
22-Jan-2020 10:44:00.848 INFO [main] org.apache.catalina.startup.HostConfig.deployDirectory Deployment of web application directory [D:\coplink\apache-tomcat-9.0.14\webapps\docs] has finished in [266] ms
22-Jan-2020 10:44:00.848 INFO [main] org.apache.catalina.startup.HostConfig.deployDirectory Deploying web application directory [D:\coplink\apache-tomcat-9.0.14\webapps\examples]
22-Jan-2020 10:44:01.596 INFO [main] org.apache.jasper.servlet.TldScanner.scanJars At least one JAR was scanned for TLDs yet contained no TLDs. Enable debug logging for this logger for a complete list of JARs that were scanned but no TLDs were found in them. Skipping unneeded JARs during scanning can improve startup time and JSP compilation time.
22-Jan-2020 10:44:01.674 INFO [main] org.apache.catalina.startup.HostConfig.deployDirectory Deployment of web application directory [D:\coplink\apache-tomcat-9.0.14\webapps\examples] has finished in [826] ms
22-Jan-2020 10:44:01.674 INFO [main] org.apache.catalina.startup.HostConfig.deployDirectory Deploying web application directory [D:\coplink\apache-tomcat-9.0.14\webapps\host-manager]
22-Jan-2020 10:44:01.955 INFO [main] org.apache.jasper.servlet.TldScanner.scanJars At least one JAR was scanned for TLDs yet contained no TLDs. Enable debug logging for this logger for a complete list of JARs that were scanned but no TLDs were found in them. Skipping unneeded JARs during scanning can improve startup time and JSP compilation time.
22-Jan-2020 10:44:01.971 INFO [main] org.apache.catalina.startup.HostConfig.deployDirectory Deployment of web application directory [D:\coplink\apache-tomcat-9.0.14\webapps\host-manager] has finished in [297] ms
22-Jan-2020 10:44:01.971 INFO [main] org.apache.catalina.startup.HostConfig.deployDirectory Deploying web application directory [D:\coplink\apache-tomcat-9.0.14\webapps\manager]
22-Jan-2020 10:44:02.189 INFO [main] org.apache.jasper.servlet.TldScanner.scanJars At least one JAR was scanned for TLDs yet contained no TLDs. Enable debug logging for this logger for a complete list of JARs that were scanned but no TLDs were found in them. Skipping unneeded JARs during scanning can improve startup time and JSP compilation time.
22-Jan-2020 10:44:02.189 INFO [main] org.apache.catalina.startup.HostConfig.deployDirectory Deployment of web application directory [D:\coplink\apache-tomcat-9.0.14\webapps\manager] has finished in [218] ms
22-Jan-2020 10:44:02.189 INFO [main] org.apache.catalina.startup.HostConfig.deployDirectory Deploying web application directory [D:\coplink\apache-tomcat-9.0.14\webapps\ROOT]
22-Jan-2020 10:44:02.361 INFO [main] org.apache.jasper.servlet.TldScanner.scanJars At least one JAR was scanned for TLDs yet contained no TLDs. Enable debug logging for this logger for a complete list of JARs that were scanned but no TLDs were found in them. Skipping unneeded JARs during scanning can improve startup time and JSP compilation time.
22-Jan-2020 10:44:02.361 INFO [main] org.apache.catalina.startup.HostConfig.deployDirectory Deployment of web application directory [D:\coplink\apache-tomcat-9.0.14\webapps\ROOT] has finished in [172] ms
22-Jan-2020 10:44:02.361 INFO [main] org.apache.coyote.AbstractProtocol.start Starting ProtocolHandler ["http-nio-6060"]
22-Jan-2020 10:44:02.376 INFO [main] org.apache.coyote.AbstractProtocol.start Starting ProtocolHandler

["ajp-nio-8009"]
22-Jan-2020 10:44:02.376 INFO [main] org.apache.catalina.startup.Catalina.start Server startup in [19,138] milliseconds
22-Jan-2020 10:44:02.376 INFO [Thread-5] org.apache.coyote.AbstractProtocol.pause Pausing ProtocolHandler ["http-nio-6060"]
22-Jan-2020 10:44:02.424 INFO [Thread-5] org.apache.coyote.AbstractProtocol.pause Pausing ProtocolHandler ["ajp-nio-8009"]
22-Jan-2020 10:44:02.472 INFO [Thread-5] org.apache.catalina.core.StandardService.stopInternal Stopping service [Catalina]
22-Jan-2020 10:44:02.534 INFO [Thread-5] com.sun.xml.ws.transport.http.servlet.WSServletDelegate.destroy WSSERVLET15: JAX-WS servlet destroyed
22-Jan-2020 10:44:02.550 INFO [Thread-5] com.sun.xml.ws.transport.http.servlet.WSServletContextListener.contextDestroyed WSSERVLET13: JAX-WS context listener destroyed
22-Jan-2020 10:44:02.550 SEVERE [Thread-5] org.apache.catalina.loader.WebappClassLoaderBase.checkThreadLocalMapForLeaks The web application [CHSBReceiver] created a ThreadLocal with key of type [com.sun.xml.ws.api.server.ThreadLocalContainerResolver$1] (value [com.sun.xml.ws.api.server.ThreadLocalContainerResolver$1@4056f033]) and a value of type [com.sun.xml.ws.api.server.Container.NoneContainer] (value [com.sun.xml.ws.api.server.Container$NoneContainer@6c999d0f]) but failed to remove it when the web application was stopped. Threads are going to be renewed over time to try and avoid a probable memory leak.
22-Jan-2020 10:44:02.566 INFO [Thread-5] org.apache.coyote.AbstractProtocol.stop Stopping ProtocolHandler ["http-nio-6060"]
22-Jan-2020 10:44:02.612 INFO [Thread-5] org.apache.coyote.AbstractProtocol.stop Stopping ProtocolHandler ["ajp-nio-8009"]

2020-01-22 10:46:23 Commons Daemon procrun stderr initialized
22-Jan-2020 10:46:24.513 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Server version name: Apache Tomcat/9.0.14
22-Jan-2020 10:46:24.513 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Server built: Dec 6 2018 21:13:53 UTC
22-Jan-2020 10:46:24.513 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Server version number: 9.0.14.0
22-Jan-2020 10:46:24.513 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log OS Name: Windows Server 2008
22-Jan-2020 10:46:24.513 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log OS Version: 6.0
22-Jan-2020 10:46:24.513 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Architecture: amd64
22-Jan-2020 10:46:24.513 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Java Home: C:\Program Files\Java\jdk1.8.0_131\jre
22-Jan-2020 10:46:24.513 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log JVM Version: 1.8.0_131-b11
22-Jan-2020 10:46:24.513 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log JVM Vendor: Oracle Corporation
22-Jan-2020 10:46:24.513 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log

CATALINA_BASE: D:\coplink\apache-tomcat-9.0.14
22-Jan-2020 10:46:24.513 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log
CATALINA_HOME: D:\coplink\apache-tomcat-9.0.14
22-Jan-2020 10:46:24.513 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Dcatalina.home=D:\coplink\apache-tomcat-9.0.14
22-Jan-2020 10:46:24.513 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Dcatalina.base=D:\coplink\apache-tomcat-9.0.14
22-Jan-2020 10:46:24.513 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Dignore.endorsed.dirs=D:\coplink\apache-tomcat-9.0.14\endorsed
22-Jan-2020 10:46:24.513 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Djava.io.tmpdir=D:\coplink\apache-tomcat-9.0.14\temp
22-Jan-2020 10:46:24.513 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager
22-Jan-2020 10:46:24.513 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Djava.util.logging.config.file=D:\coplink\apache-tomcat-9.0.14\conf\logging.properties
22-Jan-2020 10:46:24.513 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: exit
22-Jan-2020 10:46:24.513 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: abort
22-Jan-2020 10:46:24.513 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Xms128m
22-Jan-2020 10:46:24.513 INFO [main] org.apache.catalina.startup.VersionLoggerListener.log Command line argument: -Xmx1024m
22-Jan-2020 10:46:24.513 INFO [main] org.apache.catalina.core.AprLifecycleListener.lifecycleEvent Loaded APR based Apache Tomcat Native library [1.2.19] using APR version [1.6.5].
22-Jan-2020 10:46:24.513 INFO [main] org.apache.catalina.core.AprLifecycleListener.lifecycleEvent APR capabilities: IPv6 [true], sendfile [true], accept filters [false], random [true].
22-Jan-2020 10:46:24.513 INFO [main] org.apache.catalina.core.AprLifecycleListener.lifecycleEvent APR/OpenSSL configuration: useAprConnector [false], useOpenSSL [true]
22-Jan-2020 10:46:24.529 INFO [main] org.apache.catalina.core.AprLifecycleListener.initializeSSL OpenSSL successfully initialized [OpenSSL 1.1.1a 20 Nov 2018]
22-Jan-2020 10:46:24.856 INFO [main] org.apache.coyote.AbstractProtocol.init Initializing ProtocolHandler ["http-nio-6060"]
22-Jan-2020 10:46:24.997 INFO [main] org.apache.coyote.AbstractProtocol.init Initializing ProtocolHandler ["ajp-nio-8009"]
22-Jan-2020 10:46:24.997 INFO [main] org.apache.catalina.startup.Catalina.load Server initialization in [1,171] milliseconds
22-Jan-2020 10:46:25.059 INFO [main] org.apache.catalina.core.StandardService.startInternal Starting service [Catalina]
22-Jan-2020 10:46:25.059 INFO [main] org.apache.catalina.core.StandardEngine.startInternal Starting Servlet engine: [Apache Tomcat/9.0.14]
22-Jan-2020 10:46:25.090 INFO [main] org.apache.catalina.startup.HostConfig.deployWAR Deploying web application archive [D:\coplink\apache-tomcat-9.0.14\webapps\CHSBReceiver.war]
22-Jan-2020 10:46:31.143 INFO [main] com.sun.xml.ws.transport.http.servlet.WSServletDelegate.<init> WSSERVLET14: JAX-WS servlet initializing
22-Jan-2020 10:46:31.205 INFO [main] org.apache.jasper.servlet.TldScanner.scanJars At least one JAR was scanned for TLDs yet contained no TLDs. Enable debug logging for this logger for a complete list of JARs that were scanned but no TLDs were found in them. Skipping unneeded JARs during scanning can improve

startup time and JSP compilation time.
22-Jan-2020 10:46:31.237 INFO [main]
com.sun.xml.ws.transport.http.servlet.WSServletContextListener.contextInitialized WSSERVLET12: JAX-WS context listener initializing
22-Jan-2020 10:46:31.268 INFO [main] org.apache.catalina.startup.HostConfig.deployWAR Deployment of web application archive [D:\coplink\apache-tomcat-9.0.14\webapps\CHSBReceiver.war] has finished in [6,178] ms
22-Jan-2020 10:46:31.268 INFO [main] org.apache.catalina.startup.HostConfig.deployWAR Deploying web application archive [D:\coplink\apache-tomcat-9.0.14\webapps\ImageApplet.war]
22-Jan-2020 10:46:31.517 INFO [main] org.apache.jasper.servlet.TldScanner.scanJars At least one JAR was scanned for TLDs yet contained no TLDs. Enable debug logging for this logger for a complete list of JARs that were scanned but no TLDs were found in them. Skipping unneeded JARs during scanning can improve startup time and JSP compilation time.
22-Jan-2020 10:46:32.859 INFO [main] org.apache.catalina.startup.HostConfig.deployWAR Deployment of web application archive [D:\coplink\apache-tomcat-9.0.14\webapps\ImageApplet.war] has finished in [1,591] ms
22-Jan-2020 10:46:32.859 INFO [main] org.apache.catalina.startup.HostConfig.deployDirectory Deploying web application directory [D:\coplink\apache-tomcat-9.0.14\webapps\docs]
22-Jan-2020 10:46:33.093 INFO [main] org.apache.jasper.servlet.TldScanner.scanJars At least one JAR was scanned for TLDs yet contained no TLDs. Enable debug logging for this logger for a complete list of JARs that were scanned but no TLDs were found in them. Skipping unneeded JARs during scanning can improve startup time and JSP compilation time.
22-Jan-2020 10:46:33.093 INFO [main] org.apache.catalina.startup.HostConfig.deployDirectory Deployment of web application directory [D:\coplink\apache-tomcat-9.0.14\webapps\docs] has finished in [234] ms
22-Jan-2020 10:46:33.093 INFO [main] org.apache.catalina.startup.HostConfig.deployDirectory Deploying web application directory [D:\coplink\apache-tomcat-9.0.14\webapps\examples]
22-Jan-2020 10:46:33.639 INFO [main] org.apache.jasper.servlet.TldScanner.scanJars At least one JAR was scanned for TLDs yet contained no TLDs. Enable debug logging for this logger for a complete list of JARs that were scanned but no TLDs were found in them. Skipping unneeded JARs during scanning can improve startup time and JSP compilation time.
22-Jan-2020 10:46:33.701 INFO [main] org.apache.catalina.startup.HostConfig.deployDirectory Deployment of web application directory [D:\coplink\apache-tomcat-9.0.14\webapps\examples] has finished in [608] ms
22-Jan-2020 10:46:33.701 INFO [main] org.apache.catalina.startup.HostConfig.deployDirectory Deploying web application directory [D:\coplink\apache-tomcat-9.0.14\webapps\host-manager]
22-Jan-2020 10:46:33.982 INFO [main] org.apache.jasper.servlet.TldScanner.scanJars At least one JAR was scanned for TLDs yet contained no TLDs. Enable debug logging for this logger for a complete list of JARs that were scanned but no TLDs were found in them. Skipping unneeded JARs during scanning can improve startup time and JSP compilation time.
22-Jan-2020 10:46:33.998 INFO [main] org.apache.catalina.startup.HostConfig.deployDirectory Deployment of web application directory [D:\coplink\apache-tomcat-9.0.14\webapps\host-manager] has finished in [297] ms
22-Jan-2020 10:46:33.998 INFO [main] org.apache.catalina.startup.HostConfig.deployDirectory Deploying web application directory [D:\coplink\apache-tomcat-9.0.14\webapps\manager]
22-Jan-2020 10:46:34.232 INFO [main] org.apache.jasper.servlet.TldScanner.scanJars At least one JAR was scanned for TLDs yet contained no TLDs. Enable debug logging for this logger for a complete list of JARs that were scanned but no TLDs were found in them. Skipping unneeded JARs during scanning can improve startup time and JSP compilation time.
22-Jan-2020 10:46:34.232 INFO [main] org.apache.catalina.startup.HostConfig.deployDirectory Deployment

of web application directory [D:\coplink\apache-tomcat-9.0.14\webapps\manager] has finished in [234] ms
22-Jan-2020 10:46:34.232 INFO [main] org.apache.catalina.startup.HostConfig.deployDirectory Deploying web application directory [D:\coplink\apache-tomcat-9.0.14\webapps\ROOT]
22-Jan-2020 10:46:34.435 INFO [main] org.apache.jasper.servlet.TldScanner.scanJars At least one JAR was scanned for TLDs yet contained no TLDs. Enable debug logging for this logger for a complete list of JARs that were scanned but no TLDs were found in them. Skipping unneeded JARs during scanning can improve startup time and JSP compilation time.
22-Jan-2020 10:46:34.435 INFO [main] org.apache.catalina.startup.HostConfig.deployDirectory Deployment of web application directory [D:\coplink\apache-tomcat-9.0.14\webapps\ROOT] has finished in [203] ms
22-Jan-2020 10:46:34.450 INFO [main] org.apache.coyote.AbstractProtocol.start Starting ProtocolHandler ["http-nio-6060"]
22-Jan-2020 10:46:34.466 INFO [main] org.apache.coyote.AbstractProtocol.start Starting ProtocolHandler ["ajp-nio-8009"]
22-Jan-2020 10:46:34.466 INFO [main] org.apache.catalina.startup.Catalina.start Server startup in [9,466] milliseconds
22-Jan-2020 10:47:23.793 INFO [http-nio-6060-exec-1] imagebroker.ImageBrokerREST.getEncodedImage result of service call: <?xml version="1.0" encoding="UTF-8"?>
<dcjis:DataExchange xmlns:dcjis="http://www.xfact.com/schemas/eopss/dcjis/1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><dcjis:Acknowledgment>
<dcjis:AcknowledgmentHeader><dcjis:UUID>ERROR</dcjis:UUID><dcjis:CreateDateTime>2020-01-22T10:47:30-0500</dcjis:CreateDateTime><dcjis:TransactionSource>ERROR</dcjis:TransactionSource>
<dcjis:TransactionMessageKey>ERROR</dcjis:TransactionMessageKey><dcjis:TransactionOrganizationID>
<dcjis:ID>ERROR</dcjis:ID></dcjis:TransactionOrganizationID><dcjis:UserContexts /><dcjis:DeviceAddress /><dcjis:SchemaVersion>1.0</dcjis:SchemaVersion>
<dcjis:ApplicationVersion>2.0</dcjis:ApplicationVersion><dcjis:CJISUserID><dcjis:ID>ERROR</dcjis:ID>
</dcjis:CJISUserID><dcjis:CJISUserPassword>ERROR</dcjis:CJISUserPassword><dcjis:CJISQueryAuthorizer>
<dcjis:PersonFullName>ERROR</dcjis:PersonFullName></dcjis:CJISQueryAuthorizer>
<dcjis:CJISQueryOperator><dcjis:PersonFullName>ERROR</dcjis:PersonFullName>
</dcjis:CJISQueryOperator><dcjis:CJISQueryRequester>
<dcjis:PersonFullName>ERROR</dcjis:PersonFullName></dcjis:CJISQueryRequester>
<dcjis:CJISQueryPurposeCode>ERROR</dcjis:CJISQueryPurposeCode><dcjis:Transaction>
<dcjis:TransactionStatus>-903</dcjis:TransactionStatus><dcjis:TransactionDescription>Transaction failed schema validation</dcjis:TransactionDescription></dcjis:Transaction></dcjis:AcknowledgmentHeader>
<dcjis:AcknowledgmentBody /></dcjis:Acknowledgment></dcjis:DataExchange>

Regards,

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and*

privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, December 6, 2019 9:45 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hey Brian,

Can we change the subject to Broker?
LPR is the license plate reader.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, December 6, 2019 11:31 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Samson Dunatunga <mdunatunga@forensiclogic.com>; Billy Moore <bmoore@forensiclogic.com>; Rhonda Fromm <rfromm@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

Billy,
Please let the group know when this will be available. I will work with John to get it deployed and tested as soon as we have it released.

Regards,

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and*

privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.

From: Brian Kruger
Sent: Tuesday, November 26, 2019 1:17 PM
To: 'Ouellette, John (EPS)' <john.ouellette@state.ma.us>; 'Egnitz, Brian (POL)' <brian.egnitz@state.ma.us>; Samson Dunatunga <mdunatunga@forensiclogic.com>; Billy Moore <bmoore@forensiclogic.com>
Cc: 'Dunne, Michaela (CHS)' <michaela.dunne@state.ma.us>; 'Dunn-CHS, William (CHS)' <william.dunn-chs@state.ma.us>; 'Mitchell, Timothy (EPS)' <timothy.mitchell@state.ma.us>; 'Ramsay, Christopher (EPS)' <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

John,
Thank you for the information on the call this afternoon.

Samson/Billy,
We need to add some additional debug code into our service so we can see the full communication path and what is being sent and received. John is also in the process to check and make sure their three servers can reach back into our 184.171 on port 6060. I have also reattached the IP wireshark I did this morning.

Regards,

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Tuesday, November 26, 2019 8:29 AM
To: Ouellette, John (EPS) <john.ouellette@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

John,
Give me a few minutes and I will give you a call. Here is the CSV file from wireshark. I had to repull it. I don't see any actually log details in our tomcat instance. In the wireshark though I see a bunch of event code

errors like below:

Event: <Unknown eventcode 72>, <Unknown eventcode 111>, <Unknown eventcode 116>, <Unknown eventcode 121>, <Unknown eventcode 110>, <Unknown eventcode 45>, <Unknown eventcode 112>, <Unknown eventcode 110>, <Unknown eventcode 114>, <Unknown eventcode 115>, <Unknown eventcode 47>, <Unknown eventcode 110>, <Unknown eventcode 111>, <Unknown eventcode 118>, <Unknown eventcode 110>, <Unknown eventcode 111>, <Unknown eventcode 47>, ColormapNotify, <Unknown eventcode 97>, <Unknown eventcode 120>, <Unknown eventcode 58>, <Unknown eventcode 46>, <Unknown eventcode 104>, <Unknown eventcode 46>, <Unknown eventcode 117>, <Unknown eventcode 97>, <Unknown eventcode 47>, <Unknown eventcode 62>, <Unknown eventcode 114>, <Unknown eventcode 114>, <Unknown eventcode 82>, <Unknown eventcode 120>, <Unknown eventcode 101>, MappingNotify, <Unknown eventcode 109>, <Unknown eventcode 98>, <Unknown eventcode 47>, <Unknown eventcode 119>, <Unknown eventcode 62>, <Unknown eventcode 114>, ColormapNotify, <Unknown eventcode 62>, <Unknown eventcode 115>, MappingNotify, <Unknown eventcode 110>

Regards,

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Tuesday, November 26, 2019 7:29 AM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Hey Brian,

You can call me at 617-660-4775

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services

Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Monday, November 25, 2019 7:53 PM
To: Brian Kruger <bkruger@forensiclogic.com>; Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: Re: LRP network ideas?

Does it make sense to schedule a call and work through it in real time?

> On Nov 22, 2019, at 4:00 PM, Ouellette, John (EPS) <john.ouellette@mass.gov> wrote:
>
> Hi Brian,
>
> I do not see any requests for your ORI. Can you review the acknowledgements that the broker sends back as a return value? There may be error information in there.
>
> John Ouellette | Massachusetts Executive Office of Public Safety and Security
> Office of Technology and Information Services
> Enterprise Application and Database Services
> Application Support and Management
> 200 Arlington Street Suite 2200
> Chelsea, MA 02150
> john.ouellette@state.ma.us | http://www.mass.gov/eops
>
> ---
>
> **From:** Brian Kruger <bkruger@forensiclogic.com>
> **Sent:** Friday, November 22, 2019 3:47 PM
> **To:** Ouellette, John (EPS) <john.ouellette@mass.gov>
> **Cc:** Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
> **Subject:** RE: LRP network ideas?
>
> John,
> Can you check again and see if there is a request coming into the .154 server. I ran a packet capture and I do see data sent from the .171 to the .154 server.
>
> <image001.png>

Regards,

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 22, 2019 12:26 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

I'm not sure if 224.154 is a load balancer. I don't believe it is though. It doesn't matter though, that is where you will send requests. You will receive a synchronous response called an acknowledgement. That will let you know if your request was accepted or rejected.

Later, an asynchronous response will be sent from 170.154.224.155 or 170.154.224.156 to your web service.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 22, 2019 2:19 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS)

<William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
The 154 address is a load balancer for the services correct. As far as I know there should be no blocked traffic to the .171 but let me include Chris and Tim on this thread.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 22, 2019 9:36 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

I didn't find any submitted requests.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Ouellette, John (EPS)
Sent: Friday, November 22, 2019 11:34 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

I can check.

The broker will send responses from G.L. c. 4. sec. 7.cl. 26 (c)(privacy) or 17G.L. c. 4. sec. 7.cl. 26 (c)(privacy) on port 6060. Make sure you are allowing that traffic.

When you send in a request you will receive an xml document as the return value. The documents lists if the request was accepted and if it wasn't, why it wasn't. You should be checking those.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 22, 2019 11:28 AM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

Bill,
I have the service send back a no data found so it looks like we are connecting. Can you check your logs to see if our request actually made it into your system.

I am sending the following test cycle from the G.L. c. 4. sec. 7.cl. 26 (c)(privacy) web server to our FR server

http:/G.L. c. 4. sec. 7.cl. 26 (c)(privacy)60/CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123G.L. c. 4. sec. 7.cl. 26 (c)(privacy)

Just so everybody is clear, this the is the connection path

G.L. c. 4. sec. 7.cl. 26 (c)(privacy) [redacted] 6060

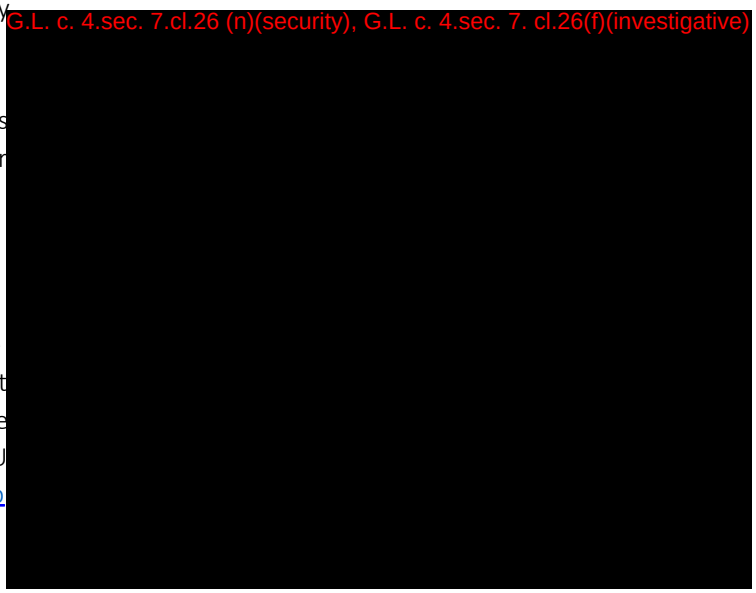
Return path

G.L. c. 4. sec. 7.cl. 26 (c)(privacy) [redacted]

Log of request:

2019-11-22 11:16:13,982 main DEBUG LoggerContext[name=MassLPRServlet,

org.apache.logging.log4j.core.LoggerContext@59303963] started OK with configuration org.apache.logging.log4j.core.config.properties.PropertiesConfiguration@61e86192.
2019-11-22 11:16:13,982 main DEBUG Log4jServletContextListener ensuring that Log4j starts up properly
2019-11-2
driversLice
remote hos
remote por
remote ad
scheme
scheme
local addr
local name
context pat
Init parame
Current UU
javax.xml.b
Request U



Rest response file contains:
no data found.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Thursday, November 21, 2019 2:11 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Ouellette, John (EPS) <john.ouellette@state.ma.us>
Subject: RE: LRP network ideas?

Thanks Bill!

It looks like we are close on this.

-Brian

From: Dunn-CHS, William (CHS)
Sent: Tuesday, November 19, 2019 7:50 AM
To: Brian Kruger; Ouellette, John (EPS)
Cc: Dunne, Michaela (CHS); Egnitz, Brian (POL); Dunn-CHS, William (CHS)
Subject: RE: LRP network ideas?

I think I see what might be part of the problem.

The R1 is either OLN or SSN, you can not send both at the same time.

There is No TEST SSN inquiry, use someone from MSP who is working on your project or if you have a developer who is from MA
The TEST OLN is S32935254

From: Brian Kruger [mailto:bkruger@forensiclogic.com]
Sent: Monday, November 18, 2019 6:33 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
Dev confirmed they are sending XML in the request. Do you have a valid License number in the test data I can try.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>

Sent: Friday, November 15, 2019 11:16 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

The broker is a web service. You need to create a client to connect. Requests are made by sending in an xml document.

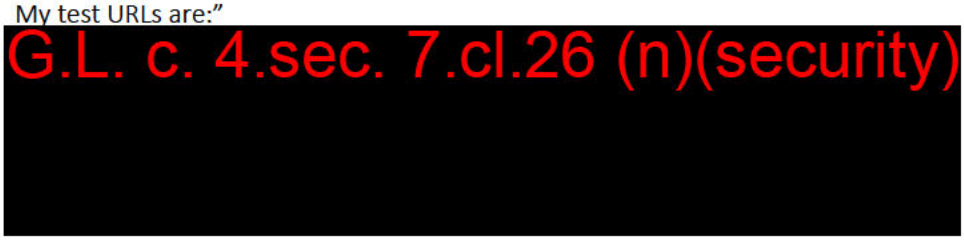
Did I forget to send you the broker documentation? Let me know.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 1:10 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
I ran two queries through IE I don't see an acknowledge me in the logs. Below is what I am seeing. Do we have a valid Lic number that is in the system I can try, or valid SSN.

My test URLs are:"



In my access log I see a 200:



ori=MAM
200 -
ori=MAM

a complete list of JARs that were scanned but no TLDs were found in them. Skipping unneeded JARs during scanning can improve startup time and JSP compilation time.
15-Nov-2019 13:02:41.167 INFO [main] org.apache.catalina.startup.HostConfig.deployDirectory Deployment of web application directory [D:\coplink\apache-tomcat-9.0.14\webapps\manager] has finished in [265] ms
15-Nov-2019 13:02:41.167 INFO [main] org.apache.catalina.startup.HostConfig.deployDirectory Deploying web application directory [D:\coplink\apache-tomcat-9.0.14\webapps\ROOT]
15-Nov-2019 13:02:41.511 INFO [main] org.apache.jasper.servlet.TldScanner.scanJars At least one JAR was scanned for TLDs yet contained no TLDs. Enable debug logging for this logger for a complete list of JARs that were scanned but no TLDs were found in them. Skipping unneeded JARs during scanning can improve startup time and JSP compilation time.
15-Nov-2019 13:02:41.526 INFO [main] org.apache.catalina.startup.HostConfig.deployDirectory Deployment of web application directory [D:\coplink\apache-tomcat-9.0.14\webapps\ROOT] has finished in [359] ms
15-Nov-2019 13:02:41.526 INFO [main] org.apache.coyote.AbstractProtocol.start Starting ProtocolHandler ["http-nio-6060"]
15-Nov-2019 13:02:41.557 INFO [main] org.apache.coyote.AbstractProtocol.start Starting ProtocolHandler ["ajp-nio-8009"]
15-Nov-2019 13:02:41.557 INFO [main] org.apache.catalina.startup.Catalina.start Server startup in [6,627] milliseconds

Regards,

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 15, 2019 9:54 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hey Brian,

When you send in a request, the return to that call is an acknowledgement. That is an xml

document that will state if your request was accepted or not; and if it is not, what the reason is.

Are you seeing any acknowledgements?

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 11:49 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
According to dev the message that is coming back: remote host not allowed. ignoring request. They are stating is a response from your system telling us we are not allowed. Is there anyway you and I can get on the phone, I can try and send some responses and see if you see anything in your log files. I am wondering if they are forming the response to you correctly.

As for the WSDL this is what I see from the 184.171 server.

<image003.png>

Full WSDL
<?xml version="1.0" encoding="UTF-8" ?>
- <wsdl:definitions xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
xmlns:tns="http://server.service.cjis.xfact.com/"
xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:ns1="http://schemas.xmlsoap.org/soap/http" name="**CJISService**"
targetNamespace="**http://server.service.cjis.xfact.com/**">
- <wsdl:types>
- <xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:tns="http://server.service.cjis.xfact.com/" attributeFormDefault="**unqualified**"
elementFormDefault="**qualified**" targetNamespace="**http://server.service.cjis.xfact.com/**">
<xsd:element name="**strEventArg**" nillable="**true**" type="**xsd:string**" />
<xsd:element name="**strResponse**" nillable="**true**" type="**xsd:string**" />
<xsd:element name="**strRequestArg**" nillable="**true**" type="**xsd:string**" />
<xsd:element name="**strResponseArg**" nillable="**true**" type="**xsd:string**" />
</xsd:schema>

```
</wsdl:types>
- <wsdl:message name="processEvent">
<wsdl:part element="tns:strEventArg" name="strEventArg" />
</wsdl:message>
- <wsdl:message name="verifyResponse">
<wsdl:part element="tns:strResponse" name="strResponse" />
</wsdl:message>
<wsdl:message name="verify" />
+ <wsdl:message name="processRequest">
<wsdl:part element="tns:strRequestArg" name="strRequestArg" />
</wsdl:message>
- <wsdl:message name="processRequestResponse">
<wsdl:part element="tns:strResponse" name="strResponse" />
</wsdl:message>
- <wsdl:message name="processResponse">
<wsdl:part element="tns:strResponseArg" name="strResponseArg" />
</wsdl:message>
- <wsdl:message name="processResponseResponse">
<wsdl:part element="tns:strResponse" name="strResponse" />
</wsdl:message>
- <wsdl:message name="processEventResponse">
<wsdl:part element="tns:strResponse" name="strResponse" />
</wsdl:message>
- <wsdl:portType name="CJISService">
- <wsdl:operation name="processEvent">
<wsdl:input message="tns:processEvent" name="processEvent" />
<wsdl:output message="tns:processEventResponse" name="processEventResponse" />
</wsdl:operation>
- <wsdl:operation name="verify">
<wsdl:input message="tns:verify" name="verify" />
<wsdl:output message="tns:verifyResponse" name="verifyResponse" />
</wsdl:operation>
- <wsdl:operation name="processRequest">
<wsdl:input message="tns:processRequest" name="processRequest" />
<wsdl:output message="tns:processRequestResponse" name="processRequestResponse" />
</wsdl:operation>
- <wsdl:operation name="processResponse">
<wsdl:input message="tns:processResponse" name="processResponse" />
<wsdl:output message="tns:processResponseResponse" name="processResponseResponse"
/>
</wsdl:operation>
</wsdl:portType>
- <wsdl:binding name="CJISServiceSoapBinding" type="tns:CJISService">
<soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http" />
- <wsdl:operation name="processEvent">
<soap:operation soapAction="/processEvent" style="document" />
- <wsdl:input name="processEvent">
<soap:body use="literal" />
```

</wsdl:input>
- <wsdl:output name="**processEventResponse**">
<soap:body use="**literal**" />
</wsdl:output>
</wsdl:operation>
- <wsdl:operation name="**verify**">
<soap:operation soapAction="**/verify**" style="**document**" />
- <wsdl:input name="**verify**">
<soap:body use="**literal**" />
</wsdl:input>
- <wsdl:output name="**verifyResponse**">
<soap:body use="**literal**" />
</wsdl:output>
</wsdl:operation>
- <wsdl:operation name="**processRequest**">
<soap:operation soapAction="**/processRequest**" style="**document**" />
- <wsdl:input name="**processRequest**">
<soap:body use="**literal**" />
</wsdl:input>
- <wsdl:output name="**processRequestResponse**">
<soap:body use="**literal**" />
</wsdl:output>
</wsdl:operation>
- <wsdl:operation name="**processResponse**">
<soap:operation soapAction="**/processResponse**" style="**document**" />
- <wsdl:input name="**processResponse**">
<soap:body use="**literal**" />
</wsdl:input>
- <wsdl:output name="**processResponseResponse**">
<soap:body use="**literal**" />
</wsdl:output>
</wsdl:operation>
</wsdl:binding>
- <wsdl:service name="**CJISService**">
- <wsdl:port binding="**t** G.L. c. 4.sec. 7.cl.26 (n)(security) **ndpointPort**">
<soap:address location
</wsdl:port>
</wsdl:service>
</wsdl:definitions>

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK

Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 15, 2019 9:36 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

If you are able to telnet, then you should be able to send in a request.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 11:06 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
This is all from the 184.171 server.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com

www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 15, 2019 8:41 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Are you doing the ping and telnet from [redacted]

Your error message from earlier seems to be your network not allowing the access.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 10:37 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
I am reaching out to the [redacted] on port 6060. I can ping the IP and also hit the port.
<image004.png>

<image005.png>

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 15, 2019 8:26 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

What is the ip address you are trying to connect to?
Are you able to ping that machine?

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 10:22 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

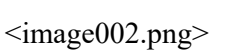
Brian,
Thank you for checking in, sorry for the delay. I had the email together but it was in my draft. I tested the connection again today.

John,
I am still getting the remote Host not allowed. This is the error below:

2019-11-15 10:15:45,808 main DEBUG Log4jServletFilter initialized.
driversLicense=987654321
remote host=[redacted]
remote port=61799
remote addr=[redacted]

scheme =http
scheme =HTTP/1.1
local addr =[redacted]
local name =EPS-CLFACEMATCH
context path = /CHSBReceiver
Init parameter1 =Value1
remote host not allowed. ignoring request.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Friday, November 8, 2019 1:17 PM
To: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

John,
Thank you, I will work on testing the connection and let you know the results. According to Dev the other queries we will be running on the R1 and RI.

Regards,

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you*

received this e-mail in error, please notify the sender and delete this e-mail from your system.

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 8, 2019 12:18 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

I have added your configuration on the test broker for R1 and RI.
Are there more queries/transactions you'd like to test? Michaela may have requirements for other queries.

The ORI is MAMSPF022
Your requests come from [G.L. c. 4.sec. 7.cl.26 (n)(security)] and responses will be sent back to
http://[G.L. c. 4.sec. 7.cl.26 (n)(security)]6060/CHSBReceiver/CHSBService

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Ouellette, John (EPS)
Sent: Tuesday, November 5, 2019 12:54 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>
Subject: RE: LRP network ideas?

Hi Brian,

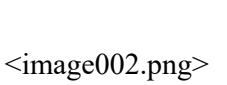
I think Bill needs to have more information on your project to assign an ORI to use on the test broker.
Is there a project name on your side?

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Monday, November 4, 2019 3:30 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
Any luck on this.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Tuesday, October 22, 2019 12:32 PM
To: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Subject: RE: LRP network ideas?

John,
Yea we should be sending the XML packet with the service that we have created. Do you know if that IP is natted to [redacted] The server that we have our service on is the [redacted] Face match server. I don't have any servers in the 170.154.226.x IP range unless it is getting natted somehow.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Tuesday, October 22, 2019 12:21 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hay Brian,

That won't work. The broker accepts an xml document containing the request, as well as other information.
Attached is a sample R1 request.

By the way, I have your requests coming G.L. c. 4.sec. 7.cl.26 (n)(security)

In order to get responses, you need a web service on your end to receive the responses and I'll need to configure it on the broker side.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Monday, October 21, 2019 5:04 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
Can you provide me with a DL that should work. From the .82 server this is what we are running:

http://G.L. c. 4.sec. 7.cl.26 (n)(security)6060/CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=987654321

I just need to update the drivers license number and hopefully it will work

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Tuesday, September 24, 2019 8:07 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

So, just R1 and RI?

I'll start configuring the test broker.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Tuesday, September 24, 2019 10:59 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
For the queries that we will using this is what I got back from Dev… let me know if this helps

…Attachments\CJISBroker_2016-03-24[13247].zip\CJISBroker_2016-03-24\CJISBroker\transactions\queries\rmv\r1\xml

…Attachments\CJISBroker_2016-03-24[13247].zip\CJISBroker_2016-03-24\CJISBroker\transactions\queries\rmv\ri\xml

The rest is correct, for testing the ORI list will grow once we go to production.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Tuesday, September 24, 2019 6:39 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hi Brian,

I haven't added your configuration to the test broker yet. Can you confirm the following:
For broker connections, we need the following:
IP Address for request: G.L. c. 4.sec. 7.cl.26 (n)(security)
URL for responses: http://G.L. c. 4.sec. 7.cl.26 (n)(security)6060/CHSBReceiver/CHSBService
ORI: MAMSP0000
Queries: I need the list of queries/transactions you will be testing

You will submit to http:/G.L. c. 4.sec. 7.cl.26 (n)(security)060/CJISService This call will return a synchronous acknowledgment.

Responses will come back from G.L. c. 4.sec. 7.cl.26 (n)(security) on port 6060. You need to return a synchronous acknowledgement for each response.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Monday, September 23, 2019 7:53 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

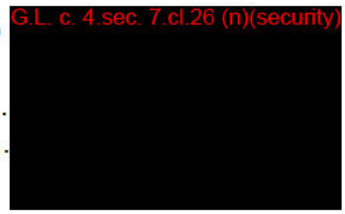
John,
I have deployed a new package, but I see this in the log.

2019-09-23 19:48:37,297 main DEBUG Registering MBean org.apache.logging.log4j2:type=MassLPRServlet,component=Appenders,name=RollingFile
2019-09-23 19:48:37,304 main DEBUG org.apache.logging.log4j.core.util.SystemClock does not support precise timestamps.

2019-09-23 19:48:37,305 main DEBUG LoggerContext[name=MassLPRServlet, org.apache.logging.log4j.core.LoggerContext@2180e789] started OK with configuration org.apache.logging.log4j.core.config.properties.PropertiesConfiguration@5e9bbd9d.
2019-09-23 19:48:37,307 main DEBUG Log4jServletContextListener ensuring that Log4j starts up properly.
2019-09-23 19:48:37,309 main DEBUG Log4jServletFilter initialized.
driversLicense=987654321
remote host=0:0:0:0:0:0:0:1
remote port=65146
remote addr=0:0:0:0:0:0:0:1
scheme =http
scheme =HTTP/1.1
local addr =0:0:0:0:0:0:0:1
local name =EPS-CLFACEMATCH
context path = /CHSBReceiver
Init parameter1 =Value1
remote host not allowed. ignoring request.

can you check and make sure this machine has access:

EPS-CLFACEMATCH
Connection-specific D
IPv4 Address. . . . . .
Subnet Mask . . . . . .
Default Gateway . . . . .



C:\Users\msp_user>
Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, September 6, 2019 6:15 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hey Brian,

I'm not sure what is in the test system either. I believe a dl of 987654321 will work; at least it used to.
Try to find something in test CJISWeb.

Remember that all queries will send in an xml document and will receive a return acknowledgement stating success or failure. If the request failed, the reason will be in the acknowledgement.

At a later time, seconds or less, the response will be returned to your web service. You must return an acknowledgement to that also to let the system know that the response was received and the next response can be sent.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Thursday, September 5, 2019 5:17 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
Not yet, I don't know what is in the test system… are they actually dls or fake ones.

Our query against our service is going to look something like, that will translate to yours.

G.L. c. 4.sec. 7.cl.26 (n)(security)

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential,*

proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Thursday, September 5, 2019 1:09 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Have you tried your DL and SSN?

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Thursday, September 5, 2019 2:36 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
Do you have a sample DL and ssn, we can try passing through the service to see if we can pull an image. According to dev we are just utilizing the XML out of R1 and Ri.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, August 9, 2019 7:04 AM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Brian Kruger <bkruger@forensiclogic.com>; Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-

chs@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

All of the broker queries use the same method and accept an xml document. The contents of the xml direct what action the system should take. I have attached documentation for the broker. It's a 5 MB zip file.

If you can't accept zip files or 5 MB files let me know how to send the file.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, August 9, 2019 9:39 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Brian Kruger <bkruger@forensiclogic.com>; Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>
Subject: Re: LRP network ideas?

Thanks John, I'll defer to Brian Kruger to respond regarding where he's sending the query. Are you able to answer his question below?

"

> I can pull back the WSDL but want to send an image request to it to see if it actually pulls the image. I am looking for something like /GetPhoto?dl_num=20180061903&ss_num=2&type=M, the actually call method

"

On Aug 9, 2019, at 9:04 AM, Ouellette, John (EPS) <john.ouellette@mass.gov> wrote:

> Hi Brian,
>
> For broker connections to test, we need the following:
> IP Address for request: [redacted] G.L. c. 4.sec. 7.cl.26 (n)(security)

URL for responses: http://[M.G.L. c. 4.sec. 7.cl.26 (n)(security)]6060/CHSBReceiver/CHSBService
ORI: MAMSP0000
Queries:

Can you confirm this information and send the list of queries you would like to run?
Please remember that this system would only be used for test. Another system would need to be used when you move to production.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, August 9, 2019 8:54 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Ouellette, John (EPS) <john.ouellette@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>
Subject: Re: LRP network ideas?

Hi Brian,

are we testing on this yet?

On Jul 22, 2019, at 1:37 PM, Brian Kruger <bkruger@forensiclogic.com> wrote:

> Tim,
> Attached is the full list of agencies and ORI that we currently have in the admin DB.
>
> Regards,
>
> <image001.png>
>
> **Brian Kruger**
> Operations and Support Manager
> **Forensic Logic / COPLINK**
> 520.488.1603
> bkruger@forensiclogic.com
> www.forensiclogic.com
>
> ***CONFIDENTIALITY:*** *This e-mail (including any attachments) may*

contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Monday, July 22, 2019 8:37 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Ouellette, John (EPS) <john.ouellette@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
Subject: RE: LRP network ideas?

Any update on this from dev, do you still need a sample RI url? Can you make sure you are also sending the CopLink user name in the UserID parameter.

Tks, Brian

From: Brian Kruger [mailto:bkruger@forensiclogic.com]
Sent: Thursday, July 18, 2019 5:19 PM
To: Mitchell, Timothy (EPS)
Cc: Ramsay, Christopher (EPS); Egnitz, Brian (POL); Ouellette, John (EPS)
Subject: RE: LRP network ideas?

Tim,

I am still pending an answer back from dev on how they are going to pull the ORI. For now can we use `MAMSP0000. That is actually in our systems as MSP.`

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>

Sent: Tuesday, July 16, 2019 4:07 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Ouellette, John (EPS) <john.ouellette@state.ma.us>
Subject: RE: LRP network ideas?

Brian
What is the ORI that you are using for this setup? There is some configuration work that needs to be done on the broker side to allow your service to run transactions.
Thanks
Tim

Timothy Mitchell
Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise and Field Services Support Division
Public Safety Data Center
200 Arlington St., Suite 2200
Chelsea, MA 02150
(P) 617.660.4665
(F) 617.884.4601
(E) timothy.mitchell@state.ma.us
http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Monday, July 15, 2019 7:05 PM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

Folks,
For the RMV pull, does anybody have an example image we can try and run through. All the connectivity looks good, I have tried a few ways to pull an image without success.

Our service
http://[G.L. c. 4.sec. 7.cl.26 (n)(security)]6060/CHSBReceiver/CHSBService?wsdl
refers to http://[G.L. c. 4.sec. 7.cl.26 (n)(security)]6060/CJISService?wsdl

I can pull back the WSDL but want to send an image request to it to see if it actually pulls the image. I am looking for something like /GetPhoto?dl_num=20180061903&ss_num=2&type=M, the

From: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
Sent: Wednesday, May 8, 2019 5:52 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: Re: LRP network ideas?

Brian
Can you test the connectivity again?
Thanks

Sent from my iPhone

On May 7, 2019, at 10:43 AM, Brian Kruger <bkruger@forensiclogic.com> wrote:

> Tim,
> Thank you sir, sorry this fell off my radar. I was working on reallocation for Dan.
>
> Regards,
>
> <image001.png>
>
> **Brian Kruger**
> Operations and Support Manager
> **Forensic Logic / COPLINK**
> 520.488.1603
> bkruger@forensiclogic.com
> www.forensiclogic.com
>
> ***CONFIDENTIALITY:*** *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*
>
> ---
>
> **From:** Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
> **Sent:** Tuesday, May 7, 2019 7:42 AM
> **To:** Brian Kruger <bkruger@forensiclogic.com>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
> **Subject:** RE: LRP network ideas?
>
> Brian
> Yes you will need to run the transactions across to the

test server first and DCJIS will need to approve it before you can run to the production server. I will check out the firewall rules today and let you know. Thanks

Timothy Mitchell
Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise and Field Services Support Division
Public Safety Data Center
200 Arlington St., Suite 2200
Chelsea, MA 02150
(P) 617.660.4665
(F) 617.884.4601
(E) timothy.mitchell@state.ma.us
http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Tuesday, May 07, 2019 10:40 AM
To: Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

Chris,
I am guessing test first, that way we can validate the broker, unless the route is setup already for production and I can switch it out to that.

Brian E.,
Your thoughts?

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any*

attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.

From: Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Sent: Tuesday, May 7, 2019 7:18 AM
To: Brian Kruger <bkruger@forensiclogic.com>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Brian,

G.L. c. 4.sec. 7.cl.26 (n)(security) is the TEST cjis broker system. Is the test system what you're looking to use?

-Chris

Christopher Ramsay | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Division of Enterprise & Field Services Support | Enterprise Systems

200 Arlington St. Suite 2200
Chelsea, MA 02150
p. 617.660.4720 | f. 617.660.4613
christopher.ramsay@mass.gov |
http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Tuesday, May 7, 2019 1:49 AM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

Tim,
I was checking the cjis broker service and I can't get to the G.L. c. 4.sec. 7.cl.26 (n)(security) on 6060 from the FR server at G.L. c. 4.sec. 7.cl.26 (n)(security) I was going through old email and just checking the status of the connections. The G.L. c. 4.sec. 7.cl.26 (n)(security) is what I received from Dev. Let me know if this is not correct.

<image003.jpg>

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
Sent: Friday, March 1, 2019 1:28 PM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Brian Kruger <bkruger@forensiclogic.com>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Hi folks
The CJIS broker transactions will need to use port 6060 as that is what they have been configured for in the past.

We have discussed the LPR port request and we think that going with a higher port seems to be more acceptable to EOTSS to allow through their public access firewall. Would port 56446 (https) work? We will need to open a ticket with EOTSS to have them allow this port through.

Thanks

Timothy Mitchell
Massachusetts Executive Office of Public Safety and

Security
Office of Technology and Information Services
Enterprise and Field Services Support Division
Public Safety Data Center
200 Arlington St., Suite 2200
Chelsea, MA 02150
(P) 617.660.4665
(F) 617.884.4601
(E) timothy.mitchell@state.ma.us
http://www.mass.gov/eops

From: Egnitz, Brian (POL)
Sent: Friday, March 01, 2019 12:44 PM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Brian Kruger <bkruger@forensiclogic.com>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

Hi Tim,

I spoke with Brian Kruger and he wants the RI image CJIS Broker return to go to the same port as the ALPR image results, are there any issues with that? If not, is your team picking the port or is CopLink? I've included his email request. It sounds like they want to use the same web service to simplify the two integrations (LPR & RMV Images).

Tks, Brian

From: Mitchell, Timothy (EPS)
Sent: Friday, February 15, 2019 9:39 AM
To: Brian Kruger; Egnitz, Brian (POL); Ramsay, Christopher (EPS)
Subject: RE: LRP network ideas?

Brian
We are in receipt and reviewing on this side. I will get back to you next week.
Thanks

Timothy Mitchell
Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services

Enterprise and Field Services Support Division
Public Safety Data Center
200 Arlington St., Suite 2200
Chelsea, MA 02150
(P) 617.660.4665
(F) 617.884.4601
(E) timothy.mitchell@state.ma.us
http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Tuesday, February 12, 2019 2:46 PM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

Tim,
Here you go.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
Sent: Tuesday, February 12, 2019 8:19 AM
To: Brian Kruger <bkruger@forensiclogic.com>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian
Did you send over a diagram for review? If yes, can

you resend as I can't come across it? We need to review this before providing any additional ports. Thanks

Timothy Mitchell
Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise and Field Services Support Division
Public Safety Data Center
200 Arlington St., Suite 2200
Chelsea, MA 02150
(P) 617.660.4665
(F) 617.884.4601
(E) timothy.mitchell@state.ma.us
http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Tuesday, February 12, 2019 12:00 AM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

Tim/Brian,
We are ready to start up the LPR ingest again, however I still need to assign a port to Tomcat on the FR server that will be accessible from both application servers. Is there any port range that we can shoot for. I would like to get the LPR data flowing as soon as possible.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary*

and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.

From: Brian Kruger
Sent: Thursday, February 7, 2019 1:47 PM
To: 'Mitchell, Timothy (EPS)' <timothy.mitchell@state.ma.us>; 'Egnitz, Brian (POL)' <brian.egnitz@state.ma.us>; 'Ramsay, Christopher (EPS)' <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Tim,
Do you have any ports you send me that would be allowed for the connection from the app servers. I can update the diagram for approval that will work on the FR server. I will need two, one for Tomcat and one for LEXSR TR.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Thursday, February 7, 2019 8:50 AM
To: 'Mitchell, Timothy (EPS)' <timothy.mitchell@state.ma.us>; 'Egnitz, Brian (POL)' <brian.egnitz@state.ma.us>; 'Ramsay, Christopher (EPS)' <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Tim/Brian,

I was thinking last night and would actually like to move the new Image service to the FR server([redacted]). We have a route in place already from both PAA and Internal web to that server. I would just need to know what port to run tomcat on. This would also work for the Thompson Reuters adapter as well. Let me know what you guys think.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Monday, February 4, 2019 11:17 AM
To: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: LRP network ideas?

Brian/Tim,
Nick is almost done with the new LPR service that will remove the images from the database and have a tomcat app that host the images for a return to the UI. What I need to know:

1. The Migration will sit on the migration

server and needs access to the LPR database to pull out the metadata and create the URL for the Image links.

2. The new service is going to be hosted in Tomcat, so this service will need access to the LPR database for images and both application servers

need to be able to query this tomcat instance. I just need to know where to put it, I can host it on both severs or if we can set it up on the internal server and have a firewall rule that will allow the DMZ server to

talk to the internal server. Let me know if you would like to have a call on this. I have attached a rough network diagram for visual reference.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

<MSP agency ORI.xlsx>

From: Brian Kruger
To: Egnitz, Brian (POL)
Subject: FW: LRP network ideas?
Date: Thursday, February 20, 2020 9:47:09 AM
Attachments: image001.png

Brian,
This is the last email from John. It looks like we are missing a XSD file for the name space. I reached out just on the side to xfact to see if they have the XSD but haven't heard back.

Regards,

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Wednesday, February 12, 2020 8:37 AM
To: Samson Dunatunga <mdunatunga@forensiclogic.com>
Cc: Billy Moore <bmoore@forensiclogic.com>; Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hi Samson,

All of the xsd files are in the package and that is the only dev package we have.
Some of these namespaces were developed some time ago and are still in use.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Samson Dunatunga <mdunatunga@forensiclogic.com>
Sent: Tuesday, February 11, 2020 11:23 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Billy Moore <bmoore@forensiclogic.com>; Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Got all three packages extracted. I still don't see the XSD file for http://www.xfact.com/schemas/eopss/dcjis/cjx/3.0
I see XSD file (CJISBroker_2016-03-24.zip\CJISBroker_2016-03-24\CJISBroker\transactions\core\xsd\dcjis\1.0\dcjis.xsd) for http://www.xfact.com/schemas/eopss/dcjis/1.0 within the package CJISBroker_2016-03-24.zip

Do you have any other dev packages that includes above XSD files?
Thanks,
-Samson

From: Ouellette, John (EPS)
Sent: Tuesday, February 11, 2020 6:37 AM
To: Samson Dunatunga
Cc: Billy Moore; Brian Kruger
Subject: RE: LRP network ideas?

HI Samson,

Attached are the dev packages. They are zipped up, let me know if you don't get them.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Samson Dunatunga <mdunatunga@forensiclogic.com>
Sent: Monday, February 10, 2020 4:11 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>; Brian Kruger <bkruger@forensiclogic.com>
Cc: Billy Moore <bmoore@forensiclogic.com>
Subject: RE: LRP network ideas?

Hi John,
Thank you for the reply. The sample you have attached is a bit different from the sample I have. Where can I get the development package with the sample file you sent? It looks like I have been using an older implementation development package to generate the request. I don't have any class files related to dcjis schema in the development package I have.

Thanks,
-Samson

From: Ouellette, John (EPS)
Sent: Friday, February 7, 2020 2:39 PM
To: Samson Dunatunga; Brian Kruger
Cc: Billy Moore
Subject: RE: LRP network ideas?

Your namespaces should be:
xmlns:dcjis="http://www.xfact.com/schemas/eopss/dcjis/1.0" xmlns:cjx="http://www.xfact.com/schemas/eopss/dcjis/cjx/3.0"
xmlns:j="http://www.it.ojp.gov/jxdm/3.0"
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance

Attached is a sample R1 request.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services

Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Samson Dunatunga <mdunatunga@forensiclogic.com>
Sent: Friday, February 7, 2020 4:26 PM
To: Brian Kruger <bkruger@forensiclogic.com>; Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Billy Moore <bmoore@forensiclogic.com>
Subject: RE: LRP network ideas?

Hi John,
I compared the XML we are sending with the sample XML in the development package. I don't see any structural differences in them, but we are still getting reply indicating XML is not valid. Any help you can provide is appreciated.
Here is the XML we are sending for transaction type R1.
Thanks,
-Samson

---request begin----

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns1:CJISRequestTransaction xmlns:ns2="http://www.it.ojp.gov/jxdm/3.0" xmlns:ns1="http://www.xfact.com/schemas/chsb/cjis/2.0">
  <ns1:CJISRequestHeader>
    <ns1:UUID>G.L. c. 4 sec. 7 cl 26 7893d578-1867-4332-b278-b71a2c72f5b3</ns1:UUID>
    <ns1:CreateDateTime>2020-02-07T16:08:03.123-05:00</ns1:CreateDateTime>
    <ns1:TransactionSource>COPLINK</ns1:TransactionSource>
    <ns1:UserID>TEST</ns1:UserID>
    <ns2:OrganizationORIID>
      <ns2:ID>MAMSP0000</ns2:ID>
    </ns2:OrganizationORIID>
    <ns1:TimeToLive>unlimited</ns1:TimeToLive>
    <ns1:SchemaVersion>2.0</ns1:SchemaVersion>
    <ns1:ApplicationVersion>2.0</ns1:ApplicationVersion>
    <ns1:ResponseMechanism>Wait</ns1:ResponseMechanism>
    <ns1:RespondTo>http://G.L. c. 4 sec. 7 cl 26 6060/CHSBReceiver/CHSBService</ns1:RespondTo>
    <ns1:CJISUserID>
      <ns2:ID>TEST</ns2:ID>
    </ns1:CJISUserID>
    <ns1:CJISUserPassword>password</ns1:CJISUserPassword>
    <ns1:CJISQueryAuthorizer>
      <ns2:PersonFullName>Joe Authorizer</ns2:PersonFullName>
    </ns1:CJISQueryAuthorizer>
    <ns1:CJISQueryOperator>
      <ns2:PersonFullName>Jane Authorizer</ns2:PersonFullName>
    </ns1:CJISQueryOperator>
    <ns1:CJISQueryRequester>
      <ns2:PersonFullName>Jane Requester</ns2:PersonFullName>
    </ns1:CJISQueryRequester>
    <ns1:CJISQueryPurposeCode>C</ns1:CJISQueryPurposeCode>
  </ns1:CJISRequestHeader>
  <ns1:CJISRequestBody>
    <ns1:R1QueryInput>
      <ns1:CJISMessageKey>R1</ns1:CJISMessageKey>
      <ns2:DriverAuthorization xsi:type="ns1:DriverAuthorizationType" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <ns2:DriverAuthorizationID>
          <ns2:ID>S32935254</ns2:ID>
        </ns2:DriverAuthorizationID>
      </ns2:DriverAuthorization>
    </ns1:R1QueryInput>
  </ns1:CJISRequestBody>
</ns1:CJISRequestTransaction>
```

--- request end ----

Here is the sample XML provided to us.

```
<?xml version="1.0" encoding="UTF-8"?>
<cjx:CJISRequestTransaction xmlns:cjx="http://www.xfact.com/schemas/chsb/cjis/2.0" xmlns:j="http://www.it.ojp.gov/jxdm/3.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <cjx:CJISRequestHeader>
    <cjx:UUID>192.168.0.18/1237228378953.1.12</cjx:UUID>
    <cjx:CreateDateTime>2009-03-16T14:32:58-04:00</cjx:CreateDateTime>
    <cjx:TransactionSource>192.168.1.137 / CHSB</cjx:TransactionSource>
    <cjx:UserID>joe_user</cjx:UserID>
    <j:OrganizationORIID>
      <j:ID>MACJIS0M0</j:ID>
    </j:OrganizationORIID>
    <cjx:DeviceAddress></cjx:DeviceAddress>
    <cjx:UserContexts></cjx:UserContexts>
    <cjx:TimeToLive>unlimited</cjx:TimeToLive>
    <cjx:SchemaVersion>2.0</cjx:SchemaVersion>
    <cjx:ApplicationVersion>2.0</cjx:ApplicationVersion>
    <cjx:ResponseMechanism>Wait</cjx:ResponseMechanism>
    <cjx:RespondTo>http://192.168.0.30:6060/public/CHSBService.asmx</cjx:RespondTo>
    <cjx:CJISUserID>
      <j:ID>cjis_user</j:ID>
    </cjx:CJISUserID>
    <cjx:CJISUserPassword>password</cjx:CJISUserPassword>
    <cjx:CJISQueryAuthorizer>
      <j:PersonFullName>Joe Authorizer</j:PersonFullName>
    </cjx:CJISQueryAuthorizer>
    <cjx:CJISQueryOperator>
      <j:PersonFullName>Jane Operator</j:PersonFullName>
    </cjx:CJISQueryOperator>
    <cjx:CJISQueryRequester>
      <j:PersonFullName>Jane Requester</j:PersonFullName>
    </cjx:CJISQueryRequester>
    <cjx:CJISQueryPurposeCode>C</cjx:CJISQueryPurposeCode>
  </cjx:CJISRequestHeader>
  <cjx:CJISRequestBody>
    <cjx:R1QueryInput>
      <cjx:CJISMessageKey>R1</cjx:CJISMessageKey>
      <j:DriverAuthorization xsi:type="cjx:DriverAuthorizationType">
        <j:DriverAuthorizationID>
          <j:ID>900000035</j:ID>
        </j:DriverAuthorizationID>
      </j:DriverAuthorization>
```

```
    </cjx:R1QueryInput>
  </cjx:CJISRequestBody>
</cjx:CJISRequestTransaction>
```

Here is the reply we got for the XML we sent.

imagebroker.ImageBrokerREST.getEncodedImage result of service call: <?xml version="1.0" encoding="UTF-8"?>
<dcjis:DataExchange xmlns:dcjis="http://www.xfact.com/schemas/eopss/dcjis/1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><dcjis:Acknowledgment><dcjis:AcknowledgmentHeader><dcjis:UUID>ERROR</dcjis:UUID>
<dcjis:CreateDateTime>2020-02-07T16:08:18-0500</dcjis:CreateDateTime><dcjis:TransactionSource>ERROR</dcjis:TransactionSource><dcjis:TransactionMessageKey>ERROR</dcjis:TransactionMessageKey>
<dcjis:TransactionOrganizationID><dcjis:ID>ERROR</dcjis:ID></dcjis:TransactionOrganizationID><dcjis:UserContexts /><dcjis:DeviceAddress /><dcjis:SchemaVersion>1.0</dcjis:SchemaVersion>
<dcjis:ApplicationVersion>2.0</dcjis:ApplicationVersion><dcjis:CJISUserID><dcjis:ID>ERROR</dcjis:ID></dcjis:CJISUserID><dcjis:CJISUserPassword>ERROR</dcjis:CJISUserPassword><dcjis:CJISQueryAuthorizer>
<dcjis:PersonFullName>ERROR</dcjis:PersonFullName></dcjis:CJISQueryAuthorizer><dcjis:CJISQueryOperator><dcjis:PersonFullName>ERROR</dcjis:PersonFullName></dcjis:CJISQueryOperator><dcjis:CJISQueryRequester>
<dcjis:PersonFullName>ERROR</dcjis:PersonFullName></dcjis:CJISQueryRequester><dcjis:CJISQueryPurposeCode>ERROR</dcjis:CJISQueryPurposeCode><dcjis:Transaction><dcjis:TransactionStatus>-903</dcjis:TransactionStatus>
<dcjis:TransactionDescription>Transaction failed schema validation</dcjis:TransactionDescription></dcjis:Transaction></dcjis:AcknowledgmentHeader><dcjis:AcknowledgmentBody /></dcjis:Acknowledgment></dcjis:DataExchange>

From: Brian Kruger
Sent: Tuesday, January 28, 2020 3:23 PM
To: Ouellette, John (EPS); Samson Dunatunga
Subject: RE: LRP network ideas?

Samson,
Did you get what you needed?

Regards,

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Thursday, January 23, 2020 9:25 AM
To: Samson Dunatunga <mdunatunga@forensiclogic.com>
Cc: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hi Samson,

Do you have the dev package? There are example xml documents in there.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Samson Dunatunga <mdunatunga@forensiclogic.com>
Sent: Thursday, January 23, 2020 11:00 AM
To: Brian Kruger <bkruger@forensiclogic.com>; Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
Here is the XML sent from our server to retrieve relevant data. The CJISMessageKey is set to R1. The response we got indicates the XML sent is invalid. Can you point me to what is not valid in the XML? By the way, I checked the XML syntax with an online XML validation tool which indicates the syntax is good.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns1:CJISRequestTransaction xmlns:ns2="http://www.it.ojp.gov/jxdm/3.0" xmlns:ns1="http://www.xfact.com/schemas/chsb/cjis/2.0">
  <ns1:CJISRequestHeader>
    <ns1:UUID>G.L. c. 4,sec. 7,cl.26487fc738-d2fa-4b4f-8841-067b2d85e636</ns1:UUID>
    <ns1:CreateDateTime>2020-01-22T10:47:23.216-05:00</ns1:CreateDateTime>
    <ns1:TransactionSource>COPLINK</ns1:TransactionSource>
    <ns1:UserID>TEST</ns1:UserID>
    <ns2:OrganizationORIID>
      <ns2:ID>MAMSP0000</ns2:ID>
    </ns2:OrganizationORIID>
    <ns1:TimeToLive>unlimited</ns1:TimeToLive>
    <ns1:SchemaVersion>2.0</ns1:SchemaVersion>
    <ns1:ApplicationVersion>2.0</ns1:ApplicationVersion>
    <ns1:ResponseMechanism>Wait</ns1:ResponseMechanism>
    <ns1:RespondTo>http://G.L. c. 4,sec. 7,cl.2665060/CHSBReceiver/CHSBService</ns1:RespondTo>
    <ns1:CJISUserID>
      <ns2:ID>TEST</ns2:ID>
    </ns1:CJISUserID>
    <ns1:CJISUserPassword>password</ns1:CJISUserPassword>
    <ns1:CJISQueryAuthorizer>
      <ns2:PersonFullName>Joe Authorizer</ns2:PersonFullName>
    </ns1:CJISQueryAuthorizer>
    <ns1:CJISQueryOperator>
      <ns2:PersonFullName>Jane Authorizer</ns2:PersonFullName>
    </ns1:CJISQueryOperator>
    <ns1:CJISQueryRequester>
      <ns2:PersonFullName>Jane Requester</ns2:PersonFullName>
    </ns1:CJISQueryRequester>
    <ns1:CJISQueryPurposeCode>C</ns1:CJISQueryPurposeCode>
  </ns1:CJISRequestHeader>
  <ns1:CJISRequestBody>
    <ns1:R1QueryInput>
      <ns1:CJISMessageKey>R1</ns1:CJISMessageKey>
      <ns2:DriverAuthorization xsi:type="ns1:DriverAuthorizationType" ns2:id="S32935254" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"/>
    </ns1:R1QueryInput>
```

</ns1:CJISRequestBody>
</ns1:CJISRequestTransaction>

Thank you,
-Samson

From: Brian Kruger
Sent: Wednesday, January 22, 2020 1:39 PM
To: Ouellette, John (EPS); Samson Dunatunga
Subject: RE: LRP network ideas?

John,
I am adding Samson on this thread.

Regards,

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Wednesday, January 22, 2020 1:35 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hi Brian,

The only namespaces I can find are:
xmlns:dcjis="http://www.xfact.com/schemas/eopss/dcjis/1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:cjx="http://www.xfact.com/schemas/eopss/dcjis/cjx/3.0"
xmlns:j="http://www.it.ojp.gov/jxdm/3.0">

Which message key are you trying to run?

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Wednesday, January 22, 2020 2:57 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
I have been putting out new versions of our Broker on this build Samson noticed that we are using xml namespace 2.0 which doesn't work. Do you know what version we should be running.

From: Samson Dunatunga <mdunatunga@forensiclogic.com>
Sent: Wednesday, January 22, 2020 11:28 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE:

Looks like the XML namespace xmlns:ns1="http://www.xfact.com/schemas/chsb/cjis/2.0"
is no longer available. Can you find out what we are supposed to use?

Thanks,
-Samson

From: Brian Kruger
Sent: Wednesday, January 22, 2020 8:56 AM
To: Samson Dunatunga
Subject:

2020-0
22-Jan-
22-Jan-
22-Jan-
22-Jan-
22-Jan-
22-Jan-
22-Jan-
22-Jan-
22-Jan-
22-Jan-
22-Jan-
22-Jan-
22-Jan-
22-Jan-
22-Jan-
22-Jan-
22-Jan-
22-Jan-
22-Jan-
22-Jan-
22-Jan-
22-Jan-
22-Jan-



ogging.properties

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

22-Jan-2020 10:43:42.3
22-Jan-2020 10:43:42.3
22-Jan-2020 10:43:42.3
22-Jan-2020 10:43:43.0
22-Jan-2020 10:43:43.2
22-Jan-2020 10:43:43.2
22-Jan-2020 10:43:43.3
22-Jan-2020 10:43:43.3
22-Jan-2020 10:43:43.3
22-Jan-2020 10:43:57.6
22-Jan-2020 10:43:57.7
no TLDs were found in t
22-Jan-2020 10:43:57.8
22-Jan-2020 10:43:57.8
22-Jan-2020 10:43:57.8
22-Jan-2020 10:43:58.2
no TLDs were found in t
22-Jan-2020 10:44:00.5
22-Jan-2020 10:44:00.5
22-Jan-2020 10:44:00.8
no TLDs were found in t
22-Jan-2020 10:44:00.8
22-Jan-2020 10:44:00.8
22-Jan-2020 10:44:01.5
no TLDs were found in t
22-Jan-2020 10:44:01.6
22-Jan-2020 10:44:01.6
22-Jan-2020 10:44:01.9
no TLDs were found in t
22-Jan-2020 10:44:01.9
22-Jan-2020 10:44:01.9
22-Jan-2020 10:44:02.1
no TLDs were found in t
22-Jan-2020 10:44:02.1
22-Jan-2020 10:44:02.1
22-Jan-2020 10:44:02.3
no TLDs were found in t
22-Jan-2020 10:44:02.3
22-Jan-2020 10:44:02.3
22-Jan-2020 10:44:02.3
22-Jan-2020 10:44:02.3
22-Jan-2020 10:44:02.3
22-Jan-2020 10:44:02.4
22-Jan-2020 10:44:02.4
22-Jan-2020 10:44:02.5
22-Jan-2020 10:44:02.5
22-Jan-2020 10:44:02.5
[com.sun.xml.ws.api.ser
[com.sun.xml.ws.api.ser
22-Jan-2020 10:44:02.5
22-Jan-2020 10:44:02.6

2020-01-22 10:46:23 Co
22-Jan-2020 10:46:24.5
22-Jan-2020 10:46:24.5
22-Jan-2020 10:46:24.5

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

22-Jan-2020 10:46:33.998 IN
22-Jan-2020 10:46:33.998 IN
22-Jan-2020 10:46:34.232 IN
no TLDs were found in them
22-Jan-2020 10:46:34.232 IN
22-Jan-2020 10:46:34.232 IN
22-Jan-2020 10:46:34.435 IN
no TLDs were found in them
22-Jan-2020 10:46:34.435 IN
22-Jan-2020 10:46:34.450 IN
22-Jan-2020 10:46:34.466 IN
22-Jan-2020 10:46:34.466 IN
22-Jan-2020 10:47:23.793 IN
<dcjis:DataExchange xmlns:d
<dcjis:CreateDateTime>2020
<dcjis:TransactionOrganizati
<dcjis:ApplicationVersion>2.
<dcjis:PersonFullName>ERR
<dcjis:PersonFullName>ERR
<dcjis:TransactionDescriptio

Regards,

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, December 6, 2019 9:45 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hey Brian,

Can we change the subject to Broker?
LPR is the license plate reader.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, December 6, 2019 11:31 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Samson Dunatunga <mdunatunga@forensiclogic.com>; Billy Moore <bmoore@forensiclogic.com>; Rhonda Fromm <rfromm@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

Billy,
Please let the group know when this will be available. I will work with John to get it deployed and tested as soon as we have it released.

Regards,

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Tuesday, November 26, 2019 1:17 PM
To: 'Ouellette, John (EPS)' <john.ouellette@state.ma.us>; 'Egnitz, Brian (POL)' <brian.egnitz@state.ma.us>; Samson Dunatunga <mdunatunga@forensiclogic.com>; Billy Moore <bmoore@forensiclogic.com>
Cc: 'Dunne, Michaela (CHS)' <michaela.dunne@state.ma.us>; 'Dunn-CHS, William (CHS)' <william.dunn-chs@state.ma.us>; 'Mitchell, Timothy (EPS)' <timothy.mitchell@state.ma.us>; 'Ramsay, Christopher (EPS)' <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

John,
Thank you for the information on the call this afternoon.

Samson/Billy,
We need to add some additional debug code into our service so we can see the full communication path and what is being sent and received. John is also in the process to check and make sure their three servers can reach back into our 184.171 on port 6060. I have also reattached the IP wireshark I did this morning.

Regards,

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Tuesday, November 26, 2019 8:29 AM
To: Ouellette, John (EPS) <john.ouellette@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

John,
Give me a few minutes and I will give you a call. Here is the CSV file from wireshark. I had to repull it. I don't see any actually log details in our tomcat instance. In the wireshark though I see a bunch of event code errors like below:

Event: <Unknown eventcode 72>, <Unknown eventcode 111>, <Unknown eventcode 116>, <Unknown eventcode 121>, <Unknown eventcode 110>, <Unknown eventcode 45>, <Unknown eventcode 112>, <Unknown eventcode 110>, <Unknown eventcode 114>, <Unknown eventcode 115>, <Unknown eventcode 47>, <Unknown eventcode 110>, <Unknown eventcode 111>, <Unknown eventcode 118>, <Unknown eventcode 110>, <Unknown eventcode 111>, <Unknown eventcode 47>, ColormapNotify, <Unknown eventcode 97>, <Unknown eventcode 120>, <Unknown eventcode 58>, <Unknown eventcode 46>, <Unknown eventcode 104>, <Unknown eventcode 46>, <Unknown eventcode 117>, <Unknown eventcode 97>, <Unknown eventcode 47>, <Unknown eventcode 62>, <Unknown eventcode 114>, <Unknown eventcode 114>, <Unknown eventcode 82>, <Unknown eventcode 120>, <Unknown eventcode 101>, MappingNotify, <Unknown eventcode 109>, <Unknown eventcode 98>, <Unknown eventcode 47>, <Unknown eventcode 119>, <Unknown eventcode 62>, <Unknown eventcode 114>, ColormapNotify, <Unknown eventcode 62>, <Unknown eventcode 115>, MappingNotify, <Unknown eventcode 110>

Regards,

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Tuesday, November 26, 2019 7:29 AM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Hey Brian,

You can call me at 617-660-4775

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Monday, November 25, 2019 7:53 PM
To: Brian Kruger <bkruger@forensiclogic.com>; Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: Re: LRP network ideas?

Does it make sense to schedule a call and work through it in real time?

> On Nov 22, 2019, at 4:00 PM, Ouellette, John (EPS) <john.ouellette@mass.gov> wrote:
>
> Hi Brian,
>
> I do not see any requests for your ORI. Can you review the acknowledgements that the broker sends back as a return value? There may be error information in there.
>
> John Ouellette | Massachusetts Executive Office of Public Safety and Security
> Office of Technology and Information Services
> Enterprise Application and Database Services
> Application Support and Management
> 200 Arlington Street Suite 2200
> Chelsea, MA 02150
> john.ouellette@state.ma.us | http://www.mass.gov/eops
>
> **From:** Brian Kruger <bkruger@forensiclogic.com>
> **Sent:** Friday, November 22, 2019 3:47 PM
> **To:** Ouellette, John (EPS) <john.ouellette@mass.gov>
> **Cc:** Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
> **Subject:** RE: LRP network ideas?
>
> John,
> Can you check again and see if there is a request coming into the .154 server. I ran a packet capture and I do see data sent from the .171 to the .154 server.
>
> <image001.png>
>
> Regards,
>
> <image002.png>
>
> **Brian Kruger**
> Operations and Support Manager
> **Forensic Logic / COPLINK**
> Office: 520.367.2775
> Mobile: 520.488.1603
> bkruger@forensiclogic.com
> www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 22, 2019 12:26 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

I'm not sure if 224.154 is a load balancer. I don't believe it is though. It doesn't matter though, that is where you will send requests. You will receive a synchronous response called an acknowledgement. That will let you know if your request was accepted or rejected.

Later, an asynchronous response will be sent from 170.154.224.155 or 170.154.224.156 to your web service.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 22, 2019 2:19 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
The 154 address is a load balancer for the services correct. As far as I know there should be no blocked traffic to the .171 but let me include Chris and Tim on this thread.

Regards,

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 22, 2019 9:36 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

I didn't find any submitted requests.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Ouellette, John (EPS)
Sent: Friday, November 22, 2019 11:34 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

I can check.

The broker will send responses from 170.154.224.155 or 170.154.224.156 on port 6060. Make sure you are allowing that traffic.

When you send in a request you will receive an xml document as the return value. The documents lists if the request was accepted and if it wasn't, why it wasn't. You should be checking those.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 22, 2019 11:28 AM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

Bill,
I have the service send back a no data found so it looks like we are connecting. Can you check your logs to see if our request actually made it into your system.

I am sending the following test cycle from the 170.154.224.82 web server to our FR server

http://[redacted]6060/CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=S32935254

Just so everybody is clear, this the is the connection path

170.154.224.82 → [redacted] port 6060 → [redacted] port 6060

Return path

[redacted] → [redacted] port 6060 → 170.154.224.82

Log of request:

2019-11-22 11:16:13,982 main DEBUG LoggerContext[name=MassLPRServlet, org.apache.logging.log4j.core.LoggerContext@59303963] started OK with configuration org.apache.logging.log4j.core.config.properties.PropertiesConfiguration@61e86192.
2019-11-22 11:16:13,982 main DEBUG Log4jServletContextListener ensuring that Log4j starts up properly.
2019-11-22 11:16:13,982 main DEBUG Log4jServletFilter initialized.
driversLicense=S32935254
remote host=170.154.224.82
remote port=60194
remote addr=170.154.224.82
scheme =http
scheme =HTTP/1.1
local addr =[redacted]
local name =EPS-CLFACEMATCH
context path = /CHSBReceiver
Init parameter1 =Value1
Current UUID : f3837e1f-0e40-4af6-8587-203e99240d92
javax.xml.bind.JAXBElement@227d5180
Request UUID:[redacted]f3837e1f-0e40-4af6-8587-203e99240d92

Rest response file contains:
no data found.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Thursday, November 21, 2019 2:11 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Ouellette, John (EPS) <john.ouellette@state.ma.us>
Subject: RE: LRP network ideas?

Thanks Bill!

It looks like we are close on this.

-Brian

From: Dunn-CHS, William (CHS)
Sent: Tuesday, November 19, 2019 7:50 AM
To: Brian Kruger; Ouellette, John (EPS)
Cc: Dunne, Michaela (CHS); Egnitz, Brian (POL); Dunn-CHS, William (CHS)
Subject: RE: LRP network ideas?

I think I see what might be part of the problem.

The R1 is either OLN or SSN, you can not send both at the same time.

There is No TEST SSN inquiry, use someone from MSP who is working on your project or if you have a developer who is from MA
The TEST OLN is S32935254

From: Brian Kruger [mailto:bkruger@forensiclogic.com]
Sent: Monday, November 18, 2019 6:33 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
Dev confirmed they are sending XML in the request. Do you have a valid License number in the test data I can try.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 15, 2019 11:16 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

The broker is a web service. You need to create a client to connect. Requests are made by sending in an xml document.

Did I forget to send you the broker documentation? Let me know.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 1:10 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
I ran two queries through IE I don't see an acknowledge me in the logs. Below is what I am seeing. Do we have a valid Lic number that is in the system I can try, or valid SSN.

My test URLs are:"
http:/[redacted]6060/CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=987654321

http:/[redacted]6060/CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=987654321

In my access log I see a 200:

[redacted] - - [15/Nov/2019:13:02:50 -0500] "GET /CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=987654321 HTTP/1.1" 200 -
[redacted] - - [15/Nov/2019:13:03:05 -0500] "GET /CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=987654321 HTTP/1.1" 200 –

In my log stdout log I see this:

2019-11-15 G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)
2019-11-15 [redacted] log4j2.properties
2019-11-15
org.apache
2019-11-15
2019-11-15
2019-11-15 [redacted] ript, javascript, ECMAScript, ecmascript],
factory clas
2019-11-15
2019-11-15
2019-11-15
2019-11-15
2019-11-15
2019-11-15
2019-11-15
2019-11-15
2019-11-15
2019-11-15
2019-11-15
2019-11-15 [redacted] tiesConfig), Filter=null)
2019-11-15
2019-11-15
2019-11-15 [redacted] ll", alwaysWriteExceptions="null",
disableAns
2019-11-15
2019-11-15
2019-11-15
2019-11-15
2019-11-15
2019-11-15
2019-11-15
2019-11-15 [redacted] pCompressedFilePattern="null",
Configurati
2019-11-15
2019-11-15 [redacted] pend="null", locking="null",
Policies(Co
DefaultRoll [redacted] ull", fileGroup="null", bufferedIo="null",
bufferSize=
2019-11-15
2019-11-15
2019-11-15
2019-11-15
SizeBasedT
2019-11-15
2019-11-15
2019-11-15
2019-11-15
2019-11-15
2019-11-15
2019-11-15
2019-11-15
2019-11-15
2019-11-15
2019-11-15
2019-11-15
2019-11-15
2019-11-15
2019-11-15
2019-11-15
2019-11-15
2019-11-15
2019-11-15
2019-11-15
2019-11-15

[redacted]

2019-11-15 13:02:
2019-11-15 13:02:
2019-11-15 13:02:
org.apache.logging
2019-11-15 13:02:
2019-11-15 13:02:
driversLicense=987654321
remote host=[redacted]
remote port=62034
remote addr=[redacted]
scheme =http
scheme =HTTP/1.1
local addr=[redacted]
local name =EPS-CLFACEMATCH
context path = /CHSBReceiver
Init parameter1 =Value1
remote host not allowed. ignoring request.
driversLicense=987654321
remote host=[redacted]
remote port=62034
remote addr=[redacted]
scheme =http
scheme =HTTP/1.1
local addr=[redacted]
local name =EPS-CLFACEMATCH
context path = /CHSBReceiver
Init parameter1 =Value1
remote host not allowed. ignoring request.

My stderr log

[redacted]

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK

Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 15, 2019 9:54 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hey Brian,

When you send in a request, the return to that call is an acknowledgement. That is an xml document that will state if your request was accepted or not; and if it is not, what the reason is.

Are you seeing any acknowledgements?

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

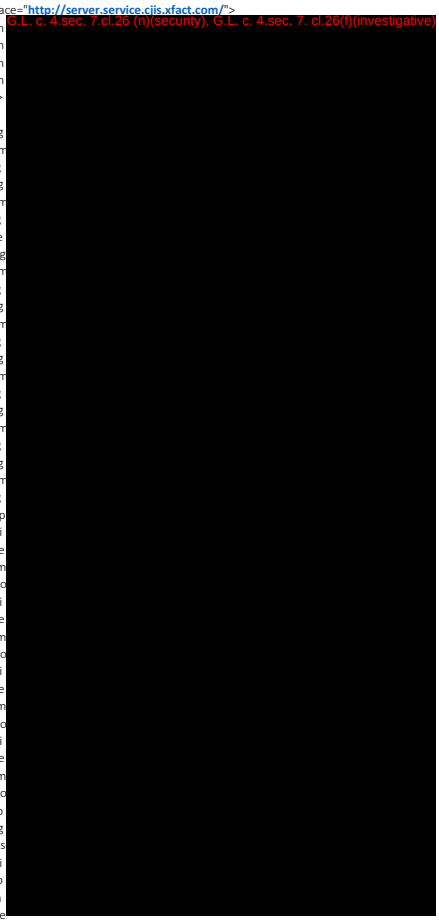
From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 11:49 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
According to dev the message that is coming back: remote host not allowed. ignoring request. They are stating is a response from your system telling us we are not allowed. Is there anyway you and I can get on the phone, I can try and send some responses and see if you see anything in your log files. I am wondering if they are forming the response to you correctly.

As for the WSDL this is what I see from the 184.171 server.

<image003.png>

Full WSDL
<?xml version="1.0" encoding="UTF-8" ?>
- <wsdl:definitions xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/" xmlns:tns="http://server.service.cjis.xfact.com/"
xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" xmlns:ns1="http://schemas.xmlsoap.org/soap/http" name="**CJISService**" targetNamespace="**http://server.service.cjis.xfact.com/**">
- <wsdl:types>
- <xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:tns="http://server.service.cjis.xfact.com/" attributeFormDefault="**unqualified**" elementFormDefault="**qualified**"
targetNamespace="**http://server.service.cjis.xfact.com/**">
<xsd:element n
<xsd:element n
<xsd:element n
<xsd:element n
</xsd:schema>
</wsdl:types>
- <wsdl:messag
<wsdl:part elem
</wsdl:messag
- <wsdl:messag
<wsdl:part elem
</wsdl:messag
<wsdl:message
+ <wsdl:messag
<wsdl:part elem
</wsdl:messag
- <wsdl:messag
<wsdl:part elem
</wsdl:messag
- <wsdl:messag
<wsdl:part elem
</wsdl:messag
- <wsdl:messag
<wsdl:part elem
</wsdl:messag
- <wsdl:messag
<wsdl:part elem
</wsdl:messag
- <wsdl:portTyp
- <wsdl:operati
<wsdl:input me
<wsdl:output m
</wsdl:operatio
- <wsdl:operati
<wsdl:input me
<wsdl:output m
</wsdl:operatio
- <wsdl:operati
<wsdl:input me
<wsdl:output m
</wsdl:operatio
- <wsdl:operati
<wsdl:input me
<wsdl:output m
</wsdl:operatio
</wsdl:portTyp
- <wsdl:binding
<soap:binding s
- <wsdl:operati
<soap:operatio
- <wsdl:input n
<soap:body use
</wsdl:input>



G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

[redacted]

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 15, 2019 9:36 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

If you are able to telnet, then you should be able to send in a request.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 11:06 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
This is all from the 184.171 server.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 15, 2019 8:41 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Are you doing the ping and telnet from [redacted]

Your error message from earlier seems to be your network not allowing the access.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 10:37 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
I am reaching out to the [redacted] on port 6060. I can ping the IP and also hit the port.
<image004.png>

<image005.png>

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 15, 2019 8:26 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

What is the ip address you are trying to connect to?
Are you able to ping that machine?

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 10:22 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

Brian,
Thank you for checking in, sorry for the delay. I had the email together but it was in my draft. I tested the connection again today.

John,
I am still getting the remote Host not allowed. This is the error below:

2019-11-15 10:15:45,808 main DEBUG Log4jServletFilter initialized.
driversLicense=987654321
remote host=[redacted]
remote port=61799
remote addr=[redacted]
scheme =http
scheme =HTTP/1.1
local addr =[redacted]
local name =EPS-CLFACEMATCH
context path = /CHSBReceiver
Init parameter1 =Value1
remote host not allowed. ignoring request.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Friday, November 8, 2019 1:17 PM
To: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>

Subject: RE: LRP network ideas?

John,
Thank you, I will work on testing the connection and let you know the results. According to Dev the other queries we will be running on the R1 and RI.

Regards,

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 8, 2019 12:18 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunn, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

I have added your configuration on the test broker for R1 and RI.
Are there more queries/transactions you'd like to test? Michaela may have requirements for other queries.

The ORI is MAMSPF022
Your requests come from [redacted] and responses will be sent back to http://[redacted]6060/CHSBReceiver/CHSBService

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Ouellette, John (EPS)
Sent: Tuesday, November 5, 2019 12:54 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunn, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>
Subject: RE: LRP network ideas?

Hi Brian,

I think Bill needs to have more information on your project to assign an ORI to use on the test broker.
Is there a project name on your side?

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Monday, November 4, 2019 3:30 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
Any luck on this.

Regards,

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Tuesday, October 22, 2019 12:32 PM
To: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Subject: RE: LRP network ideas?

John,
Yea we should be sending the XML packet with the service that we have created. Do you know if that IP is natted to [redacted] The server that we have our service on is the [redacted] Face match server. I don't have any servers in the 170.154.226.x IP range unless it is getting natted somehow.

Regards,

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify*

the sender and delete this e-mail from your system.

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Tuesday, October 22, 2019 12:21 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hay Brian,

That won't work. The broker accepts an xml document containing the request, as well as other information.
Attached is a sample R1 request.

By the way, I have your requests coming from 170.154.226.47

In order to get responses, you need a web service on your end to receive the responses and I'll need to configure it on the broker side.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Monday, October 21, 2019 5:04 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
Can you provide me with a DL that should work. From the .82 server this is what we are running:

http://[redacted]6060/CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=987654321

I just need to update the drivers license number and hopefully it will work

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Tuesday, September 24, 2019 8:07 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

So, just R1 and RI?

I'll start configuring the test broker.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Tuesday, September 24, 2019 10:59 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
For the queries that we will using this is what I got back from Dev… let me know if this helps

…Attachments\CJISBroker_2016-03-24[13247].zip\CJISBroker_2016-03-24\CJISBroker\transactions\queries\rmv\r1\xml

…Attachments\CJISBroker_2016-03-24[13247].zip\CJISBroker_2016-03-24\CJISBroker\transactions\queries\rmv\ri\xml

The rest is correct, for testing the ORI list will grow once we go to production.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Tuesday, September 24, 2019 6:39 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hi Brian,

I haven't added your configuration to the test broker yet. Can you confirm the following:

For broker connections, we need the following:
IP Address for request: [redacted]
URL for responses: http://[redacted]6060/CHSBReceiver/CHSBService
ORI: MAMSP0000
Queries: I need the list of queries/transactions you will be testing

You will submit to http://[redacted]6060/CJISService This call will return a synchronous acknowledgment.

Responses will come back from 170.154.224.155 or 170.154.224.156 on port 6060. You need to return a synchronous acknowledgement for each response.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Monday, September 23, 2019 7:53 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
I have deployed a new package, but I see this in the log.

2019-09-23 19:48:37,297 main DEBUG Registering MBean org.apache.logging.log4j2:type=MassLPRServlet,component=Appenders,name=RollingFile
2019-09-23 19:48:37,304 main DEBUG org.apache.logging.log4j.core.util.SystemClock does not support precise timestamps.
2019-09-23 19:48:37,305 main DEBUG LoggerContext[name=MassLPRServlet, org.apache.logging.log4j.core.LoggerContext@2180e789] started OK with configuration org.apache.logging.log4j.core.config.properties.PropertiesConfiguration@5e9bbd9d.
2019-09-23 19:48:37,307 main DEBUG Log4jServletContextListener ensuring that Log4j starts up properly.
2019-09-23 19:48:37,309 main DEBUG Log4jServletFilter initialized.
driversLicense=987654321
remote host=0:0:0:0:0:0:0:1
remote port=65146
remote addr=0:0:0:0:0:0:0:1
scheme =http
scheme =HTTP/1.1
local addr =0:0:0:0:0:0:0:1
local name =EPS-CLFACEMATCH
context path = /CHSBReceiver
Init parameter1 =Value1
remote host not allowed. ignoring request.

can you check and make sure this machine has access:

EPS-CLFACEMATCH
Connection-specific DNS Suffix . :
IPv4 Address. . . . . : [redacted]
Subnet Mask . . . . . : 255.255.255.128
Default Gateway . . . . . : 170.154.184.129

C:\Users\msp_user>
Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, September 6, 2019 6:15 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hey Brian,

I'm not sure what is in the test system either. I believe a dl of 987654321 will work; at least it used to.
Try to find something in test CJISWeb.

Remember that all queries will send in an xml document and will receive a return acknowledgement stating success or failure. If the request failed, the reason will be in the acknowledgement.

At a later time, seconds or less, the response will be returned to your web service. You must return an acknowledgement to that also to let the system know that the response was received and the next response can be sent.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Thursday, September 5, 2019 5:17 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
Not yet, I don't know what is in the test system… are they actually dls or fake ones.

Our query against our service is going to look something like, that will translate to yours.

http://[redacted]6060/CHSBReceiver/CHSBService?ori=REM000001&username=TEST&ssn=123123123&driversLicense=AZ67676767

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Thursday, September 5, 2019 1:09 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Have you tried your DL and SSN?

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Thursday, September 5, 2019 2:36 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
Do you have a sample DL and ssn, we can try passing through the service to see if we can pull an image. According to dev we are just utilizing the XML out of R1 and Ri.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, August 9, 2019 7:04 AM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Brian Kruger <bkruger@forensiclogic.com>; Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

All of the broker queries use the same method and accept an xml document. The contents of the xml direct what action the system should take. I have attached documentation for the broker. It's a 5 MB zip file.

If you can't accept zip files or 5 MB files let me know how to send the file.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, August 9, 2019 9:39 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Brian Kruger <bkruger@forensiclogic.com>; Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>
Subject: Re: LRP network ideas?

Thanks John, I'll defer to Brian Kruger to respond regarding where he's sending the query. Are you able to answer his question below?

"

> I can pull back the WSDL but want to send an image request to it to see if it actually pulls the image. I am looking for something like /GetPhoto?dl_num=20180061903&ss_num=2&type=M, the actually call method

"

On Aug 9, 2019, at 9:04 AM, Ouellette, John (EPS) <john.ouellette@mass.gov> wrote:

> Hi Brian,
>
> For broker connections to test, we need the following:
> IP Address for request: [redacted]
> URL for responses: http://[redacted]:6060/CHSBReceiver/CHSBService
> ORI: MAMSP0000
> Queries:
>
> Can you confirm this information and send the list of queries you would like to run?
> Please remember that this system would only be used for test. Another system would need to be used when you move to production.
>
> John Ouellette | Massachusetts Executive Office of Public Safety and Security

Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, August 9, 2019 8:54 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Ouellette, John (EPS) <john.ouellette@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>
Subject: Re: LRP network ideas?

Hi Brian,

are we testing on this yet?

On Jul 22, 2019, at 1:37 PM, Brian Kruger <bkruger@forensiclogic.com> wrote:

> Tim,
> Attached is the full list of agencies and ORI that we currently have in the admin DB.
>
> Regards,
>
> <image001.png>
>
> **Brian Kruger**
> Operations and Support Manager
> **Forensic Logic / COPLINK**
> 520.488.1603
> bkruger@forensiclogic.com
> www.forensiclogic.com
>
> ***CONFIDENTIALITY:*** *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*
>
> **From:** Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
> **Sent:** Monday, July 22, 2019 8:37 AM
> **To:** Brian Kruger <bkruger@forensiclogic.com>
> **Cc:** Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Ouellette, John (EPS) <john.ouellette@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
> **Subject:** RE: LRP network ideas?
>
> Any update on this from dev, do you still need a sample RI url? Can you make sure you are also sending the CopLink user name in the UserID parameter.
>
> Tks, Brian
>
> **From:** Brian Kruger [mailto:bkruger@forensiclogic.com]
> **Sent:** Thursday, July 18, 2019 5:19 PM
> **To:** Mitchell, Timothy (EPS)
> **Cc:** Ramsay, Christopher (EPS); Egnitz, Brian (POL); Ouellette, John (EPS)
> **Subject:** RE: LRP network ideas?
>
> Tim,
> I am still pending an answer back from dev on how they are going to pull the ORI. For now can we use `MAMSP0000. That is actually in our systems as MSP.`
>
> Regards,
>
> <image001.png>
>
> **Brian Kruger**
> Operations and Support Manager
> **Forensic Logic / COPLINK**
> 520.488.1603
> bkruger@forensiclogic.com
> www.forensiclogic.com
>
> ***CONFIDENTIALITY:*** *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*
>
> **From:** Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
> **Sent:** Tuesday, July 16, 2019 4:07 AM
> **To:** Brian Kruger <bkruger@forensiclogic.com>
> **Cc:** Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Ouellette, John (EPS) <john.ouellette@state.ma.us>
> **Subject:** RE: LRP network ideas?
>
> Brian
> What is the ORI that you are using for this setup? There is some configuration work that needs to be done on the broker side to allow your service to run transactions.
> Thanks
> Tim
>
> Timothy Mitchell
> Massachusetts Executive Office of Public Safety and Security
> Office of Technology and Information Services
> Enterprise and Field Services Support Division
> Public Safety Data Center
> 200 Arlington St., Suite 2200
> Chelsea, MA 02150
> (P) 617.660.4665
> (F) 617.884.4601
> (E) timothy.mitchell@state.ma.us
> http://www.mass.gov/eops
>
> **From:** Brian Kruger <bkruger@forensiclogic.com>
> **Sent:** Monday, July 15, 2019 7:05 PM
> **To:** Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>
> **Cc:** Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Subject:** RE: LRP network ideas?
>
> Folks,
> For the RMV pull, does anybody have an example image we can try and run through. All the connectivity looks good, I have tried a few ways to pull an image without success.

Our service
http://[redacted]:6060/CHSBReceiver/CHSBService?wsdl refers to http://[redacted]:6060/CJISService?wsdl

I can pull back the WSDL but want to send an image request to it to see if it actually pulls the image. I am looking for something like /GetPhoto?dl_num=20180061903&ss_num=2&type=M, the actually call method

To pull b
<?xml ve
- <wsdl:d
xmlns:so
- <wsdl:t
- <xsd:sc
targetNa
<xsd:ele
<xsd:ele
<xsd:ele
<xsd:ele
</xsd:sc
</wsdl:t
- <wsdl:
<wsdl:pa
</wsdl:m
- <wsdl:
<wsdl:pa
</wsdl:m
<wsdl:m
- <wsdl:
<wsdl:pa
</wsdl:m
- <wsdl:
<wsdl:pa
</wsdl:m
- <wsdl:
<wsdl:pa
</wsdl:m
- <wsdl:
<wsdl:pa
</wsdl:m
- <wsdl:
<wsdl:pa
</wsdl:m
- <wsdl:p
- <wsdl:o
<wsdl:in
<wsdl:ou
</wsdl:o
- <wsdl:o
<wsdl:in
<wsdl:ou
</wsdl:o
- <wsdl:o
<wsdl:in
<wsdl:ou
</wsdl:o
- <wsdl:o
<wsdl:in
<wsdl:ou
</wsdl:o
</wsdl:p
- <wsdl:b
<soap:bi
- <wsdl:o
<soap:op
- <wsdl:i
<soap:bo
</wsdl:in
- <wsdl:o
<soap:bo
</wsdl:o
</wsdl:o
- <wsdl:o
<soap:op
- <wsdl:i
<soap:bo
</wsdl:in
- <wsdl:o
<soap:bo
</wsdl:o
</wsdl:o
- <wsdl:o
<soap:op
- <wsdl:i
<soap:bo
</wsdl:in
- <wsdl:o
<soap:bo
</wsdl:o
</wsdl:o
- <wsdl:o
<soap:op
- <wsdl:i
<soap:bo
</wsdl:in
- <wsdl:o
<soap:bo
</wsdl:o
</wsdl:o
</wsdl:b
- <wsdl:s
- <wsdl:p
<soap:ad
</wsdl:p

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

[redacted]

wsdl/" xmlns:tns="http://server.service.cjis.xfact.com/"
="**CJISService**" targetNamespace="**http://server.service.cjis.xfact.com/**">

" attributeFormDefault="**unqualified**" elementFormDefault="**qualified**"

</wsdl:service>
</wsdl:definitions>

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
Sent: Wednesday, May 8, 2019 5:52 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: Re: LRP network ideas?

Brian
Can you test the connectivity again?
Thanks

Sent from my iPhone

On May 7, 2019, at 10:43 AM, Brian Kruger <bkruger@forensiclogic.com> wrote:

> Tim,
> Thank you sir, sorry this fell off my radar. I was working on reallocation for Dan.
>
> Regards,
>
> <image001.png>
>
> **Brian Kruger**
> Operations and Support Manager
> **Forensic Logic / COPLINK**
> 520.488.1603
> bkruger@forensiclogic.com
> www.forensiclogic.com
>
> ***CONFIDENTIALITY:*** *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*
>
> ---
>
> **From:** Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
> **Sent:** Tuesday, May 7, 2019 7:42 AM
> **To:** Brian Kruger <bkruger@forensiclogic.com>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
> **Subject:** RE: LRP network ideas?
>
> Brian
> Yes you will need to run the transactions across to the test server first and DCJIS will need to approve it before you can run to the production server. I will check out the firewall rules today and let you know.
> Thanks
>
> Timothy Mitchell
> Massachusetts Executive Office of Public Safety and Security
> Office of Technology and Information Services
> Enterprise and Field Services Support Division
> Public Safety Data Center
> 200 Arlington St., Suite 2200
> Chelsea, MA 02150
> (P) 617.660.4665
> (F) 617.884.4601
> (E) timothy.mitchell@state.ma.us
> http://www.mass.gov/eops
>
> ---
>
> **From:** Brian Kruger <bkruger@forensiclogic.com>
> **Sent:** Tuesday, May 07, 2019 10:40 AM
> **To:** Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Subject:** RE: LRP network ideas?
>
> Chris,
> I am guessing test first, that way we can validate the broker, unless the route is setup already for production and I can switch it out to that.
>
> Brian E.,
> Your thoughts?
>
> Regards,
>
> <image001.png>
>
> **Brian Kruger**
> Operations and Support Manager
> **Forensic Logic / COPLINK**
> 520.488.1603
> bkruger@forensiclogic.com
> www.forensiclogic.com
>
> ***CONFIDENTIALITY:*** *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*
>
> ---
>
> **From:** Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
> **Sent:** Tuesday, May 7, 2019 7:18 AM
> **To:** Brian Kruger <bkruger@forensiclogic.com>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
> **Subject:** RE: LRP network ideas?
>
> Brian,

[redacted] Is the TEST cjis broker system. Is the test system what you're looking to use?

-Chris

Christopher Ramsay | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Division of Enterprise & Field Services Support | Enterprise Systems

200 Arlington St. Suite 2200
Chelsea, MA 02150
p. 617.660.4720 | f. 617.660.4613
christopher.ramsay@mass.gov | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Tuesday, May 7, 2019 1:49 AM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

Tim,
I was checking the cjis broker service and I can't get to the [redacted] on 6060 from the FR server at [redacted] I was going through old email and just checking the status of the connections. The [redacted] is what I received from Dev. Let me know if this is not correct.

<image003.jpg>

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
Sent: Friday, March 1, 2019 1:28 PM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Brian Kruger <bkruger@forensiclogic.com>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Hi folks
The CJIS broker transactions will need to use port 6060 as that is what they have been configured for in the past.

We have discussed the LPR port request and we think that going with a higher port seems to be more acceptable to EOTSS to allow through their public access firewall. Would port 56446 (https) work? We will need to open a ticket with EOTSS to have them allow this port through.

Thanks

Timothy Mitchell
Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise and Field Services Support Division
Public Safety Data Center
200 Arlington St., Suite 2200
Chelsea, MA 02150
(P) 617.660.4665
(F) 617.884.4601
(E) timothy.mitchell@state.ma.us
http://www.mass.gov/eops

From: Egnitz, Brian (POL)
Sent: Friday, March 01, 2019 12:44 PM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Brian Kruger <bkruger@forensiclogic.com>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

Hi Tim,

I spoke with Brian Kruger and he wants the RI image CJIS Broker return to go to the same port as the ALPR image results, are there any issues with that? If not, is your team picking the port or is CopLink? I've included his email request. It sounds like they want to use the same web service to simplify the two integrations (LPR & RMV Images).

Tks, Brian

From: Mitchell, Timothy (EPS)
Sent: Friday, February 15, 2019 9:39 AM
To: Brian Kruger; Egnitz, Brian (POL); Ramsay, Christopher (EPS)
Subject: RE: LRP network ideas?

Brian
We are in receipt and reviewing on this side. I will get back to you next week.
Thanks

Timothy Mitchell
Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise and Field Services Support Division
Public Safety Data Center
200 Arlington St., Suite 2200
Chelsea, MA 02150
(P) 617.660.4665
(F) 617.884.4601
(E) timothy.mitchell@state.ma.us
http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Tuesday, February 12, 2019 2:46 PM

To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

Tim,
Here you go.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
Sent: Tuesday, February 12, 2019 8:19 AM
To: Brian Kruger <bkruger@forensiclogic.com>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian
Did you send over a diagram for review? If yes, can you resend as I can't come across it? We need to review this before providing any additional ports.
Thanks

Timothy Mitchell
Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise and Field Services Support Division
Public Safety Data Center
200 Arlington St., Suite 2200
Chelsea, MA 02150
(P) 617.660.4665
(F) 617.884.4601
(E) timothy.mitchell@state.ma.us
http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Tuesday, February 12, 2019 12:00 AM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

Tim/Brian,
We are ready to start up the LPR ingest again, however I still need to assign a port to Tomcat on the FR server that will be accessible from both application servers. Is there any port range that we can shoot for. I would like to get the LPR data flowing as soon as possible.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Thursday, February 7, 2019 1:47 PM
To: 'Mitchell, Timothy (EPS)' <timothy.mitchell@state.ma.us>; 'Egnitz, Brian (POL)' <brian.egnitz@state.ma.us>; 'Ramsay, Christopher (EPS)' <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Tim,
Do you have any ports you send me that would be allowed for the connection from the app servers. I can update the diagram for approval that will work on the FR server. I will need two, one for Tomcat and one for LEXSR TR.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Thursday, February 7, 2019 8:50 AM
To: 'Mitchell, Timothy (EPS)' <timothy.mitchell@state.ma.us>; 'Egnitz, Brian (POL)' <brian.egnitz@state.ma.us>; 'Ramsay, Christopher (EPS)' <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Tim/Brian,
I was thinking last night and would actually like to move the new Image service to the FR server s.L. c. 4.sec. 7.cl.26. We have a route in place already from both PAA and Internal web to that server. I would just need to know what port to run tomcat on. This would also work for the Thompson Reuters adapter as well. Let me know what you guys think.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK

520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Monday, February 4, 2019 11:17 AM
To: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: LRP network ideas?

Brian/Tim,
Nick is almost done with the new LPR service that will remove the images from the database and have a tomcat app that host the images for a return to the UI. What I need to know:

1. The Migration will sit on the migration server and needs access to the LPR database to pull out the metadata and create the URL for the Image links.
2. The new service is going to be hosted in Tomcat, so this service will need access to the LPR database for images and both application servers need to be able to query this tomcat instance. I just need to know where to put it, I can host it on both severs or if we can set it up

on the internal server and have a firewall rule that will allow the DMZ server to talk to the internal server. Let me know if you would like to have a call on this. I have attached a rough network diagram for visual reference.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

<MSP agency ORI.xlsx>

From: Egnitz, Brian (POL)
To: Silva, Kyra (POL)
Subject: FW: MassPort LPR Cameras
Date: Thursday, April 9, 2020 4:06:00 PM
Attachments: SierraQuoteForMassPort.pdf

Hi Kyra,

Can you please see below and attached. Let me know if you have any questions.

Thanks, Brian

-----Original Message-----
From: Quinn, Dermot (POL)
Sent: Thursday, April 9, 2020 2:00 PM
To: Egnitz, Brian (POL)
Cc: Warren, Rosemary (POL)
Subject: RE: MassPort LPR Cameras

This is to allow the Massport ALPR cameras to write to thestate ALPR server in Chelsea. Approved at DHS. Please forward to Kyra Silva in Fiscal for funding.

Lieutenant Colonel Dermot J. Quinn #1765
Division Commander
Division of Homeland Security & Preparedness
Massachusetts State Police

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Thursday, April 9, 2020 1:58 PM
To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: RE: MassPort LPR Cameras

Do you know if this was moved on? We need it for the MassPort modem project.

-----Original Message-----
From: Egnitz, Brian (POL)
Sent: Tuesday, March 10, 2020 10:52 AM
To: Quinn, Dermot (POL)
Subject: FW: MassPort LPR Cameras

Hi LTC.,

Can we order this equipment for the MassPort project?

Thanks, Brian

-----Original Message-----
From: Slater, James (CHS)
Sent: Tuesday, March 10, 2020 10:26 AM

To: Egnitz, Brian (POL)
Subject: RE: MassPort LPR Cameras

Hi, Brian!

This needs to go through MSP fiscal. They need to enter the purchase in OPAS.

Jim

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Tuesday, March 10, 2020 08:06
To: Slater, James (CHS) <james.slater@mass.gov>
Subject: RE: MassPort LPR Cameras

Is this something you can order or does it need to go through MSP?

-----Original Message-----
From: Slater, James (CHS)
Sent: Monday, March 9, 2020 10:36 AM
To: Egnitz, Brian (POL)
Subject: RE: MassPort LPR Cameras

Thanks, Brian...I will check with TSS.

Jim

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Monday, March 9, 2020 10:29
To: Slater, James (CHS) <james.slater@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: RE: MassPort LPR Cameras

Thanks Jim,

I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need 6 sierra wireless AC adapters and 12 antennas. I have reached out to BCM for a quote.

I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.

I plan to cut one sector (5-6 cameras per sector) over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?

-Brian

-----Original Message-----
From: Slater, James (CHS)
Sent: Friday, March 6, 2020 1:43 PM
To: Egnitz, Brian (POL)
Cc: Quinn, Dermot (POL)
Subject: RE: MassPort LPR Cameras

Hi, Brian!

I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.

So, assuming you move forward with this, who would actually make this happen?

Thanks.

Jim

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Wednesday, March 4, 2020 17:53
To: Slater, James (CHS) <james.slater@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: Re: MassPort LPR Cameras

Hi Jim,

Regarding the Massport cameras; in the early days of AVL we installed 39 Sierra wireless modem‘s in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don’t we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn’t have to do any firewall work either because they have a 166. and communicate like all of the MDT‘s . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.

We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.

Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.

> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>
> Thank you sir
>
> Major Charles W. Atchison III
> Troop F Commander
> Massachusetts State Police
> Director of Aviation Security
> 2 Service Road
> East Boston, Ma 02128
> Office: 617-568-7555
> Cell: 508-[redacted]
>
>
> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>
> All,
> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>
> Thanks
>
> CW

>
> From: Quinn, Dermot (POL)
> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
> Sent: Monday, February 10, 2020 10:31 AM
> To: Egnitz, Brian (POL)
> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
> Slater, James (CHS)
> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
> Robert (EOTSS)
> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
> Warmington, Scott (POL)
> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
> .us>>; Peek, Brian T. (EOTSS)
> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
> Timothy (EPS)
> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
> Michalski, Maria (EPS)
> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
> Christopher (POL)
> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
> Hughes, Sean M. (EOTSS)
> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
> Atchison, Charles (POL)
> <catchison@massport.com<mailto:catchison@massport.com>>
> Subject: RE: MassPort LPR Cameras
>
> Good Morning,
>
> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>
> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>
> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>
> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>

> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>
> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>
> I can't overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security's technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>
> Respectfully,
>
>
> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
> of Homeland Security & Preparedness Massachusetts State Police
> <image006.png>
>
>
>
>
> From: Egnitz, Brian (POL)
> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
> Sent: Friday, January 17, 2020 1:10 PM
> To: Slater, James (CHS)
> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
> Cc: Quinn, Dermot (POL)
> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
> Guerriero, Robert (EOTSS)
> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
> Brian T. (EOTSS)
> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
> Timothy (EPS)
> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
> Maria (EPS)
> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
> Subject: RE: MassPort LPR Cameras
>
> Hi Jim,
>
> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>
> -Brian
>
>
> From: Egnitz, Brian (POL)
> Sent: Monday, January 6, 2020 1:33 PM
> To: Slater, James (CHS)

> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
> Crary
> Subject: RE: MassPort LPR Cameras
>
> Hi Jim,
>
> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>
> Thanks Brian
>
>
> From: John Tedona [mailto:jtedona@neology.net]
> Sent: Monday, December 9, 2019 4:55 PM
> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS); Slater, James (CHS)
> Subject: RE: MassPort LPR Cameras
>
> Alex,
>
> I can be available most anytime tomorrow for a call.
>
>
> Regards,
>
> John Tedona
> PIPS TECHNOLOGY - A Neology Business
> Sales Manager
> 12760 Danielson Ct. Suite A
> Poway, CA 92064
> Phone: 201-841-6237
> Email: jtedona@neology.net<mailto:jtedona@neology.net>
> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ
> U2sB_fmM6g&e=>
>
>
> From: Chute, Alexander
> <AChute@massport.com<mailto:AChute@massport.com>>
> Sent: Monday, December 9, 2019 4:38 PM
> To: Egnitz, Brian (POL)
> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
> <pcrary@neology.net<mailto:pcrary@neology.net>>
> Cc: Guerriero, Robert (MASSIT)
> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
> Peek, Brian T. (EOTSS)
> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,

> Timothy (EPS)
> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
> Slater III, James F (CHS)
> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
> Subject: RE: MassPort LPR Cameras
>
> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>
> Hello All,
>
> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>
> Respectfully,
>
> ~Alex
>
>
> <image007.png>
>
> Alexander B. Chute
> Program Manager, Public Safety Systems Massachusetts Port Authority
> Cell: [redacted]
> Office: 617.568.5942
> achute@massport.com<mailto:achute@massport.com>
>
> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>
>
>
> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
> Sent: Monday, November 18, 2019 3:26 PM
> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
> pcrary@neology.net<mailto:pcrary@neology.net>
> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
> Subject: RE: MassPort LPR Cameras
>
> Hi John, Peter
>
> Any issues with moving Massports cameras to the Chelsea DB?
>
> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>
> The current app server
> <image008.png>
>
> Current DB server
>
> <image009.png>

> <image010.png>
>
> Our current reads by month for about 66 active cameras
>
> Year
>
> Month
>
> Day
>
> Month Name
>
> Reads Count
>
> 2019
>
> 11
>
> 1
>
> November
>
> 495,113
>
> 2019
>
> 11
>
> 2
>
> November
>
> 472,907
>
> 2019
>
> 11
>
> 3
>
> November
>
> 384,409
>
> 2019
>
> 11
>
> 4
>
> November
>
> 411,440
>
> 2019
>
> 11

>
> 5
>
> November
>
> 434,085
>
> 2019
>
> 11
>
> 6
>
> November
>
> 495,537
>
> 2019
>
> 11
>
> 7
>
> November
>
> 444,123
>
> 2019
>
> 11
>
> 8
>
> November
>
> 542,492
>
> 2019
>
> 11
>
> 9
>
> November
>
> 443,463
>
> 2019
>
> 11
>
> 10
>
> November
>
> 389,514
>

> 2019
>
> 11
>
> 11
>
> November
>
> 362,548
>
> 2019
>
> 11
>
> 12
>
> November
>
> 236,539
>
>
>
>
>
>
> From: Chute, Alexander [mailto:AChute@massport.com]
> Sent: Wednesday, November 13, 2019 2:49 PM
> To: Egnitz, Brian (POL)
> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS)
> Subject: RE: MassPort LPR Cameras
>
> These stats are from the 18 active cameras we have in the system for this month:
>
> <image011.png>
>
> ~Alex
>
>
> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
> Sent: Tuesday, November 12, 2019 5:28 PM
> To: Chute, Alexander
> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS)
> Subject: RE: MassPort LPR Cameras
>
> Hi Alex,
>
> Can you please provide the updated reads per day? Previously you were interested in sharing 6 cameras at approximately 75,000 reads per day.
>
> Here is the P492 confi I mentioned.
>
> Set host to boss [redacted]
> Set image [redacted]
> Set number of [redacted]
> Set Ping interval [redacted]
> Set udp ping [redacted]

> Set ping wait time [redacted]
> Set security [redacted]
>
> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>
> -Brian
>
>
>
> From: Chute, Alexander [mailto:AChute@massport.com]
> Sent: Tuesday, November 12, 2019 2:08 PM
> To: Egnitz, Brian (POL)
> Subject: MassPort LPR Cameras
>
> Brian,
>
> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the Troop F building. I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the roadway cameras are fed to 2 primary network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have 18 cameras in production, with another 19 scheduled to come online within the next two months. I anticipate this number growing to approximately 50 fixed cameras within our campus over the next year. Let me know what you think the appropriate next steps would be.
>
> Respectfully,
>
> ~Alex
>
> <image007.png>
>
> Alexander B. Chute
> Program Manager, Public Safety Systems Massachusetts Port Authority
> Cell: [redacted]
> Office: 617.568.5942
> achute@massport.com<mailto:achute@massport.com>
>
> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>

To: Silva, Kyra (POL)
Subject: FW: MassPort LPR Cameras
Date: Thursday, April 9, 2020 3:52:35 PM
Attachments: SierraQuoteForMassPort.pdf

Hi Kyra,

-----Original Message-----
From: Quinn, Dermot (POL)
Sent: Thursday, April 9, 2020 2:00 PM
To: Egnitz, Brian (POL)
Cc: Warren, Rosemary (POL)
Subject: RE: MassPort LPR Cameras

This is to allow the Massport ALPR cameras to write to thestate ALPR server in Chelsea. Approved at DHS. Please forward to Kyra Silva in Fiscal for funding.

Lieutenant Colonel Dermot J. Quinn #1765
Division Commander
Division of Homeland Security & Preparedness
Massachusetts State Police

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Thursday, April 9, 2020 1:58 PM
To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: RE: MassPort LPR Cameras

Do you know if this was moved on? We need it for the MassPort modem project.

-----Original Message-----
From: Egnitz, Brian (POL)
Sent: Tuesday, March 10, 2020 10:52 AM
To: Quinn, Dermot (POL)
Subject: FW: MassPort LPR Cameras

Hi LTC.,

Can we order this equipment for the MassPort project?

Thanks, Brian

-----Original Message-----
From: Slater, James (CHS)
Sent: Tuesday, March 10, 2020 10:26 AM
To: Egnitz, Brian (POL)
Subject: RE: MassPort LPR Cameras

Hi, Brian!

This needs to go through MSP fiscal. They need to enter the purchase in OPAS.

Jim

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Tuesday, March 10, 2020 08:06
To: Slater, James (CHS) <james.slater@mass.gov>
Subject: RE: MassPort LPR Cameras

Is this something you can order or does it need to go through MSP?

-----Original Message-----
From: Slater, James (CHS)
Sent: Monday, March 9, 2020 10:36 AM
To: Egnitz, Brian (POL)
Subject: RE: MassPort LPR Cameras

Thanks, Brian...I will check with TSS.

Jim

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Monday, March 9, 2020 10:29
To: Slater, James (CHS) <james.slater@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: RE: MassPort LPR Cameras

Thanks Jim,

I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need 6 sierra wireless AC adapters and 12 antennas. I have reached out to BCM for a quote.

I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.

I plan to cut one sector (5-6 cameras per sector) over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?

-Brian

-----Original Message-----
From: Slater, James (CHS)
Sent: Friday, March 6, 2020 1:43 PM
To: Egnitz, Brian (POL)
Cc: Quinn, Dermot (POL)
Subject: RE: MassPort LPR Cameras

Hi, Brian!

I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.

So, assuming you move forward with this, who would actually make this happen?

Thanks.

Jim

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Wednesday, March 4, 2020 17:53
To: Slater, James (CHS) <james.slater@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: Re: MassPort LPR Cameras

Hi Jim,

Regarding the Massport cameras; in the early days of AVL we installed 39 Sierra wireless modem‘s in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don’t we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn’t have to do any firewall work either because they have a 166. and communicate like all of the MDT‘s . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.

We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.

Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.

> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>
> Thank you sir
>
> Major Charles W. Atchison III
> Troop F Commander
> Massachusetts State Police
> Director of Aviation Security
> 2 Service Road
> East Boston, Ma 02128
> Office: 617-568-7555
> Cell: 508-[redacted]
>
>
> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>
> All,
> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>
> Thanks
>
> CW
>
> From: Quinn, Dermot (POL)
> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>

> Sent: Monday, February 10, 2020 10:31 AM
> To: Egnitz, Brian (POL)
> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
> Slater, James (CHS)
> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
> Robert (EOTSS)
> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
> Warmington, Scott (POL)
> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
> .us>>; Peek, Brian T. (EOTSS)
> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
> Timothy (EPS)
> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
> Michalski, Maria (EPS)
> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
> Christopher (POL)
> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
> Hughes, Sean M. (EOTSS)
> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
> Atchison, Charles (POL)
> <catchison@massport.com<mailto:catchison@massport.com>>
> Subject: RE: MassPort LPR Cameras
>
> Good Morning,
>
> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>
> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>
> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>
> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>
> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread

in case I have misstated their intent.
>
> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>
> I can't overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security's technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>
> Respectfully,
>
>
> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
> of Homeland Security & Preparedness Massachusetts State Police
> <image006.png>
>
>
>
>
> From: Egnitz, Brian (POL)
> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
> Sent: Friday, January 17, 2020 1:10 PM
> To: Slater, James (CHS)
> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
> Cc: Quinn, Dermot (POL)
> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
> Guerriero, Robert (EOTSS)
> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
> Brian T. (EOTSS)
> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
> Timothy (EPS)
> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
> Maria (EPS)
> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
> Subject: RE: MassPort LPR Cameras
>
> Hi Jim,
>
> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>
> -Brian
>
>
> From: Egnitz, Brian (POL)
> Sent: Monday, January 6, 2020 1:33 PM
> To: Slater, James (CHS)
> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
> Crary

> Subject: RE: MassPort LPR Cameras
>
> Hi Jim,
>
> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>
> Thanks Brian
>
>
> From: John Tedona [mailto:jtedona@neology.net]
> Sent: Monday, December 9, 2019 4:55 PM
> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS); Slater, James (CHS)
> Subject: RE: MassPort LPR Cameras
>
> Alex,
>
> I can be available most anytime tomorrow for a call.
>
>
> Regards,
>
> John Tedona
> PIPS TECHNOLOGY - A Neology Business
> Sales Manager
> 12760 Danielson Ct. Suite A
> Poway, CA 92064
> Phone: 201-841-6237
> Email: jtedona@neology.net<mailto:jtedona@neology.net>
> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ
> U2sB_fmM6g&e=>
>
>
> From: Chute, Alexander
> <AChute@massport.com<mailto:AChute@massport.com>>
> Sent: Monday, December 9, 2019 4:38 PM
> To: Egnitz, Brian (POL)
> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
> <pcrary@neology.net<mailto:pcrary@neology.net>>
> Cc: Guerriero, Robert (MASSIT)
> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
> Peek, Brian T. (EOTSS)
> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
> Timothy (EPS)
> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
> Slater III, James F (CHS)

> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
> Subject: RE: MassPort LPR Cameras
>
> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>
> Hello All,
>
> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>
> Respectfully,
>
> ~Alex
>
>
> <image007.png>
>
> Alexander B. Chute
> Program Manager, Public Safety Systems Massachusetts Port Authority
> Cell: [redacted]
> Office: 617.568.5942
> achute@massport.com<mailto:achute@massport.com>
>
> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>
>
>
> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
> Sent: Monday, November 18, 2019 3:26 PM
> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
> pcrary@neology.net<mailto:pcrary@neology.net>
> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
> Subject: RE: MassPort LPR Cameras
>
> Hi John, Peter
>
> Any issues with moving Massports cameras to the Chelsea DB?
>
> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>
> The current app server
> <image008.png>
>
> Current DB server
>
> <image009.png>
> <image010.png>
>
> Our current reads by month for about 66 active cameras

>
> Year
>
> Month
>
> Day
>
> Month Name
>
> Reads Count
>
> 2019
>
> 11
>
> 1
>
> November
>
> 495,113
>
> 2019
>
> 11
>
> 2
>
> November
>
> 472,907
>
> 2019
>
> 11
>
> 3
>
> November
>
> 384,409
>
> 2019
>
> 11
>
> 4
>
> November
>
> 411,440
>
> 2019
>
> 11
>
> 5
>

> November
>
> 434,085
>
> 2019
>
> 11
>
> 6
>
> November
>
> 495,537
>
> 2019
>
> 11
>
> 7
>
> November
>
> 444,123
>
> 2019
>
> 11
>
> 8
>
> November
>
> 542,492
>
> 2019
>
> 11
>
> 9
>
> November
>
> 443,463
>
> 2019
>
> 11
>
> 10
>
> November
>
> 389,514
>
> 2019
>
> 11

>
> 11
>
> November
>
> 362,548
>
> 2019
>
> 11
>
> 12
>
> November
>
> 236,539
>
>
>
>
>
> From: Chute, Alexander [mailto:AChute@massport.com]
> Sent: Wednesday, November 13, 2019 2:49 PM
> To: Egnitz, Brian (POL)
> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS)
> Subject: RE: MassPort LPR Cameras
>
> These stats are from the 18 active cameras we have in the system for this month:
>
> <image011.png>
>
> ~Alex
>
>
> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
> Sent: Tuesday, November 12, 2019 5:28 PM
> To: Chute, Alexander
> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS)
> Subject: RE: MassPort LPR Cameras
>
> Hi Alex,
>
> Can you please provide the updated reads per day? Previously you were interested in sharing 6 cameras at approximately 75,000 reads per day.
>
> Here is the P492 confi I mentioned.
>
> Set host to boss [redacted]
> Set image [redacted]
> Set number of [redacted]
> Set Ping interval [redacted]
> Set udp ping [redacted]
> Set ping wait time [redacted]
> Set security [redacted]
>

> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>
> -Brian
>
>
>
> From: Chute, Alexander [mailto:AChute@massport.com]
> Sent: Tuesday, November 12, 2019 2:08 PM
> To: Egnitz, Brian (POL)
> Subject: MassPort LPR Cameras
>
> Brian,
>
> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the Troop F building. I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the roadway cameras are fed to 2 primary network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have 18 cameras in production, with another 19 scheduled to come online within the next two months. I anticipate this number growing to approximately 50 fixed cameras within our campus over the next year. Let me know what you think the appropriate next steps would be.
>
> Respectfully,
>
> ~Alex
>
> <image007.png>
>
> Alexander B. Chute
> Program Manager, Public Safety Systems Massachusetts Port Authority
> Cell: [redacted]
> Office: 617.568.5942
> achute@massport.com<mailto:achute@massport.com>
>
> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>

From: Small, Michelle (POL)
To: Harney, Michael
Subject: FW: MassPort LPR Cameras
Date: Tuesday, March 10, 2020 8:47:00 PM
Attachments: SierraQuoteForMassPort.pdf

FYI

-----Original Message-----
From: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Sent: Tuesday, March 10, 2020 11:29 AM
To: Small, Michelle (POL) <Michelle.E.Small@pol.state.ma.us>; Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>; Slater, James (CHS) <james.slater@mass.gov>
Cc: Mason, Christopher (POL) <Chris.Mason@pol.state.ma.us>; Warmington, Scott (POL) <Scott.Warmington@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>; Shaw, Harold <HShaw@massport.com>; Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>; Ball, Richard (POL) <Richard.Ball@pol.state.ma.us>
Subject: FW: MassPort LPR Cameras

Michelle and Kyra,

This purchase request is for equipment to allow Mass Port Sierra Wireless modems to communicate directly with the existing ALPR Boss server in Chelsea. This is the fastest way to bring the Massport LPR cameras on line. EOTSS and EOPSS are OK with this solution as is Major Deb Ryan, the CO at Troop F.

As you can see from the thread, this has been going on for some time. I think we can close it out with this small purchase.

This does not resolve the replacement of the existing ALPR equipment that we discussed at Command Staff yesterday. That is a different issue.

Thanks

Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division of Homeland Security & Preparedness Massachusetts State Police

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Tuesday, March 10, 2020 10:52 AM
To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: FW: MassPort LPR Cameras

Hi LTC.,

Can we order this equipment for the MassPort project?

Thanks, Brian

-----Original Message-----
From: Slater, James (CHS)

Sent: Tuesday, March 10, 2020 10:26 AM
To: Egnitz, Brian (POL)
Subject: RE: MassPort LPR Cameras

Hi, Brian!

This needs to go through MSP fiscal. They need to enter the purchase in OPAS.

Jim

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Tuesday, March 10, 2020 08:06
To: Slater, James (CHS) <james.slater@mass.gov>
Subject: RE: MassPort LPR Cameras

Is this something you can order or does it need to go through MSP?

-----Original Message-----
From: Slater, James (CHS)
Sent: Monday, March 9, 2020 10:36 AM
To: Egnitz, Brian (POL)
Subject: RE: MassPort LPR Cameras

Thanks, Brian...I will check with TSS.

Jim

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Monday, March 9, 2020 10:29
To: Slater, James (CHS) <james.slater@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: RE: MassPort LPR Cameras

Thanks Jim,

I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need 6 sierra wireless AC adapters and 12 antennas. I have reached out to BCM for a quote.

I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.

I plan to cut one sector (5-6 cameras per sector) over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?

-Brian

-----Original Message-----
From: Slater, James (CHS)
Sent: Friday, March 6, 2020 1:43 PM
To: Egnitz, Brian (POL)
Cc: Quinn, Dermot (POL)
Subject: RE: MassPort LPR Cameras

Hi, Brian!

I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.

So, assuming you move forward with this, who would actually make this happen?

Thanks.

Jim

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Wednesday, March 4, 2020 17:53
To: Slater, James (CHS) <james.slater@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: Re: MassPort LPR Cameras

Hi Jim,

Regarding the Massport cameras; in the early days of AVL we installed 39 Sierra wireless modem‘s in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don’t we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn’t have to do any firewall work either because they have a 166. and communicate like all of the MDT‘s . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.

We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.

Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.

> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>
> Thank you sir
>
> Major Charles W. Atchison III
> Troop F Commander
> Massachusetts State Police
> Director of Aviation Security
> 2 Service Road
> East Boston, Ma 02128
> Office: 617-568-7555
> Cell: 508-[redacted]
>
>
> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>
> All,
> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>
> Thanks
>

> CW
>
> From: Quinn, Dermot (POL)
> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
> Sent: Monday, February 10, 2020 10:31 AM
> To: Egnitz, Brian (POL)
> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
> Slater, James (CHS)
> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
> Robert (EOTSS)
> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
> Warmington, Scott (POL)
> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
> .us>>; Peek, Brian T. (EOTSS)
> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
> Timothy (EPS)
> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
> Michalski, Maria (EPS)
> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
> Christopher (POL)
> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
> Hughes, Sean M. (EOTSS)
> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
> Atchison, Charles (POL)
> <catchison@massport.com<mailto:catchison@massport.com>>
> Subject: RE: MassPort LPR Cameras
>
> Good Morning,
>
> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>
> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>
> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>
> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.

>
> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>
> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>
> I can't overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security's technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>
> Respectfully,
>
>
> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
> of Homeland Security & Preparedness Massachusetts State Police
> <image006.png>
>
>
>
>
> From: Egnitz, Brian (POL)
> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
> Sent: Friday, January 17, 2020 1:10 PM
> To: Slater, James (CHS)
> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
> Cc: Quinn, Dermot (POL)
> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
> Guerriero, Robert (EOTSS)
> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
> Brian T. (EOTSS)
> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
> Timothy (EPS)
> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
> Maria (EPS)
> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
> Subject: RE: MassPort LPR Cameras
>
> Hi Jim,
>
> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>
> -Brian
>
>
> From: Egnitz, Brian (POL)
> Sent: Monday, January 6, 2020 1:33 PM

> To: Slater, James (CHS)
> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
> Crary
> Subject: RE: MassPort LPR Cameras
>
> Hi Jim,
>
> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>
> Thanks Brian
>
>
> From: John Tedona [mailto:jtedona@neology.net]
> Sent: Monday, December 9, 2019 4:55 PM
> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS); Slater, James (CHS)
> Subject: RE: MassPort LPR Cameras
>
> Alex,
>
> I can be available most anytime tomorrow for a call.
>
>
> Regards,
>
> John Tedona
> PIPS TECHNOLOGY - A Neology Business
> Sales Manager
> 12760 Danielson Ct. Suite A
> Poway, CA 92064
> Phone: 201-841-6237
> Email: jtedona@neology.net<mailto:jtedona@neology.net>
> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ
> U2sB_fmM6g&e=>
>
>
> From: Chute, Alexander
> <AChute@massport.com<mailto:AChute@massport.com>>
> Sent: Monday, December 9, 2019 4:38 PM
> To: Egnitz, Brian (POL)
> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
> <pcrary@neology.net<mailto:pcrary@neology.net>>
> Cc: Guerriero, Robert (MASSIT)
> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
> Peek, Brian T. (EOTSS)

> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
> Timothy (EPS)
> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
> Slater III, James F (CHS)
> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
> Subject: RE: MassPort LPR Cameras
>
> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>
> Hello All,
>
> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>
> Respectfully,
>
> ~Alex
>
>
> <image007.png>
>
> Alexander B. Chute
> Program Manager, Public Safety Systems Massachusetts Port Authority
> Cell: [redacted]
> Office: 617.568.5942
> achute@massport.com<mailto:achute@massport.com>
>
> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>
>
>
> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
> Sent: Monday, November 18, 2019 3:26 PM
> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
> pcrary@neology.net<mailto:pcrary@neology.net>
> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
> Subject: RE: MassPort LPR Cameras
>
> Hi John, Peter
>
> Any issues with moving Massports cameras to the Chelsea DB?
>
> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>
> The current app server
> <image008.png>
>
> Current DB server
>

> <image009.png>
> <image010.png>
>
> Our current reads by month for about 66 active cameras
>
> Year
>
> Month
>
> Day
>
> Month Name
>
> Reads Count
>
> 2019
>
> 11
>
> 1
>
> November
>
> 495,113
>
> 2019
>
> 11
>
> 2
>
> November
>
> 472,907
>
> 2019
>
> 11
>
> 3
>
> November
>
> 384,409
>
> 2019
>
> 11
>
> 4
>
> November
>
> 411,440
>
> 2019
>

> 11
>
> 5
>
> November
>
> 434,085
>
> 2019
>
> 11
>
> 6
>
> November
>
> 495,537
>
> 2019
>
> 11
>
> 7
>
> November
>
> 444,123
>
> 2019
>
> 11
>
> 8
>
> November
>
> 542,492
>
> 2019
>
> 11
>
> 9
>
> November
>
> 443,463
>
> 2019
>
> 11
>
> 10
>
> November
>
> 389,514

>
> 2019
>
> 11
>
> 11
>
> November
>
> 362,548
>
> 2019
>
> 11
>
> 12
>
> November
>
> 236,539
>
>
>
>
>
>
> From: Chute, Alexander [mailto:AChute@massport.com]
> Sent: Wednesday, November 13, 2019 2:49 PM
> To: Egnitz, Brian (POL)
> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS)
> Subject: RE: MassPort LPR Cameras
>
> These stats are from the 18 active cameras we have in the system for this month:
>
> <image011.png>
>
> ~Alex
>
>
> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
> Sent: Tuesday, November 12, 2019 5:28 PM
> To: Chute, Alexander
> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS)
> Subject: RE: MassPort LPR Cameras
>
> Hi Alex,
>
> Can you please provide the updated reads per day? Previously you were interested in sharing 6 cameras at approximately 75,000 reads per day.
>
> Here is the P492 confi I mentioned.
>
> Set host to boss [redacted]
> Set image [redacted]
> Set number of [redacted]
> Set Ping interval [redacted]

> Set udp ping [redacted]
> Set ping wait time [redacted]
> Set security [redacted]
>
> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>
> -Brian
>
>
>
> From: Chute, Alexander [mailto:AChute@massport.com]
> Sent: Tuesday, November 12, 2019 2:08 PM
> To: Egnitz, Brian (POL)
> Subject: MassPort LPR Cameras
>
> Brian,
>
> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the Troop F building. I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the roadway cameras are fed to 2 primary network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have 18 cameras in production, with another 19 scheduled to come online within the next two months. I anticipate this number growing to approximately 50 fixed cameras within our campus over the next year. Let me know what you think the appropriate next steps would be.
>
> Respectfully,
>
> ~Alex
>
> <image007.png>
>
> Alexander B. Chute
> Program Manager, Public Safety Systems Massachusetts Port Authority
> Cell: [redacted]
> Office: 617.568.5942
> achute@massport.com<mailto:achute@massport.com>
>
> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>

From: Quinn, Dermot (POL)
To: Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS)
Cc: Mason, Christopher (POL); Warmington, Scott (POL); Egnitz, Brian (POL); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL)
Subject: FW: MassPort LPR Cameras
Date: Tuesday, March 10, 2020 11:28:35 AM
Attachments: SierraQuoteForMassPort.pdf

Michelle and Kyra,

This purchase request is for equipment to allow Mass Port Sierra Wireless modems to communicate directly with the existing ALPR Boss server in Chelsea. This is the fastest way to bring the Massport LPR cameras on line. EOTSS and EOPSS are OK with this solution as is Major Deb Ryan, the CO at Troop F.

As you can see from the thread, this has been going on for some time. I think we can close it out with this small purchase.

This does not resolve the replacement of the existing ALPR equipment that we discussed at Command Staff yesterday. That is a different issue.

Thanks

Lieutenant Colonel Dermot J. Quinn #1765
Division Commander
Division of Homeland Security & Preparedness
Massachusetts State Police

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Tuesday, March 10, 2020 10:52 AM
To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: FW: MassPort LPR Cameras

Hi LTC.,

Can we order this equipment for the MassPort project?

Thanks, Brian

-----Original Message-----
From: Slater, James (CHS)
Sent: Tuesday, March 10, 2020 10:26 AM
To: Egnitz, Brian (POL)
Subject: RE: MassPort LPR Cameras

Hi, Brian!

This needs to go through MSP fiscal. They need to enter the purchase in OPAS.

Jim

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Tuesday, March 10, 2020 08:06
To: Slater, James (CHS) <james.slater@mass.gov>
Subject: RE: MassPort LPR Cameras

Is this something you can order or does it need to go through MSP?

-----Original Message-----
From: Slater, James (CHS)
Sent: Monday, March 9, 2020 10:36 AM
To: Egnitz, Brian (POL)
Subject: RE: MassPort LPR Cameras

Thanks, Brian...I will check with TSS.

Jim

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Monday, March 9, 2020 10:29
To: Slater, James (CHS) <james.slater@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: RE: MassPort LPR Cameras

Thanks Jim,

I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need 6 sierra wireless AC adapters and 12 antennas. I have reached out to BCM for a quote.

I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.

I plan to cut one sector (5-6 cameras per sector) over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?

-Brian

-----Original Message-----
From: Slater, James (CHS)
Sent: Friday, March 6, 2020 1:43 PM
To: Egnitz, Brian (POL)
Cc: Quinn, Dermot (POL)
Subject: RE: MassPort LPR Cameras

Hi, Brian!

I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.

So, assuming you move forward with this, who would actually make this happen?

Thanks.

Jim

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Wednesday, March 4, 2020 17:53
To: Slater, James (CHS) <james.slater@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: Re: MassPort LPR Cameras

Hi Jim,

Regarding the Massport cameras; in the early days of AVL we installed 39 Sierra wireless modem‘s in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don’t we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn’t have to do any firewall work either because they have a 166. and communicate like all of the MDT‘s . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.

We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.

Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.

> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>
> Thank you sir
>
> Major Charles W. Atchison III
> Troop F Commander
> Massachusetts State Police
> Director of Aviation Security
> 2 Service Road
> East Boston, Ma 02128
> Office: 617-568-7555
> Cell: 508-[redacted]
>
>
> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>
> All,
> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>
> Thanks
>
> CW
>
> From: Quinn, Dermot (POL)
> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
> Sent: Monday, February 10, 2020 10:31 AM
> To: Egnitz, Brian (POL)
> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
> Slater, James (CHS)
> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
> Robert (EOTSS)

> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
> Warmington, Scott (POL)
> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
> .us>>; Peek, Brian T. (EOTSS)
> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
> Timothy (EPS)
> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
> Michalski, Maria (EPS)
> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
> Christopher (POL)
> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
> Hughes, Sean M. (EOTSS)
> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
> Atchison, Charles (POL)
> <catchison@massport.com<mailto:catchison@massport.com>>
> Subject: RE: MassPort LPR Cameras
>
> Good Morning,
>
> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>
> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>
> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>
> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>
> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>
> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.

>
> I can't overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security's technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>
> Respectfully,
>
>
> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
> of Homeland Security & Preparedness Massachusetts State Police
> <image006.png>
>
>
>
>
> From: Egnitz, Brian (POL)
> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
> Sent: Friday, January 17, 2020 1:10 PM
> To: Slater, James (CHS)
> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
> Cc: Quinn, Dermot (POL)
> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
> Guerriero, Robert (EOTSS)
> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
> Brian T. (EOTSS)
> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
> Timothy (EPS)
> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
> Maria (EPS)
> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
> Subject: RE: MassPort LPR Cameras
>
> Hi Jim,
>
> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>
> -Brian
>
>
> From: Egnitz, Brian (POL)
> Sent: Monday, January 6, 2020 1:33 PM
> To: Slater, James (CHS)
> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
> Crary
> Subject: RE: MassPort LPR Cameras
>
> Hi Jim,
>
> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network

presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>
> Thanks Brian
>
>
> From: John Tedona [mailto:jtedona@neology.net]
> Sent: Monday, December 9, 2019 4:55 PM
> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS); Slater, James (CHS)
> Subject: RE: MassPort LPR Cameras
>
> Alex,
>
> I can be available most anytime tomorrow for a call.
>
>
> Regards,
>
> John Tedona
> PIPS TECHNOLOGY - A Neology Business
> Sales Manager
> 12760 Danielson Ct. Suite A
> Poway, CA 92064
> Phone: 201-841-6237
> Email: jtedona@neology.net<mailto:jtedona@neology.net>
> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ
> U2sB_fmM6g&e=>
>
>
> From: Chute, Alexander
> <AChute@massport.com<mailto:AChute@massport.com>>
> Sent: Monday, December 9, 2019 4:38 PM
> To: Egnitz, Brian (POL)
> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
> <pcrary@neology.net<mailto:pcrary@neology.net>>
> Cc: Guerriero, Robert (MASSIT)
> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
> Peek, Brian T. (EOTSS)
> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
> Timothy (EPS)
> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
> Slater III, James F (CHS)
> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
> Subject: RE: MassPort LPR Cameras
>
> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>

> Hello All,
>
> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>
> Respectfully,
>
> ~Alex
>
>
> <image007.png>
>
> Alexander B. Chute
> Program Manager, Public Safety Systems Massachusetts Port Authority
> Cell: [redacted]
> Office: 617.568.5942
> achute@massport.com<mailto:achute@massport.com>
>
> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>
>
>
> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
> Sent: Monday, November 18, 2019 3:26 PM
> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
> pcrary@neology.net<mailto:pcrary@neology.net>
> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
> Subject: RE: MassPort LPR Cameras
>
> Hi John, Peter
>
> Any issues with moving Massports cameras to the Chelsea DB?
>
> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>
> The current app server
> <image008.png>
>
> Current DB server
>
> <image009.png>
> <image010.png>
>
> Our current reads by month for about 66 active cameras
>
> Year
>
> Month
>
> Day

>
> Month Name
>
> Reads Count
>
> 2019
>
> 11
>
> 1
>
> November
>
> 495,113
>
> 2019
>
> 11
>
> 2
>
> November
>
> 472,907
>
> 2019
>
> 11
>
> 3
>
> November
>
> 384,409
>
> 2019
>
> 11
>
> 4
>
> November
>
> 411,440
>
> 2019
>
> 11
>
> 5
>
> November
>
> 434,085
>
> 2019
>

> 11
>
> 6
>
> November
>
> 495,537
>
> 2019
>
> 11
>
> 7
>
> November
>
> 444,123
>
> 2019
>
> 11
>
> 8
>
> November
>
> 542,492
>
> 2019
>
> 11
>
> 9
>
> November
>
> 443,463
>
> 2019
>
> 11
>
> 10
>
> November
>
> 389,514
>
> 2019
>
> 11
>
> 11
>
> November
>
> 362,548

>
> 2019
>
> 11
>
> 12
>
> November
>
> 236,539
>
>
>
>
>
> From: Chute, Alexander [mailto:AChute@massport.com]
> Sent: Wednesday, November 13, 2019 2:49 PM
> To: Egnitz, Brian (POL)
> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS)
> Subject: RE: MassPort LPR Cameras
>
> These stats are from the 18 active cameras we have in the system for this month:
>
> <image011.png>
>
> ~Alex
>
>
> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
> Sent: Tuesday, November 12, 2019 5:28 PM
> To: Chute, Alexander
> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS)
> Subject: RE: MassPort LPR Cameras
>
> Hi Alex,
>
> Can you please provide the updated reads per day? Previously you were interested in sharing 6 cameras at approximately 75,000 reads per day.
>
> Here is the P492 confi I mentioned.
>
> Set host to boss [redacted]
> Set image [redacted]
> Set number of [redacted]
> Set Ping interval [redacted]
> Set udp ping [redacted]
> Set ping wait time [redacted]
> Set security [redacted]
>
> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>
> -Brian

>
>
>
> From: Chute, Alexander [mailto:AChute@massport.com]
> Sent: Tuesday, November 12, 2019 2:08 PM
> To: Egnitz, Brian (POL)
> Subject: MassPort LPR Cameras
>
> Brian,
>
> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the Troop F building. I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the roadway cameras are fed to 2 primary network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have 18 cameras in production, with another 19 scheduled to come online within the next two months. I anticipate this number growing to approximately 50 fixed cameras within our campus over the next year. Let me know what you think the appropriate next steps would be.
>
> Respectfully,
>
> ~Alex
>
> <image007.png>
>
> Alexander B. Chute
> Program Manager, Public Safety Systems Massachusetts Port Authority
> Cell: [redacted]
> Office: 617.568.5942
> achute@massport.com<mailto:achute@massport.com>
>
> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>

To:	Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS)
Cc:	Mason, Christopher (POL); Warmington, Scott (POL); Egnitz, Brian (POL); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL)
Subject:	FW: MassPort LPR Cameras
Date:	Tuesday, March 10, 2020 11:26:31 AM
Attachments:	SierraQuoteForMassPort.pdf

Michelle and Kyra,

This purchase request is for equipment to allow Mass Port Sierra Wireless modems to communicate directly with the existing ALPR Boss server in Chelsea. This is the fastest way to bring the Massport LPR cameras on line. EOTSS and EOPSS are OK with this solution as is Major Ryan.

As you can see from the thread, this has been going on for some time. I think we can close it out with this small purchase.

This does not resolve the replacement of the existing ALPR equipment that we discussed at Command Staff yesterday. That is a different issue.

Thanks

Lieutenant Colonel Dermot J. Quinn #1765
Division Commander
Division of Homeland Security & Preparedness
Massachusetts State Police

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Tuesday, March 10, 2020 10:52 AM
To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: FW: MassPort LPR Cameras

Hi LTC.,

Can we order this equipment for the MassPort project?

Thanks, Brian

-----Original Message-----
From: Slater, James (CHS)
Sent: Tuesday, March 10, 2020 10:26 AM
To: Egnitz, Brian (POL)
Subject: RE: MassPort LPR Cameras

Hi, Brian!

This needs to go through MSP fiscal. They need to enter the purchase in OPAS.

Jim

-----Original Message-----

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Tuesday, March 10, 2020 08:06
To: Slater, James (CHS) <james.slater@mass.gov>
Subject: RE: MassPort LPR Cameras

Is this something you can order or does it need to go through MSP?

-----Original Message-----
From: Slater, James (CHS)
Sent: Monday, March 9, 2020 10:36 AM
To: Egnitz, Brian (POL)
Subject: RE: MassPort LPR Cameras

Thanks, Brian...I will check with TSS.

Jim

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Monday, March 9, 2020 10:29
To: Slater, James (CHS) <james.slater@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: RE: MassPort LPR Cameras

Thanks Jim,

I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need 6 sierra wireless AC adapters and 12 antennas. I have reached out to BCM for a quote.

I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.

I plan to cut one sector (5-6 cameras per sector) over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?

-Brian

-----Original Message-----
From: Slater, James (CHS)
Sent: Friday, March 6, 2020 1:43 PM
To: Egnitz, Brian (POL)
Cc: Quinn, Dermot (POL)
Subject: RE: MassPort LPR Cameras

Hi, Brian!

I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.

So, assuming you move forward with this, who would actually make this happen?

Thanks.

Jim

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Wednesday, March 4, 2020 17:53
To: Slater, James (CHS) <james.slater@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: Re: MassPort LPR Cameras

Hi Jim,

Regarding the Massport cameras; in the early days of AVL we installed 39 Sierra wireless modem‘s in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don’t we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn’t have to do any firewall work either because they have a 166. and communicate like all of the MDT‘s . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.

We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.

Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.

> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>
> Thank you sir
>
> Major Charles W. Atchison III
> Troop F Commander
> Massachusetts State Police
> Director of Aviation Security
> 2 Service Road
> East Boston, Ma 02128
> Office: 617-568-7555
> Cell: 508-[redacted]
>
>
> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>
> All,
> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>
> Thanks
>
> CW
>
> From: Quinn, Dermot (POL)
> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
> Sent: Monday, February 10, 2020 10:31 AM
> To: Egnitz, Brian (POL)
> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
> Slater, James (CHS)
> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
> Robert (EOTSS)
> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;

> Warmington, Scott (POL)
> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
> .us>>; Peek, Brian T. (EOTSS)
> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
> Timothy (EPS)
> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
> Michalski, Maria (EPS)
> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
> Christopher (POL)
> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
> Hughes, Sean M. (EOTSS)
> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
> Atchison, Charles (POL)
> <catchison@massport.com<mailto:catchison@massport.com>>
> Subject: RE: MassPort LPR Cameras
>
> Good Morning,
>
> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>
> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>
> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>
> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>
> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>
> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>

> I can't overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security's technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>
> Respectfully,
>
>
> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
> of Homeland Security & Preparedness Massachusetts State Police
> <image006.png>
>
>
>
>
> From: Egnitz, Brian (POL)
> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
> Sent: Friday, January 17, 2020 1:10 PM
> To: Slater, James (CHS)
> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
> Cc: Quinn, Dermot (POL)
> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
> Guerriero, Robert (EOTSS)
> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
> Brian T. (EOTSS)
> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
> Timothy (EPS)
> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
> Maria (EPS)
> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
> Subject: RE: MassPort LPR Cameras
>
> Hi Jim,
>
> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>
> -Brian
>
>
> From: Egnitz, Brian (POL)
> Sent: Monday, January 6, 2020 1:33 PM
> To: Slater, James (CHS)
> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
> Crary
> Subject: RE: MassPort LPR Cameras
>
> Hi Jim,
>
> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to

Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>
> Thanks Brian
>
>
> From: John Tedona [mailto:jtedona@neology.net]
> Sent: Monday, December 9, 2019 4:55 PM
> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS); Slater, James (CHS)
> Subject: RE: MassPort LPR Cameras
>
> Alex,
>
> I can be available most anytime tomorrow for a call.
>
>
> Regards,
>
> John Tedona
> PIPS TECHNOLOGY - A Neology Business
> Sales Manager
> 12760 Danielson Ct. Suite A
> Poway, CA 92064
> Phone: 201-841-6237
> Email: jtedona@neology.net<mailto:jtedona@neology.net>
> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ
> U2sB_fmM6g&e=>
>
>
> From: Chute, Alexander
> <AChute@massport.com<mailto:AChute@massport.com>>
> Sent: Monday, December 9, 2019 4:38 PM
> To: Egnitz, Brian (POL)
> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
> <pcrary@neology.net<mailto:pcrary@neology.net>>
> Cc: Guerriero, Robert (MASSIT)
> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
> Peek, Brian T. (EOTSS)
> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
> Timothy (EPS)
> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
> Slater III, James F (CHS)
> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
> Subject: RE: MassPort LPR Cameras
>
> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>
> Hello All,

>
> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>
> Respectfully,
>
> ~Alex
>
>
> <image007.png>
>
> Alexander B. Chute
> Program Manager, Public Safety Systems Massachusetts Port Authority
> Cell: [redacted]
> Office: 617.568.5942
> achute@massport.com<mailto:achute@massport.com>
>
> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>
>
>
> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
> Sent: Monday, November 18, 2019 3:26 PM
> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
> pcrary@neology.net<mailto:pcrary@neology.net>
> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
> Subject: RE: MassPort LPR Cameras
>
> Hi John, Peter
>
> Any issues with moving Massports cameras to the Chelsea DB?
>
> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>
> The current app server
> <image008.png>
>
> Current DB server
>
> <image009.png>
> <image010.png>
>
> Our current reads by month for about 66 active cameras
>
> Year
>
> Month
>
> Day
>

> Month Name
>
> Reads Count
>
> 2019
>
> 11
>
> 1
>
> November
>
> 495,113
>
> 2019
>
> 11
>
> 2
>
> November
>
> 472,907
>
> 2019
>
> 11
>
> 3
>
> November
>
> 384,409
>
> 2019
>
> 11
>
> 4
>
> November
>
> 411,440
>
> 2019
>
> 11
>
> 5
>
> November
>
> 434,085
>
> 2019
>
> 11

>
> 6
>
> November
>
> 495,537
>
> 2019
>
> 11
>
> 7
>
> November
>
> 444,123
>
> 2019
>
> 11
>
> 8
>
> November
>
> 542,492
>
> 2019
>
> 11
>
> 9
>
> November
>
> 443,463
>
> 2019
>
> 11
>
> 10
>
> November
>
> 389,514
>
> 2019
>
> 11
>
> 11
>
> November
>
> 362,548
>

> 2019
>
> 11
>
> 12
>
> November
>
> 236,539
>
>
>
>
>
> From: Chute, Alexander [mailto:AChute@massport.com]
> Sent: Wednesday, November 13, 2019 2:49 PM
> To: Egnitz, Brian (POL)
> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS)
> Subject: RE: MassPort LPR Cameras
>
> These stats are from the 18 active cameras we have in the system for this month:
>
> <image011.png>
>
> ~Alex
>
>
> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
> Sent: Tuesday, November 12, 2019 5:28 PM
> To: Chute, Alexander
> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS)
> Subject: RE: MassPort LPR Cameras
>
> Hi Alex,
>
> Can you please provide the updated reads per day? Previously you were interested in sharing 6 cameras at approximately 75,000 reads per day.
>
> Here is the P492 confi I mentioned.
>
> Set host to boss [redacted]
> Set image [redacted]
> Set number of [redacted]
> Set Ping interval [redacted]
> Set udp ping [redacted]
> Set ping wait time [redacted]
> Set security [redacted]
>
> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>
> -Brian
>

>
>
> From: Chute, Alexander [mailto:AChute@massport.com]
> Sent: Tuesday, November 12, 2019 2:08 PM
> To: Egnitz, Brian (POL)
> Subject: MassPort LPR Cameras
>
> Brian,
>
> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the Troop F building. I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the roadway cameras are fed to 2 primary network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have 18 cameras in production, with another 19 scheduled to come online within the next two months. I anticipate this number growing to approximately 50 fixed cameras within our campus over the next year. Let me know what you think the appropriate next steps would be.
>
> Respectfully,
>
> ~Alex
>
> <image007.png>
>
> Alexander B. Chute
> Program Manager, Public Safety Systems Massachusetts Port Authority
> Cell: [redacted]
> Office: 617.568.5942
> achute@massport.com<mailto:achute@massport.com>
>
> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>

From: Egnitz, Brian (POL)
To: Quinn, Dermot (POL)
Subject: FW: MassPort LPR Cameras
Date: Tuesday, March 10, 2020 10:52:00 AM
Attachments: SierraQuoteForMassPort.pdf

Hi LTC.,

Can we order this equipment for the MassPort project?

Thanks, Brian

-----Original Message-----
From: Slater, James (CHS)
Sent: Tuesday, March 10, 2020 10:26 AM
To: Egnitz, Brian (POL)
Subject: RE: MassPort LPR Cameras

Hi, Brian!

This needs to go through MSP fiscal. They need to enter the purchase in OPAS.

Jim

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Tuesday, March 10, 2020 08:06
To: Slater, James (CHS) <james.slater@mass.gov>
Subject: RE: MassPort LPR Cameras

Is this something you can order or does it need to go through MSP?

-----Original Message-----
From: Slater, James (CHS)
Sent: Monday, March 9, 2020 10:36 AM
To: Egnitz, Brian (POL)
Subject: RE: MassPort LPR Cameras

Thanks, Brian...I will check with TSS.

Jim

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Monday, March 9, 2020 10:29
To: Slater, James (CHS) <james.slater@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: RE: MassPort LPR Cameras

Thanks Jim,

I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need 6 sierra wireless AC adapters and 12 antennas. I have reached out to BCM for a quote.

I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.

I plan to cut one sector (5-6 cameras per sector) over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?

-Brian

-----Original Message-----
From: Slater, James (CHS)
Sent: Friday, March 6, 2020 1:43 PM
To: Egnitz, Brian (POL)
Cc: Quinn, Dermot (POL)
Subject: RE: MassPort LPR Cameras

Hi, Brian!

I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.

So, assuming you move forward with this, who would actually make this happen?

Thanks.

Jim

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Wednesday, March 4, 2020 17:53
To: Slater, James (CHS) <james.slater@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: Re: MassPort LPR Cameras

Hi Jim,

Regarding the Massport cameras; in the early days of AVL we installed 39 Sierra wireless modem‘s in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don’t we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn’t have to do any firewall work either because they have a 166. and communicate like all of the MDT‘s . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.

We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.

Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.

> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>
> Thank you sir
>
> Major Charles W. Atchison III
> Troop F Commander
> Massachusetts State Police

> Director of Aviation Security
> 2 Service Road
> East Boston, Ma 02128
> Office: 617-568-7555
> Cell: 508-[redacted]
>
>
> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>
> All,
> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>
> Thanks
>
> CW
>
> From: Quinn, Dermot (POL)
> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
> Sent: Monday, February 10, 2020 10:31 AM
> To: Egnitz, Brian (POL)
> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
> Slater, James (CHS)
> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
> Robert (EOTSS)
> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
> Warmington, Scott (POL)
> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
> .us>>; Peek, Brian T. (EOTSS)
> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
> Timothy (EPS)
> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
> Michalski, Maria (EPS)
> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
> Christopher (POL)
> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
> Hughes, Sean M. (EOTSS)
> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
> Atchison, Charles (POL)
> <catchison@massport.com<mailto:catchison@massport.com>>
> Subject: RE: MassPort LPR Cameras
>
> Good Morning,
>
> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.

>
> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>
> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>
> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>
> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>
> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>
> I can’t overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security’s technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>
> Respectfully,
>
>
> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
> of Homeland Security & Preparedness Massachusetts State Police
> <image006.png>
>
>
>
>
> From: Egnitz, Brian (POL)
> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
> Sent: Friday, January 17, 2020 1:10 PM
> To: Slater, James (CHS)
> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
> Cc: Quinn, Dermot (POL)
> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
> Guerriero, Robert (EOTSS)
> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
> Brian T. (EOTSS)
> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
> Timothy (EPS)
> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,

> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
> Maria (EPS)
> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
> Subject: RE: MassPort LPR Cameras
>
> Hi Jim,
>
> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>
> -Brian
>
>
> From: Egnitz, Brian (POL)
> Sent: Monday, January 6, 2020 1:33 PM
> To: Slater, James (CHS)
> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
> Crary
> Subject: RE: MassPort LPR Cameras
>
> Hi Jim,
>
> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>
> Thanks Brian
>
>
> From: John Tedona [mailto:jtedona@neology.net]
> Sent: Monday, December 9, 2019 4:55 PM
> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS); Slater, James (CHS)
> Subject: RE: MassPort LPR Cameras
>
> Alex,
>
> I can be available most anytime tomorrow for a call.
>
>
> Regards,
>
> John Tedona
> PIPS TECHNOLOGY - A Neology Business
> Sales Manager
> 12760 Danielson Ct. Suite A
> Poway, CA 92064
> Phone: 201-841-6237
> Email: jtedona@neology.net<mailto:jtedona@neology.net>
> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http

> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ
> U2sB_fmM6g&e=>
>
>
> From: Chute, Alexander
> <AChute@massport.com<mailto:AChute@massport.com>>
> Sent: Monday, December 9, 2019 4:38 PM
> To: Egnitz, Brian (POL)
> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
> <pcrary@neology.net<mailto:pcrary@neology.net>>
> Cc: Guerriero, Robert (MASSIT)
> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
> Peek, Brian T. (EOTSS)
> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
> Timothy (EPS)
> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
> Slater III, James F (CHS)
> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
> Subject: RE: MassPort LPR Cameras
>
> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>
> Hello All,
>
> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>
> Respectfully,
>
> ~Alex
>
>
> <image007.png>
>
> Alexander B. Chute
> Program Manager, Public Safety Systems Massachusetts Port Authority
> Cell: [redacted]
> Office: 617.568.5942
> achute@massport.com<mailto:achute@massport.com>
>
> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>
>
>
> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
> Sent: Monday, November 18, 2019 3:26 PM
> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);

> pcrary@neology.net<mailto:pcrary@neology.net>
> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
> Subject: RE: MassPort LPR Cameras
>
> Hi John, Peter
>
> Any issues with moving Massports cameras to the Chelsea DB?
>
> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>
> The current app server
> <image008.png>
>
> Current DB server
>
> <image009.png>
> <image010.png>
>
> Our current reads by month for about 66 active cameras
>
> Year
>
> Month
>
> Day
>
> Month Name
>
> Reads Count
>
> 2019
>
> 11
>
> 1
>
> November
>
> 495,113
>
> 2019
>
> 11
>
> 2
>
> November
>
> 472,907
>
> 2019
>
> 11
>
> 3
>

> November
>
> 384,409
>
> 2019
>
> 11
>
> 4
>
> November
>
> 411,440
>
> 2019
>
> 11
>
> 5
>
> November
>
> 434,085
>
> 2019
>
> 11
>
> 6
>
> November
>
> 495,537
>
> 2019
>
> 11
>
> 7
>
> November
>
> 444,123
>
> 2019
>
> 11
>
> 8
>
> November
>
> 542,492
>
> 2019
>
> 11

>
> 9
>
> November
>
> 443,463
>
> 2019
>
> 11
>
> 10
>
> November
>
> 389,514
>
> 2019
>
> 11
>
> 11
>
> November
>
> 362,548
>
> 2019
>
> 11
>
> 12
>
> November
>
> 236,539
>
>
>
>
>
> From: Chute, Alexander [mailto:AChute@massport.com]
> Sent: Wednesday, November 13, 2019 2:49 PM
> To: Egnitz, Brian (POL)
> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS)
> Subject: RE: MassPort LPR Cameras
>
> These stats are from the 18 active cameras we have in the system for this month:
>
> <image011.png>
>
> ~Alex
>
>
> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
> Sent: Tuesday, November 12, 2019 5:28 PM

> To: Chute, Alexander
> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS)
> Subject: RE: MassPort LPR Cameras
>
> Hi Alex,
>
> Can you please provide the updated reads per day? Previously you were interested in sharing 6 cameras at approximately 75,000 reads per day.
>
> Here is the P492 confi I mentioned.
>
> Set host to boss [redacted]
> Set image [redacted]
> Set number of [redacted]
> Set Ping interval [redacted]
> Set udp ping [redacted]
> Set ping wait time [redacted]
> Set security [redacted]
>
> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>
> -Brian
>
>
>
> From: Chute, Alexander [mailto:AChute@massport.com]
> Sent: Tuesday, November 12, 2019 2:08 PM
> To: Egnitz, Brian (POL)
> Subject: MassPort LPR Cameras
>
> Brian,
>
> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the Troop F building. I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the roadway cameras are fed to 2 primary network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have 18 cameras in production, with another 19 scheduled to come online within the next two months. I anticipate this number growing to approximately 50 fixed cameras within our campus over the next year. Let me know what you think the appropriate next steps would be.
>
> Respectfully,
>
> ~Alex
>
> <image007.png>
>
> Alexander B. Chute
> Program Manager, Public Safety Systems Massachusetts Port Authority
> Cell: [redacted]
> Office: 617.568.5942
> achute@massport.com<mailto:achute@massport.com>

>
> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>

From:	Egnitz, Brian (POL)
To:	Quinn, Dermot (POL)
Subject:	FW: Massport
Date:	Wednesday, February 12, 2020 9:38:00 AM
Attachments:	RE MassPort LPR Cameras.msg

From: Egnitz, Brian (POL)
Sent: Wednesday, February 12, 2020 9:30 AM
To: Peek, Brian T. (EOTSS)
Cc: Guerriero, Robert (EOTSS); Mitchell, Timothy P. (EOTSS)
Subject: RE: Massport

Sure;

Stakeholders are users of ALPR, MSP, and Public Safety Agencies and MassPort.

The Goal is to get the current and new ALPR MassPort cameras redirected to the EOPSS boss server

Deliverables are when reads are coming into the database and the application is stable

Current Environment is MassPort submitting reads to their own BOSS internal server.

Attached is the thread history.

-Brian

From: Peek, Brian T. (EOTSS)
Sent: Wednesday, February 12, 2020 8:38 AM
To: Egnitz, Brian (POL)
Cc: Guerriero, Robert (EOTSS); Mitchell, Timothy P. (EOTSS)
Subject: Massport

Morning Brian,

Can we get a high level overview of this Project:

- Stakeholders
- Goals
- Define Deliverables
- Current Environment

There will be a Project Manager assigned so we would like to have some information to present him\her.

thanks

Brian Peek | Massachusetts Executive Office of Technical Services and Security
Network Services/WAN
Phone: 508.922.2740
brian.t.peek@mass.gov | www.mass.gov/eotss

From: Egnitz, Brian (POL)
To: Doherty, Gregory (POL)
Subject: FW: Mobile ALPR Processor System
Date: Tuesday, July 14, 2020 10:46:00 PM
Attachments: image001.png
PAGIS 2.14 MANUAL_ADMIN.pdf
PAGIS 2.14 MANUAL_USERS.pdf
SX4e Mobile Installation Guide.pdf
FedX Track.pdf
image002.png

FYI

From: John Tedona [mailto:jtedona@neology.net]
Sent: Thursday, July 2, 2020 9:38 AM
To: Egnitz, Brian (POL)
Subject: Mobile ALPR Processor System

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Brian,

The mobile SX4e processor and 25mm camera is scheduled to arrive this Monday. I'm not sure how you will use the system so I included two different power cords. One you can plug into a cigarette lighter, the other you can wire the pig tails to your power source. (Black is (-) ground, Red is (+) hot, Blue goes to ignition source if on a vehicle). If you're wiring to a non automotive power supply both Red and Blue leads go to (+) hot. See the attached Installation manual for more info and display/laptop wiring.

As for setup, the processor is configured for "Standalone" mode meaning you would use a monitor and keyboard. If you want to use the processor via a laptop you need to configure the processor for "VPRelay" (see page 47 in the attached admin manual on how to switch between the two.

As for usage, the processor already has the MA OCR engine installed, the camera's flash tables are already set and port C1 on the processor is where you plug in the 25mm PIPS camera. This camera has a 45' focus range, so for placement purposes start at a distance of 45' then incrementally increase the distance to see how far out you can maintain plate capture and read accuracy. The camera Port C3 has been setup for a 3rd party webcam. Running both PIPS and 3rd party cameras simultaneously will let you compare both cameras performance in real time. You will need to speak with Dave Bynum (PIPS IT Tech) to ensure the proper SDK is loaded for the web cam….I'll get you guys together when you're ready.

Call me when you're ready to use the system so I can walk you through how to use it.

Have Fun!



A NEOLOGY Business

John Tedona
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

To: aut
Subject: FW: Mobile ALPR Processor System
Date: Wednesday, July 15, 2020 3:02:07 AM
Attachments: image001.png
image003.png
PAGIS 2.14 MANUAL_ADMIN.pdf
PAGIS 2.14 MANUAL_USERS.pdf
SX4e Mobile Installation Guide.pdf
FedX Track.pdf
image002.png

From: John Tedona [mailto:jtedona@neology.net]
Sent: Thursday, July 2, 2020 9:38 AM
To: Egnitz, Brian (POL)
Subject: Mobile ALPR Processor System

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Brian,

The mobile SX4e processor and 25mm camera is scheduled to arrive this Monday. I'm not sure how you will use the system so I included two different power cords. One you can plug into a cigarette lighter, the other you can wire the pig tails to your power source. (Black is (-) ground, Red is (+) hot, Blue goes to ignition source if on a vehicle). If you're wiring to a non automotive power supply both Red and Blue leads go to (+) hot. See the attached Installation manual for more info and display/laptop wiring.

As for setup, the processor is configured for "Standalone" mode meaning you would use a monitor and keyboard. If you want to use the processor via a laptop you need to configure the processor for "VPRelay" (see page 47 in the attached admin manual on how to switch between the two.

As for usage, the processor already has the MA OCR engine installed, the camera's flash tables are already set and port C1 on the processor is where you plug in the 25mm PIPS camera. This camera has a 45' focus range, so for placement purposes start at a distance of 45' then incrementally increase the distance to see how far out you can maintain plate capture and read accuracy. The camera Port C3 has been setup for a 3rd party webcam. Running both PIPS and 3rd party cameras simultaneously will let you compare both cameras performance in real time. You will need to speak with Dave Bynum (PIPS IT Tech) to ensure the proper SDK is loaded for the web cam….I'll get you guys together when you're ready.

Call me when you're ready to use the system so I can walk you through how to use it.

Have Fun!



A Business

John Tedona
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: Silva, Kyra (POL)
To: Small, Michelle (POL)
Subject: FW: OGR and DOC > Automatic License Plate Reader Policy
Date: Tuesday, December 15, 2020 1:35:00 PM
Attachments: TRF-11 Automatic License Plate Recognition Revised 10-1-2019.pdf

---

Hi,

Is the TRF-11 ALPR ok to share with OGR and DOC?

From: Miller, Dianne (POL)
Sent: Tuesday, December 15, 2020 9:38 AM
To: Silva, Kyra (POL)
Cc: Comeau, Melissa (POL); Biagi, Pamela (POL)
Subject: OGR and DOC > Automatic License Plate Reader Policy

Hi Kyra,

Please see email chain below.

Please confirm I can forward the attached policy to Gina (OGR) for review by DOC staff ordering ALPRs.
I will also refer them to the DCJIS policy below and remind them that Commonwealth IT Terms and Conditions apply (to the vendor) because we order ALPRs through OTIS.

Thanks
Di

From: Gallagher, David (POL)
Sent: Tuesday, December 15, 2020 9:30 AM
To: Miller, Dianne (POL); Thibault, Amy (POL)
Cc: Range, Scott (POL)
Subject: Re: Automatic License Plate Reader Policy

Dianne,

I believe this is the policy you were inquiring about. Please feel free to share. If you or anyone else has any questions, please contact me.

Thank you,

David M. Gallagher
Major, Massachusetts State Police
Special Operations
508-820-2162
David.Gallagher3@MassMail.state.ma.us

Good Morning Dianne,

I've copied Major Gallagher on this because I think he is now the MSP Department ALPR Coordinator if I'm not mistaken.

TRF-11 is the MSP policy for ALPR.

EOPSS – DCJIS has a policy as listed below. I don't have a copy of it but EOPSS – DCJIS must so Gina or DOC should be able to check with them directly.

Executive Office of Public Safety and Security (EOPSS) - *The Commonwealth of Massachusetts Global Justice and Public Safety Information Sharing Policy*
Executive Office of Public Safety and Security (EOPSS) - Department of Criminal Justice Information Services - *Automatic License Plate Recognition System Central Repository Companion Policy.*

Major Gallagher – Please feel free to weigh in. Is it ok for Dianne to give the DOC TRF-11?

Finally, Gina and DOC should probably check with EOPSS legal and/or MSP legal in case they have any additional insights on ALPR policy developments.

Thank you/Respectfully,
Scott

From: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Sent: Tuesday, December 15, 2020 8:48 AM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Range, Scott (POL) <scott.range@pol.state.ma.us>
Subject: RE: Automatic License Plate Reader Policy

Good morning Major Range and Amy,
Is there a law enforcement policy relative to ALPR's? See below email from EOPSS…
Thanks
Di

From: Papagiorgakis, Gina (OGR)
Sent: Tuesday, December 15, 2020 8:23 AM
To: Miller, Dianne (POL)
Subject: Automatic License Plate Reader Policy

Good morning Dianne,

I am hoping you can put me in touch with the right contact on your end. The DOC was awarded grant funds to procure an automatic license plate reader system, and thus will need to implement a policy. They are looking to reference existing policies to guide a draft of their own. Is there a policy at MSP that can be shared with the DOC, or is there anyone else who I

should reach out to at MSP?

Thank you in advance.

Gina Papagiorgakis
Homeland Security Division
Office of Grants and Research
10 Park Plaza, Suite 3720-A
Boston, MA 02116
gina.papagiorgakis1@mass.gov

From: Range, Scott (POL) <scott.range@pol.state.ma.us>
Sent: Tuesday, December 15, 2020 9:19 AM
To: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Cc: Gallagher, David (POL) <david.gallagher3@MassMail.State.MA.US>; Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: RE: Automatic License Plate Reader Policy

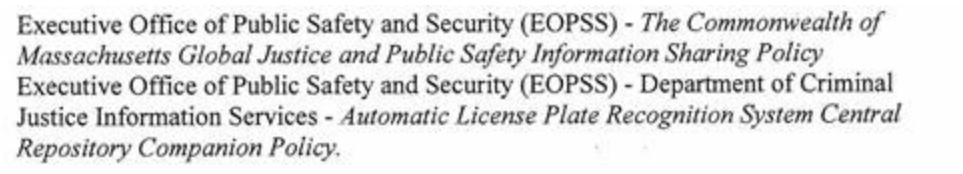
Good Morning Dianne,

I've copied Major Gallagher on this because I think he is now the MSP Department ALPR Coordinator if I'm not mistaken.

TRF-11 is the MSP policy for ALPR.

EOPSS – DCJIS has a policy as listed below. I don't have a copy of it but EOPSS – DCJIS must so Gina

or DOC should be able to check with them directly.


Executive Office of Public Safety and Security (EOPSS) - *The Commonwealth of Massachusetts Global Justice and Public Safety Information Sharing Policy*
Executive Office of Public Safety and Security (EOPSS) - Department of Criminal Justice Information Services - *Automatic License Plate Recognition System Central Repository Companion Policy.*

Major Gallagher – Please feel free to weigh in. Is it ok for Dianne to give the DOC TRF-11?

Finally, Gina and DOC should probably check with EOPSS legal and/or MSP legal in case they have any additional insights on ALPR policy developments.

Thank you/Respectfully,
Scott

From: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Sent: Tuesday, December 15, 2020 8:48 AM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Range, Scott (POL) <scott.range@pol.state.ma.us>
Subject: RE: Automatic License Plate Reader Policy

Good morning Major Range and Amy,
Is there a law enforcement policy relative to ALPR's? See below email from EOPSS…
Thanks
Di

From: Papagiorgakis, Gina (OGR)
Sent: Tuesday, December 15, 2020 8:23 AM
To: Miller, Dianne (POL)
Subject: Automatic License Plate Reader Policy

Good morning Dianne,

I am hoping you can put me in touch with the right contact on your end. The DOC was awarded grant funds to procure an automatic license plate reader system, and thus will need to implement a policy. They are looking to reference existing policies to guide a draft of their own. Is there a policy at MSP that can be shared with the DOC, or is there anyone else who I should reach out to at MSP?

Thank you in advance.

Gina Papagiorgakis
Homeland Security Division
Office of Grants and Research
10 Park Plaza, Suite 3720-A
Boston, MA 02116

gina.papagiorgakis1@mass.gov

From:	Small, Michelle (POL)
To:	Staples, Jennifer (POL)
Subject:	FW: OGR and DOC > Automatic License Plate Reader Policy
Date:	Tuesday, December 15, 2020 1:41:15 PM
Attachments:	TRF-11 Automatic License Plate Recognition Revised 10-1-2019.pdf

Hi Jenn,

The DOC is purchasing LPRs and OGR requested the state police policy. Due to the recent issues, I wanted to check with you first. Is it ok to share?

-Michelle

From: Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>
Sent: Tuesday, December 15, 2020 1:35 PM
To: Small, Michelle (POL) <Michelle.E.Small@pol.state.ma.us>
Subject: FW: OGR and DOC > Automatic License Plate Reader Policy

Hi,

Is the TRF-11 ALPR ok to share with OGR and DOC?

From: Miller, Dianne (POL)
Sent: Tuesday, December 15, 2020 9:38 AM
To: Silva, Kyra (POL)
Cc: Comeau, Melissa (POL); Biagi, Pamela (POL)
Subject: OGR and DOC > Automatic License Plate Reader Policy

Hi Kyra,

Please see email chain below.

Please confirm I can forward the attached policy to Gina (OGR) for review by DOC staff ordering ALPRs.
I will also refer them to the DCJIS policy below and remind them that Commonwealth IT Terms and Conditions apply (to the vendor) because we order ALPRs through OTIS.

Thanks
Di

From: Gallagher, David (POL)
Sent: Tuesday, December 15, 2020 9:30 AM
To: Miller, Dianne (POL); Thibault, Amy (POL)
Cc: Range, Scott (POL)
Subject: Re: Automatic License Plate Reader Policy

Dianne,

I believe this is the policy you were inquiring about. Please feel free to share. If you or anyone else has any questions, please contact me.

Thank you,

David M. Gallagher
Major, Massachusetts State Police
Special Operations
508-820-2162
David.Gallagher3@MassMail.state.ma.us

Good Morning Dianne,

I've copied Major Gallagher on this because I think he is now the MSP Department ALPR Coordinator if I'm not mistaken.

TRF-11 is the MSP policy for ALPR.

EOPSS – DCJIS has a policy as listed below. I don't have a copy of it but EOPSS – DCJIS must so Gina or DOC should be able to check with them directly.

Executive Office of Public Safety and Security (EOPSS) - *The Commonwealth of Massachusetts Global Justice and Public Safety Information Sharing Policy*
Executive Office of Public Safety and Security (EOPSS) - Department of Criminal Justice Information Services - *Automatic License Plate Recognition System Central Repository Companion Policy.*

Major Gallagher – Please feel free to weigh in. Is it ok for Dianne to give the DOC TRF-11?

Finally, Gina and DOC should probably check with EOPSS legal and/or MSP legal in case they have any additional insights on ALPR policy developments.

Thank you/Respectfully,
Scott

From: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Sent: Tuesday, December 15, 2020 8:48 AM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Range, Scott (POL) <scott.range@pol.state.ma.us>
Subject: RE: Automatic License Plate Reader Policy

Good morning Major Range and Amy,
Is there a law enforcement policy relative to ALPR's? See below email from EOPSS…
Thanks
Di

From: Papagiorgakis, Gina (OGR)
Sent: Tuesday, December 15, 2020 8:23 AM
To: Miller, Dianne (POL)
Subject: Automatic License Plate Reader Policy

Good morning Dianne,

I am hoping you can put me in touch with the right contact on your end. The DOC was awarded grant funds to procure an automatic license plate reader system, and thus will need to implement a policy. They are looking to reference existing policies to guide a draft of their own. Is there a policy at MSP that can be shared with the DOC, or is there anyone else who I should reach out to at MSP?

Thank you in advance.

Gina Papagiorgakis
Homeland Security Division
Office of Grants and Research
10 Park Plaza, Suite 3720-A
Boston, MA 02116
gina.papagiorgakis1@mass.gov

From: Range, Scott (POL) <scott.range@pol.state.ma.us>
Sent: Tuesday, December 15, 2020 9:19 AM
To: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>

Cc: Gallagher, David (POL) <david.gallagher3@MassMail.State.MA.US>; Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: RE: Automatic License Plate Reader Policy

Good Morning Dianne,

I've copied Major Gallagher on this because I think he is now the MSP Department ALPR Coordinator if I'm not mistaken.

TRF-11 is the MSP policy for ALPR.

EOPSS – DCJIS has a policy as listed below. I don't have a copy of it but EOPSS – DCJIS must so Gina or DOC should be able to check with them directly.

Executive Office of Public Safety and Security (EOPSS) - *The Commonwealth of Massachusetts Global Justice and Public Safety Information Sharing Policy*
Executive Office of Public Safety and Security (EOPSS) - Department of Criminal Justice Information Services - *Automatic License Plate Recognition System Central Repository Companion Policy.*

Major Gallagher – Please feel free to weigh in. Is it ok for Dianne to give the DOC TRF-11?

Finally, Gina and DOC should probably check with EOPSS legal and/or MSP legal in case they have any additional insights on ALPR policy developments.

Thank you/Respectfully,
Scott

From: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Sent: Tuesday, December 15, 2020 8:48 AM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Range, Scott (POL) <scott.range@pol.state.ma.us>
Subject: RE: Automatic License Plate Reader Policy

Good morning Major Range and Amy,
Is there a law enforcement policy relative to ALPR's? See below email from EOPSS…
Thanks
Di

From: Papagiorgakis, Gina (OGR)
Sent: Tuesday, December 15, 2020 8:23 AM
To: Miller, Dianne (POL)
Subject: Automatic License Plate Reader Policy

Good morning Dianne,

I am hoping you can put me in touch with the right contact on your end. The DOC was awarded

grant funds to procure an automatic license plate reader system, and thus will need to implement a policy. They are looking to reference existing policies to guide a draft of their own. Is there a policy at MSP that can be shared with the DOC, or is there anyone else who I should reach out to at MSP?

Thank you in advance.

Gina Papagiorgakis
Homeland Security Division
Office of Grants and Research
10 Park Plaza, Suite 3720-A
Boston, MA 02116
gina.papagiorgakis1@mass.gov

From: Wilkerson, Diane A. (EOTSS)
To: Clement, Michael (POL)
Subject: FW: Pagis Software/ Windows Fix
Date: Friday, October 2, 2020 4:47:37 PM
Attachments: PAGIS 2.14 MANUAL_ADMIN Windows Fix.pdf

Diane Wilkerson
Deskside Support Southeast
326 West Grove Street, Middleboro, MA 02346
Office: (508) 923-4036 |
diane.a.wilkerson@mass.gov | www.mass.gov/eotss

Executive Office of Technology Services and Security (EOTSS)
EOTSS provides secure and quality digital information, services, and tools to constituents and service providers when and where they need them.

From: Kory Koster <KKoster@itsg.us.com>
Sent: Thursday, October 1, 2020 1:12 PM
To: Cronin, Timothy M. (EOTSS) <Timothy.M.Cronin@mass.gov>; Henderson, Phillip W. (EOTSS) <Phillip.W.Henderson@mass.gov>; Wilkerson, Diane A. (EOTSS) <diane.a.wilkerson@mass.gov>
Subject: Pagis Software/ Windows Fix

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Hello Diane, Tim and Phil

Attached is the Pagis Software info. This is the newest version of Pagis that MSP is NOT running at this time. When Lt Fitzgerald from the truck team moves forward with the new LPR systems this will be the software he will be running. I wanted to send this out because in this document is the info on the newest windows update that is causing Issues with either the processor not communicating or the internal aircard disconnecting when the computer is connected via ethernet cable. Page 58 half way down and page 59 addresses these issue with the current fix/work around. You will all probably start to run into this as Diane already has. Please let me know how this works out for you. Any questions please let me know. As I get more info on this product I will send along to all of you. As an outside vendor it makes my job 100 times easier when I can get someone to return an email or answer their phone. So for that I thank you all very much!!

Thank you
Kory Koster
Partner - New England Operations

Island Tech Services (ITS)
O: 888.615.2770 x281
M: 508.989.2783
kkoster@itsg.us.com
itsg.us.com



From: Tucker, Daniel T (POL)
To: dtuck2938@yahoo.com
Subject: FW: Promulgation of 19-SO-12
Date: Thursday, March 26, 2020 9:35:00 AM
Attachments: 19-SO-12 Distribution of General Order.pdf
TRF-11 Automatic License Plate Recognition Revised 10-1-2019 with highlights.pdf

---

From: Strategic Planning (POL)
Sent: Tuesday, October 01, 2019 5:20 PM
To: POL-DL-All Users
Subject: Promulgation of 19-SO-12

Please be advised that the following Special Order has been promulgated:

- **19-SO-12 Distribution of General Order**
  TRF-11 Automatic License Plate Recognition

Please also be advised that the official General Order listed in the above Special Order has been promulgated.

Strategic Planning Section
470 Worcester Road
Framingham, Massachusetts 01702

From: Egnitz, Brian (POL)
To: Quinn, Dermot (POL)
Subject: Fwd: BOSS 4.0 Pricing
Date: Monday, February 10, 2020 8:49:27 PM
Attachments: image001.png
ATT00001.htm
image002.png
ATT00002.htm
BOSS 4 subscription layers.xlsx
ATT00003.htm

Mantis pricing below

Begin forwarded message:

From: John Tedona <jtedona@neology.net>
Date: February 10, 2020 at 11:40:25 AM EST
To: "Egnitz, Brian (POL)" <brian.egnitz@pol.state.ma.us>
Subject: RE: BOSS 4.0 Pricing

BOSS 4.0 Software was quoted at $16,995 per year.
Hosting services for BOSS4 was quoted an additional $118,000 per year
Mantis based on the expected data volume would be $125,000 per year. Hosting Mantis is only about 10% of the overall Mantis price, so on-prem Mantis would be in the $112,000

I attached an outline that highlights what is included in the hosted services.

John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Monday, February 10, 2020 8:34 AM
To: John Tedona <jtedona@neology.net>
Subject: RE: BOSS 4.0 Pricing

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

What's the on-prem mantis add-on cost? Is it 125K or was that 125K you guys hosting everything and having mantis?

From: John Tedona [mailto:jtedona@neology.net]
Sent: Thursday, January 23, 2020 4:40 PM
To: Egnitz, Brian (POL)
Subject: BOSS 4.0 Pricing

I understand you don't need this now, but for your reference I've attached pricing for BOSS 4.0 software, pricing for AWS hosting services that is to be added to the BOSS 4.0 license fee if you decide to have PIPS host (see notes in the Cloud/SAS quote that gives an overview of host services and discounts for a 3 or 5 year contact) and the Mantis price adder if you decide to include vehicle classification.

Let me know if you have any questions.

From:	brian.egnitz@pol.state.ma.us
To:	Slater, James (CHS)
Cc:	Quinn, Dermot (POL)
Subject:	Fwd: BOSS4 Requirements
Date:	Thursday, March 5, 2020 6:52:43 PM
Attachments:	image001.png ATT00001.htm image003.png ATT00002.htm PIPS BOSS4 Specifications.pdf ATT00003.htm BOSS4 Questionnaire Form.pdf ATT00004.htm

---

FYI

I received clarification from Neology, attached is the on-prem specs, they do not support native AWS for BOSS4 hosted on Amazon Web Services infrastructure.

-Brian

Begin forwarded message:

> **From:** John Tedona <jtedona@neology.net>
> **Date:** March 5, 2020 at 6:02:19 PM EST
> **To:** "Egnitz, Brian (POL)" <brian.egnitz@pol.state.ma.us>
> **Subject: BOSS4 Requirements**
>
> Brian -Here's the On-Prem "Only" spec requirements for BOSS4 plus a questionnaire we send out to assist with growth.

From:	brian.egnitz@pol.state.ma.us
To:	Slater, James (CHS)
Cc:	Quinn, Dermot (POL)
Subject:	Fwd: BOSS4 Requirements
Date:	Thursday, March 5, 2020 6:49:15 PM
Attachments:	image001.png ATT00001.htm image003.png ATT00002.htm PIPS BOSS4 Specifications.pdf ATT00003.htm BOSS4 Questionnaire Form.pdf ATT00004.htm

---

FYI

This is the on prem specs, they do not support native AWS on-prem.

Begin forwarded message:

> **From:** John Tedona <jtedona@neology.net>
> **Date:** March 5, 2020 at 6:02:19 PM EST
> **To:** "Egnitz, Brian (POL)" <brian.egnitz@pol.state.ma.us>
> **Subject: BOSS4 Requirements**
>
> Brian -Here's the On-Prem "Only" spec requirements for BOSS4 plus a questionnaire we send out to assist with growth.

From:	Egnitz, Brian (POL)
To:	Slater, James (CHS)
Cc:	Quinn, Dermot (POL)
Subject:	Fwd: BOSS4 Requirements
Date:	Thursday, March 5, 2020 6:52:45 PM
Attachments:	image001.png ATT00001.htm image003.png ATT00002.htm PIPS BOSS4 Specifications.pdf ATT00003.htm BOSS4 Questionnaire Form.pdf ATT00004.htm

---

FYI

I received clarification from Neology, attached is the on-prem specs, they do not support native AWS for BOSS4 hosted on Amazon Web Services infrastructure.

-Brian

Begin forwarded message:

> **From:** John Tedona <jtedona@neology.net>
> **Date:** March 5, 2020 at 6:02:19 PM EST
> **To:** "Egnitz, Brian (POL)" <brian.egnitz@pol.state.ma.us>
> **Subject: BOSS4 Requirements**
>
> Brian -Here's the On-Prem "Only" spec requirements for BOSS4 plus a questionnaire we send out to assist with growth.

From: Egnitz, Brian (POL)
To: Quinn, Dermot (POL)
Subject: Fwd: New Solutions and End-Of-Life Announcement
Date: Friday, January 17, 2020 7:51:50 AM
Attachments: image001.png
ATT00001.htm
image002.png
ATT00002.htm
PIPS 2020 Bulletin.pdf
ATT00003.htm

Please see attached document regarding the 525 camera GMT issue.

Begin forwarded message:

From: John Tedona <jtedona@neology.net>
Date: January 16, 2020 at 5:52:18 PM EST
To: "Egnitz, Brian (POL)" <brian.egnitz@pol.state.ma.us>
Cc: Miranda Fischer <mfischer@neology.net>, Luke Normington <LNormington@uk.neology.net>
Subject: New Solutions and End-Of-Life Announcement

Mr. Egnitz,

As we step into a new year, and decade, we wanted to take a moment to thank you for your continued loyalty and use of the PIPS Technology by Neology solutions. We are incredibly grateful of the customers, resellers and partners who, over the last years have remained loyal and supported us in our vision of “Driving Detection Innovation”. Each day we strive to make a difference in supporting you to achieve your goals, solve your challenges and achieve your mission.

2019 was a major year for us as we finalised significant elements of the overhaul of our products and solutions, culminating with the release of BOSS 4 in the fall, alongside brand new Fixed and Mobile ALPR solutions. Attached you will find the latest reminders in relation to our products and software versions to ensure you are getting the most out of your Neology products and solutions.

The year ahead is primed to be an exciting one! At Neology we firmly believe that the development doesn’t stop – we have almost 30% of our workforce working specifically in the product development area of our business in order to constantly evolve our solutions, improve performance and add new features. We have some exciting additions to the portfolio which are imminent that will provide not only performance improvements to the existing solutions but also provide the ability for greater inter-operability across the Law Enforcement ALPR market in the US more generally. We believe that you retaining the control and ownership of your data is paramount and we continue to respect that as we always have while supporting those customers who

choose to share and provide secure, trusted data sharing between neighbours and friends.

We are always keen to hear your feedback – if there are any elements of our services, solutions or products which you would like to feedback on, please don't hesitate to get in touch with me so I can provide personal attention to both positive and negative feedback. Email me here

Thank you for your continued support – we look forward to serving you in 2020 and beyond.

Best Regards,
Luke & the PIPS Technology team

From:	Egnitz, Brian (POL)
To:	Cleve Daniels; Connolly, Kevin; Scott Lundegren
Subject:	Fwd: New Solutions and End-Of-Life Announcement
Date:	Friday, January 17, 2020 7:52:21 AM
Attachments:	image001.png ATT00001.htm image002.png ATT00002.htm PIPS 2020 Bulletin.pdf ATT00003.htm

---

FYI

Begin forwarded message:

From: John Tedona <jtedona@neology.net>
Date: January 16, 2020 at 5:52:18 PM EST
To: "Egnitz, Brian (POL)" <brian.egnitz@pol.state.ma.us>
Cc: Miranda Fischer <mfischer@neology.net>, Luke Normington <LNormington@uk.neology.net>
Subject: New Solutions and End-Of-Life Announcement

Mr. Egnitz,

As we step into a new year, and decade, we wanted to take a moment to thank you for your continued loyalty and use of the PIPS Technology by Neology solutions. We are incredibly grateful of the customers, resellers and partners who, over the last years have remained loyal and supported us in our vision of “Driving Detection Innovation”. Each day we strive to make a difference in supporting you to achieve your goals, solve your challenges and achieve your mission.

2019 was a major year for us as we finalised significant elements of the overhaul of our products and solutions, culminating with the release of BOSS 4 in the fall, alongside brand new Fixed and Mobile ALPR solutions. Attached you will find the latest reminders in relation to our products and software versions to ensure you are getting the most out of your Neology products and solutions.

The year ahead is primed to be an exciting one! At Neology we firmly believe that the development doesn’t stop – we have almost 30% of our workforce working specifically in the product development area of our business in order to constantly evolve our solutions, improve performance and add new features. We have some exciting additions to the portfolio which are imminent that will provide not only performance improvements to the existing solutions but also provide the ability for greater inter-operability across the Law Enforcement ALPR market in the US more generally. We believe that you retaining the control and ownership of your data is paramount and we

continue to respect that as we always have while supporting those customers who choose to share and provide secure, trusted data sharing between neighbours and friends.

We are always keen to hear your feedback – if there are any elements of our services, solutions or products which you would like to feedback on, please don't hesitate to get in touch with me so I can provide personal attention to both positive and negative feedback. Email me here

Thank you for your continued support – we look forward to serving you in 2020 and beyond.

Best Regards,
Luke & the PIPS Technology team

From: Pamela Biagi
To: Biagi, Pamela (POL)
Subject: Fwd: POL.xlsx
Date: Tuesday, November 24, 2020 1:25:12 PM
Attachments: POL.xlsx

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Sent from my iPhone

Begin forwarded message:

> **From:** "Biagi, Pam (DOC)" <pam.biagi@state.ma.us>
> **Date:** November 17, 2020 at 5:44:28 PM EST
> **To:** Biagifam@comcast.net
> **Subject: POL.xlsx**

From: John Tedona
To: Egnitz, Brian (POL)
Subject: Good News -Court Decision
Date: Thursday, April 16, 2020 7:22:29 PM
Attachments: image001.png
image004.png

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Yeah!

Commonwealth v. McCarthy
Supreme Judicial Court, April 16, 2020
(Search and Seizure/Automatic License Plate Readers)

The use of four automatic license plate reader cameras, placed at two fixed locations on the ends of the Bourne and Sagamore bridges and used to "hit" on the defendant's license when he drove over either bridge,, does not constitute a search within the meaning of either art. 14 or the Fourth Amendment.

"While we recognize that the widespread use of ALPRs in the Commonwealth could implicate constitutional protections against unreasonable searches, the limited use of the technology in this case does not."

Note:
The Court did not find error in the fact that the Bourne Police Department did not have a separate policy, apart from State Police TRF-11, regarding ALPRs.

Additionally, the Court ruled that the government's use of ALPR data is not subject to the Stored Communication Act nor the Electronic Communications Privacy Act

See attached opinion.

For other recent case law decisions, go to the MDAA website at www.mass.gov/mdaa

A NEOLOGY Business
John Tedona
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: John Tedona
To: Egnitz, Brian (POL)
Cc: Peter Crary
Subject: Interoperability
Date: Monday, August 10, 2020 1:32:30 PM
Attachments: image001.png
image002.png
UTMC Protocol - TR007 001c.doc

Brian -Here's a draft of a document we'll soon be releasing that outlines the protocol for data exchange between PIPS and 3rd ALPR providers.

Curious of any comments you may have.



A NEOLOGY Business

John Tedona
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: jdowling@motorolasolutions.com
To: Quinn, Dermot (POL); Venkatachalam, Krishna (EPS); chris.perez@motorolasolutions.com; Slater, James (CHS); McCarthy, Steven (POL); kevin.coughlin@motorolasolutions.com
Subject: Invitation: Discuss ALPR @ Mon Jun 15, 2020 3pm - 4pm (EDT) (dermot.quinn@state.ma.us)
Attachments: invite.ics

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

You have been invited to the following event.

Discuss ALPR

When
Mon Jun 15, 2020 3pm – 4pm Eastern Time - New York
Joining info
Join with Google Meet
meet.google.com/qvd-pama-fpp <https://urldefense.proofpoint.com/v2/url?u=https-3A__meet.google.com_qvd-2Dpama-2Dfpp&d=DwMFaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=52iQJxugFItm50WNOI-wrgNwBz296DG2ltCJ4cn6yHs&m=83yHly1dDaSGFlAVLUJ0MPqWlrcoOyVtNvNmLbXLiwY&s=GwTjyskH4cLti8eMgT2y3-0TBmhBRkebVHo8v7CoYXw&e=>

Join by phone
+1 650-535-0555 <about:invalid#zSoyz> (PIN: 564593383)

More phone numbers <https://urldefense.proofpoint.com/v2/url?u=https-3A__tel.meet_qvd-2Dpama-2Dfpp-3Fpin-3D3789348892710-26hs-3D0&d=DwMFaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=52iQJxugFItm50WNOI-wrgNwBz296DG2ltCJ4cn6yHs&m=83yHly1dDaSGFlAVLUJ0MPqWlrcoOyVtNvNmLbXLiwY&s=1G-3D7ZGRbWf1a4OP5J4WumSUyOs7lXMl-t8XuXAsrI&e=>
Calendar
dermot.quinn@state.ma.us
Who
•
jdowling@motorolasolutions.com
- organizer
•
dermot.quinn@state.ma.us
•
krishna.venkatachalam@state.ma.us
•
chris.perez@motorolasolutions.com
•
james.slater@state.ma.us
•
steven.mccarthy@state.ma.us
•
kevin.coughlin@motorolasolutions.com
more details » <https://urldefense.proofpoint.com/v2/url?u=https-3A__www.google.com_calendar_event-3Faction-3DVIEW-26eid-3DNmxpZjQ3b2RrZW82ZTNmNWJmMXZtbGx0dmIgZGVybW90LnF1aW5uQHN0YXRlLm1hLnVz-26tok-3DMzAjamRvd2xpbmdAbW90b3JvbGFzb2x1dGlvbnMuY29tNWEzMDFiYmJkY2RiMTUyNDNiNTM5MmVmNjZlZmQ4NTA5YTE4OTljOQ-26ctz-3DAmerica-252FNew-5FYork-26hl-3Den-26es-3D0&d=DwMFaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=52iQJxugFItm50WNOI-wrgNwBz296DG2ltCJ4cn6yHs&m=83yHly1dDaSGFlAVLUJ0MPqWlrcoOyVtNvNmLbXLiwY&s=X3Xii-ghXjD3_X81jtkzQug0TwMyooNzXV9GT-Kq1qQ&e=>

Going (dermot.quinn@state.ma.us)?
Yes <https://urldefense.proofpoint.com/v2/url?u=https-3A__www.google.com_calendar_event-3Faction-3DRESPOND-26eid-3DNmxpZjQ3b2RrZW82ZTNmNWJmMXZtbGx0dmIgZGVybW90LnF1aW5uQHN0YXRlLm1hLnVz-26rst-3D1-26tok-3DMzAjamRvd2xpbmdAbW90b3JvbGFzb2x1dGlvbnMuY29tNWEzMDFiYmJkY2RiMTUyNDNiNTM5MmVmNjZlZmQ4NTA5YTE4OTljOQ-26ctz-3DAmerica-252FNew-5FYork-26hl-3Den-26es-3D0&d=DwMFaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=52iQJxugFItm50WNOI-wrgNwBz296DG2ltCJ4cn6yHs&m=83yHly1dDaSGFlAVLUJ0MPqWlrcoOyVtNvNmLbXLiwY&s=im3YeBBoc6tpRI52kk4gpzfcTTqy-TMCgkrSOdBTC8k&e=> -
Maybe <https://urldefense.proofpoint.com/v2/url?u=https-3A__www.google.com_calendar_event-3Faction-3DRESPOND-26eid-3DNmxpZjQ3b2RrZW82ZTNmNWJmMXZtbGx0dmIgZGVybW90LnF1aW5uQHN0YXRlLm1hLnVz-26rst-3D3-26tok-3DMzAjamRvd2xpbmdAbW90b3JvbGFzb2x1dGlvbnMuY29tNWEzMDFiYmJkY2RiMTUyNDNiNTM5MmVmNjZlZmQ4NTA5YTE4OTljOQ-26ctz-3DAmerica-252FNew-5FYork-26hl-3Den-26es-3D0&d=DwMFaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=52iQJxugFItm50WNOI-wrgNwBz296DG2ltCJ4cn6yHs&m=83yHly1dDaSGFlAVLUJ0MPqWlrcoOyVtNvNmLbXLiwY&s=z2M6AZ5pI7oNu2Cs_N8YtpP0_wEk-2FcFs-o9NmmuO0&e=> -
No <https://urldefense.proofpoint.com/v2/url?u=https-3A__www.google.com_calendar_event-3Faction-3DRESPOND-26eid-3DNmxpZjQ3b2RrZW82ZTNmNWJmMXZtbGx0dmIgZGVybW90LnF1aW5uQHN0YXRlLm1hLnVz-26rst-3D2-26tok-3DMzAjamRvd2xpbmdAbW90b3JvbGFzb2x1dGlvbnMuY29tNWEzMDFiYmJkY2RiMTUyNDNiNTM5MmVmNjZlZmQ4NTA5YTE4OTljOQ-26ctz-3DAmerica-252FNew-5FYork-26hl-3Den-26es-3D0&d=DwMFaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=52iQJxugFItm50WNOI-wrgNwBz296DG2ltCJ4cn6yHs&m=83yHly1dDaSGFlAVLUJ0MPqWlrcoOyVtNvNmLbXLiwY&s=FOqT74zCZXR3LiS3vsmFdTsqVBXZhR29E0Pklp8LmJ8&e=>
more options » <https://urldefense.proofpoint.com/v2/url?u=https-3A__www.google.com_calendar_event-3Faction-3DVIEW-26eid-3DNmxpZjQ3b2RrZW82ZTNmNWJmMXZtbGx0dmIgZGVybW90LnF1aW5uQHN0YXRlLm1hLnVz-26tok-3DMzAjamRvd2xpbmdAbW90b3JvbGFzb2x1dGlvbnMuY29tNWEzMDFiYmJkY2RiMTUyNDNiNTM5MmVmNjZlZmQ4NTA5YTE4OTljOQ-26ctz-3DAmerica-252FNew-5FYork-26hl-3Den-26es-3D0&d=DwMFaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=52iQJxugFItm50WNOI-wrgNwBz296DG2ltCJ4cn6yHs&m=83yHly1dDaSGFlAVLUJ0MPqWlrcoOyVtNvNmLbXLiwY&s=X3Xii-ghXjD3_X81jtkzQug0TwMyooNzXV9GT-Kq1qQ&e=>

Invitation from Google Calendar <https://urldefense.proofpoint.com/v2/url?u=https-3A__www.google.com_calendar_&d=DwMFaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=52iQJxugFItm50WNOI-wrgNwBz296DG2ltCJ4cn6yHs&m=83yHly1dDaSGFlAVLUJ0MPqWlrcoOyVtNvNmLbXLiwY&s=0YDN8oT0TBVi4YDkc4ajDELOgbCKeXdR8MqhQof7mKs&e=>

You are receiving this courtesy email at the account dermot.quinn@state.ma.us because you are an attendee of this event.

To stop receiving future updates for this event, decline this event. Alternatively you can sign up for a Google account at https://www.google.com/calendar/ and control your notification settings for your entire calendar.

Forwarding this invitation could allow any recipient to send a response to the organizer and be added to the guest list, or invite others regardless of their own invitation status, or to modify your RSVP. Learn More <https://urldefense.proofpoint.com/v2/url?u=https-3A__support.google.com_calendar_answer_37135-23forwarding&d=DwMFaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=52iQJxugFItm50WNOI-wrgNwBz296DG2ltCJ4cn6yHs&m=83yHly1dDaSGFlAVLUJ0MPqWlrcoOyVtNvNmLbXLiwY&s=Pzv7ScZwmuVA4NXFPwMfQNThJgL8SCxGDqUT8Uc9uGQ&e=>

.

Your privacy is important to us. That is why we have taken appropriate measures to ensure the data you provide to us is kept secure. To learn more about how we process your personal information, how we comply with applicable data protection laws, and care for the security and privacy of your personal data, please review our Privacy Policy. If you have any questions related to data protection and compliance with applicable laws, please contact us at our Security Operations Center at 1-800-674-4357.

From: jdowling@motorolasolutions.com
To: Quinn, Dermot (POL); Venkatachalam, Krishna (EPS); chris.perez@motorolasolutions.com; Slater, James (CHS); McCarthy, Steven (POL); kevin.coughlin@motorolasolutions.com
Subject: Invitation: Discuss ALPR @ Mon Jun 15, 2020 3pm - 4pm (EDT) (steven.mccarthy@state.ma.us)
Attachments: invite.ics

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

You have been invited to the following event.

Discuss ALPR

When
Mon Jun 15, 2020 3pm – 4pm Eastern Time - New York
Joining info
Join with Google Meet
meet.google.com/qvd-pama-fpp <https://urldefense.proofpoint.com/v2/url?u=https-3A__meet.google.com_qvd-2Dpama-2Dfpp&d=DwMFaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=S9uhpCwEr9VmLHlJVB8aUBoSpJsh_3f_pPyNlM4FFLA&m=N5Kp7NT0FULuHc193N-2vNxayGznDsMepBVwSHMAtW0&s=ciC0bitZiGYdnZHivSzAf05F2QySkma-LmFSbMrgvMU&e=>

Join by phone
+1 650-535-0555 <about:invalid#zSoyz> (PIN: 564593383)

More phone numbers <https://urldefense.proofpoint.com/v2/url?u=https-3A__tel.meet_qvd-2Dpama-2Dfpp-3Fpin-3D3789348892710-26hs-3D0&d=DwMFaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=S9uhpCwEr9VmLHlJVB8aUBoSpJsh_3f_pPyNlM4FFLA&m=N5Kp7NT0FULuHc193N-2vNxayGznDsMepBVwSHMAtW0&s=PPvM28lsZsExoI7j9eCIE1S03EJC0mj7yBAGdKAOWPs&e=>
Calendar
steven.mccarthy@state.ma.us
Who
•
jdowling@motorolasolutions.com
- organizer
•
dermot.quinn@state.ma.us
•
krishna.venkatachalam@state.ma.us
•
chris.perez@motorolasolutions.com
•
james.slater@state.ma.us
•
steven.mccarthy@state.ma.us
•
kevin.coughlin@motorolasolutions.com
more details » <https://urldefense.proofpoint.com/v2/url?u=https-3A__www.google.com_calendar_event-3Faction-3DVIEW-26eid-3DNmxpZjQ3b2RrZW82ZTNmNWJmMXZtbGx0dmIgc3RldmVuLm1jY2FydGh5QHN0YXRlLm1hLnVz-26tok-3DMzAjamRvd2xpbmdAbW90b3JvbGFzb2x1dGlvbnMuY29tMGRmZDdjOTRlMTFjZGFhNjZiZWEyMTA3NTdmNjNjNzJhY2M0MTM0Mg-26ctz-3DAmerica-252FNew-5FYork-26hl-3Den-26es-3D0&d=DwMFaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=S9uhpCwEr9VmLHlJVB8aUBoSpJsh_3f_pPyNlM4FFLA&m=N5Kp7NT0FULuHc193N-2vNxayGznDsMepBVwSHMAtW0&s=xsNNacVHE_rDgCIzCcGaDYph4fNEz1wTDmI4YBeu7hc&e=>

Going (steven.mccarthy@state.ma.us)?
Yes <https://urldefense.proofpoint.com/v2/url?u=https-3A__www.google.com_calendar_event-3Faction-3DRESPOND-26eid-3DNmxpZjQ3b2RrZW82ZTNmNWJmMXZtbGx0dmIgc3RldmVuLm1jY2FydGh5QHN0YXRlLm1hLnVz-26rst-3D1-26tok-3DMzAjamRvd2xpbmdAbW90b3JvbGFzb2x1dGlvbnMuY29tMGRmZDdjOTRlMTFjZGFhNjZiZWEyMTA3NTdmNjNjNzJhY2M0MTM0Mg-26ctz-3DAmerica-252FNew-5FYork-26hl-3Den-26es-3D0&d=DwMFaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=S9uhpCwEr9VmLHlJVB8aUBoSpJsh_3f_pPyNlM4FFLA&m=N5Kp7NT0FULuHc193N-2vNxayGznDsMepBVwSHMAtW0&s=-mBf_wprdBGt0SZCAwf--5ZkZBA0xAu2eu9PGsrZhAI&e=> -
Maybe <https://urldefense.proofpoint.com/v2/url?u=https-3A__www.google.com_calendar_event-3Faction-3DRESPOND-26eid-3DNmxpZjQ3b2RrZW82ZTNmNWJmMXZtbGx0dmIgc3RldmVuLm1jY2FydGh5QHN0YXRlLm1hLnVz-26rst-3D3-26tok-3DMzAjamRvd2xpbmdAbW90b3JvbGFzb2x1dGlvbnMuY29tMGRmZDdjOTRlMTFjZGFhNjZiZWEyMTA3NTdmNjNjNzJhY2M0MTM0Mg-26ctz-3DAmerica-252FNew-5FYork-26hl-3Den-26es-3D0&d=DwMFaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=S9uhpCwEr9VmLHlJVB8aUBoSpJsh_3f_pPyNlM4FFLA&m=N5Kp7NT0FULuHc193N-2vNxayGznDsMepBVwSHMAtW0&s=KvoDcPNW7qKJ9n0i3__IgM13nTmdg9OUTLyQrI6xU4c&e=> -
No <https://urldefense.proofpoint.com/v2/url?u=https-3A__www.google.com_calendar_event-3Faction-3DRESPOND-26eid-3DNmxpZjQ3b2RrZW82ZTNmNWJmMXZtbGx0dmIgc3RldmVuLm1jY2FydGh5QHN0YXRlLm1hLnVz-26rst-3D2-26tok-3DMzAjamRvd2xpbmdAbW90b3JvbGFzb2x1dGlvbnMuY29tMGRmZDdjOTRlMTFjZGFhNjZiZWEyMTA3NTdmNjNjNzJhY2M0MTM0Mg-26ctz-3DAmerica-252FNew-5FYork-26hl-3Den-26es-3D0&d=DwMFaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=S9uhpCwEr9VmLHlJVB8aUBoSpJsh_3f_pPyNlM4FFLA&m=N5Kp7NT0FULuHc193N-2vNxayGznDsMepBVwSHMAtW0&s=EE-O58cIoOe8n9P0CTU8G6iI-QrBS-zlzbeKZ0GvqtM&e=> more options »
<https://urldefense.proofpoint.com/v2/url?u=https-3A__www.google.com_calendar_event-3Faction-3DVIEW-26eid-3DNmxpZjQ3b2RrZW82ZTNmNWJmMXZtbGx0dmIgc3RldmVuLm1jY2FydGh5QHN0YXRlLm1hLnVz-26tok-3DMzAjamRvd2xpbmdAbW90b3JvbGFzb2x1dGlvbnMuY29tMGRmZDdjOTRlMTFjZGFhNjZiZWEyMTA3NTdmNjNjNzJhY2M0MTM0Mg-

26ctz-3DAmerica-252FNew-5FYork-26hl-3Den-26es-3D0&d=DwMFaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=S9uhpCwEr9VmLHlJVB8aUBoSpJsh_3f_pPyNlM4FFLA&m=N5Kp7NT0FULuHc193N-2vNxayGznDsMepBVwSHMAtW0&s=xsNNacVHE_rDgCIzCcGaDYph4fNEz1wTDmI4YBeu7hc&e=>

Invitation from Google Calendar <https://urldefense.proofpoint.com/v2/url?u=https-3A__www.google.com_calendar_&d=DwMFaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=S9uhpCwEr9VmLHlJVB8aUBoSpJsh_3f_pPyNlM4FFLA&m=N5Kp7NT0FULuHc193N-2vNxayGznDsMepBVwSHMAtW0&s=7f6QldQD1Vi1vai-aHFDFX-lcoVuzka7sCkOc4Yj7hM&e=>

You are receiving this courtesy email at the account steven.mccarthy@state.ma.us because you are an attendee of this event.

To stop receiving future updates for this event, decline this event. Alternatively you can sign up for a Google account at https://www.google.com/calendar/ and control your notification settings for your entire calendar.

Forwarding this invitation could allow any recipient to send a response to the organizer and be added to the guest list, or invite others regardless of their own invitation status, or to modify your RSVP. Learn More <https://urldefense.proofpoint.com/v2/url?u=https-3A__support.google.com_calendar_answer_37135-23forwarding&d=DwMFaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=S9uhpCwEr9VmLHlJVB8aUBoSpJsh_3f_pPyNlM4FFLA&m=N5Kp7NT0FULuHc193N-2vNxayGznDsMepBVwSHMAtW0&s=8E6FEVmkNzyoDyEBn5Ijro1VBNJ9tYRGS_r0F5qY9QY&e=> .

Your privacy is important to us. That is why we have taken appropriate measures to ensure the data you provide to us is kept secure. To learn more about how we process your personal information, how we comply with applicable data protection laws, and care for the security and privacy of your personal data, please review our Privacy Policy. If you have any questions related to data protection and compliance with applicable laws, please contact us at our Security Operations Center at 1-800-674-4357.

From: jdowling@motorolasolutions.com
To: Bennett, Marcy (POL)
Subject: Invitation: Discuss ALPR @ Mon Jun 15, 2020 3pm - 4pm (EDT) (dermot.quinn@state.ma.us)
Attachments: invite.ics

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

You have been invited to the following event.

Discuss ALPR

When
Mon Jun 15, 2020 3pm – 4pm Eastern Time - New York
Joining info
Join with Google Meet
meet.google.com/qvd-pama-fpp <https://urldefense.proofpoint.com/v2/url?u=https-3A__meet.google.com_qvd-2Dpama-2Dfpp&d=DwMFaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=52iQJxugFItm50WNOI-wrgNwBz296DG2ltCJ4cn6yHs&m=83yHly1dDaSGFlAVLUJ0MPqWlrcoOyVtNvNmLbXLiwY&s=GwTjyskH4cLti8eMgT2y3-0TBmhBRkebVHo8v7CoYXw&e=>

Join by phone
+1 650-535-0555 <about:invalid#zSoyz> (PIN: 564593383)

More phone numbers <https://urldefense.proofpoint.com/v2/url?u=https-3A__tel.meet_qvd-2Dpama-2Dfpp-3Fpin-3D3789348892710-26hs-3D0&d=DwMFaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=52iQJxugFItm50WNOI-wrgNwBz296DG2ltCJ4cn6yHs&m=83yHly1dDaSGFlAVLUJ0MPqWlrcoOyVtNvNmLbXLiwY&s=1G-3D7ZGRbWf1a4OP5J4WumSUyOs7lXMl-t8XuXAsrI&e=>
Calendar
dermot.quinn@state.ma.us
Who
•
jdowling@motorolasolutions.com
- organizer
•
dermot.quinn@state.ma.us
•
krishna.venkatachalam@state.ma.us
•
chris.perez@motorolasolutions.com
•
james.slater@state.ma.us
•
steven.mccarthy@state.ma.us
•
kevin.coughlin@motorolasolutions.com
more details » <https://urldefense.proofpoint.com/v2/url?u=https-3A__www.google.com_calendar_event-3Faction-3DVIEW-26eid-3DNmxpZjQ3b2RrZW82ZTNmNWJmMXZtbGx0dmIgZGVybW90LnF1aW5uQHN0YXRlLm1hLnVz-26tok-3DMzAjamRvd2xpbmdAbW90b3JvbGFzb2x1dGlvbnMuY29tNWEzMDFiYmJkY2RiMTUyNDNiNTM5MmVmNjZlZmQ4NTA5YTE4OTljOQ-26ctz-3DAmerica-252FNew-5FYork-26hl-3Den-26es-3D0&d=DwMFaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=52iQJxugFItm50WNOI-wrgNwBz296DG2ltCJ4cn6yHs&m=83yHly1dDaSGFlAVLUJ0MPqWlrcoOyVtNvNmLbXLiwY&s=X3Xii-ghXjD3_X81jtkzQug0TwMyooNzXV9GT-Kq1qQ&e=>

Going (dermot.quinn@state.ma.us)?
Yes <https://urldefense.proofpoint.com/v2/url?u=https-3A__www.google.com_calendar_event-3Faction-3DRESPOND-26eid-3DNmxpZjQ3b2RrZW82ZTNmNWJmMXZtbGx0dmIgZGVybW90LnF1aW5uQHN0YXRlLm1hLnVz-26rst-3D1-26tok-3DMzAjamRvd2xpbmdAbW90b3JvbGFzb2x1dGlvbnMuY29tNWEzMDFiYmJkY2RiMTUyNDNiNTM5MmVmNjZlZmQ4NTA5YTE4OTljOQ-26ctz-3DAmerica-252FNew-5FYork-26hl-3Den-26es-3D0&d=DwMFaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=52iQJxugFItm50WNOI-wrgNwBz296DG2ltCJ4cn6yHs&m=83yHly1dDaSGFlAVLUJ0MPqWlrcoOyVtNvNmLbXLiwY&s=im3YeBBoc6tpRI52kk4gpzfcTTqy-TMCgkrSOdBTC8k&e=> - Maybe <https://urldefense.proofpoint.com/v2/url?u=https-3A__www.google.com_calendar_event-3Faction-3DRESPOND-26eid-3DNmxpZjQ3b2RrZW82ZTNmNWJmMXZtbGx0dmIgZGVybW90LnF1aW5uQHN0YXRlLm1hLnVz-26rst-3D3-26tok-3DMzAjamRvd2xpbmdAbW90b3JvbGFzb2x1dGlvbnMuY29tNWEzMDFiYmJkY2RiMTUyNDNiNTM5MmVmNjZlZmQ4NTA5YTE4OTljOQ-26ctz-3DAmerica-252FNew-5FYork-26hl-3Den-26es-3D0&d=DwMFaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=52iQJxugFItm50WNOI-wrgNwBz296DG2ltCJ4cn6yHs&m=83yHly1dDaSGFlAVLUJ0MPqWlrcoOyVtNvNmLbXLiwY&s=z2M6AZ5pI7oNu2Cs_N8YtpP0_wEk-2FcFs-o9NmmuO0&e=> - No <https://urldefense.proofpoint.com/v2/url?u=https-3A__www.google.com_calendar_event-3Faction-3DRESPOND-26eid-3DNmxpZjQ3b2RrZW82ZTNmNWJmMXZtbGx0dmIgZGVybW90LnF1aW5uQHN0YXRlLm1hLnVz-26rst-3D2-26tok-3DMzAjamRvd2xpbmdAbW90b3JvbGFzb2x1dGlvbnMuY29tNWEzMDFiYmJkY2RiMTUyNDNiNTM5MmVmNjZlZmQ4NTA5YTE4OTljOQ-26ctz-3DAmerica-252FNew-5FYork-26hl-3Den-26es-3D0&d=DwMFaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=52iQJxugFItm50WNOI-wrgNwBz296DG2ltCJ4cn6yHs&m=83yHly1dDaSGFlAVLUJ0MPqWlrcoOyVtNvNmLbXLiwY&s=FOqT74zCZXR3LiS3vsmFdTsqVBXZhR29E0Pklp8LmJ8&e=>
more options » <https://urldefense.proofpoint.com/v2/url?u=https-3A__www.google.com_calendar_event-3Faction-3DVIEW-26eid-3DNmxpZjQ3b2RrZW82ZTNmNWJmMXZtbGx0dmIgZGVybW90LnF1aW5uQHN0YXRlLm1hLnVz-26tok-3DMzAjamRvd2xpbmdAbW90b3JvbGFzb2x1dGlvbnMuY29tNWEzMDFiYmJkY2RiMTUyNDNiNTM5MmVmNjZlZmQ4NTA5YTE4OTljOQ-26ctz-3DAmerica-252FNew-5FYork-26hl-3Den-26es-3D0&d=DwMFaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=52iQJxugFItm50WNOI-wrgNwBz296DG2ltCJ4cn6yHs&m=83yHly1dDaSGFlAVLUJ0MPqWlrcoOyVtNvNmLbXLiwY&s=X3Xii-ghXjD3_X81jtkzQug0TwMyooNzXV9GT-Kq1qQ&e=>

Invitation from Google Calendar <https://urldefense.proofpoint.com/v2/url?u=https-3A__www.google.com_calendar_&d=DwMFaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=52iQJxugFItm50WNOI-wrgNwBz296DG2ltCJ4cn6yHs&m=83yHly1dDaSGFlAVLUJ0MPqWlrcoOyVtNvNmLbXLiwY&s=0YDN8oT0TBVi4YDkc4ajDELOgbCKeXdR8MqhQof7mKs&e=>

You are receiving this courtesy email at the account dermot.quinn@state.ma.us because you are an attendee of this event.

To stop receiving future updates for this event, decline this event. Alternatively you can sign up for a Google account at https://www.google.com/calendar/ and control your notification settings for your entire calendar.

Forwarding this invitation could allow any recipient to send a response to the organizer and be added to the guest list, or invite others regardless of their own invitation status, or to modify your RSVP. Learn More <https://urldefense.proofpoint.com/v2/url?u=https-3A__support.google.com_calendar_answer_37135-23forwarding&d=DwMFaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=52iQJxugFItm50WNOI-wrgNwBz296DG2ltCJ4cn6yHs&m=83yHly1dDaSGFlAVLUJ0MPqWlrcoOyVtNvNmLbXLiwY&s=Pzv7ScZwmuVA4NXFPwMfQNThJgL8SCxGDqUT8Uc9uGQ&e=>
.

Your privacy is important to us. That is why we have taken appropriate measures to ensure the data you provide to us is kept secure. To learn more about how we process your personal information, how we comply with applicable data protection laws, and care for the security and privacy of your personal data, please review our Privacy Policy. If you have any questions related to data protection and compliance with applicable laws, please contact us at our Security Operations Center at 1-800-674-4357.

From: Strategic Planning (POL)
To: mark.justice@delaware.gov
Subject: License Plate Readers
Date: Tuesday, September 15, 2020 10:37:12 AM
Attachments: Automatic License Plate Recognition - Policy.pdf

---

Sgt. Justice,

Per your request, please see attached for the Massachusetts State Police Policy in regards to License Plate Readers.

Respectfully,

Tpr. Michael Abany
Strategic Planning
Massachusetts State Police

From: Quinn, Dermot (POL)
To: Mason, Christopher (POL); Warmington, Scott (POL)
Subject: LPR
Date: Monday, February 10, 2020 9:34:37 AM
Attachments: image001.png
image002.png
image003.png
image004.png
image005.png
image006.png

Sirs,

Are you ok with this email? I would like to send to EOPSS and EOTSS and Massport teams.

Respectfully,

DJQ

Good Morning,

I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.

Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.

Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as "BOSS" and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport's cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.

MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.

I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.

To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.

I can't overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security's technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.

Respectfully,

Lieutenant Colonel Dermot J. Quinn #1765
Division Commander
Division of Homeland Security & Preparedness
Massachusetts State Police

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, January 17, 2020 1:10 PM
To: Slater, James (CHS) <james.slater@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>; Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; John Tedona <jtedona@neology.net>; Chute, Alexander <AChute@massport.com>; Peter Crary <pcrary@neology.net>; Michalski, Maria (EPS) <maria.michalski@mass.gov>
Subject: RE: MassPort LPR Cameras

Hi Jim,

BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for

infrastructure. The below is still outstanding.

-Brian

From: Egnitz, Brian (POL)
Sent: Monday, January 6, 2020 1:33 PM
To: Slater, James (CHS)
Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter Crary
Subject: RE: MassPort LPR Cameras

Hi Jim,

We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?

Thanks Brian

From: John Tedona [mailto:jtedona@neology.net]
Sent: Monday, December 9, 2019 4:55 PM
To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); Slater, James (CHS)
Subject: RE: MassPort LPR Cameras

Alex,

I can be available most anytime tomorrow for a call.

Regards,

John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: Chute, Alexander <AChute@massport.com>
Sent: Monday, December 9, 2019 4:38 PM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; John Tedona <jtedona@neology.net>; Peter Crary <pcrary@neology.net>
Cc: Guerriero, Robert (MASSIT) <robert.guerriero@state.ma.us>; Peek, Brian T. (EOTSS) <brian.t.peek@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Slater III, James F (CHS) <james.slater@state.ma.us>
Subject: RE: MassPort LPR Cameras

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Hello All,

I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.

Respectfully,

~Alex

Alexander B. Chute
Program Manager, Public Safety Systems
Massachusetts Port Authority
Cell: [redacted]
Office: 617.568.5942
achute@massport.com

WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

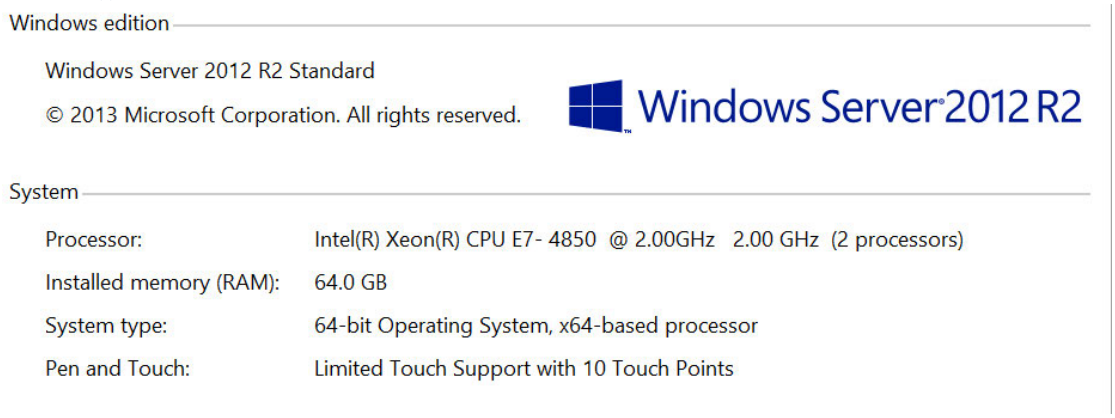
From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Monday, November 18, 2019 3:26 PM
To: John Tedona (jtedona@neology.net); pcrary@neology.net
Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
Subject: RE: MassPort LPR Cameras

Hi John, Peter

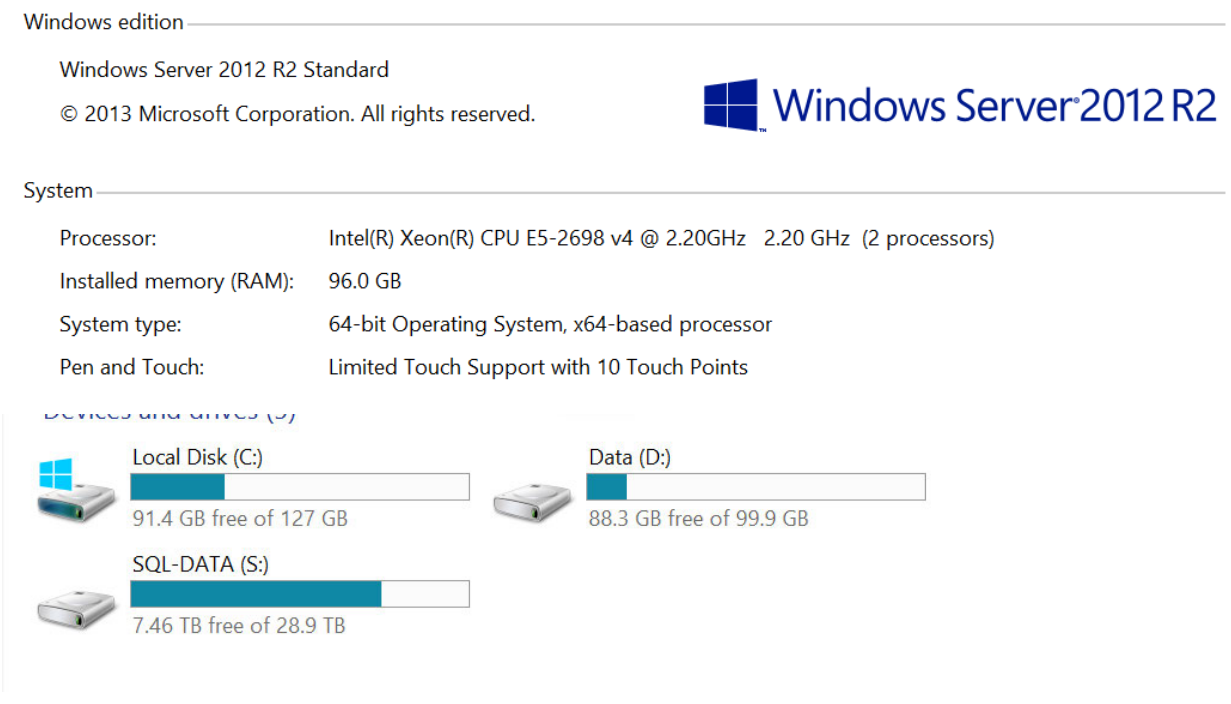
Any issues with moving Massports cameras to the Chelsea DB?

Using the Boss calculator, I estimate that we would need 9-10 TB of storage.

The current app server



Current DB server



Our current reads by month for about 66 active cameras

Year	Month	Day	Month Name	Reads Count
2019	11	1	November	495,113
2019	11	2	November	472,907
2019	11	3	November	384,409

2019	11	4	November	411,440
2019	11	5	November	434,085
2019	11	6	November	495,537
2019	11	7	November	444,123
2019	11	8	November	542,492
2019	11	9	November	443,463
2019	11	10	November	389,514
2019	11	11	November	362,548
2019	11	12	November	236,539

From: Chute, Alexander [mailto:AChute@massport.com]
Sent: Wednesday, November 13, 2019 2:49 PM
To: Egnitz, Brian (POL)
Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
Subject: RE: MassPort LPR Cameras

These stats are from the 18 active cameras we have in the system for this month:

Month	Day	Total Scans
⊟ November		
	1	169551
	2	115486
	3	169178
	4	201136
	5	162319
	6	171825
	7	192996
	8	202159
	9	136410
	10	165834
	11	193613
	12	183947

~Alex

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Tuesday, November 12, 2019 5:28 PM
To: Chute, Alexander
Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
Subject: RE: MassPort LPR Cameras

Hi Alex,

Can you please provide the updated reads per day? Previously you were interested in sharing 6 cameras at approximately 75,000 reads per day.

Here is the P492 confi I mentioned.

Set host to boss[redacted]
Set image[redacted]
Set number of[redacted]
Set Ping interval[redacted]
Set udp ping[redacted]
Set ping wait time[redacted]
Set security[redacted]

I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.

-Brian

From: Chute, Alexander [mailto:AChute@massport.com]
Sent: Tuesday, November 12, 2019 2:08 PM
To: Egnitz, Brian (POL)

Subject: MassPort LPR Cameras

Brian,

Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the Troop F building. I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the roadway cameras are fed to 2 primary network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have 18 cameras in production, with another 19 scheduled to come online within the next two months. I anticipate this number growing to approximately 50 fixed cameras within our campus over the next year. Let me know what you think the appropriate next steps would be.

Respectfully,

~Alex

Alexander B. Chute
Program Manager, Public Safety Systems
Massachusetts Port Authority
Cell: [redacted]
Office: 617.568.5942
achute@massport.com

WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

Lieutenant Colonel Dermot J. Quinn #1765
Division Commander
Division of Investigative Services
Massachusetts State Police

From: Brooks, Brian (POL)
To: Bender, Sean (POL)
Subject: LPR
Date: Friday, January 24, 2020 8:45:00 AM
Attachments: Commonwealth Fusion Center - Weekly Activity Report - 17 January 2020 - 23 January 2020.docx

---

Lieutenant Brian Brooks #2601
Massachusetts State Police
Division of Homeland Security and Preparedness
Commonwealth Fusion Center
470 Worcester Road
Framingham, MA 01702
(W) 508-820-2233
(F) 508-988-7121

From: McCarthy, Maura (AGO)
To: Egnitz, Brian (POL)
Subject: LPR
Date: Thursday, April 23, 2020 9:45:15 AM
Attachments: e12750.pdf
ATT00001.htm

Sir:

Thank you for your response-
The SJC handed down the McCarthy case just last week while we were making our inquiry...!
This is the case that dealt with the issue of whether the collection or search of LPR data without a warrant was an unconstitutional search. The case is important for everyone as it is a Carpenter-centric discussion of technology-facilitated surveillance techniques.
The SJC held that the a person has a constitutionally protected REP in the whole of their public movements, including, potentially, widespread LPR data, but that in this case that interest was not invaded by the limited use. It is very interesting and relevant. Link is below.
Respectfully,
Maura

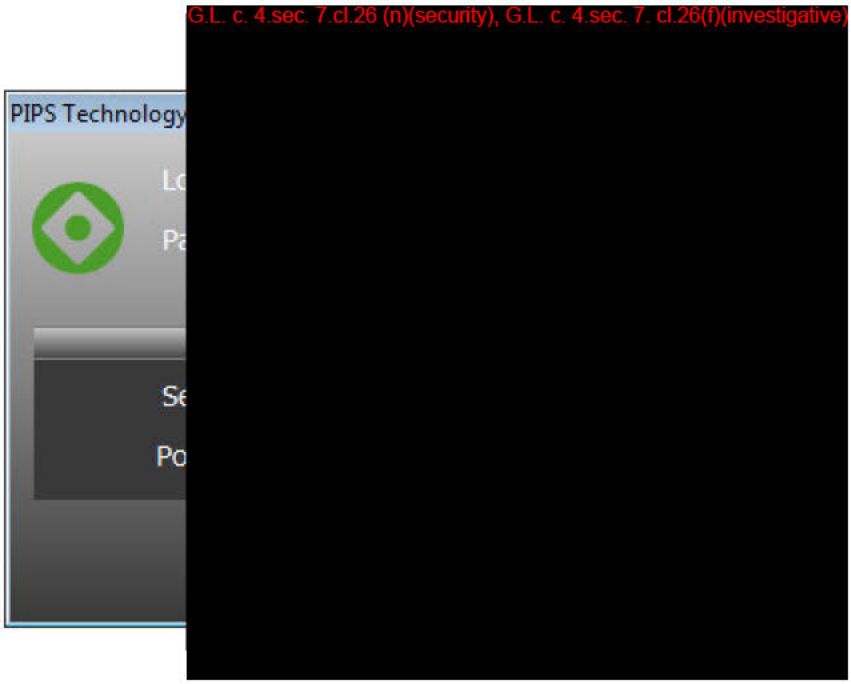
https://www.mass.gov/files/documents/2020/04/16/e12750.pdf

From: Gallagher, David (POL)
To: Walls, Francis (POL)
Date: Tuesday, July 14, 2020 2:23:35 PM
Attachments: BOSS 3.6 USER MANUAL Rev2.pdf
Outlook-cid_image0.png

Frank,

To download the software cut and paste the following into your browser http://[redacted]9988/publish.htm once loaded you will need to configure the port and perhaps the IP address. Click on the "Boss server" which will open the box below and make sure you have the correct server/port info. Once you connect to the server you won't have to do it again.

Your login would be msp2473 and the password I sent you would obviously go in the password section



David M. Gallagher
Captain, Massachusetts State Police
Special Operations
508-988-7442
David.Gallagher3@MassMail.state.ma.us

Date: Tuesday, December 29, 2020 5:23:03 PM
Attachments: image001.png
image003.png

Good Afternoon Kevin,

Based on our telephone conversation, I am inquiring about the possibility of reprogramming $66,420.00 from the ALPR Upgrade and Rhodium projects into the upgrade of our existing case management system.

At the present time we are unable to move forward on the LPR upgrade project (57,000.00) and our Incident Management Assistance Team was able to leverage a Google Docs solution to an existing problem that made it unnecessary to acquire the Rhodium software upgrade at this time ($9,420.00). That leaves us $66,420.00 in unspent funds.

Within the Massachusetts State Police the Division of Investigative Services and the Division of Homeland Security use a commercial records/case management system known as ACISS Case Management. The Division of Field Services (the uniform patrol division) uses a “in house” developed system called RAMS for its record management system. While there is some communication between the two systems, the situation is far from optimal when it comes to information sharing both internally at MSP and with our local and federal partners. MSP is currently creating modules within ACISS that will serve the needs of the Division of Field Services in an effort to have all MSP Divisions contribute all information into one unified database.

The project has been broken down into two scopes of work. The second scope of work will allow for the creation of a customized “Vehicle Crash” module that would allow MSP to centrally locate all crash data inside the ACISS records/case management system. Given that MSP investigates over

Deliverables

Crash enhancements
Enhancing the crash module with all fields needed by MSP,
A web based diagramming tool,
crash report exchange form, insurance information pushed from CJISWEB
CRA65, CRA23, SP425 forms
RMV submission interface
Towing module
A new module that will handle picking a tow company in rotation when needed to to a crash or arrest based
on geographical boundaries
linked to call for service or arrest

Lieutenant Colonel Dermot J. Quinn #1765
Division Commander
Division of Investigative Services
Massachusetts State Police

From: John Tedona
To: Egnitz, Brian (POL)
Subject: Mobile ALPR Processor System
Date: Thursday, July 2, 2020 9:41:28 AM
Attachments: image001.png
image003.png
PAGIS 2.14 MANUAL_ADMIN.pdf
PAGIS 2.14 MANUAL_USERS.pdf
SX4e Mobile Installation Guide.pdf
FedX Track.pdf

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Brian,

The mobile SX4e processor and 25mm camera is scheduled to arrive this Monday. I'm not sure how you will use the system so I included two different power cords. One you can plug into a cigarette lighter, the other you can wire the pig tails to your power source. (Black is (-) ground, Red is (+) hot, Blue goes to ignition source if on a vehicle). If you're wiring to a non automotive power supply both Red and Blue leads go to (+) hot. See the attached Installation manual for more info and display/laptop wiring.

As for setup, the processor is configured for "Standalone" mode meaning you would use a monitor and keyboard. If you want to use the processor via a laptop you need to configure the processor for "VPRelay" (see page 47 in the attached admin manual on how to switch between the two.

As for usage, the processor already has the MA OCR engine installed, the camera's flash tables are already set and port C1 on the processor is where you plug in the 25mm PIPS camera. This camera has a 45' focus range, so for placement purposes start at a distance of 45' then incrementally increase the distance to see how far out you can maintain plate capture and read accuracy. The camera Port C3 has been setup for a 3rd party webcam. Running both PIPS and 3rd party cameras simultaneously will let you compare both cameras performance in real time. You will need to speak with Dave Bynum (PIPS IT Tech) to ensure the proper SDK is loaded for the web cam….I'll get you guys together when you're ready.

Call me when you're ready to use the system so I can walk you through how to use it.

Have Fun!

PIPS TECHNOLOGY
A NEOLOGY Business

John Tedona

Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: McCarthy, Steven (POL)
To: Quinn, Dermot (POL)
Subject: Motorola response
Date: Thursday, June 11, 2020 12:47:00 PM
Attachments: FINAL - MSP Proposal Response - WatchGuard signed.pdf

---

FYI Col.,

Vigilant section starts at page 187.

Steve

Detective Captain Steven McCarthy
Division of Homeland Security and Preparedness
Massachusetts State Police
480 Worcester Road
Framingham, MA 01702
508-988-7314

From: Connolly, Steven (AGO)
To: Morrissette, Brock A (POL)
Subject: new case law
Date: Thursday, April 16, 2020 11:32:16 AM
Attachments: comm v mccarthy plate readers.pdf

Lieutenant Steven Connolly #2719
Massachusetts State Police
Office of the Attorney General

From: Bender, Sean (POL)
To: Brooks, Brian (POL)
Subject: New Lieutenant Checklist
Date: Wednesday, March 25, 2020 7:24:10 AM
Attachments: Transfer Checklist.docx

Good Morning, Lieutenant -

Since I have an idea of what you'll be doing for the next three days...

I've attached some housekeeping items, links, and points of contact for the new Lieutenants. I'm sure there are some things missing, but this hopefully at least has the essentials and who to contact to get them up and running ASAP.

Give me a shout if you have any questions or need anything.

Respectfully,

Sean Bender
Intelligence Analyst
Massachusetts State Police | Commonwealth Fusion Center
470 Worcester Road | Framingham | MA 01702
508-820-2233

From: John Tedona
To: Egnitz, Brian (POL)
Cc: Miranda Fischer; Luke Normington
Subject: New Solutions and End-Of-Life Announcement
Date: Thursday, January 16, 2020 5:52:19 PM
Attachments: image001.png
image002.png
PIPS 2020 Bulletin.pdf

Mr. Egnitz,

As we step into a new year, and decade, we wanted to take a moment to thank you for your continued loyalty and use of the PIPS Technology by Neology solutions. We are incredibly grateful of the customers, resellers and partners who, over the last years have remained loyal and supported us in our vision of "Driving Detection Innovation". Each day we strive to make a difference in supporting you to achieve your goals, solve your challenges and achieve your mission.

2019 was a major year for us as we finalised significant elements of the overhaul of our products and solutions, culminating with the release of BOSS 4 in the fall, alongside brand new Fixed and Mobile ALPR solutions. Attached you will find the latest reminders in relation to our products and software versions to ensure you are getting the most out of your Neology products and solutions.

The year ahead is primed to be an exciting one! At Neology we firmly believe that the development doesn't stop – we have almost 30% of our workforce working specifically in the product development area of our business in order to constantly evolve our solutions, improve performance and add new features. We have some exciting additions to the portfolio which are imminent that will provide not only performance improvements to the existing solutions but also provide the ability for greater inter-operability across the Law Enforcement ALPR market in the US more generally. We believe that you retaining the control and ownership of your data is paramount and we continue to respect that as we always have while supporting those customers who choose to share and provide secure, trusted data sharing between neighbours and friends.

We are always keen to hear your feedback – if there are any elements of our services, solutions or products which you would like to feedback on, please don't hesitate to get in touch with me so I can provide personal attention to both positive and negative feedback. Email me here

Thank you for your continued support – we look forward to serving you in 2020 and beyond.

Best Regards,
Luke & the PIPS Technology team



A NEOLOGY Business

John Tedona
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: Miller, Dianne (POL)
To: Silva, Kyra (POL)
Cc: Comeau, Melissa (POL); Biagi, Pamela (POL)
Subject: OGR and DOC > Automatic License Plate Reader Policy
Date: Tuesday, December 15, 2020 9:37:44 AM
Attachments: TRF-11 Automatic License Plate Recognition Revised 10-1-2019.pdf

---

Hi Kyra,

Please see email chain below.

Please confirm I can forward the attached policy to Gina (OGR) for review by DOC staff ordering ALPRs.
I will also refer them to the DCJIS policy below and remind them that Commonwealth IT Terms and Conditions apply (to the vendor) because we order ALPRs through OTIS.

Thanks
Di

From: Gallagher, David (POL)
Sent: Tuesday, December 15, 2020 9:30 AM
To: Miller, Dianne (POL); Thibault, Amy (POL)
Cc: Range, Scott (POL)
Subject: Re: Automatic License Plate Reader Policy

Dianne,

I believe this is the policy you were inquiring about. Please feel free to share. If you or anyone else has any questions, please contact me.

Thank you,

David M. Gallagher
Major, Massachusetts State Police
Special Operations
508-820-2162
David.Gallagher3@MassMail.state.ma.us

Good Morning Dianne,

I've copied Major Gallagher on this because I think he is now the MSP Department ALPR Coordinator if I'm not mistaken.

TRF-11 is the MSP policy for ALPR.

EOPSS – DCJIS has a policy as listed below. I don't have a copy of it but EOPSS – DCJIS must so Gina or DOC should be able to check with them directly.

Executive Office of Public Safety and Security (EOPSS) - *The Commonwealth of Massachusetts Global Justice and Public Safety Information Sharing Policy*
Executive Office of Public Safety and Security (EOPSS) - Department of Criminal Justice Information Services - *Automatic License Plate Recognition System Central Repository Companion Policy.*

Major Gallagher – Please feel free to weigh in. Is it ok for Dianne to give the DOC TRF-11?

Finally, Gina and DOC should probably check with EOPSS legal and/or MSP legal in case they have any additional insights on ALPR policy developments.

Thank you/Respectfully,
Scott

From: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Sent: Tuesday, December 15, 2020 8:48 AM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Range, Scott (POL) <scott.range@pol.state.ma.us>
Subject: RE: Automatic License Plate Reader Policy

Good morning Major Range and Amy,
Is there a law enforcement policy relative to ALPR's? See below email from EOPSS…
Thanks
Di

From: Papagiorgakis, Gina (OGR)
Sent: Tuesday, December 15, 2020 8:23 AM
To: Miller, Dianne (POL)
Subject: Automatic License Plate Reader Policy

Good morning Dianne,

I am hoping you can put me in touch with the right contact on your end. The DOC was awarded grant funds to procure an automatic license plate reader system, and thus will need to implement a policy. They are looking to reference existing policies to guide a draft of their own. Is there a policy at MSP that can be shared with the DOC, or is there anyone else who I should reach out to at MSP?

Thank you in advance.

Gina Papagiorgakis
Homeland Security Division
Office of Grants and Research
10 Park Plaza, Suite 3720-A
Boston, MA 02116

gina.papagiorgakis1@mass.gov

From: Range, Scott (POL) <scott.range@pol.state.ma.us>
Sent: Tuesday, December 15, 2020 9:19 AM
To: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>; Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Cc: Gallagher, David (POL) <david.gallagher3@MassMail.State.MA.US>; Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: RE: Automatic License Plate Reader Policy

Good Morning Dianne,

I've copied Major Gallagher on this because I think he is now the MSP Department ALPR Coordinator if I'm not mistaken.

TRF-11 is the MSP policy for ALPR.

EOPSS – DCJIS has a policy as listed below. I don't have a copy of it but EOPSS – DCJIS must so Gina or DOC should be able to check with them directly.

Executive Office of Public Safety and Security (EOPSS) - *The Commonwealth of Massachusetts Global Justice and Public Safety Information Sharing Policy*
Executive Office of Public Safety and Security (EOPSS) - Department of Criminal Justice Information Services - *Automatic License Plate Recognition System Central Repository Companion Policy.*

Major Gallagher – Please feel free to weigh in. Is it ok for Dianne to give the DOC TRF-11?

Finally, Gina and DOC should probably check with EOPSS legal and/or MSP legal in case they have any additional insights on ALPR policy developments.

Thank you/Respectfully,
Scott

From: Miller, Dianne (POL) <Dianne.Miller@pol.state.ma.us>
Sent: Tuesday, December 15, 2020 8:48 AM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>; Range, Scott (POL) <scott.range@pol.state.ma.us>
Subject: RE: Automatic License Plate Reader Policy

Good morning Major Range and Amy,
Is there a law enforcement policy relative to ALPR's? See below email from EOPSS…
Thanks
Di

From: Papagiorgakis, Gina (OGR)
Sent: Tuesday, December 15, 2020 8:23 AM
To: Miller, Dianne (POL)
Subject: Automatic License Plate Reader Policy

Good morning Dianne,

I am hoping you can put me in touch with the right contact on your end. The DOC was awarded grant funds to procure an automatic license plate reader system, and thus will need to implement a policy. They are looking to reference existing policies to guide a draft of their own. Is there a policy at MSP that can be shared with the DOC, or is there anyone else who I should reach out to at MSP?

Thank you in advance.

Gina Papagiorgakis
Homeland Security Division
Office of Grants and Research
10 Park Plaza, Suite 3720-A
Boston, MA 02116
gina.papagiorgakis1@mass.gov

From: Jim Charron
To: Schwarz, William J
Cc: Egnitz, Brian (POL); Tiffany Tran; Mitchell, Timothy P. (EOTSS)
Subject: Re: [EXTERNAL]RE: Plate reader access
Date: Friday, October 23, 2020 3:42:06 PM
Attachments: image.png

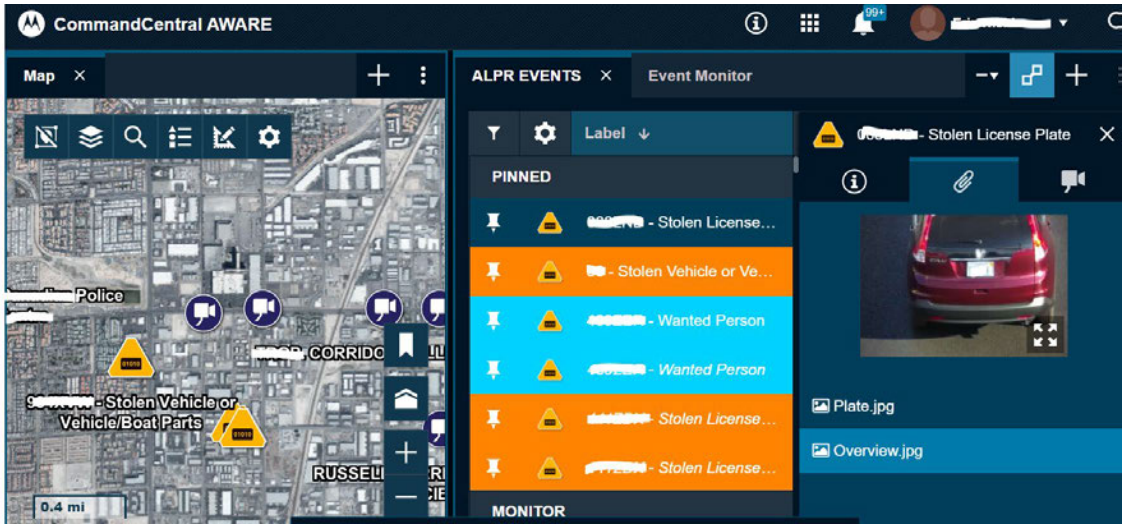
CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

All,

I will send out a calendar appointment so that we can discuss in detail.

Just a quick explanation for the Fusion Center team, Bill's Analysts use our CommandCentral Aware platform to make it easier to identify cameras near an incident so that they can feed intelligence to first responders as they are enroute or after they get on the scene of an incident. Triggers to start the process include events from their CAD, Shotspotter hits and ALPR hits.

Specific to ALPR hits, the Aware workstation essentially serves as another PIPS client, though by design it is limited to receiving hit notifications and not for using the database search tools. Below is a sample of what the Aware user sees: the ALPR hit icon on the map, and event details to include location and the photos of the vehicle and license plate. You can see nearby traffic cameras on the map that the Aware operator can click on to bring up and view live, or playback as appropriate to help out responding officers.



Aware is not set up for investigative queries. Those can be conducted by other analysts or detectives on the regular Pips client.

To get Aware setup to receive the PIPS hit notifications, we typically need the URL to reach the PIPS server, a UserID and password with the appropriate permissions to get the event type and other standard hit data, and the network path opened in the Springfield firewall to allow the data to pass.

Looking forward to discussing further next week.

Thank you,

Jim

On Fri, Oct 23, 2020 at 6:35 AM Schwarz, William J <WSchwarz@springfieldpolice.net> wrote:

> I would just like you to have a quick conversation with our vendors to clarify the process if you can.
>
> Bill
>
> ---
>
> **From:** Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
> **Sent:** Friday, October 23, 2020 9:18 AM
> **To:** Schwarz, William J <WSchwarz@springfieldpolice.net>; Jim Charron <jim.charron@motorolasolutions.com>; Tiffany Tran <tiffanytran@motorolasolutions.com>
> **Cc:** Mitchell, Timothy P (MASSIT) <timothy.p.mitchell@state.ma.us>
> **Subject:** [EXTERNAL]RE: Plate reader access
>
> Did EOTSS give you access to the DB? Neology does not support direct access to the SQL nor do I recommend it, it could have unintended consequences to the systems ability to keep up with reads and alerts. The current supported method for sharing BOSS data is via a PIPS plugin. I am currently working with a cloud vendor and the plug in. If the cloud vendor I'm working with pans out we would have an API for you to use. I'll know more in a few weeks, please hold off if possible.
>
> -Brian
>
> ---
>
> **From:** Schwarz, William J <WSchwarz@springfieldpolice.net>
> **Sent:** Thursday, October 22, 2020 2:38 PM
> **To:** Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Jim Charron <jim.charron@motorolasolutions.com>; Tiffany Tran <tiffanytran@motorolasolutions.com>
> **Subject:** Plate reader access
>
> CAUTION: This email originated from a sender outside of the Commonwealth of

Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Brian:

Can we please chat on a conference call about the access credentials and connections to the alpr system? Jim will send out a link if you have a date and time that your available.

Bill

William Schwarz

Director of Crime Analysis / Real Time Analysis Center

130 Pearl St.

Springfield, MA 01105

413-886-5282

--
Jim Charron
Program Manager
CommandCentral Solutions - West
Motorola Solutions
m: +1.571.485.0926
jim.charron@motorolasolutions.com

Learn More



This email and any attachments are for the authorized recipient's use only. If you receive this email in error, please immediately delete it from your system and notify the sender. You must not disclose, print, re-transmit, store, copy or rely on any part of this email and any attachments if you are not the authorized recipient. This email and any attachments are confidential and may contain confidential information and/or copyright material of Motorola Solutions, Inc.

For more information on how and why we collect your personal information, please visit our Privacy Policy.

To: Peek, Brian T. (EOTSS)
Cc: Guerriero, Robert (EOTSS); Quinn, Dermot (POL); Hughes, Sean M. (EOTSS); Slater, James (CHS); Crouse, David (POL); Michalski, Maria (EPS)
Subject: RE: ALPR Cameras
Date: Thursday, May 14, 2020 10:07:04 AM
Attachments: image001.png
image002.png
image003.png
image004.png
image005.png
image006.png

Hi Brian,

If possible, I'd like to include 70+ more devices in the conversation and discuss the TSU covert cameras. It has recently been brought to our attention that a local Department's covert camera (running VZW 166.) was discovered and has been targeted by a reddit forum post and by members who appear to be actively looking for covert cameras. Are you available the first week in June for a meeting or should I direct this to someone else in TSS?

Agenda could include:

- Overview of our long term goal to consolidate the current video management systems (BOSCH, View Commander, Vigilion, Genetec at the Watch, Genetec in Maynard) into the new Chelsea environment
- ALPR network – how to allow remote management and prepare for the cloud migration
- Covert Camera Network – how we currently handle cameras and could in the future. Can we bring in IPC to manage the TSU network?
- Can we build out one wireless MSP camera network, using sierra modems at the edge, VPN back to Chelsea and scale and store in the new environment.
- E55 Esplanade cutover to the State Fiber (in discussions currently)
- Bandwidth, how much, what's currently in Maynard, what's available
- How we would access Evidence (video on disc)
- VMS networking limitations

Please let me know, Thanks Brian

Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
Phone: 978-451-3710 (Maynard) 508-988-7302 (GHQ)
Email: Brian.Egnitz@massmail.state.ma.us
Monday - Friday, 8 to 4

CONFIDENTIALITY NOTICE: *The information contained in this email and any attachment is privileged and confidential law enforcement information. If you have received this email in error, please call 978-451-3700 immediately. Thank you.*

From: Peek, Brian T. (EOTSS)
Sent: Wednesday, May 6, 2020 8:43 AM
To: Egnitz, Brian (POL)
Cc: Guerriero, Robert (EOTSS); Quinn, Dermot (POL); Hughes, Sean M. (EOTSS); Slater, James (CHS); Crouse, David (POL)
Subject: Re: ALPR Cameras

Brian,

How many MP70's would you be looking to add to the network?

thanks
bp

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Tuesday, May 5, 2020 3:11 PM
To: Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>

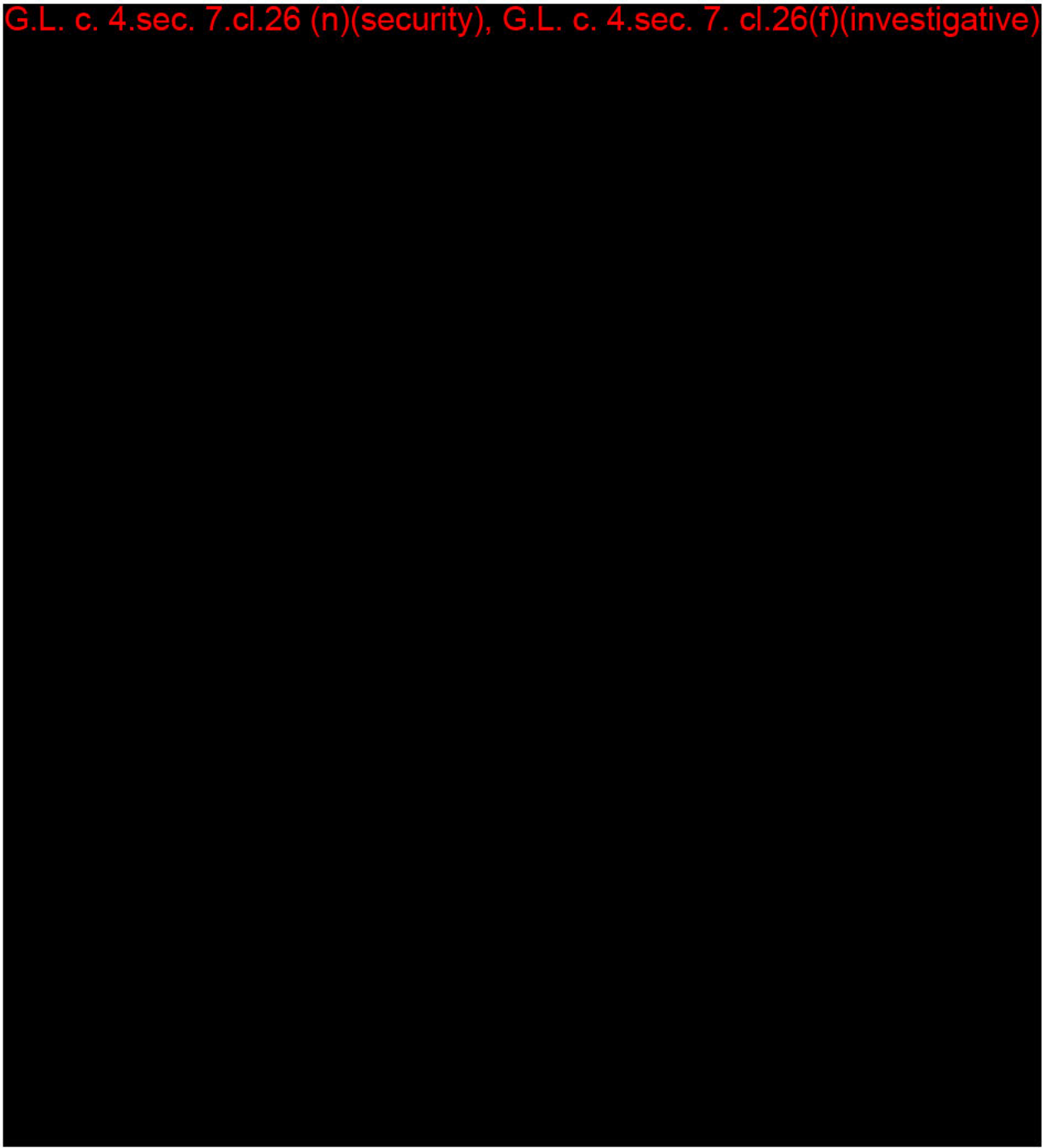
Cc: Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>; Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Hughes, Sean M. (EOTSS) <sean.hughes@mass.gov>; Slater, James (CHS) <james.slater@mass.gov>; Crouse, David (POL) <david.crouse@pol.state.ma.us>
Subject: RE: ALPR Cameras

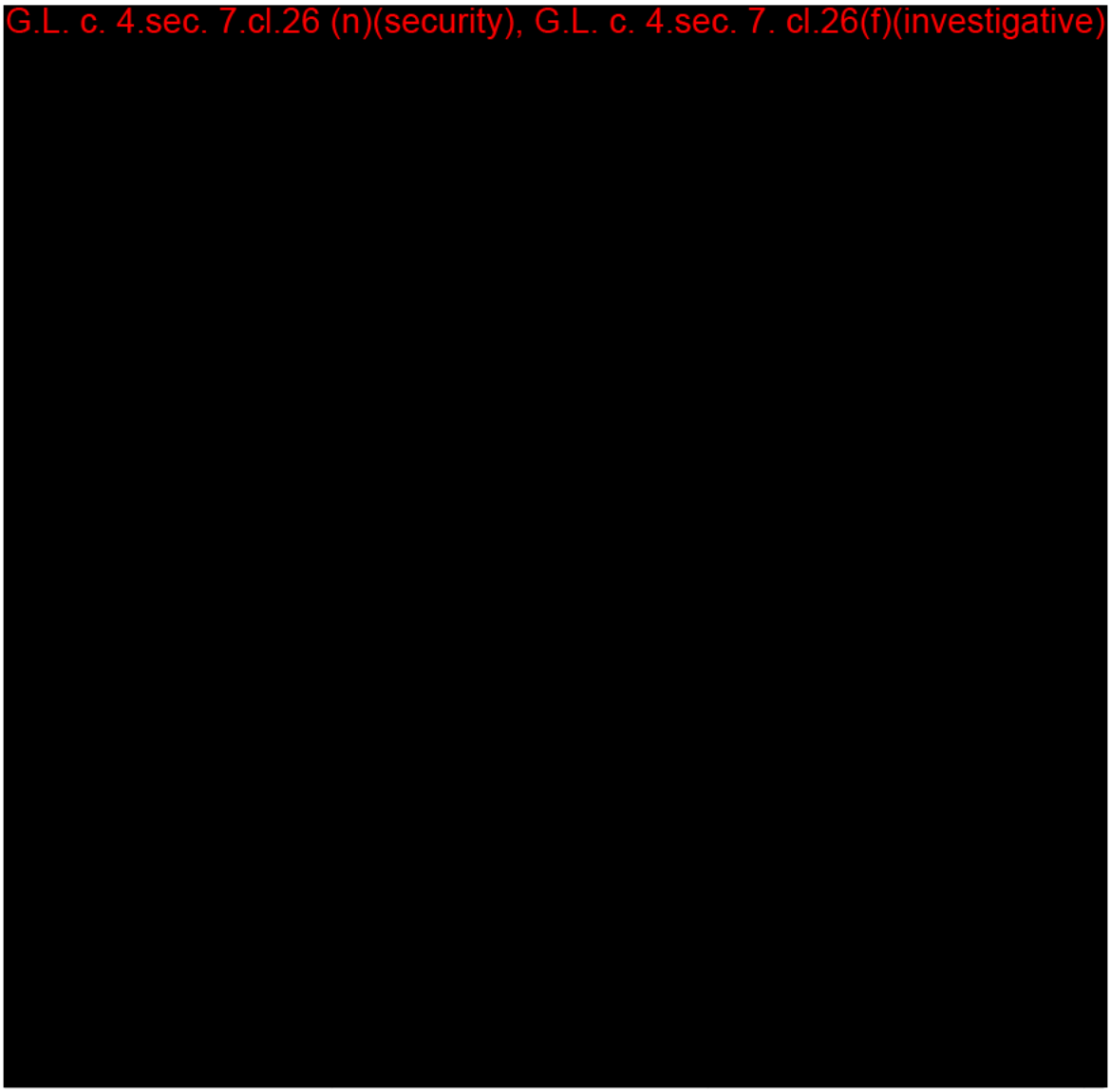
Hi Brian,

I will be cutting over MassPort cameras tomorrow. We have the MassPort modems, I've updated the firmware and double checked connectivity back to the BOSS server from the MassPort SIMS and there is no firewall work needed. For your records, I've included the details below of the modems and IPs/Accounts.

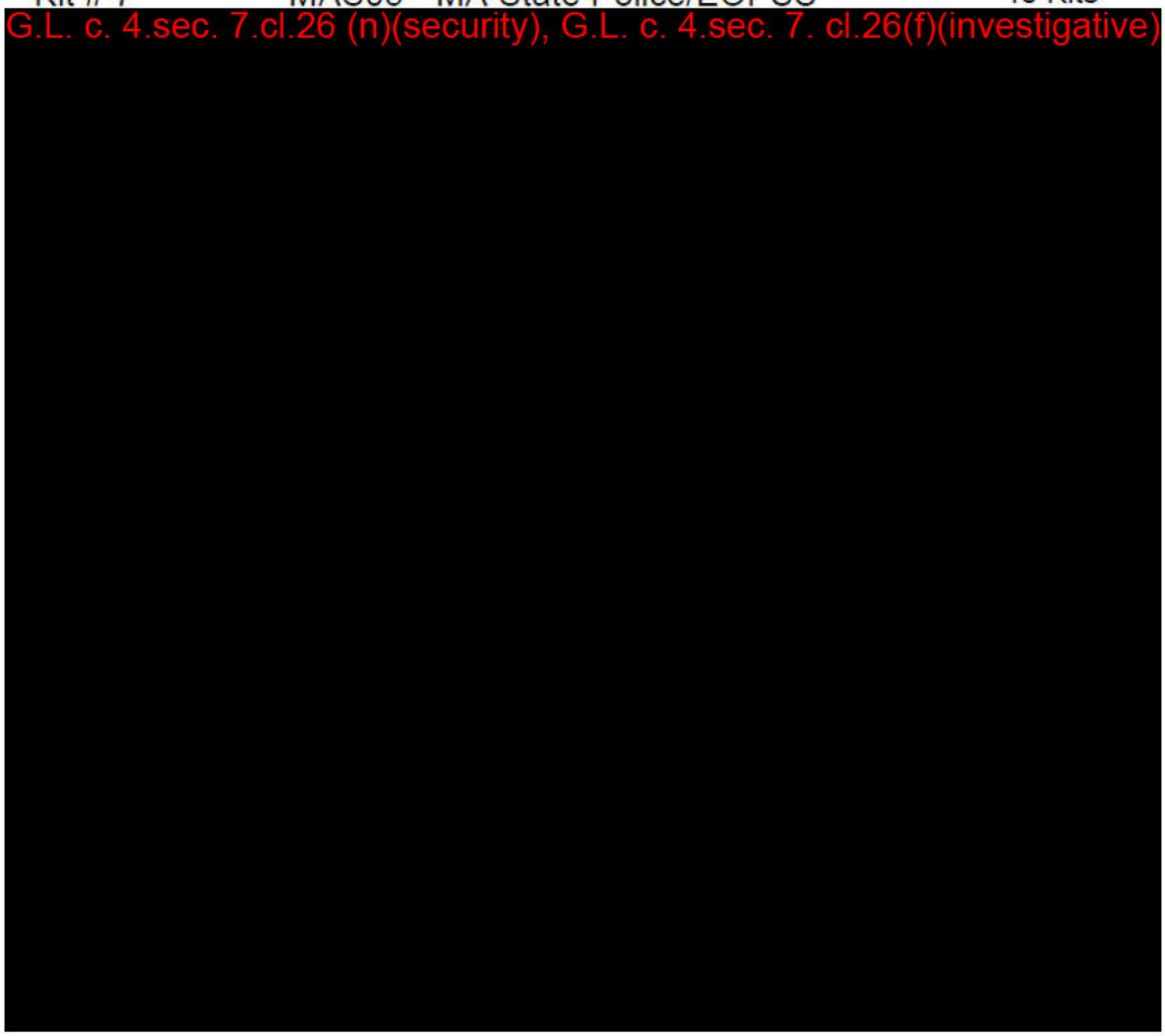
If possible, I would like to review with you or a member of the TSS network Team using the same solution now in place for the new DHS Livescans. We feel this is a good solution for all the MSP LPRS and it would allow us both the remote management needed for the project. If there are no objection, I can reach out to IPC for a quote, but I would prefer to get on a quick call to discuss. Please advise.

Thanks, Brian

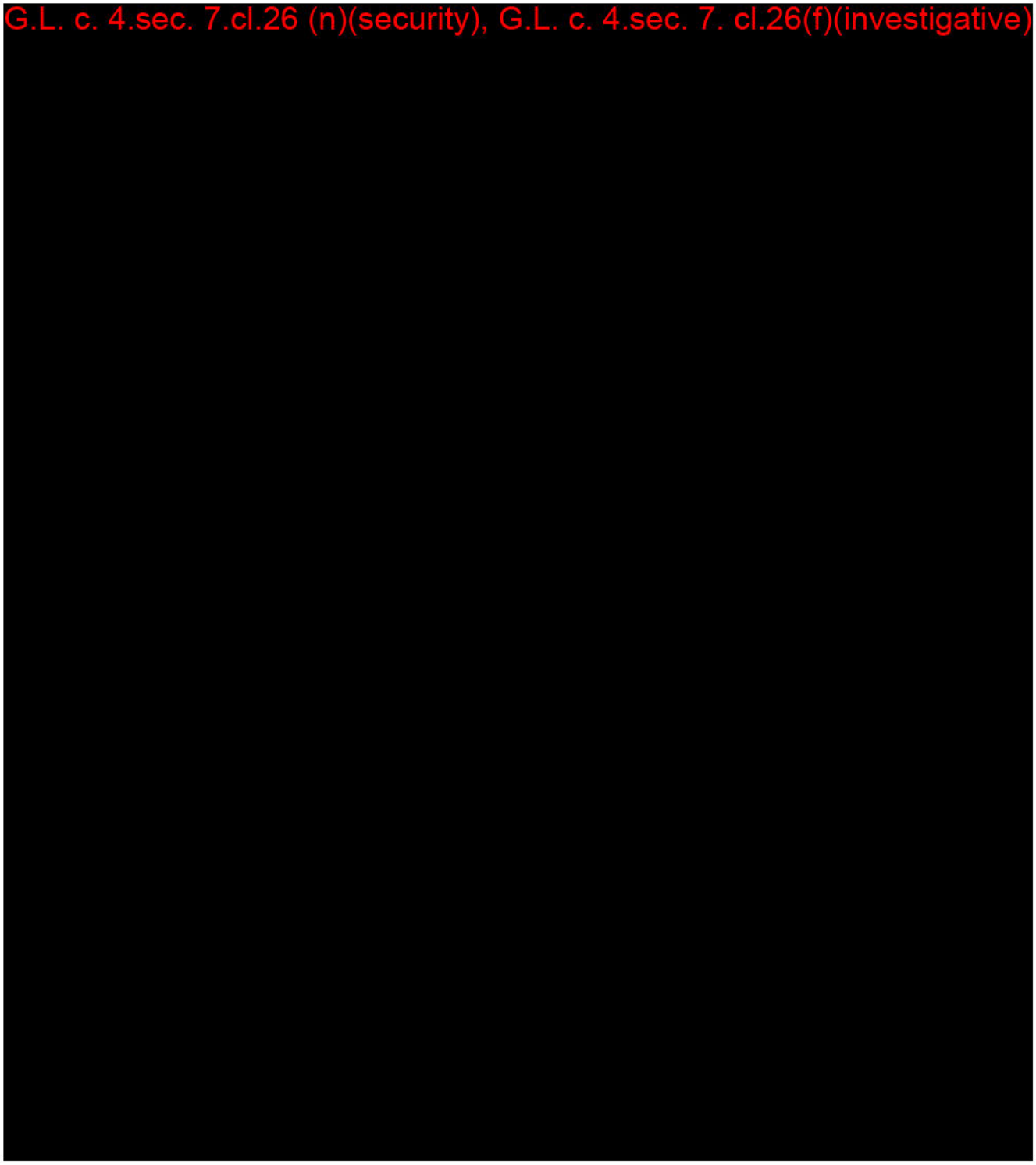


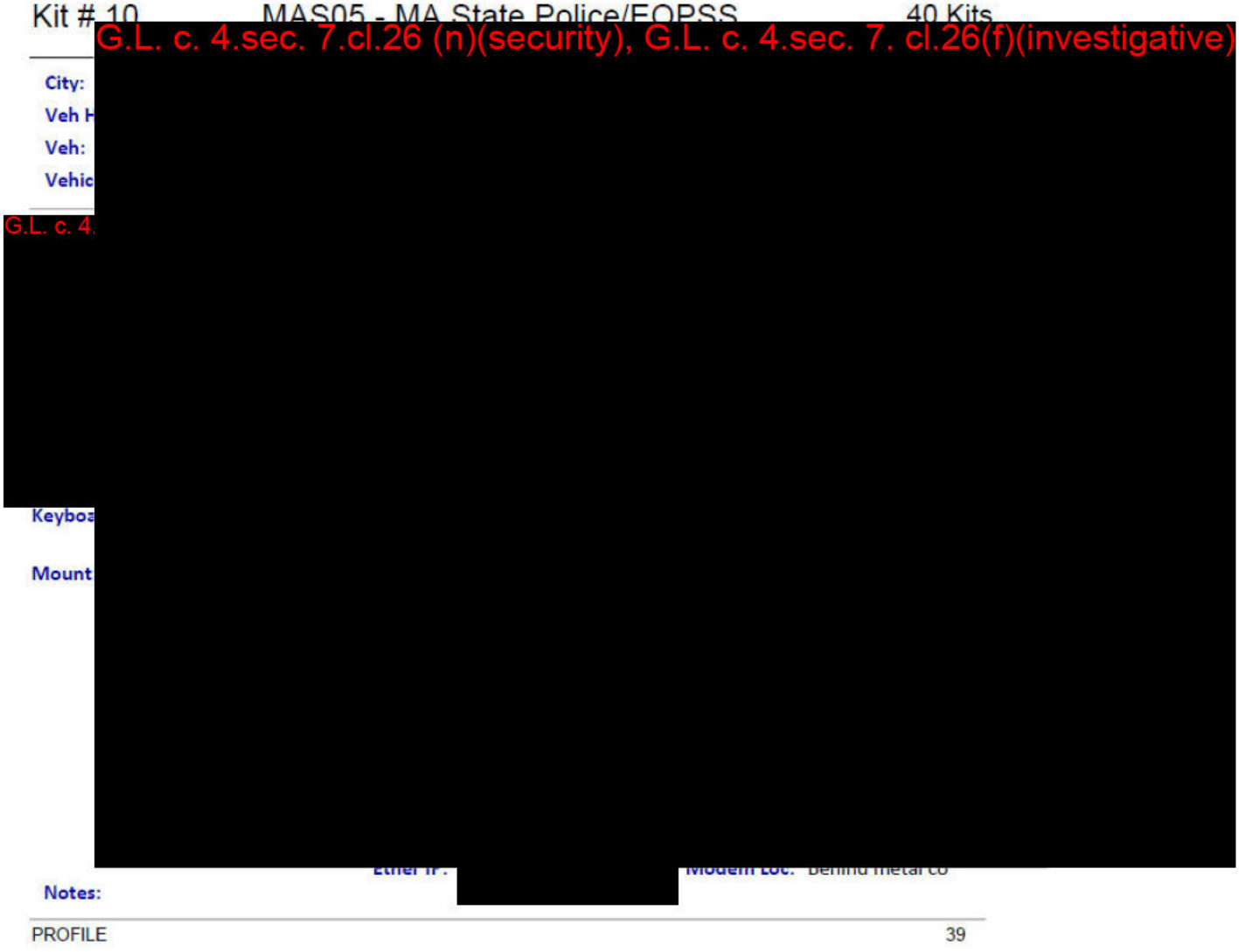

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

Kit # 7 MAS05 - MA State Police/EOPSS 40 Kits



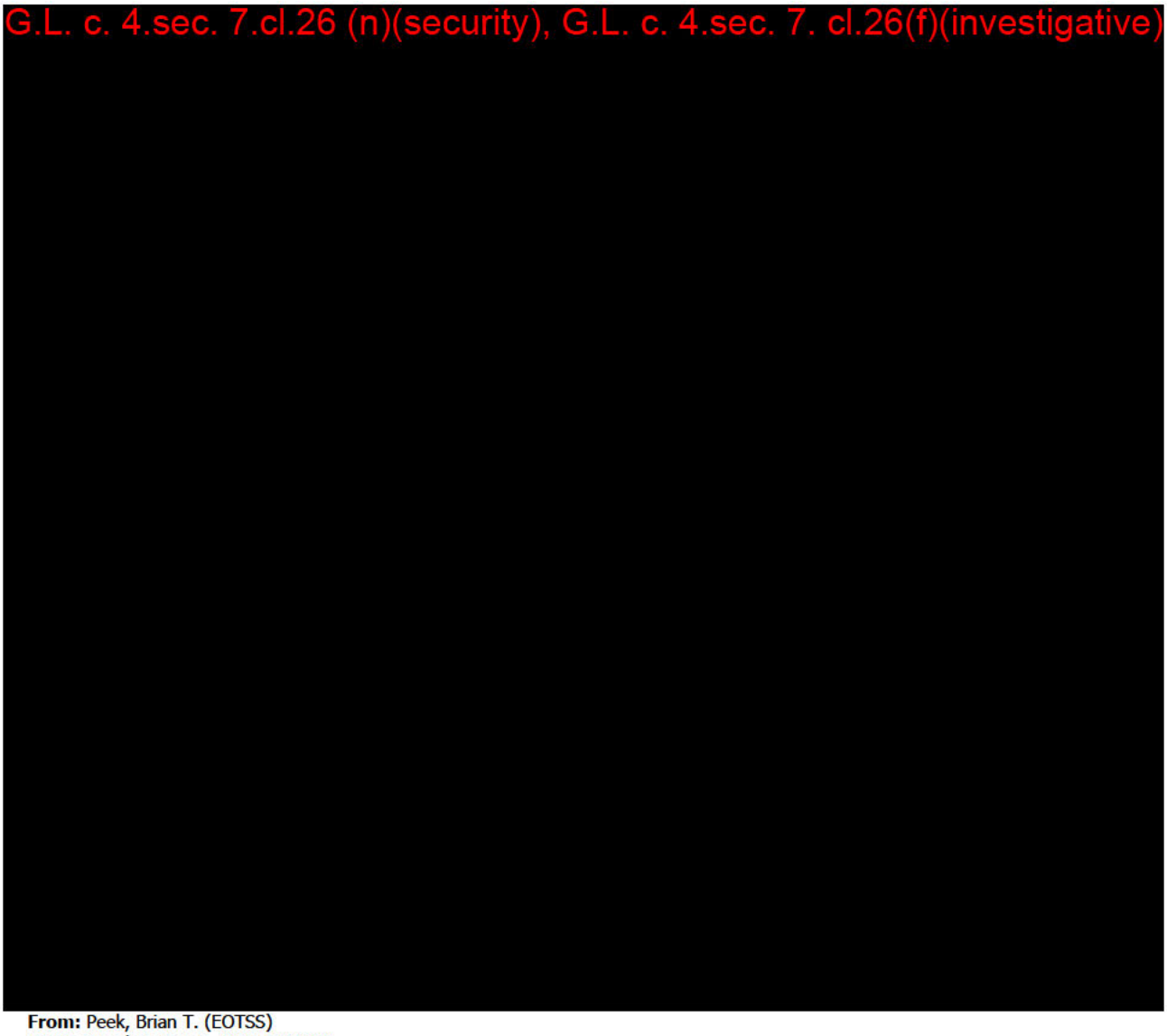
Kit # 13 MAS05 - MA State Police/EOPSS 40 Kits




Kit # 10
MAS05 - MA State Police/EOPSS
40 Kits
G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)
City:
Veh H
Veh:
Vehic
G.L. c. 4.
Keyboa
Mount
Notes:
PROFILE
39

Kit # 16 MAS05 - MA State Police/EOPSS 40 Kits

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)



From: Peek, Brian T. (EOTSS)
Sent: Tuesday, May 5, 2020 2:43 PM
To: Egnitz, Brian (POL)
Cc: Guerriero, Robert (EOTSS); Quinn, Dermot (POL); Hughes, Sean M. (EOTSS); Slater, James (CHS); Crouse, David (POL)
Subject: Re: ALPR Cameras

Hi Brian,

I just wanted to confirm that you are not waiting on us for anything? There are no network changes requested correct?

thanks
bp

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, April 17, 2020 10:51 AM
To: Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>
Cc: Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>; Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Hughes, Sean M. (EOTSS) <sean.hughes@mass.gov>; Slater, James (CHS) <james.slater@mass.gov>; Crouse, David (POL) <david.crouse@pol.state.ma.us>
Subject: Re: ALPR Cameras

You are the correct, the current plan is VZW, no network changes required. This is a new request to review if the below would be a better solution long term for ALPR.

On Apr 17, 2020, at 9:22 AM, Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov> wrote:

Hi Brian,

Is this different from the initial request? If I remember correctly the traffic was going to flow over the VZW network and no FW or Network configurations would need to be changed.

Thanks
Brian

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, April 17, 2020 6:56 AM
To: Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Hughes, Sean M. (EOTSS) <sean.hughes@mass.gov>; Slater, James (CHS) <james.slater@mass.gov>; Crouse, David (POL) <david.crouse@pol.state.ma.us>; Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>
Subject: ALPR Cameras

Hi Rob,

As you are probably aware the MassPort project to migrate their ALPR Cameras over to the MSP is moving forward over Verizon Wireless. We have identified modems, data plans and purchased the accessories needed for the project and hope to begin cutting over in the next 2-3 weeks.

I wanted to run something by you and the team to review; we just completed the Sierra MP70 VPN project with IPC and it went well (thanks for your teams help - BTW). Do you want to use the same approach (OneNetwork) for these ALPRS? I think it would give us the same functionality originally discussed by pushing the traffic over MassPorts network back to the core, but we would run it over Verizon.

A couple of thoughts;

This could be a good long term approach for all ALPRs we are hosting, we've begun to standardized on MP70s
This could give us much needed remote access to the cameras
If we moved to the Neology Hosted solution, we could do a split tunnel and pipe the traffic straight over the internet, but only allow remote management via the tunnel.
IPC was the prime on the sierra project and work would be minimal to expand, we also want to begin leveraging them more for our other wire/ covert/camera networks we run down the road (when Jim decides to retire).
If MassPort wants us off Verizon (since they are paying for the data plans), they could get us a straight internet route and connect to the MP70 (Our MP70 establishes internet via a LAN Port, Wifi and Cell, all establishing the VPN tunnel after connection).

Let me know what you think and if you want to get on a call to discuss. Otherwise, we can just get MassPort done with the normal static plan.

Thanks, Brian

Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
Phone: 978-451-3710 (Maynard) 508-988-7302 (GHQ)
Email: Brian.Egnitz@massmail.state.ma.us
Monday - Friday, 8 to 4

From: Peek, Brian T. (EOTSS)
To: Egnitz, Brian (POL)
Cc: Guerriero, Robert (EOTSS); Quinn, Dermot (POL); Hughes, Sean M. (EOTSS); Slater, James (CHS); Crouse, David (POL)
Subject: Re: ALPR Cameras
Date: Wednesday, May 6, 2020 8:42:57 AM
Attachments: image001.png
image002.png
image003.png
image004.png
image005.png
image006.png

Brian,

How many MP70's would you be looking to add to the network?

thanks
bp

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Tuesday, May 5, 2020 3:11 PM
To: Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>
Cc: Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>; Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Hughes, Sean M. (EOTSS) <sean.hughes@mass.gov>; Slater, James (CHS) <james.slater@mass.gov>; Crouse, David (POL) <david.crouse@pol.state.ma.us>
Subject: RE: ALPR Cameras

Hi Brian,

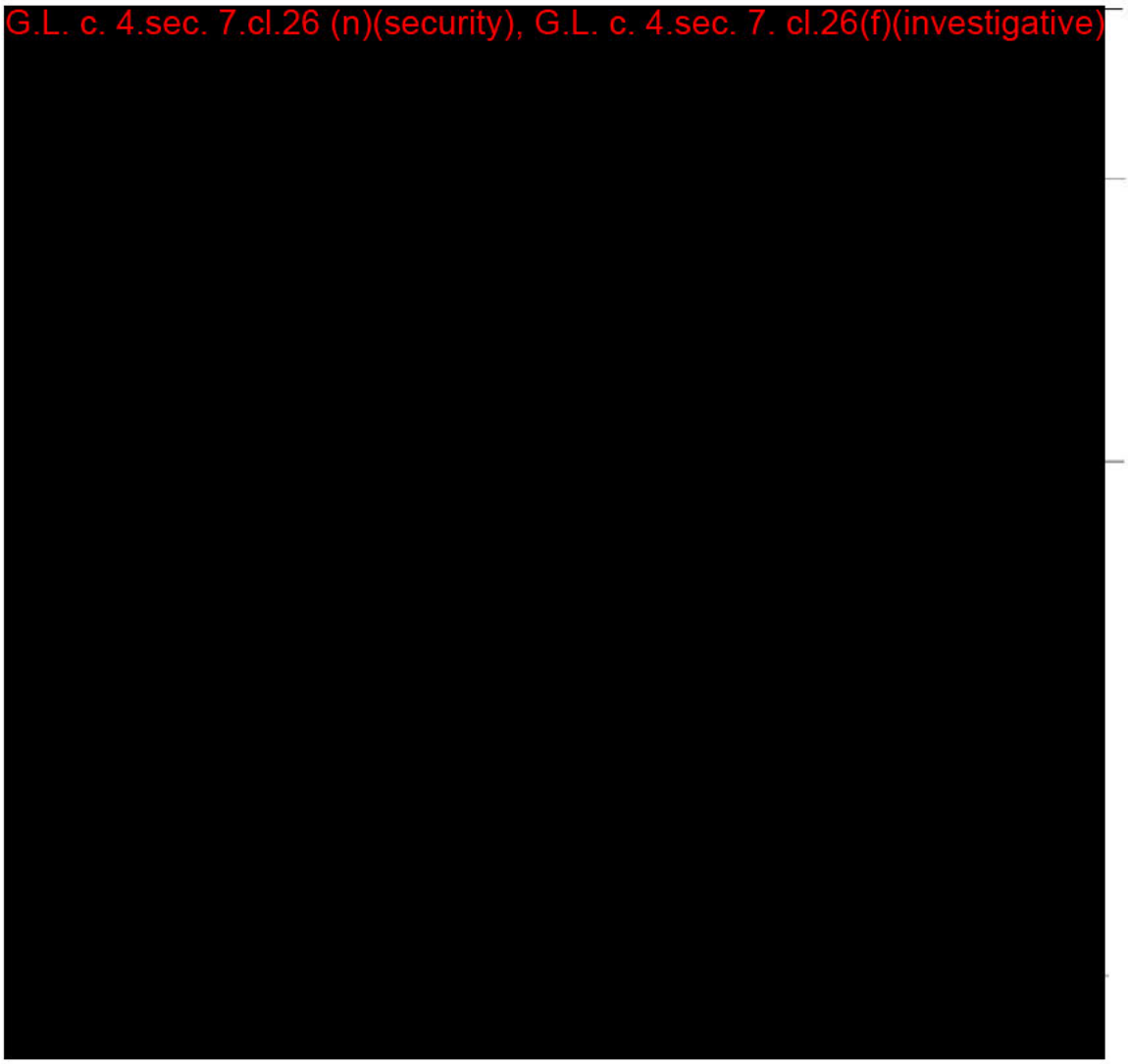
I will be cutting over MassPort cameras tomorrow. We have the MassPort modems, I've updated the firmware and double checked connectivity back to the BOSS server from the MassPort SIMS and there is no firewall work needed. For your records, I've included the details below of the modems and IPs/Accounts.

If possible, I would like to review with you or a member of the TSS network Team using the same solution now in place for the new DHS Livescans. We feel this is a good solution for all the MSP LPRS and it would allow us both the remote management needed for the project. If there are no objection, I can reach out to IPC for a quote, but I would prefer to get on a quick call to discuss. Please advise.

Thanks, Brian

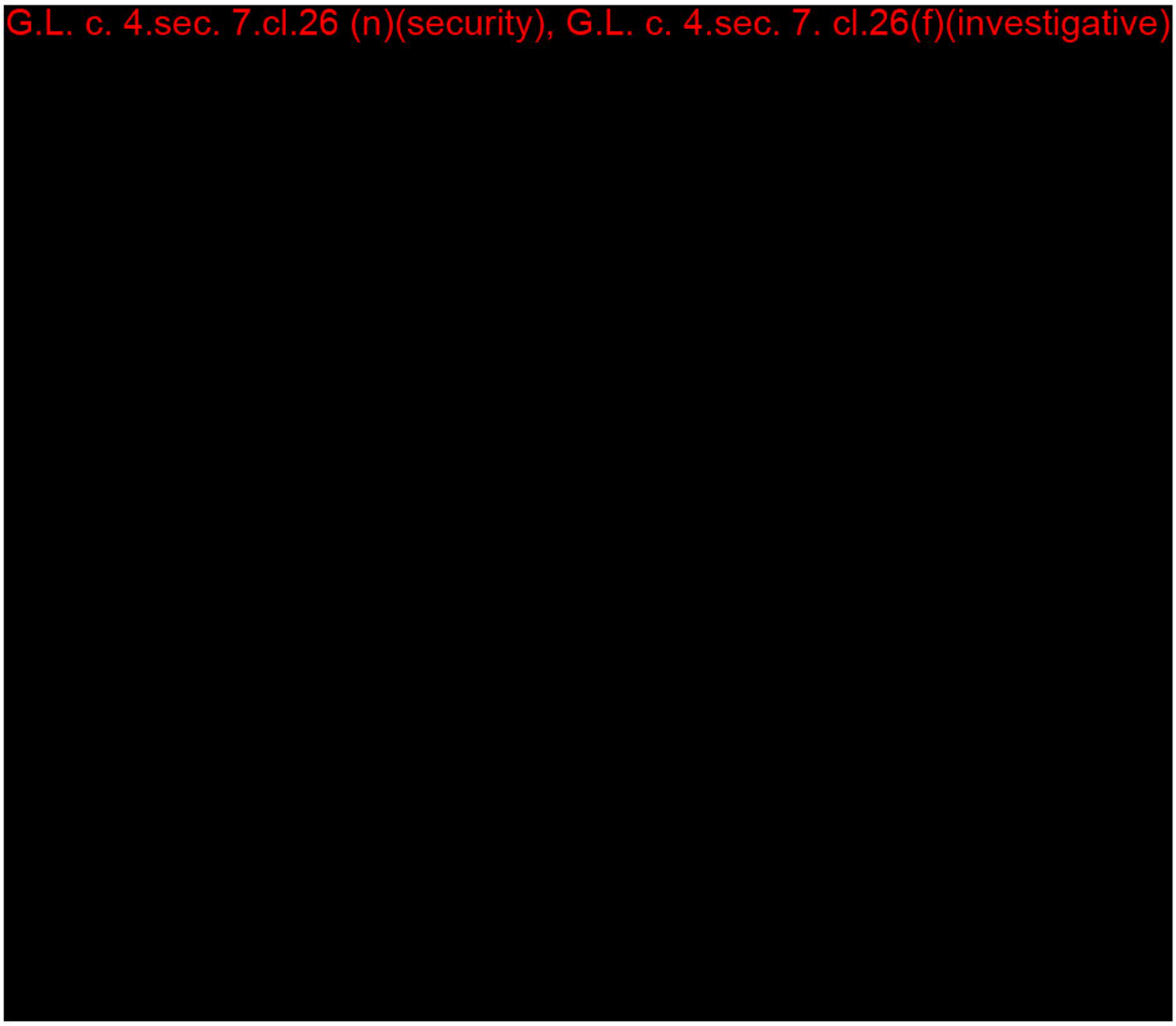
Information Technologies

Kit # 15 MAS05 - MA State Police/EOPSS 40 Kits

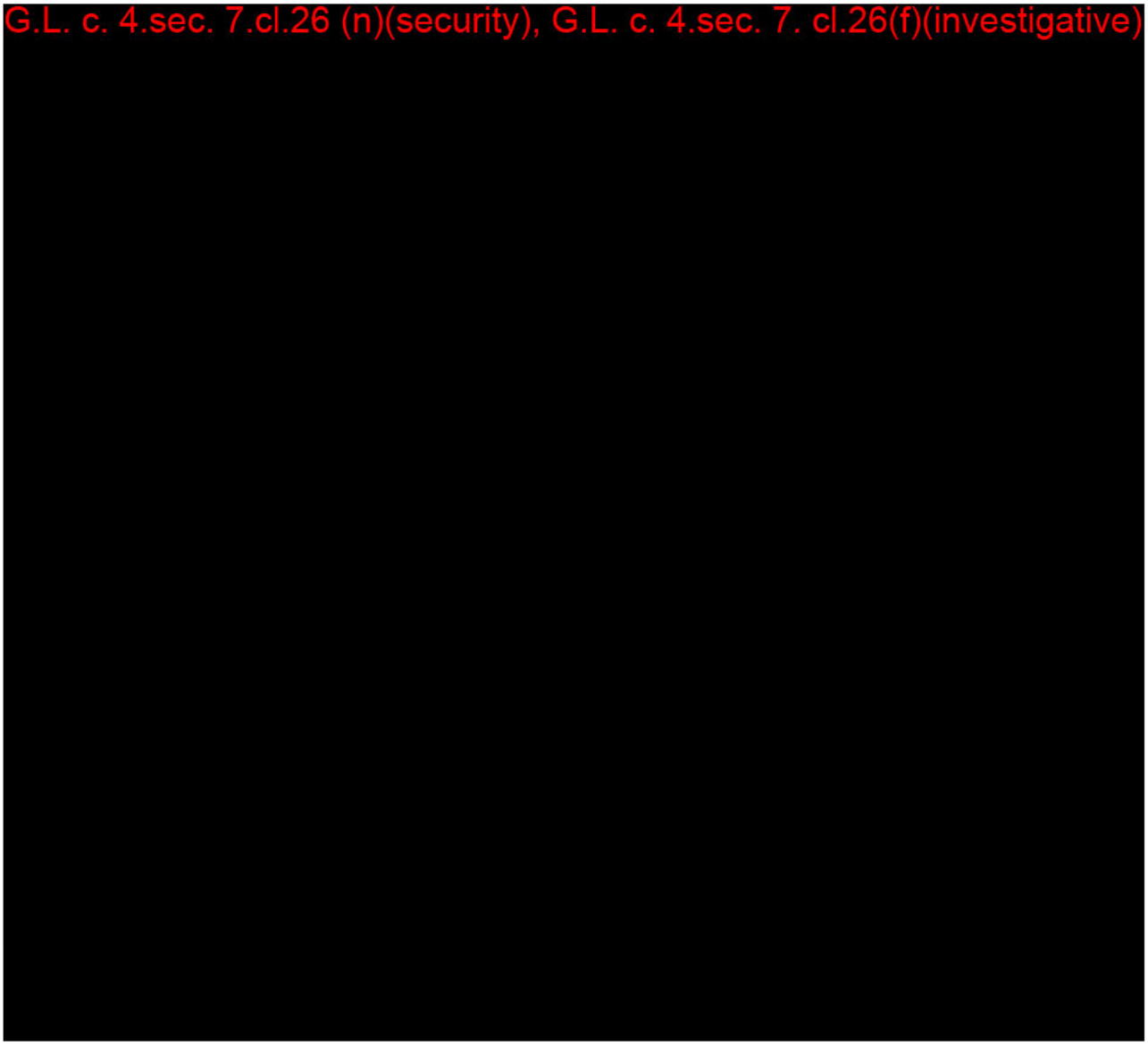


Kit # 11 MAS05 - MA State Police/EOPSS 40 Kits

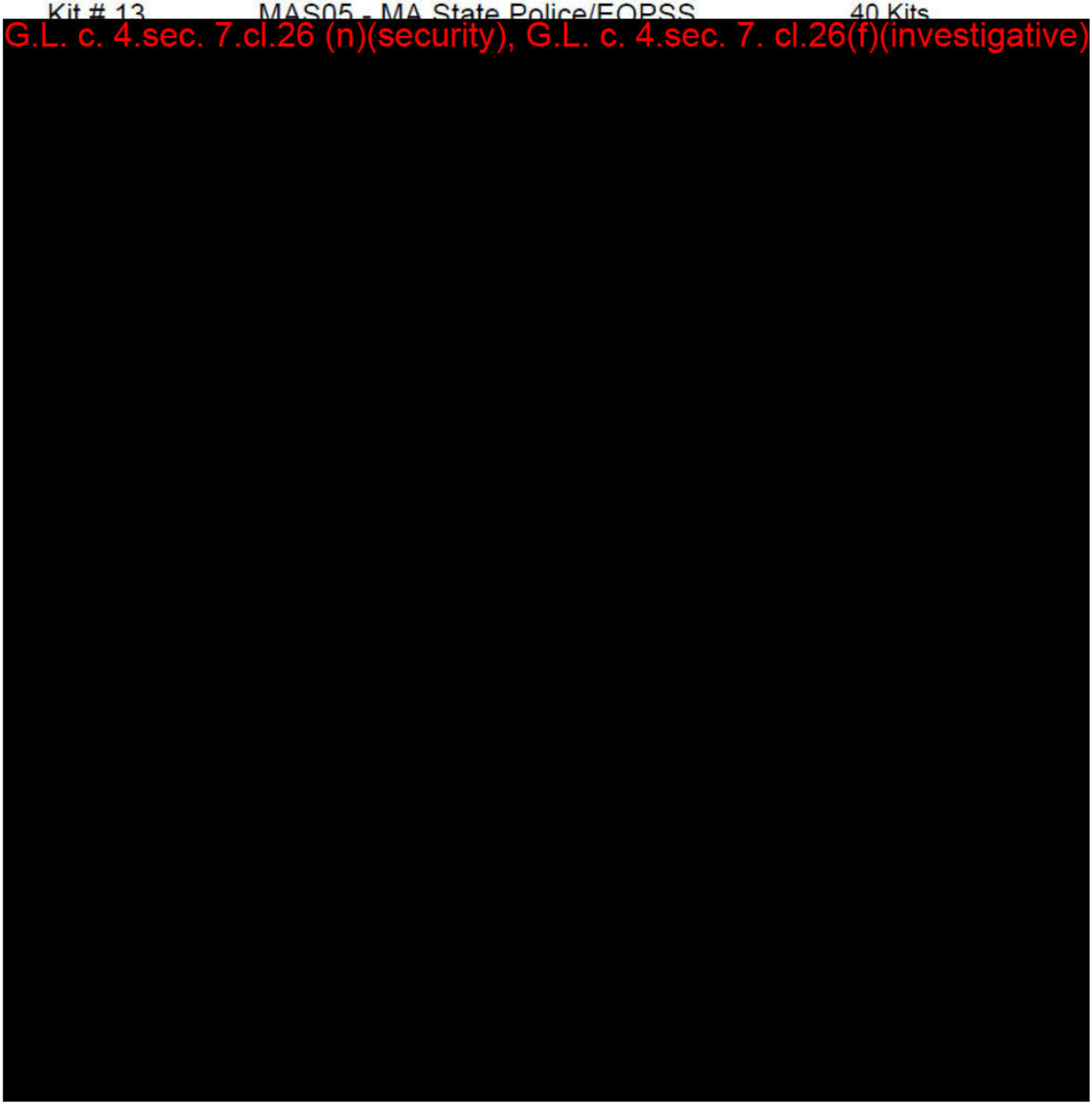
G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)



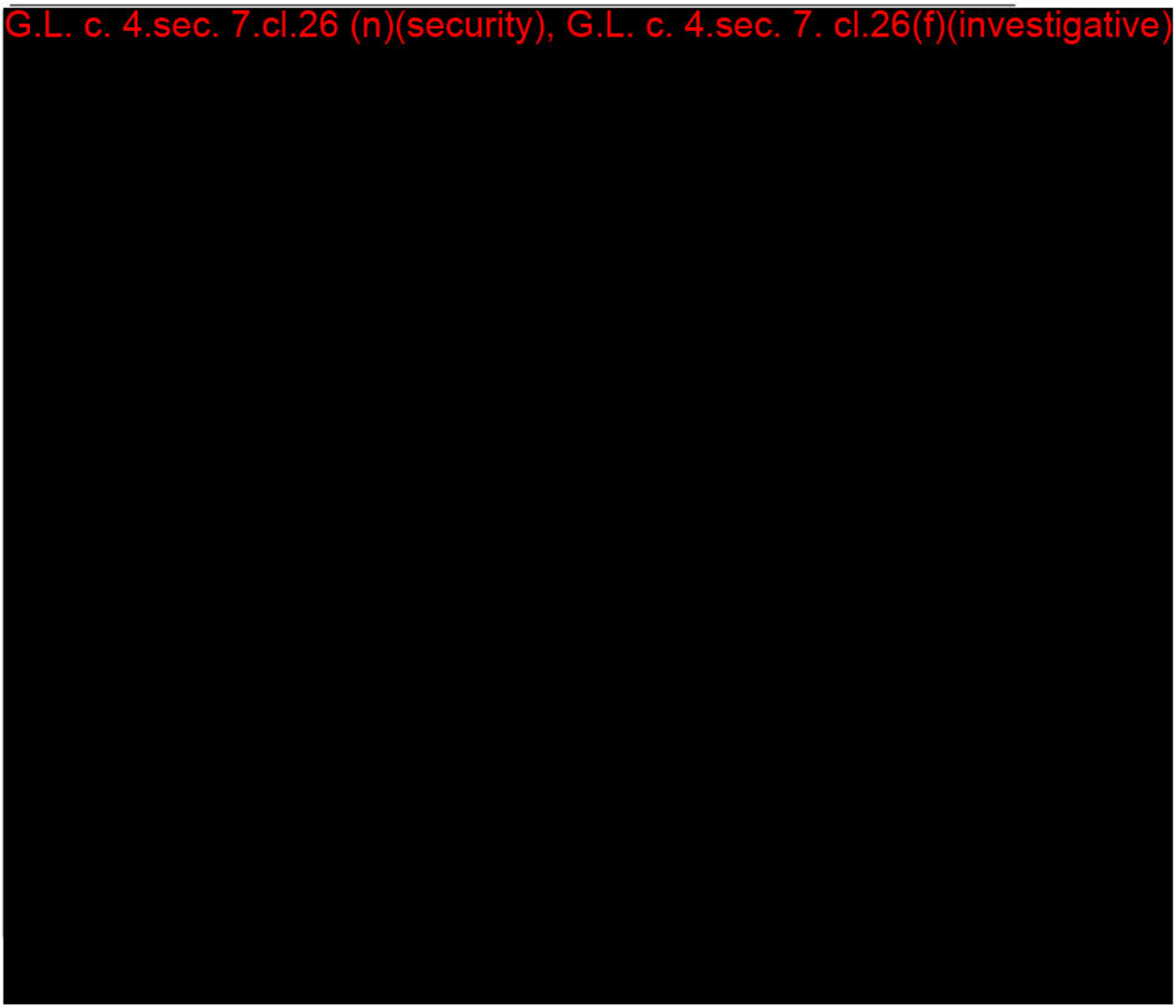
Kit # 7 MAS05 - MA State Police/EOPSS 40 Kits



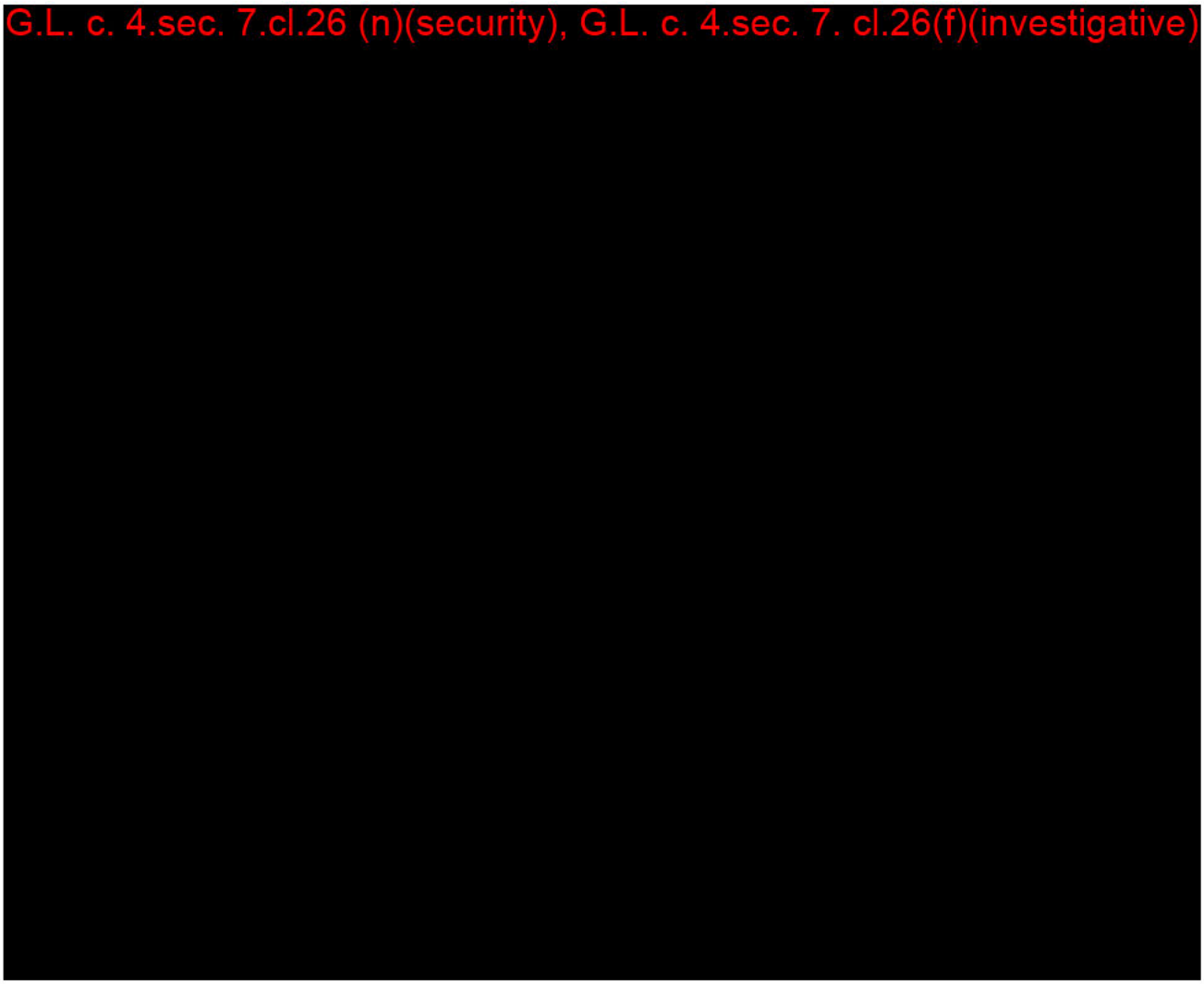
Kit # 13 MAS05 - MA State Police/EOPSS 40 Kits



Kit # 10 MAS05 - MA State Police/EOPSS 40 Kits



Kit # 16 MAS05 - MA State Police/EOPSS 40 Kits



From: Peek, Brian T. (EOTSS)
Sent: Tuesday, May 5, 2020 2:43 PM
To: Egnitz, Brian (POL)
Cc: Guerriero, Robert (EOTSS); Quinn, Dermot (POL); Hughes, Sean M. (EOTSS); Slater, James (CHS); Crouse, David (POL)
Subject: Re: ALPR Cameras

Hi Brian,

I just wanted to confirm that you are not waiting on us for anything? There are no network changes requested correct?

thanks
bp

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, April 17, 2020 10:51 AM
To: Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>
Cc: Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>; Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Hughes, Sean M. (EOTSS) <sean.hughes@mass.gov>; Slater, James (CHS) <james.slater@mass.gov>; Crouse, David (POL) <david.crouse@pol.state.ma.us>
Subject: Re: ALPR Cameras

You are the correct, the current plan is VZW, no network changes required. This is a new request to review if the below would be a better solution long term for ALPR.

On Apr 17, 2020, at 9:22 AM, Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov> wrote:

Hi Brian,

Is this different from the initial request? If I remember correctly the traffic was going to flow over the VZW network and no FW or Network configurations would need to be changed.

Thanks
Brian

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, April 17, 2020 6:56 AM
To: Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Hughes, Sean M. (EOTSS) <sean.hughes@mass.gov>; Slater, James (CHS) <james.slater@mass.gov>; Crouse, David (POL) <david.crouse@pol.state.ma.us>; Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>
Subject: ALPR Cameras

Hi Rob,

As you are probably aware the MassPort project to migrate their ALPR Cameras over to the MSP is moving forward over Verizon Wireless. We have identified modems, data plans and purchased the accessories needed for the project and hope to begin cutting over in the next 2-3 weeks.

I wanted to run something by you and the team to review; we just completed the Sierra MP70 VPN project with IPC and it went well (thanks for your teams help - BTW). Do you want to use the same approach (OneNetwork) for these ALPRS? I think it would give us the same functionality originally discussed by pushing the traffic over MassPorts network back to the core, but we would run it over Verizon.

A couple of thoughts;

This could be a good long term approach for all ALPRs we are hosting, we've begun to standardized on MP70s
This could give us much needed remote access to the cameras
If we moved to the Neology Hosted solution, we could do a split tunnel and pipe the traffic straight over the internet, but only allow remote management via the tunnel.
IPC was the prime on the sierra project and work would be minimal to expand, we also want to begin leveraging them more for our other wire/ covert/camera networks we run down the road (when Jim decides to retire).
If MassPort wants us off Verizon (since they are paying for the data plans), they could get us a straight internet route and connect to the MP70 (Our MP70 establishes internet via a LAN Port, Wifi and Cell, all establishing the VPN tunnel after connection).

Let me know what you think and if you want to get on a call to discuss. Otherwise, we can just get MassPort done with the normal static plan.

Thanks, Brian

Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
Phone: 978-451-3710 (Maynard) 508-988-7302 (GHQ)
Email: Brian.Egnitz@massmail.state.ma.us
Monday - Friday, 8 to 4

CONFIDENTIALITY NOTICE: *The information contained in this email and any attachment is privileged and confidential law enforcement information. If you have received this email in error, please call 978-451-3700 immediately. Thank you.*

From:	Egnitz, Brian (POL)
To:	Peek, Brian T. (EOTSS)
Cc:	Guerriero, Robert (EOTSS); Quinn, Dermot (POL); Hughes, Sean M. (EOTSS); Slater, James (CHS); Crouse, David (POL)
Subject:	Re: ALPR Cameras
Date:	Wednesday, May 6, 2020 8:52:27 AM
Attachments:	image001.png image002.png image003.png image004.png image005.png image006.png

---

Approximately30, but would need support growth for up to 100 in the next 2-3 years.

> On May 6, 2020, at 8:42 AM, Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov> wrote:
>
> Brian,
>
> How many MP70's would you be looking to add to the network?
>
> thanks
> bp
>
> ---
>
> **From:** Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Sent:** Tuesday, May 5, 2020 3:11 PM
> **To:** Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>
> **Cc:** Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>; Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Hughes, Sean M. (EOTSS) <sean.hughes@mass.gov>; Slater, James (CHS) <james.slater@mass.gov>; Crouse, David (POL) <david.crouse@pol.state.ma.us>
> **Subject:** RE: ALPR Cameras
>
> Hi Brian,
>
> I will be cutting over MassPort cameras tomorrow. We have the MassPort modems, I've updated the firmware and double checked connectivity back to the BOSS server from the MassPort SIMS and there is no firewall work needed. For your records, I've included the details below of the modems and IPs/Accounts.
>
> If possible, I would like to review with you or a member of the TSS network Team using the same solution now in place for the new DHS Livescans. We feel this is a good solution for all the MSP LPRS and it would allow us both the remote management needed for the project. If there are no objection, I can reach out to IPC for a quote, but I would prefer to get on a quick call to discuss. Please advise.

Thanks, Brian

<image001.png>

<image002.png>

<image003.png>
<image004.png>
<image005.png>
<image006.png>

From: Peek, Brian T. (EOTSS)
Sent: Tuesday, May 5, 2020 2:43 PM
To: Egnitz, Brian (POL)
Cc: Guerriero, Robert (EOTSS); Quinn, Dermot (POL); Hughes, Sean M. (EOTSS); Slater, James (CHS); Crouse, David (POL)
Subject: Re: ALPR Cameras

Hi Brian,

I just wanted to confirm that you are not waiting on us for anything? There are no network changes requested correct?

thanks
bp

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, April 17, 2020 10:51 AM
To: Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>
Cc: Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>; Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Hughes, Sean M. (EOTSS) <sean.hughes@mass.gov>; Slater, James (CHS) <james.slater@mass.gov>; Crouse, David (POL) <david.crouse@pol.state.ma.us>
Subject: Re: ALPR Cameras

You are the correct, the current plan is VZW, no network changes required. This is a new request to review if the below would be a better solution long term for ALPR.

On Apr 17, 2020, at 9:22 AM, Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov> wrote:

Hi Brian,

Is this different from the initial request? If I remember correctly the traffic was going to flow over the VZW network and no FW or Network configurations would need to be changed.

Thanks
Brian

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, April 17, 2020 6:56 AM
To: Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Hughes, Sean M. (EOTSS) <sean.hughes@mass.gov>; Slater, James (CHS) <james.slater@mass.gov>; Crouse, David (POL) <david.crouse@pol.state.ma.us>; Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>
Subject: ALPR Cameras

Hi Rob,

As you are probably aware the MassPort project to migrate their ALPR Cameras over to the MSP is moving forward over Verizon Wireless. We have identified modems, data plans and purchased the accessories needed for the project and hope to begin cutting over in the next 2-3 weeks.

I wanted to run something by you and the team to review; we just completed the Sierra MP70 VPN project with IPC and it went well (thanks for your teams help - BTW). Do you want to use the same approach (OneNetwork) for these ALPRS? I think it would give us the same functionality originally discussed by pushing the traffic over MassPorts network back to the core, but we would run it over Verizon.

A couple of thoughts;

This could be a good long term approach for all ALPRs we are hosting, we've begun to standardized on MP70s
This could give us much needed remote access to the cameras
If we moved to the Neology Hosted solution, we could do a split tunnel and pipe the traffic straight over the internet, but only allow remote management via the tunnel.
IPC was the prime on the sierra project and work would be minimal to expand, we also want to begin leveraging them more for our other wire/ covert/camera networks we run down the road (when Jim decides to retire).
If MassPort wants us off Verizon (since they are paying for the data plans),

they could get us a straight internet route and connect to the MP70 (Our MP70 establishes internet via a LAN Port, Wifi and Cell, all establishing the VPN tunnel after connection).

Let me know what you think and if you want to get on a call to discuss. Otherwise, we can just get MassPort done with the normal static plan.

Thanks, Brian

Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
Phone: 978-451-3710 (Maynard) 508-988-7302 (GHQ)
Email: Brian.Egnitz@massmail.state.ma.us
Monday - Friday, 8 to 4

CONFIDENTIALITY NOTICE: *The information contained in this email and any attachment is privileged and confidential law enforcement information. If you have received this email in error, please call 978-451-3700 immediately. Thank you.*

From:	Wark, Jake (EPS)
To:	Terrey, Susan (EPS); Collins, Kerry (EPS); Staples, Jennifer (POL); Koulouris, Agapi (CHS); Lord, Spencer (EPS); McGarry, Matthew (CHS); Mullaney, Arielle (EPS)
Subject:	RE: ALPR eopss 122220 swt NDB
Date:	Tuesday, December 22, 2020 11:53:13 AM
Attachments:	ALPR eopss 122220 swt NDB revision.docx

A few suggestions highlighted here, some just stylistic and others that I hope may be helpful.

From: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>
Sent: Tuesday, December 22, 2020 11:31 AM
To: Collins, Kerry (EPS) <Kerry.Collins@mass.gov>; Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>; Koulouris, Agapi (CHS) <agapi.koulouris@mass.gov>; Lord, Spencer (EPS) <spencer.b.lord@mass.gov>; McGarry, Matthew (CHS) <Matthew.McGarry@mass.gov>; Mullaney, Arielle (EPS) <Arielle.Mullaney@mass.gov>; Wark, Jake (EPS) <Jake.Wark@mass.gov>
Subject: ALPR eopss 122220 swt NDB

See the last two small changes if we can live with it let me know

To:	Egnitz, Brian (POL)
Subject:	RE: ALPR notice confidential
Date:	Wednesday, December 9, 2020 11:44:12 AM
Attachments:	National standards for compliance and audit of law enforcement ANPR - September 2020 (accessible version) - GOV.UK.docx

Rosemary J. Warren
Division of Homeland Security and Preparedness
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
Office: 508-988-7310
Rosemary.Warren@mass.gov

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Wednesday, December 9, 2020 11:41 AM
To: Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>
Subject: RE: ALPR notice confidential

From: Egnitz, Brian (POL)
To: Warren, Rosemary (POL)
Subject: RE: ALPR notice confidential
Date: Wednesday, December 9, 2020 11:40:00 AM
Attachments: National_ANPR_Service_technical_specifications.pdf
NASPLE_Version_2.1_November_2020.pdf
National standards for compliance and audit of law enforcement ANPR - September 2020 (accessible version) - GOV.UK.pdf

To:	Staples, Jennifer (POL)
Subject:	RE: ALPR notice confidential
Date:	Tuesday, December 8, 2020 2:24:05 PM
Attachments:	National_ANPR_Service_technical_specifications.pdf NASPLE_Version_2.1_November_2020.pdf

https://www.gov.uk/government/publications/national-anpr-standards

From: Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>
Sent: Tuesday, December 8, 2020 1:55 PM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: Re: ALPR notice confidential

Thank Brian. I think that may be a bit too soon for the group. We have a phone call on Friday to talk about the NDA and the notice.

I'm thinking we talk to the vendor next week.

I'll let you and Colonel Quinn know how the Friday meeting goes.

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Tuesday, December 8, 2020 12:47 PM
To: Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>
Subject: Re: ALPR notice confidential

Thanks, the vendor can do a meeting tomorrow at 11 am EST if that works.

> On Dec 8, 2020, at 9:07 AM, Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us> wrote:
>
> Here you go
>
> ---
>
> **From:** Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>
> **Sent:** Monday, December 7, 2020 5:39 PM
> **To:** Koulouris, Agapi (CHS) <agapi.koulouris@mass.gov>; Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>; Lord, Spencer (EPS) <spencer.b.lord@mass.gov>; McGarry, Matthew (CHS) <Matthew.McGarry@mass.gov>
> **Subject:** ALPR notice confidential
>
> Hello All: attached please find an edit version of the ALPR notice that incorporates changes requested by Gov. legal. Can you review and let me know (1) if it is still accurate and (2) your thoughts and comments many thanks

Susan
<2020.11.25 ALPR notice december.docx>

From:	Egnitz, Brian (POL)
To:	Staples, Jennifer (POL)
Subject:	RE: ALPR notice confidential
Date:	Tuesday, December 8, 2020 2:24:00 PM
Attachments:	National_ANPR_Service_technical_specifications.pdf NASPLE_Version_2.1_November_2020.pdf National standards for compliance and audit of law enforcement ANPR - September 2020 (accessible version) - GOV.UK.pdf

https://www.gov.uk/government/publications/national-anpr-standards

---

From: Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>
Sent: Tuesday, December 8, 2020 1:55 PM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: Re: ALPR notice confidential

Thank Brian. I think that may be a bit too soon for the group. We have a phone call on Friday to talk about the NDA and the notice.

I'm thinking we talk to the vendor next week.

I'll let you and Colonel Quinn know how the Friday meeting goes.

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Tuesday, December 8, 2020 12:47 PM
To: Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>
Subject: Re: ALPR notice confidential

Thanks, the vendor can do a meeting tomorrow at 11 am EST if that works.

> On Dec 8, 2020, at 9:07 AM, Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us> wrote:
>
> Here you go
>
> ---
>
> **From:** Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>
> **Sent:** Monday, December 7, 2020 5:39 PM
> **To:** Koulouris, Agapi (CHS) <agapi.koulouris@mass.gov>; Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>; Lord, Spencer (EPS) <spencer.b.lord@mass.gov>; McGarry, Matthew (CHS) <Matthew.McGarry@mass.gov>
> **Subject:** ALPR notice confidential
>
> Hello All: attached please find an edit version of the ALPR notice that incorporates

changes requested by Gov. legal. Can you review and let me know (1) if it is still accurate and (2) your thoughts and comments many thanks

Susan
<2020.11.25 ALPR notice december.docx>

From: Terrey, Susan (EPS)
To: McGarry, Matthew (CHS); Lord, Spencer (EPS)
Cc: Koulouris, Agapi (CHS); Staples, Jennifer (POL)
Subject: RE: ALPR notice confidential
Date: Monday, December 7, 2020 8:06:03 PM
Attachments: MSP - Data analysis snapshot.pptx
ALPR DCJIS Policy - Final 20131008.pdf

Matt and Spencer: thank you for your thoughtful and quick review! We definitely have a different view of the call. I really felt they said if you have two pieces of data (upload and time stamp) you can use one to confirm the accuracy of the other. See power point attached. I still agree its exculpatory and we need to disclose just feel that we can solve for this moving forward by the way we turn off the data. When you guys get a chance to review lets connect by phone

Substantive

- From our call with MSP and the vendor, I would be cautious about using this line: "An ALPR date and time stamp's accuracy can be determined through comparison with the upload date and time." My impression was that there was no window within which the times were necessarily accurate. They couldn't give us a benchmark or basis to determine what was good and what was bad. Maybe you have different info at this point, but that was my impression. If that's right, then we need to be cautious about using language that could be interpreted as a definitive statement validating certain readings. It seems intuitive that if the times are close, it's less likely to be an error, but I'm not sure we can even say that definitively. If that is something we can say, then we should still be clear and use terms such as "likely" that accurately reflect that it isn't a bright line Matt: I understood that they we looking for errors by comparing the delta between the upload time and the timestamp on the photo. If the upload time and the time stamp on the photo were less than one minute apart they were presumed to be accurate and more than a minute was an "error" If that is true as long as you have both the photo and the upload data you can determine if the time stamp is accurate. i.e. if the photo time stamp and the upload time stamp are within one minute of each other you can presume the photo time stamp was accurate. When Colonel Quinn said that he didn't think the system would be usable because it would never be able to assure accuracy, Brian responded, if you provided both the photo and the upload you would be able to show accuracy. The problem is that we could only do this for approx. one year of data
- I thought this was a little unclear: "The issue is limited to the ALPR, the date and time stamps of the upload are accurate." My impression is that the date and timestamps of the upload are accurate as to when it was uploaded, but they don't speak to when the car passed the camera. Someone reading that statement could be confused. Agreed its not artful but the idea is that the time when the data is uploaded is recorded accurately so you can look at the delta between photo time stamp and upload to determine accuracy.
- In the last paragraph, we suggest that the times can be verified by "a confirmation with upload time." From our call with the vendor, I did not think this was the case. Again, we didn't get any benchmark for what was and wasn't an error. I would leave this part of the sentence as "ALPR cameras should not be relied upon absent further information or independent evidence that establishes their accuracy." This phrasing covers verification by timestamp if that can be shown to be helpful, and it also covers everything else. Again, I may be wrong but I thought in the power point they showed that of the 126 million records they had 10 million with upload times that were

more than a minute or more different. So the way we found the problem was a non-industry accepted difference between the time on the photo and the time of the upload. The vendor put this at .4% see attached

- I'd like to see a little more explanation re the DCJIS Policy to show (assuming it's true – I wasn't involved with that policy so can't say) that it was promulgated in the interest of citizens' privacy. I attached a copy of the policy

Non-substantive (agree with all of these and Thank you !!)

I know these aren't important suggestion, but because this will be going out to a lot of people, I figured it would be helpful to suggest these style/grammatical edits anyway:

- First paragraph is indented but others are not;
- There should be two spaces after conclusion of each sentence -- in current draft, some have one and some have two; I agree with this but I read that the way you can tell the age of a person (and if you are doing your kids homework) is if you use two spaces because apparently you don't do that anymore
- There should be a comma after "passes" in the fourth line of the second paragraph;
- There should be a comma after "data" in the first line of the third paragraph;
- Lose the comma after "plates" in the second line of the third paragraph;
- MSP is referred to in shorthand as both the State Police and MSP – we should pick one shorthand version;
- In paragraph three, it simply mentions "the vendor," and it is not until paragraph six that we refer to "the relevant vendor, Neology, Inc." We should reverse the order so that paragraph three says "the relevant vendor, Neology, Inc." Then later on, we can refer simply to "the vendor" and it will make sense to the reader.
- Lose comma after "absent" in last paragraph.

From: McGarry, Matthew (CHS) <Matthew.McGarry@mass.gov>
Sent: Monday, December 7, 2020 6:36 PM
To: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>; Lord, Spencer (EPS) <spencer.b.lord@mass.gov>
Cc: Koulouris, Agapi (CHS) <agapi.koulouris@mass.gov>; Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>
Subject: RE: ALPR notice confidential

Sue and Spence:

Here are my thoughts for your consideration.

Hope this helps!

Matt

Substantive

- From our call with MSP and the vendor, I would be cautious about using this line: "An ALPR date and time stamp's accuracy can be determined through comparison with the upload date and time." My impression was that there was no window within which the times were necessarily accurate. They couldn't give us a benchmark or basis to determine what was good and what was bad. Maybe you have different info at this point, but that was my impression. If that's right, then we need to be cautious about using language that could be interpreted as a definitive statement validating certain readings. It seems intuitive that if the times are close, it's less likely to be an error, but I'm not sure we can even say that definitively. If that is something we can say, then we should still be clear and use terms such as "likely" that accurately reflect that it isn't a bright line.
- I thought this was a little unclear: "The issue is limited to the ALPR, the date and time stamps of the upload are accurate." My impression is that the date and timestamps of the upload are accurate as to when it was uploaded, but they don't speak to when the car passed the camera. Someone reading that statement could be confused.
- In the last paragraph, we suggest that the times can be verified by "a confirmation with upload time." From our call with the vendor, I did not think this was the case. Again, we didn't get any benchmark for what was and wasn't an error. I would leave this part of the sentence as "ALPR cameras should not be relied upon absent further information or independent evidence that establishes their accuracy." This phrasing covers verification by timestamp if that can be shown to be helpful, and it also covers everything else.
- I'd like to see a little more explanation re the DCJIS Policy to show (assuming it's true – I wasn't involved with that policy so can't say) that it was promulgated in the interest of citizens' privacy.

Non-substantive

I know these aren't important suggestion, but because this will be going out to a lot of people, I figured it would be helpful to suggest these style/grammatical edits anyway:

- First paragraph is indented but others are not;
- There should be two spaces after conclusion of each sentence -- in current draft, some have one and some have two;
- There should be a comma after "passes" in the fourth line of the second paragraph;
- There should be a comma after "data" in the first line of the third paragraph;
- Lose the comma after "plates" in the second line of the third paragraph;
- MSP is referred to in shorthand as both the State Police and MSP – we should pick one shorthand version;
- In paragraph three, it simply mentions "the vendor," and it is not until paragraph six that we refer to "the relevant vendor, Neology, Inc." We should reverse the order so that paragraph three says "the relevant vendor, Neology, Inc." Then later on, we can refer simply to "the vendor" and it will make sense to the reader.
- Lose comma after "absent" in last paragraph.

From: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>
Sent: Monday, December 7, 2020 5:40 PM
To: Koulouris, Agapi (CHS) <agapi.koulouris@mass.gov>; Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>; Lord, Spencer (EPS) <spencer.b.lord@mass.gov>; McGarry,

Matthew (CHS) <Matthew.McGarry@mass.gov>
Subject: ALPR notice confidential

Hello All: attached please find an edit version of the ALPR notice that incorporates changes requested by Gov. legal. Can you review and let me know (1) if it is still accurate and (2) your thoughts and comments many thanks

Susan

From:	Warren, Rosemary (POL)
To:	Egnitz, Brian (POL)
Subject:	RE: ALPR notice confidential
Date:	Wednesday, December 9, 2020 11:44:37 AM
Attachments:	National standards for compliance and audit of law enforcement ANPR - September 2020 (accessible version) - GOV.UK.docx NASPLE_Version_2.1_November_2020.docx National_ANPR_Service_technical_specifications.docx

Did it work?

Rosemary J. Warren
Division of Homeland Security and Preparedness
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
Office: 508-988-7310
Rosemary.Warren@mass.gov

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Wednesday, December 9, 2020 11:41 AM
To: Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>
Subject: RE: ALPR notice confidential

From:	Egnitz, Brian (POL)
To:	Connolly, Kevin
Subject:	RE: ALPR Program
Date:	Friday, May 29, 2020 1:40:00 PM
Attachments:	TRF-11 Automatic License Plate Recognition Revised 10-1-2019.pdf

From: Connolly, Kevin [mailto:connollyk@barnstablepolice.com]
Sent: Friday, May 29, 2020 12:55 PM
To: Egnitz, Brian (POL); 'jbukunt@avon-ma.gov'; 'dlinehan@avon-ma.gov'
Cc: Murphy, John
Subject: ALPR Program

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Chief/Deputy Chief

Please find attached to this email Brian Egnitz, he is with the Massachusetts State Police and is my main contact for ALPR questions and service. I am not sure who the actual person in charge of the program is, but if it is not Brian he will be able to point you in the right direction.

We have been extremely happy with utilizing the ALPR data with other evidence in assisting with our investigations. The link below is a presentation we were preparing for the courtroom, however after viewing this presentation defense agreed to a plea in the case. This was a Breaking & Entering case where we utilized cell site location information, ALPR data, and records from victims and stores to put a presentation together for grand jury. At the 1:35 mark of the video you will see where we utilized the ALPR data in conjunction with the CSLI to show where the suspect's vehicle was and the ALPR actually had a partial picture of the stolen bike in the bed of the truck.

This is just one of the many successes we have had where the ALPR has been key to solving and assisting with our cases.

https://www.dropbox.com/s/avcjr0kkgdwxfvp/June%2016.avi?dl=0

Please feel free to contact me if you have any questions at all.
Kevin

Kevin A. Connolly
Sergeant
Barnstable Police Department
508-958-6522
connollyk@barnstablepolice.com



Confidentiality Notice | This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential, proprietary, legally privileged and/or CORI information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient or have received this email in error, immediately contact the sender by reply e-mail and destroy all copies of the original message. This email message may be monitored by the Barnstable Police Department.

From:	Koulouris, Agapi (CHS)
To:	Staples, Jennifer (POL); Terrey, Susan (EPS); McGarry, Matthew (CHS); Lord, Spencer (EPS); Mullaney, Arielle (EPS)
Subject:	RE: ALPR
Date:	Wednesday, December 16, 2020 4:22:13 PM
Attachments:	image001.png Model ALPR Policy DCJIS updated 11-9-2020.doc

We can discuss tomorrow. I don't think they will be incorporating these soon. We can share our model policy if they would like to start reviewing it. I have attached it here.

From: Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>
Sent: Wednesday, December 16, 2020 3:59 PM
To: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>; McGarry, Matthew (CHS) <Matthew.McGarry@mass.gov>; Koulouris, Agapi (CHS) <agapi.koulouris@mass.gov>; Lord, Spencer (EPS) <spencer.b.lord@mass.gov>; Mullaney, Arielle (EPS) <Arielle.Mullaney@mass.gov>
Subject: RE: ALPR

Not to add any pressure to this issue, but we just received this email yesterday:

From: Papagiorgakis, Gina (OGR)
Sent: Tuesday, December 15, 2020 8:23 AM
To: Miller, Dianne (POL)
Subject: Automatic License Plate Reader Policy

Good morning Dianne,

I am hoping you can put me in touch with the right contact on your end. The DOC was awarded grant funds to procure an automatic license plate reader system, and thus will need to implement a policy. They are looking to reference existing policies to guide a draft of their own. Is there a policy at MSP that can be shared with the DOC, or is there anyone else who I should reach out to at MSP?

Thank you in advance.

Gina Papagiorgakis
Homeland Security Division
Office of Grants and Research
10 Park Plaza, Suite 3720-A
Boston, MA 02116
gina.papagiorgakis1@mass.gov

Jennifer M. Staples
Chief Legal Counsel
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702

Tel: (508) 820-2307
Cell: (774) [redacted]

The preceding email message (including any attachments) contains information that may be confidential, may be protected by the attorney-client or other applicable privileges, or may constitute non-public information. It is intended to be conveyed only to the designated recipient(s) named above. If you are not an intended recipient of this message, please notify the sender by replying to this message and then delete all copies of it from your computer system. Any use, dissemination, distribution, or reproduction of this message by unintended recipients is not authorized and may be unlawful.

From: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>
Sent: Wednesday, December 16, 2020 2:21 PM
To: McGarry, Matthew (CHS) <Matthew.McGarry@mass.gov>; Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>; Koulouris, Agapi (CHS) <agapi.koulouris@mass.gov>; Lord, Spencer (EPS) <spencer.b.lord@mass.gov>; Mullaney, Arielle (EPS) <Arielle.Mullaney@mass.gov>
Subject: RE: ALPR

Back at you with another stab

From: McGarry, Matthew (CHS) <Matthew.McGarry@mass.gov>
Sent: Tuesday, December 15, 2020 3:58 PM
To: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>; Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>; Koulouris, Agapi (CHS) <agapi.koulouris@mass.gov>; Lord, Spencer (EPS) <spencer.b.lord@mass.gov>; Mullaney, Arielle (EPS) <Arielle.Mullaney@mass.gov>
Subject: RE: ALPR

Sue:

Here are the suggested edits from Agapi and me to the extent they're helpful to you. We accepted Nick's edits and put our own suggestions in redline with suggested responses in comments.

Hope this helps,

Matt

From: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>
Sent: Tuesday, December 15, 2020 2:59 PM
To: Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>; Koulouris, Agapi (CHS) <agapi.koulouris@mass.gov>; Lord, Spencer (EPS) <spencer.b.lord@mass.gov>; McGarry, Matthew

(CHS) <Matthew.McGarry@mass.gov>; Mullaney, Arielle (EPS) <Arielle.Mullaney@mass.gov>
Subject: RE: ALPR

From: Terrey, Susan (EPS)
Sent: Tuesday, December 15, 2020 2:59 PM
To: Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>; Agapi Koulous (agapi.koulouris@mass.gov) <agapi.koulouris@mass.gov>; Lord, Spencer (EPS) <spencer.b.lord@mass.gov>; McGarry, Matthew (CHS) <Matthew.McGarry@mass.gov>
Subject: ALPR

Hi guys -- heard back from Nick – really the only sticking point is what is the "acceptable upload time" Is there any ball park we can put out ? Within a minute ? No more than 5 minutes. Not sure we could get away with "close in time" ? I put in some suggestions but they are still incredibly vague

Open to any and all suggestions

From: Whitcher, Toni (POL)
To: Mills, Melissa (POL)
Subject: RE: AMU data check for Retiree List
Date: Monday, August 10, 2020 3:20:30 PM
Attachments: Working Copy of AMU data check for retirees.xlsx

Hi Melissa,
Attached is the completed list for the retiree's I have completed today.

If you have any questions please let me know.

Thank you,

Toni D. Whitcher
Program Coordinator
Compliance Unit
Division of Administrative Services
Massachusetts State Police
470 Worcester Road
Framingham, Massachusetts 01702

508.820.2164 – office
508.820.2359 – facsimile
toni.whitcher@pol.state.ma.us

This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may include privileged or otherwise confidential information. Any unauthorized review, use, forwarding, printing, copying, disclosure or distribution is strictly prohibited. If you received this message in error, or have reason to believe you are not authorized to receive it, please notify me and promptly delete this message and attachments. This email, including any attachments, could possibly contain viruses. The receiver assumes all responsibility for checking and deleting any potential viruses.

From: Whitcher, Toni (POL)
Sent: Friday, August 07, 2020 11:44 AM
To: Mills, Melissa (POL) <Melissa.Mills@pol.state.ma.us>
Subject: AMU data check for Retiree List

Hi Melissa,
Here is the retiree list that is just about complete..i have a few more toward the end to finish up but it wont take very long, I should have it all done by Monday

If you have any questions please let me know.

Thank you,

Toni D. Whitcher
Program Coordinator
Compliance Unit
Division of Administrative Services
Massachusetts State Police
470 Worcester Road
Framingham, Massachusetts 01702

508.820.2164 – office
508.820.2359 – facsimile
toni.whitcher@pol.state.ma.us

This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may include privileged or otherwise confidential information. Any unauthorized review, use, forwarding, printing, copying, disclosure or distribution is strictly prohibited. If you received this message in error, or have reason to believe you are not authorized to receive it, please notify me and promptly delete this message and attachments. This email, including any attachments, could possibly contain viruses. The receiver assumes all responsibility for checking and deleting any potential viruses.

From:	Lord, Spencer (EPS)
To:	Collins, Kerry (EPS); Wark, Jake (EPS); Staples, Jennifer (POL); Mullaney, Arielle (EPS)
Cc:	Terrey, Susan (EPS)
Subject:	RE: APLR
Date:	Wednesday, December 23, 2020 11:01:59 AM
Attachments:	image001.png

Yes, I think Brian Egnitz at MSP has access to it since he'll be the one checking it.

Jenn, I can reach out to him if you'd like? Just let me know. Ty.

-Spence

From: Collins, Kerry (EPS) <Kerry.Collins@mass.gov>
Sent: Wednesday, December 23, 2020 11:01 AM
To: Lord, Spencer (EPS) <spencer.b.lord@mass.gov>; Wark, Jake (EPS) <Jake.Wark@mass.gov>; Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>; Mullaney, Arielle (EPS) <Arielle.Mullaney@mass.gov>
Cc: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>
Subject: RE: APLR

Who can physically send it out from that ALPR address? Does it have to be someone from MSP?

Kerry A. Collins
Undersecretary for Forensic Science and Technology
Executive Office of Public Safety and Security
1 Ashburton Place
Boston, MA 02108
Cell [redacted]
kerry.collins@mass.gov

From: Lord, Spencer (EPS) <spencer.b.lord@mass.gov>
Sent: Wednesday, December 23, 2020 10:57 AM
To: Wark, Jake (EPS) <Jake.Wark@mass.gov>; Collins, Kerry (EPS) <Kerry.Collins@mass.gov>; Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>; Mullaney, Arielle (EPS) <Arielle.Mullaney@mass.gov>
Cc: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>
Subject: RE: APLR

Great, here it is on letter head. Ty!

From: Wark, Jake (EPS) <Jake.Wark@mass.gov>
Sent: Wednesday, December 23, 2020 10:56 AM
To: Lord, Spencer (EPS) <spencer.b.lord@mass.gov>; Collins, Kerry (EPS) <Kerry.Collins@mass.gov>; Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>; Mullaney, Arielle (EPS) <Arielle.Mullaney@mass.gov>

Cc: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>
Subject: RE: APLR

Smart. That works for me, Spence.

From: Lord, Spencer (EPS) <spencer.b.lord@mass.gov>
Sent: Wednesday, December 23, 2020 10:45 AM
To: Collins, Kerry (EPS) <Kerry.Collins@mass.gov>; Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>; Mullaney, Arielle (EPS) <Arielle.Mullaney@mass.gov>
Cc: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>; Wark, Jake (EPS) <Jake.Wark@mass.gov>
Subject: RE: APLR

Why don't we put it on EOPSS letter head and send it from the ALPR email address in the notice? That way any replies will go right to that email? Does that work for everyone?

-Spence

From: Lord, Spencer (EPS)
Sent: Wednesday, December 23, 2020 10:42 AM
To: Collins, Kerry (EPS) <Kerry.Collins@mass.gov>; Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>; Mullaney, Arielle (EPS) <Arielle.Mullaney@mass.gov>
Cc: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>; Wark, Jake (EPS) <Jake.Wark@mass.gov>
Subject: RE: APLR

Do we have a generic email address this could come from? I'm afraid that whoever sends it is going to get bombarded with a million questions.

-Spence

From: Collins, Kerry (EPS) <Kerry.Collins@mass.gov>
Sent: Wednesday, December 23, 2020 10:32 AM
To: Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>; Mullaney, Arielle (EPS) <Arielle.Mullaney@mass.gov>; Lord, Spencer (EPS) <spencer.b.lord@mass.gov>
Cc: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>; Wark, Jake (EPS) <Jake.Wark@mass.gov>
Subject: RE: APLR

Thanks Jen, I think to make it stream lined, EOPSS should send it out.
Spence/Arielle- Can Lis or Micheala send this out today? Let me know when this is ready to out, I put Jake on this as well so he knows when it is out there.
Thanks
Kerry

Kerry A. Collins
Undersecretary for Forensic Science and Technology
Executive Office of Public Safety and Security

1 Ashburton Place
Boston, MA 02108
Cell [redacted]
kerry.collins@mass.gov

From: Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>
Sent: Wednesday, December 23, 2020 10:28 AM
To: Mullaney, Arielle (EPS) <Arielle.Mullaney@mass.gov>; Lord, Spencer (EPS) <spencer.b.lord@mass.gov>
Cc: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>; Collins, Kerry (EPS) <Kerry.Collins@mass.gov>
Subject: RE: APLR

Nancy White should be DOC, not DOT.

I can send to her if you want. Let me know.

Jennifer M. Staples
Chief Legal Counsel
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
Tel: (508) 820-2307
Cell: (774) [redacted]

The preceding email message (including any attachments) contains information that may be confidential, may be protected by the attorney-client or other applicable privileges, or may constitute non-public information. It is intended to be conveyed only to the designated recipient(s) named above. If you are not an intended recipient of this message, please notify the sender by replying to this message and then delete all copies of it from your computer system. Any use, dissemination, distribution, or reproduction of this message by unintended recipients is not authorized and may be unlawful.

From: Mullaney, Arielle (EPS) <Arielle.Mullaney@mass.gov>
Sent: Wednesday, December 23, 2020 10:01 AM
To: Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>; Lord, Spencer (EPS) <spencer.b.lord@mass.gov>
Cc: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>; Collins, Kerry (EPS) <Kerry.Collins@mass.gov>
Subject: RE: APLR

Here is the final version with the watermark removed, EOPSS as the sender, and today's date. I've attached a pdf and word document for us.

Here is the distribution list which I've updated to fill in the missing emails. I was unable to find the email for the Nantucket Bar association, the Greater Lowell Bar Association, Plymouth County Bar Association, or Victoria Kelleher at MACDL. I found the regular info email so I've included that below. I've also added Gina Kwon from AGO.

Tara Maguire, Executive Director, Massachusetts District Attorney's Office
1. Tara.maguire@mass.gov

Jason Scally, Director of Media/Communications, Massachusetts Bar Association,
2. jscally@massbar.org

Michael Avitzur, Director of Gov't Relations & Public Affairs, Boston Bar Association
3. mavitzur@bostonbar.org

Barnstable County Bar Association
4. info@barnstablebar.org

Berkshire County Bar Association
5. info@berkshirebar.com

Bristol County Bar Association
6. info@bristolcountybar.org

Essex County Bar Association Advocates
7. ecbaa@ecbaa.net

Franklin County Bar Association
8. franklinba@publiccounsel.net

Rob Normandin, Greater Lowell Bar Association

Noreen Nardi, Hampden County Bar Association
9. noreen@hcbar.org

Hampshire County Bar Association
10. hcba@crocker.com

Diane Verner, Middlesex County Bar Association
11. franklinba@publiccounsel.net

Robert Moriarty, Nantucket Bar Association

Jonathan Moriarty, Plymouth County Bar Association

Terry McLaughlin, Worcester County Bar Association
12. terry.mclaughlin@state.ma.us

Richard Dohoney, Berkshire District Attorney's Office
13. Richard.dohoney@massmail.state.ma.us

Patrick Bomberg, Bristol District Attorney's Office
14. Patrick.O.Bomberg@massmail.state.ma.us

Daniel Higgins, Cape and Islands District Attorney's Office
15. Dan.T.Higgins@mass.gov

Mary Alice Doyle, Essex District Attorney's Office
16. Mary-Alice.Doyle@massmail.state.ma.us

Ed Kivari, Hamden District Attorney's Office
17. Ekivari@massmail.state.ma.us

Michael Connolly, Norfolk District Attorney's Office
18. Michael.C.Connolly@massmail.state.ma.us

Alice Casey, Middlesex District Attorney's Office
19. Alice.Casey@massmail.state.ma.us

Michael Russo, Northwest District Attorney's Office
20. Michael.Russo@massmail.state.ma.us
Richard Linehan, Plymouth District Attorney's Office
21. Richard.Linehan@massmail.state.ma.us
Dana Pierce, Suffolk District Attorney's Office
22. Dana.Pierce@massmail.state.ma.us
Donald Xenos, Worcester District Attorney's Office
23. Don.Xenos@massmail.state.ma.us
Matthew Landry, General Counsel, Department of Transportation
24. Matthew.Landry@dot.state.ma.us
Joanne Norman, Chief Compliance Officer, Department of Transportation
25. Joanne.Norman@dot.state.ma.us
Anthony J. Benedetti, CPCS
26. Abenedetti@publiccounsel.net
Victoria Kelleher, MACDL
27. info@macdl.com
Eric R. Atstupenas, Massachusetts Chiefs of Police Association, Inc.
28. legal@masschiefs.org
Nancy White, Massachusetts Department of Correction
29. Nancy.White@dot.state.ma.us
Gina Kwon, AGO
30. gina.kwon@mass.gov

From: Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>
Sent: Wednesday, December 23, 2020 9:28 AM
To: Mullaney, Arielle (EPS) <Arielle.Mullaney@mass.gov>; Lord, Spencer (EPS) <spencer.b.lord@mass.gov>
Cc: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>
Subject: FW: APLR

This is the last version we have.

Jennifer M. Staples
Chief Legal Counsel
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
Tel: (508) 820-2307
Cell: (774) [redacted]

The preceding email message (including any attachments) contains information that may be confidential, may be protected by the attorney-client or other applicable privileges, or may constitute non-public information. It is intended to be conveyed only to the designated recipient(s) named above. If you are not an intended recipient of this message, please notify the sender by

replying to this message and then delete all copies of it from your computer system. Any use, dissemination, distribution, or reproduction of this message by unintended recipients is not authorized and may be unlawful.

From: Brandt, Nick (GOV) <Nick.Brandt@mass.gov>
Sent: Tuesday, December 22, 2020 5:30 PM
To: Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>; Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>
Cc: Collins, Kerry (EPS) <Kerry.Collins@mass.gov>; Koulouris, Agapi (CHS) <agapi.koulouris@mass.gov>; Wark, Jake (EPS) <Jake.Wark@mass.gov>
Subject: RE: APLR

All:

See attached for a few final suggested tweaks.

This can be distributed prior to the hearing tomorrow morning. I know it's not ideal, but I'd ask that you hold for tonight to allow for internal updates.

-Nick

Nick Brandt
Deputy Legal Counsel
Office of the Governor
State House, Room 271
Boston, MA 02133
617-725-4030

From: Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>
Sent: Tuesday, December 22, 2020 4:23 PM
To: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>; Brandt, Nick (GOV) <Nick.Brandt@mass.gov>
Cc: Collins, Kerry (EPS) <Kerry.Collins@mass.gov>; Koulouris, Agapi (CHS) <agapi.koulouris@mass.gov>; Wark, Jake (EPS) <Jake.Wark@mass.gov>
Subject: RE: APLR

9:00 a.m. Via Zoom.

Jennifer M. Staples
Chief Legal Counsel
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
Tel: (508) 820-2307
Cell: (774) [redacted] G.L. c. 4, sec. 7, cl. 26 (f)

The preceding email message (including any attachments) contains information that may be confidential, may be protected by the attorney-client or other applicable privileges, or may constitute non-public information. It is intended to be conveyed only to the designated recipient(s) named above. If you are not an intended recipient of this message, please notify the sender by replying to this message and then delete all copies of it from your computer system. Any use, dissemination, distribution, or reproduction of this message by unintended recipients is not authorized and may be unlawful.

From: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>
Sent: Tuesday, December 22, 2020 4:22 PM
To: Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>; Brandt, Nick (GOV) <Nick.Brandt@mass.gov>
Cc: Collins, Kerry (EPS) <Kerry.Collins@mass.gov>; Koulouris, Agapi (CHS) <agapi.koulouris@mass.gov>; Wark, Jake (EPS) <Jake.Wark@mass.gov>
Subject: RE: APLR

What time is the hearing

From: Staples, Jennifer (POL)
Sent: Tuesday, December 22, 2020 4:01 PM
To: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>; Brandt, Nick (GOV) <Nick.Brandt@mass.gov>
Cc: Collins, Kerry (EPS) <Kerry.Collins@mass.gov>; Koulouris, Agapi (CHS) <agapi.koulouris@mass.gov>; Wark, Jake (EPS) <Jake.Wark@mass.gov>
Subject: Re: APLR

Hi all. I think we need to decide how to handle this hearing tomorrow. I'm not sure this notice will make it out tonight. And the court will not be sympathetic to another extension.

Get Outlook for iOS

From: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>
Sent: Tuesday, December 22, 2020 3:55:16 PM
To: Brandt, Nick (GOV) <Nick.Brandt@mass.gov>; Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>
Cc: Collins, Kerry (EPS) <Kerry.Collins@mass.gov>; Koulouris, Agapi (CHS) <agapi.koulouris@mass.gov>; Wark, Jake (EPS) <Jake.Wark@mass.gov>
Subject: RE: APLR

Sorry all -- I am in a very long call and cannot weigh in meaning fully

---

From: Brandt, Nick (GOV)
Sent: Tuesday, December 22, 2020 2:56 PM
To: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>; Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>

Cc: Collins, Kerry (EPS) <Kerry.Collins@mass.gov>; Koulouris, Agapi (CHS) <agapi.koulouris@mass.gov>; Wark, Jake (EPS) <Jake.Wark@mass.gov>
Subject: RE: APLR

I agree with Jenn that the point is implicit in the current draft of the letter.

Sue, where would you propose to add language to that effect?

Nick Brandt
Deputy Legal Counsel
Office of the Governor
State House, Room 271
Boston, MA 02133
617-725-4030

From: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>
Sent: Tuesday, December 22, 2020 2:32 PM
To: Brandt, Nick (GOV) <Nick.Brandt@mass.gov>; Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>
Cc: Collins, Kerry (EPS) <Kerry.Collins@mass.gov>; Koulouris, Agapi (CHS) <agapi.koulouris@mass.gov>; Wark, Jake (EPS) <Jake.Wark@mass.gov>
Subject: RE: APLR

Sorry hit send too soon – adding Jake

From: Brandt, Nick (GOV)
Sent: Tuesday, December 22, 2020 2:22 PM
To: Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>; Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>
Cc: Collins, Kerry (EPS) <Kerry.Collins@mass.gov>; Koulouris, Agapi (CHS) <agapi.koulouris@mass.gov>
Subject: RE: APLR

Are you suggesting that the point (which is well-taken) needs to be added to the letter?

Nick Brandt
Deputy Legal Counsel
Office of the Governor
State House, Room 271
Boston, MA 02133
617-725-4030

From: Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>
Sent: Tuesday, December 22, 2020 2:19 PM
To: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>; Brandt, Nick (GOV) <Nick.Brandt@mass.gov>
Cc: Collins, Kerry (EPS) <Kerry.Collins@mass.gov>; Koulouris, Agapi (CHS) <agapi.koulouris@mass.gov>
Subject: RE: APLR

I agree. That's important.

Jennifer M. Staples
Chief Legal Counsel
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
Tel: (508) 820-2307
Cell: (774) [redacted]

The preceding email message (including any attachments) contains information that may be confidential, may be protected by the attorney-client or other applicable privileges, or may constitute non-public information. It is intended to be conveyed only to the designated recipient(s) named above. If you are not an intended recipient of this message, please notify the sender by replying to this message and then delete all copies of it from your computer system. Any use, dissemination, distribution, or reproduction of this message by unintended recipients is not authorized and may be unlawful.

From: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>
Sent: Tuesday, December 22, 2020 2:18 PM
To: Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>; Brandt, Nick (GOV) <Nick.Brandt@mass.gov>
Cc: Collins, Kerry (EPS) <Kerry.Collins@mass.gov>; Koulouris, Agapi (CHS) <agapi.koulouris@mass.gov>
Subject: RE: APLR

Just a reminder in the same way we can't show the cameras were accurate without a comparison to the upload we can't show that they were inaccurate either – saying they can't be relied on absent someother confirming data. It's a small nuance I agree

---

From: Staples, Jennifer (POL)
Sent: Tuesday, December 22, 2020 1:55 PM
To: Brandt, Nick (GOV) <Nick.Brandt@mass.gov>; Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>
Cc: Collins, Kerry (EPS) <Kerry.Collins@mass.gov>; Koulouris, Agapi (CHS) <agapi.koulouris@mass.gov>
Subject: RE: APLR

According to Brian, this problem most likely has existed since the first camera was installed in May of 2015.

Jennifer M. Staples
Chief Legal Counsel
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
Tel: (508) 820-2307
Cell: (774) [redacted]

The preceding email message (including any attachments) contains information that may be confidential, may be protected by the attorney-client or other applicable privileges, or may constitute non-public information. It is intended to be conveyed only to the designated recipient(s) named above. If you are not an intended recipient of this message, please notify the sender by replying to this message and then delete all copies of it from your computer system. Any use, dissemination, distribution, or reproduction of this message by unintended recipients is not authorized and may be unlawful.

From: Brandt, Nick (GOV) <Nick.Brandt@mass.gov>
Sent: Tuesday, December 22, 2020 12:43 PM
To: Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>; Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>
Cc: Collins, Kerry (EPS) <Kerry.Collins@mass.gov>; Koulouris, Agapi (CHS) <agapi.koulouris@mass.gov>
Subject: RE: APLR

OK thanks. I think the simpler way to ask the question is: what is the time frame during which this issue could potentially exist?

Nick Brandt
Deputy Legal Counsel
Office of the Governor
State House, Room 271
Boston, MA 02133
617-725-4030

From: Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>
Sent: Tuesday, December 22, 2020 12:41 PM
To: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>; Brandt, Nick (GOV) <Nick.Brandt@mass.gov>
Cc: Collins, Kerry (EPS) <Kerry.Collins@mass.gov>; Koulouris, Agapi (CHS) <agapi.koulouris@mass.gov>
Subject: RE: APLR

I believe the cameras were first put in 5 years ago with this vendor who had a different name or was bought out by Neology.

I will double check with Brian and Colonel Quinn and get back to you.

Jennifer M. Staples
Chief Legal Counsel
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
Tel: (508) 820-2307
Cell: (774) [redacted]

The preceding email message (including any attachments) contains information that may be confidential, may be protected by the attorney-client or other applicable privileges, or may constitute non-public information. It is intended to be conveyed only to the designated recipient(s) named above. If you are not an intended recipient of this message, please notify the sender by replying to this message and then delete all copies of it from your computer system. Any use, dissemination, distribution, or reproduction of this message by unintended recipients is not authorized and may be unlawful.

From: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>
Sent: Tuesday, December 22, 2020 12:39 PM
To: Brandt, Nick (GOV) <Nick.Brandt@mass.gov>
Cc: Collins, Kerry (EPS) <Kerry.Collins@mass.gov>; Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>; Koulouris, Agapi (CHS) <agapi.koulouris@mass.gov>
Subject: RE: APLR

Anyone know the answer to this one

From: Brandt, Nick (GOV)
Sent: Tuesday, December 22, 2020 12:38 PM
To: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>
Subject: RE: APLR

When were these Neology cameras first put into use? There's an interest in making clear how far back the problem stretches.

Nick Brandt
Deputy Legal Counsel
Office of the Governor
State House, Room 271
Boston, MA 02133

617-725-4030

From: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>
Sent: Tuesday, December 22, 2020 12:18 PM
To: Brandt, Nick (GOV) <Nick.Brandt@mass.gov>
Subject: APLR

Just need to add the sender to this one

To: Kennedy, Edward (DOC)
Cc: Black, Scott W. (DOC); Russell, Todd C. (DOC); DePalo, Patrick (DOC); Russell, Todd C. (DOC); Turcotte, Ray (DOC); Belrhitri, Mounir (DOC)
Subject: RE: APLR Followup from meetingm
Date: Wednesday, November 18, 2020 1:10:47 PM
Attachments: TRF-11 Automatic License Plate Recognition Revised 10-1-2019 (1).pdf
image001.png
Inv_ACS164281_from_Access_Control_Systems_7776.pdf
image002.png

Our P492s are 5 amp. Our trailers are spec to 600 amp hours

Attached is our policy and an old invoice for some trailers.

Our speed trailer gets about 1-3 days in worst sun conditions of continues power
Maybe a day without sun

Two 85 watt
solar panels - Three 12VDC AGM
batteries, 600 Ah total capacity

Wanco Systems- Custom Mast Trailer: As
per picture w/ previous mount for 3M LPR,
500 W Solar/ 3 x 200Ah, AGM Batteries
(600 total Ah),

ALPR System Vehicle Power Draw

When off, the ALPR system should draw around 20miliamps. The chart below shows the power draw when operational.

Component	Current Draw	Total Draw
SX Processor	3.5 A @ 12VDC	3.5 A @12VDC
Camera 1	1.0 A @ 12VDC	4.5 A @12VDC
Camera 2	1.0 A @ 12VDC	5.5 A @12VDC
Camera 3	1.0 A @ 12VDC	6.5 A @12VDC
Camera 4	1.0 A @ 12VDC	7.5 A @12VDC

NOTE: *These calculations do NOT include load from the MDC, Touchscreen monitor, or GPS antenna*

From: Kennedy, Edward (DOC) <Edward.M.Kennedy@doc.state.ma.us>
Sent: Wednesday, November 18, 2020 11:14 AM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Cc: Black, Scott W. (DOC) <Scott.Black@doc.state.ma.us>; Russell, Todd C. (DOC) <Todd.C.Russell@doc.state.ma.us>; DePalo, Patrick (DOC) <Patrick.Depalo@doc.state.ma.us>; Russell, Todd C. (DOC) <Todd.C.Russell@doc.state.ma.us>; Turcotte, Ray (DOC) <Ray.Turcotte@doc.state.ma.us>; Belrhitri, Mounir (DOC) <Mounir.Belrhitri@doc.state.ma.us>
Subject: APLR Followup from meetingm

Brian,
Thank you for taking the time to come over to DOC and help us get this off the ground.
As you requested we are looking for the word document for the Policies and procedures from MSP and EOPPS on the ALPR program so we can start laying down our ground work.
Also looking for the specs on the solar setups.
Thank you and stay safe, and have a great Thanksgiving.

Edward M. Kennedy
Director of Security & Technology
DOC Headquarters
50 Maple Street
Milford, Ma 01757
Cell [redacted]
Edward.M. Kennedy@doc.state.ma.us

From: Egnitz, Brian (POL)
To: Kennedy, Edward (DOC)
Cc: Black, Scott W. (DOC); Russell, Todd C. (DOC); DePalo, Patrick (DOC); Russell, Todd C. (DOC); Turcotte, Ray (DOC); Belrhitri, Mounir (DOC)
Subject: RE: APLR Followup from meetingm
Date: Wednesday, November 18, 2020 1:18:00 PM
Attachments: TRF-11 Automatic License Plate Recognition Revised 10-1-2019 (1).pdf
image001.png
Inv_ACS164281_from_Access_Control_Systems_7776.pdf
image002.png

Attached is our policy and an old invoice for some trailers.

Our P492s are 5 amps. Most of or our trailers are spec to 600 amp hours

Our speed trailer gets about 1-2 days in worst sun conditions of continues power
Maybe a day without sun

Two 85 watt
solar panels - Three 12VDC AGM
batteries, 600 Ah total capacity

These are the ones we use mostly and can go for 3-4 days without sun
Wanco Systems- Custom Mast Trailer: As
per picture w/ previous mount for 3M LPR,
500 W Solar/ 3 x 200Ah, AGM Batteries
(600 total Ah),

These are the specs for the mobile setup you were looking at, so it looks like you would want to be 600+ amp hours and 500w + of solar

ALPR System Vehicle Power Draw

When off, the ALPR system should draw around 20miliamps. The chart below shows the power draw when operational.

Component	Current Draw	Total Draw
SX Processor	3.5 A @ 12VDC	3.5 A @12VDC
Camera 1	1.0 A @ 12VDC	4.5 A @12VDC
Camera 2	1.0 A @ 12VDC	5.5 A @12VDC
Camera 3	1.0 A @ 12VDC	6.5 A @12VDC
Camera 4	1.0 A @ 12VDC	7.5 A @12VDC

NOTE: *These calculations do NOT include load from the MDC, Touchscreen monitor, or GPS antenna*

From: Kennedy, Edward (DOC) <Edward.M.Kennedy@doc.state.ma.us>
Sent: Wednesday, November 18, 2020 11:14 AM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Cc: Black, Scott W. (DOC) <Scott.Black@doc.state.ma.us>; Russell, Todd C. (DOC) <Todd.C.Russell@doc.state.ma.us>; DePalo, Patrick (DOC) <Patrick.Depalo@doc.state.ma.us>; Russell, Todd C. (DOC) <Todd.C.Russell@doc.state.ma.us>; Turcotte, Ray (DOC) <Ray.Turcotte@doc.state.ma.us>; Belrhitri, Mounir (DOC) <Mounir.Belrhitri@doc.state.ma.us>
Subject: APLR Followup from meetingm

Brian,
Thank you for taking the time to come over to DOC and help us get this off the ground.
As you requested we are looking for the word document for the Policies and procedures from MSP and EOPPS on the ALPR program so we can start laying down our ground work.
Also looking for the specs on the solar setups.
Thank you and stay safe, and have a great Thanksgiving.

Edward M. Kennedy
Director of Security & Technology
DOC Headquarters
50 Maple Street
Milford, Ma 01757
Cell [redacted]
Edward.M. Kennedy@doc.state.ma.us

From:	Staples, Jennifer (POL)
To:	Collins, Kerry (EPS)
Cc:	Terrey, Susan (EPS); Koulouris, Agapi (CHS); Lord, Spencer (EPS); McGarry, Matthew (CHS); Mullaney, Arielle (EPS); Gagnon, Jamison R. (CHS)
Subject:	Re: APLR
Date:	Saturday, December 19, 2020 10:42:31 AM
Attachments:	ALPR1217 thursday pm.Final.12.19.20.docx

Hi All:

Here is the notice with the dates added. I will reach out to Colonel Quinn and Brian about how they want to handle inquiries and will get back to everyone,

Thanks!

From: Collins, Kerry (EPS) <Kerry.Collins@mass.gov>
Sent: Saturday, December 19, 2020 10:16 AM
To: Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>
Cc: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>; Koulouris, Agapi (CHS) <agapi.koulouris@mass.gov>; Lord, Spencer (EPS) <spencer.b.lord@mass.gov>; McGarry, Matthew (CHS) <Matthew.McGarry@mass.gov>; Mullaney, Arielle (EPS) <Arielle.Mullaney@mass.gov>; Gagnon, Jamison R. (CHS) <Jamison.R.Gagnon@mass.gov>
Subject: Re: APLR

An MSP attorney should field the questions

Sent from my iPhone

> On Dec 19, 2020, at 10:14 AM, Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us> wrote:
>
> MSP can handle verification of time and date stamps of particular reads. But do we want them fielding questions from attorneys and courts?
>
> Get Outlook for iOS
>
> ---
>
> **From:** Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>
> **Sent:** Saturday, December 19, 2020 10:12:16 AM
> **To:** Collins, Kerry (EPS) <Kerry.Collins@mass.gov>
> **Cc:** Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>; Koulouris, Agapi (CHS) <agapi.koulouris@mass.gov>; Lord, Spencer (EPS) <spencer.b.lord@mass.gov>; McGarry, Matthew (CHS) <Matthew.McGarry@mass.gov>; Mullaney, Arielle (EPS) <Arielle.Mullaney@mass.gov>
> **Subject:** Re: APLR

They will need access to the upload time and date data

> On Dec 19, 2020, at 9:57 AM, Collins, Kerry (EPS) <Kerry.Collins@mass.gov> wrote:
>
> Who manages the cameras now? I would think it would be that person?
>
> Sent from my iPhone
>
> > On Dec 19, 2020, at 9:35 AM, Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us> wrote:
> >
> > I provided the dates but can plug them in. Who is the contact person going to be?
> >
> > Get Outlook for iOS
> >
> > ---
> >
> > **From:** Collins, Kerry (EPS) <Kerry.Collins@mass.gov>
> > **Sent:** Saturday, December 19, 2020 8:55:10 AM
> > **To:** Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>
> > **Cc:** Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>; Koulouris, Agapi (CHS) <agapi.koulouris@mass.gov>; Lord, Spencer (EPS) <spencer.b.lord@mass.gov>; McGarry, Matthew (CHS) <Matthew.McGarry@mass.gov>; Mullaney, Arielle (EPS) <Arielle.Mullaney@mass.gov>
> > **Subject:** Re: APLR
> >
> > Good morning,
> > Thank you Sue for your work on this.
> > Jen- are you going to fill in the date of the shut down and the contact person? If not, who should do this?
> > I would like this ready for the Gov's office by tomorrow.
> > Thanks
> > Kerry
> >
> > Sent from my iPhone
> >
> > > On Dec 19, 2020, at 8:24 AM, Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov> wrote:

Hello All: This is in good shape the final step is the fill in the dates and the contact info. If we can get that in place it will move up the chain over at Governor's office

Susan

From: Terrey, Susan (EPS)
Sent: Thursday, December 17, 2020 1:42 PM
To: Collins, Kerry (EPS) <Kerry.Collins@mass.gov>; Agapi Koulous (agapi.koulouris@mass.gov) <agapi.koulouris@mass.gov>; Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>; Lord, Spencer (EPS) <spencer.b.lord@mass.gov>; McGarry, Matthew (CHS) <Matthew.McGarry@mass.gov>; Mullaney, Arielle (EPS) <Arielle.Mullaney@mass.gov>
Subject: APLR

With edits. Just waiting on the answer to shutting down the cameras until the patch is in place

Susan Terrey
General Counsel – Executive Office of Public Safety and Security
617-274-5522 (office)
781-379-9923 (mobile)

<ALPR1217 thursday pm.docx>

From: Miller, Dianne (POL)
To: Papagiorgakis, Gina (OGR)
Cc: Silva, Kyra (POL); Comeau, Melissa (POL); Biagi, Pamela (POL)
Subject: RE: Automatic License Plate Reader Policy
Date: Tuesday, December 15, 2020 2:59:34 PM
Attachments: TRF-11 Automatic License Plate Recognition Revised 10-1-2019.pdf
IT Terms and Conditions.pdf
image002.png

Hi Gina,

Attached please find MSP policy TRF-11 relative to ALPR's.

DOC staff should also obtain the policy referenced below from DCJIS:

Executive Office of Public Safety and Security (EOPSS) - *The Commonwealth of Massachusetts Global Justice and Public Safety Information Sharing Policy*
Executive Office of Public Safety and Security (EOPSS) - Department of Criminal Justice Information Services - *Automatic License Plate Recognition System Central Repository Companion Policy.*

Lastly, the vendor would need to comply with the IT Terms and Conditions attached. We order ALPRs through the EOPSS OTIS requisition process.

Thank you

Dianne Miller
Program Coordinator III
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
(508) 820-2143

The preceding email message (including any attachments) contains information that may be confidential, may be protected by the attorney-client or other applicable privileges, or may constitute non-public information. It is intended to be conveyed only to the designated recipient(s) named above. If you are not an intended recipient of this message, please notify the sender by replying to this message and then delete all copies of it from your computer system. Any use, dissemination, distribution, or reproduction of this message by unintended recipients is not authorized and may be unlawful.

From: Papagiorgakis, Gina (OGR)
Sent: Tuesday, December 15, 2020 8:23 AM
To: Miller, Dianne (POL)
Subject: Automatic License Plate Reader Policy

Good morning Dianne,

I am hoping you can put me in touch with the right contact on your end. The DOC was awarded grant funds to procure an automatic license plate reader system, and thus will need to implement a policy. They are looking to reference existing policies to guide a draft of their own. Is there a policy at MSP that can be shared with the DOC, or is there anyone else who I should reach out to at MSP?

Thank you in advance.

Gina Papagiorgakis
Homeland Security Division
Office of Grants and Research
10 Park Plaza, Suite 3720-A
Boston, MA 02116
gina.papagiorgakis1@mass.gov

From: John Tedona
To: Egnitz, Brian (POL)
Subject: RE: BOSS 4.0 Pricing
Date: Monday, February 10, 2020 11:40:25 AM
Attachments: image001.png
image002.png
BOSS 4 subscription layers.xlsx

BOSS 4.0 Software was quoted at $16,995 per year.
Hosting services for BOSS4 was quoted an additional $118,000 per year
Mantis based on the expected data volume would be $125,000 per year. Hosting Mantis is only about 10% of the overall Mantis price, so on-prem Mantis would be in the $112,000

I attached an outline that highlights what is included in the hosted services.

John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Monday, February 10, 2020 8:34 AM
To: John Tedona <jtedona@neology.net>
Subject: RE: BOSS 4.0 Pricing

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

What's the on-prem mantis add-on cost? Is it 125K or was that 125K you guys hosting everything and having mantis?

From: John Tedona [mailto:jtedona@neology.net]
Sent: Thursday, January 23, 2020 4:40 PM
To: Egnitz, Brian (POL)
Subject: BOSS 4.0 Pricing

I understand you don't need this now, but for your reference I've attached pricing for BOSS 4.0 software, pricing for AWS hosting services that is to be added to the BOSS 4.0 license fee if you decide to have PIPS host (see notes in the Cloud/SAS quote that gives an overview of host services and discounts for a 3 or 5 year contact) and the Mantis price adder if you decide to include vehicle classification.

Let me know if you have any questions.



A NEOLOGY Business

John Tedona
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: John Tedona
To: Egnitz, Brian (POL)
Subject: RE: BOSS 4.0 Pricing
Date: Tuesday, February 11, 2020 9:14:11 AM
Attachments: BOSS 4 subscription layers.xlsx

Yes.

1. BOSS 4 software on prem is $16,995
2. If you prefer we host it and maintain and provide the AWS services outlined in this attachment, the total would be $16,995 plus $118,000 for hosting.
3. If you want Mantis its an additional $125,000 on top of either (1) or (2) We can provide Mantis for 30 to 90 days at no cost to see how well it fits your needs.

John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Monday, February 10, 2020 9:11 PM
To: John Tedona <jtedona@neology.net>
Subject: Re: BOSS 4.0 Pricing

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

So if we had you host everything and have mantis, is it 118,000+125,000+16,995?

Or is it Just $125,000 for everything hosted?

If on-prem, mantis is 16995 + 112,000?

> On Feb 10, 2020, at 11:40 AM, John Tedona <jtedona@neology.net> wrote:
>
> BOSS 4.0 Software was quoted at $16,995 per year.
> Hosting services for BOSS4 was quoted an additional $118,000 per year
> Mantis based on the expected data volume would be $125,000 per year. Hosting

Mantis is only about 10% of the overall Mantis price, so on-prem Mantis would be in the $112,000

I attached an outline that highlights what is included in the hosted services.

John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Monday, February 10, 2020 8:34 AM
To: John Tedona <jtedona@neology.net>
Subject: RE: BOSS 4.0 Pricing

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

What's the on-prem mantis add-on cost? Is it 125K or was that 125K you guys hosting everything and having mantis?

From: John Tedona [mailto:jtedona@neology.net]
Sent: Thursday, January 23, 2020 4:40 PM
To: Egnitz, Brian (POL)
Subject: BOSS 4.0 Pricing

I understand you don't need this now, but for your reference I've attached pricing for BOSS 4.0 software, pricing for AWS hosting services that is to be added to the BOSS 4.0 license fee if you decide to have PIPS host (see notes in the Cloud/SAS quote that gives an overview of host services and discounts for a 3 or 5 year contact) and the Mantis price adder if you decide to include vehicle classification.

Let me know if you have any questions.

<image001.png>
A
<image002.png>
Business

John Tedona
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

<BOSS 4 subscription layers.xlsx>

From: Shea, Scott (POL)
To: Egnitz, Brian (POL)
Subject: Re: BOSS License Plate#: V630437 Alert FROM CIL49231181438_I84E
Date: Thursday, November 5, 2020 8:18:22 AM
Attachments: LPR hits.xlsx

Sgt. Scott Shea #3179

Massachusetts State Police
CHQ Community Action Team
612 Main Street (Rte 122A)
Holden, MA 01520
508-829-8382
Scott.shea@pol.state.ma.us

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Thursday, November 5, 2020 7:46 AM
To: Shea, Scott (POL) <scott.shea@pol.state.ma.us>
Subject: Re: BOSS License Plate#: V630437 Alert FROM CIL49231181438_I84E

That's a good one!

> On Nov 4, 2020, at 8:26 PM, Shea, Scott (POL) <scott.shea@pol.state.ma.us> wrote:
>
> Great hit today. Stolen during a carjacking in NYC.
> 3 arrests, 2 kilos and a gun recovered this afternoon
>
> *Sgt. Scott Shea #3179*
>
> Massachusetts State Police
> CHQ Community Action Team
> 612 Main Street (Rte 122A)
> Holden, MA 01520
> 508-829-8382
> *Scott.shea@pol.state.ma.us*
>
> ---
>
> **From:** ALPR Alerts (POL) <ALPRAlerts@pol.state.ma.us>
> **Sent:** Wednesday, November 4, 2020 2:55 PM
> **To:** Shea, Scott (POL) <scott.shea@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Barrera, Michael (POL) <michael.barrera@pol.state.ma.us>; POL-DL-C10LPR <C10LPR@mass.gov>; POL-DL-C5LPR <C5LPR@mass.gov>; Gilbert, Jeffrey (POL) <jeffrey.gilbert@pol.state.ma.us>; Moran, Mathew (POL) <mathew.moran@pol.state.ma.us>; Bertozzi, Paul (POL) <paul.bertozzi@pol.state.ma.us>
> **Subject:** FW: BOSS License Plate#: V630437 Alert FROM CIL49231181438_I84E
>
> ---
>
> From: BossAlerts@state.ma.us
> Sent: Wednesday, November 4, 2020 2:55:12 PM (UTC-05:00) Eastern Time (US & Canada)
> To: ALPR Alerts (POL)
> Subject: BOSS License Plate#: V630437 Alert FROM CIL49231181438_I84E
>
> Hit on LPR Hotlist: NCIC - ETL - NORTHEAST
> License Plate#: V630437
> Date Time of Hit: 11/4/2020 2:54:39 PM
> Location Description - MA/CT border comming into MA I84E bound
> Hit Location Details: Source - CIL49231181438_I84E Site - CURRENT FIXED LPR PORTABLE
> Lat & Long - 42.03127,-72.13544 https://urldefense.proofpoint.com/v2/url?u=http-3A__maps.google.com_-3Ft-3Dm-26q-3D42.03127-2C-2D72.13544&d=DwIFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=qnhzpiL-hyLp8QyNVVsZfaWkYVkMcQfSbVt9Dw79kKk&m=CznSB6WL1l9xiaFhO3H8G8dbUEwbCLad68hdQKkMoWw&s=UOSwRKN-

0p-k_1sC1uP_k713W9eLisRpsMUyuf61l2E&e=

Hotlist Detailed Information:
NJ
2018
MERZ
GRY
03030P1
712467974
Stolen Vehicle
License Plate#: V630437
<247b2dd2-2cf4-4932-beac-bc4eee710e63.jpeg>
<c50463bd-0d8b-43a1-80c0-676144e7a68c.jpeg>

From: Peter Crary
To: Egnitz, Brian (POL); John Tedona
Subject: RE: BOSS update
Date: Tuesday, January 14, 2020 1:34:20 PM
Attachments: image002.png
BOSS4 Specifications 20191015.pdf

No, attached are the current server specs.

-Peter Crary
Global R&D Director, ANPR/ALPR
(858) 391-0260 x1153 (d)
(865) 386-3821 (m)

The information contained in this communication is confidential and intended only for the use of the recipient named and may also be legally privileged. If you are not the intended recipient (named addressee), you are hereby notified that any dissemination, distribution, copying or making use of this communication, or any of its contents, is strictly prohibited. Please notify the sender immediately by email and delete the original message and any copy of it from your computer system. The integrity, security of and absence of viruses in this message cannot be guaranteed on the internet. The sender therefore does not accept liability for any errors or omissions in the contents of this message, nor any damage caused, which arise as a result of e-mail transmission.

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Tuesday, 14 January, 2020 05:07
To: Peter Crary <pcrary@neology.net>; John Tedona <jtedona@neology.net>
Subject: FW: BOSS update

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Are this still current for Boss 4.0?

From: Egnitz, Brian (POL)
Sent: Tuesday, March 12, 2019 4:14 PM
To: Stockwell, Matt (EPS); Mitchell, Timothy (EPS)
Subject: RE: BOSS update

From: Stockwell, Matt (EPS)
Sent: Tuesday, March 12, 2019 4:14 PM
To: Egnitz, Brian (POL); Mitchell, Timothy (EPS)
Subject: RE: BOSS update

Hi Brian –

If there was an attachment or additional details on the sizing they did not come through via e-mail.

Matt

From: Egnitz, Brian (POL)
Sent: Tuesday, March 12, 2019 3:04 PM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Stockwell, Matt (EPS) <matt.stockwell@mass.gov>
Subject: FW: BOSS update

FYI

From: John Tedona [mailto:jtedona@neology.net]
Sent: Tuesday, March 12, 2019 11:00 AM
To: Egnitz, Brian (POL)
Cc: Michael Roth
Subject: RE: BOSS update

Brian,

Here's the recommended sizing criteria for the application and database servers. With more fixed cameras pushing data to BOSS it's highly recommended you keep this sizing criteria in mind.

John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Tuesday, March 12, 2019 10:49 AM

To: Michael Roth <mroth@neology.net>
Cc: Peter Crary <pcrary@neology.net>; Israel Padilla <ipadilla@neology.mx>; Michell Itallekzi Garcia Garcia <colaborador6@neopartners.mx>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; John Tedona <jtedona@neology.net>; PIPS Technology Support <support@pipstechnology.com>; Quinn, Dermot (POL) <dermot.quinn@state.ma.us>; Clarke, Shannon (EPS) <shannon.clarke@state.ma.us>
Subject: RE: BOSS update

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Thanks Mike, Ive sent that to the tech. here is the license key. I saw the 5 concurrent number in the boss log folder

---

From: Michael Roth [mailto:mroth@neology.net]
Sent: Tuesday, March 12, 2019 10:33 AM
To: Egnitz, Brian (POL); Peter Crary; Israel Padilla; Michell Itallekzi Garcia Garcia; Mitchell, Timothy (EPS); John Tedona; PIPS Technology Support; Quinn, Dermot (POL); Clarke, Shannon (EPS)
Subject: RE: BOSS update

Can you send me screen shoot of the licenses.

That error occurs when using other browser than IE.

1. Prerequisites needed to successful install of BossUI client, the below settings pertain to OS where client is being installed.
    a. "Active Scripting" needs to be enabled in Windows "Internet Options"- "Security"- "Internet"- "Custom level". (This setting is for Bing maps to function).
    b. Can you add http:// address to "Local Intranet" in Intranet Zones Sites. (This can be taken out after installation as it is only needed for deployment).

2. Internet Explorer must be use.

Michael B. Roth
ALPR Technician
O: 858.391.0260 Ext. 1234
C: 513.767.7610
mroth@neology.net
A Business
www.pipstechnology.com

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Tuesday, March 12, 2019 7:06 AM
To: Peter Crary <pcrary@neology.net>; Michael Roth <mroth@neology.net>; Israel Padilla <ipadilla@neology.mx>; Michell Itallekzi Garcia Garcia <colaborador6@neopartners.mx>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; John Tedona <jtedona@neology.net>; PIPS Technology Support <support@pipstechnology.com>; Quinn, Dermot (POL) <dermot.quinn@state.ma.us>; Clarke, Shannon (EPS) <shannon.clarke@state.ma.us>
Subject: RE: BOSS update

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

I addition, I believe we may need a new license file. The logs say "5 concurrent" licenses available.

From: Egnitz, Brian (POL)
Sent: Tuesday, March 12, 2019 6:43 AM
To: Peter Crary; Michael Roth; Israel Padilla; Michell Itallekzi Garcia Garcia; Mitchell, Timothy (EPS); John Tedona; PIPS Technology Support; Quinn, Dermot (POL); Clarke, Shannon (EPS)
Subject: Fwd: BOSS update

Hi guys,

Is there an updated client? This on appears to be calling the Spanish version of dot net, it's also not using the updated version already installed. Do you have one that is properly signed too???

Begin forwarded message:

> **From:** "Ghasemi, Kiarash (POL)" <Kiarash.Ghasemi@pol.state.ma.us>
> **Date:** March 11, 2019 at 10:35:38 PM EDT
> **To:** "Egnitz, Brian (POL)" <brian.egnitz@pol.state.ma.us>, "Sullivan, Margaret (POL)" <Margaret.Sullivan@pol.state.ma.us>
> **Cc:** "Quinn, Dermot (POL)" <dermot.quinn@pol.state.ma.us>, "Kelly, Edward (POL)" <Edward.Kelly@pol.state.ma.us>, "Hernandez, Oscar (POL)" <Oscar.Hernandez@pol.state.ma.us>, "Weldon, Stephen (POL)" <Stephen.Weldon@pol.State.MA.US>, "Griffin, Daniel (POL)" <daniel.griffin@MassMail.State.MA.US>

Subject: RE: BOSS update

Hi Brian,

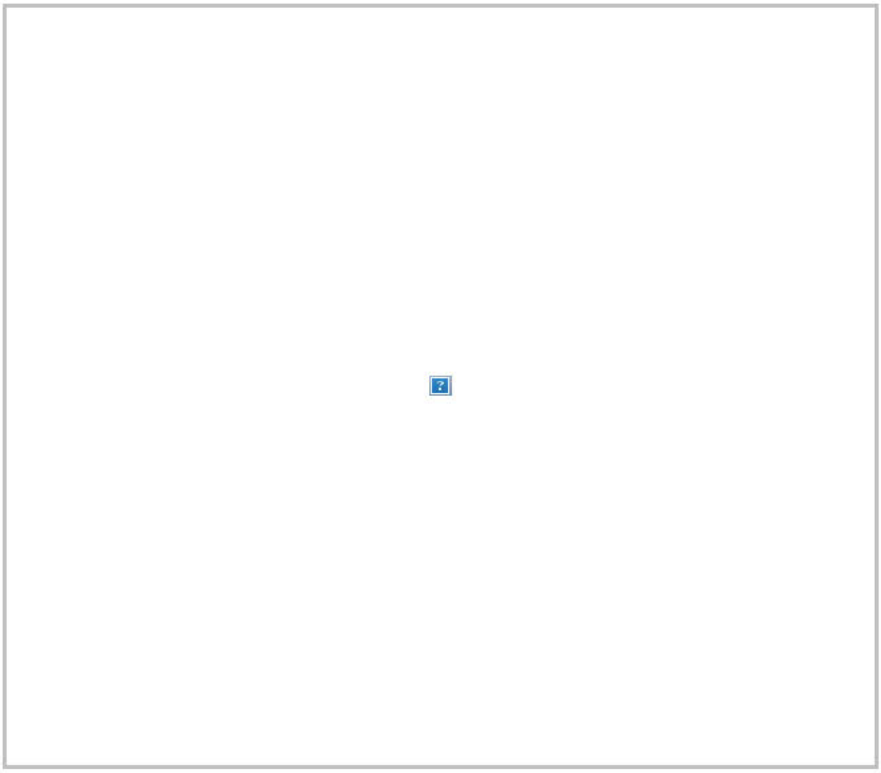
Before this update, On computers that needed access to LPR reporting, we have a copied a folder called "SA Client" and "SA.UI" within that folder, we create a shortcut to that file and that eliminated installation of any program.

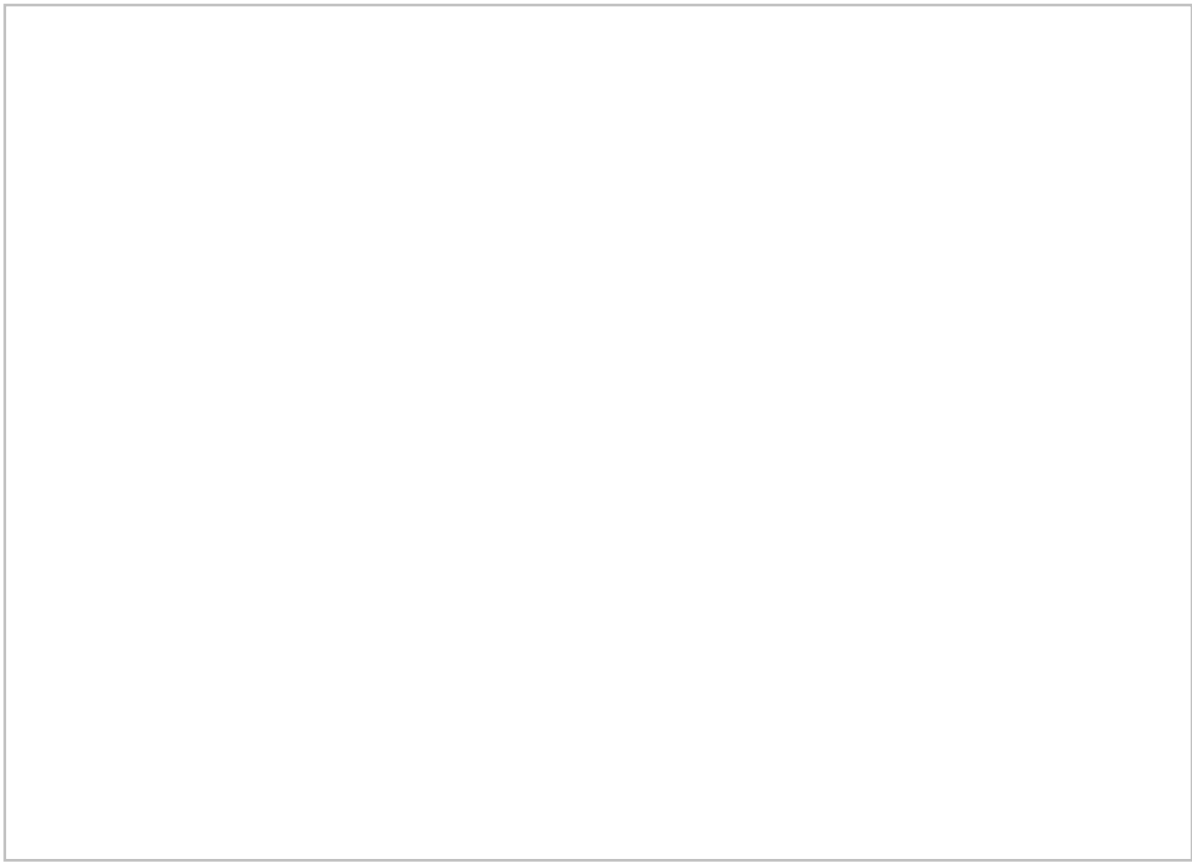
But I have tried the link that you have provided us and I'm getting an error message in Spanish during the installation! (Please see below) What I get from it, it need .Net. 4.5.2 but my computer already has 4.7 installed on it. I also tried to install it on Watchcenter computers and I got the same error message in Spanish and .Net 4.5.2 wont install on top of the current version of 4.7

Also translation of other part of the error message is that:

"The Microsoft .NET Framework 4.5.2 installation is not supported on this operating system. Please contact the administrator."

I have CC Lt. Griffin on this email, since he has done many installation of the old one too and all his stations are also effected too.





Error de comprobación de los requisitos previos del componente del sistema Microsoft .NET Framework 4.5.2 (x86 y x64) con el siguiente mensaje: "La instalación de Microsoft .NET Framework 4.5.2 no se admite en este sistema operativo. Póngase en contacto con el administrador."

Vea el archivo de registro de la instalación que se encuentra en 'C:\Users\MJACKS~1\AppData\Local\Temp\VSD1947.tmp\install.log' para obtener más información.

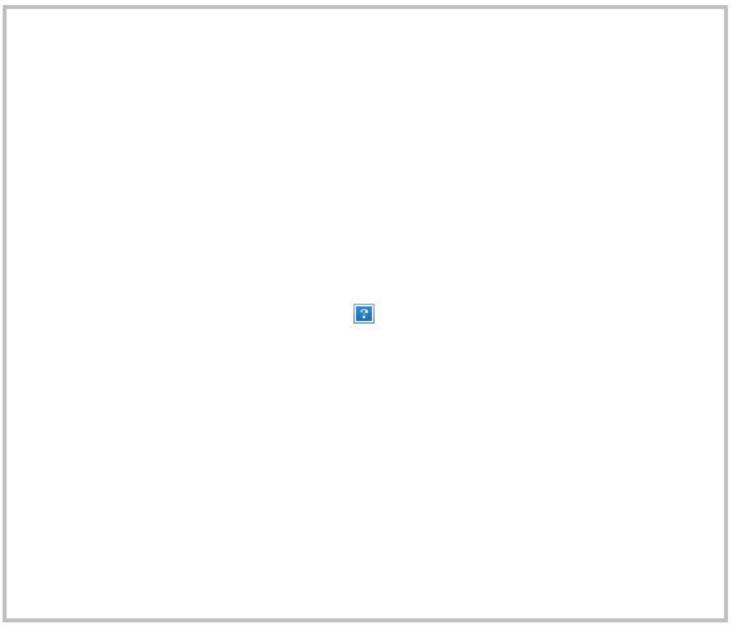
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Monday, March 11, 2019 9:58 PM
To: Sullivan, Margaret (POL) <Margaret.Sullivan@pol.state.ma.us>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Kelly, Edward (POL) <Edward.Kelly@pol.state.ma.us>; Hernandez, Oscar (POL) <Oscar.Hernandez@pol.state.ma.us>; Weldon, Stephen (POL) <Stephen.Weldon@pol.State.MA.US>; Ghasemi, Kiarash (POL) <Kiarash.Ghasemi@pol.state.ma.us>
Subject: BOSS update

Hi Peg,

The BOSS ALPR application has been updated in case you get some calls regarding ALPR. The client can be updated using the url below if it doesn't do it automatically. Configure IP and port as below.

-Brian

http://[redacted]9988/publish.htm



Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
Phone: 978-451-3710 (Maynard) 508-988-7302 (GHQ)
Email: Brian.Egnitz@massmail.state.ma.us
Monday - Friday, 8 to 4

CONFIDENTIALITY NOTICE: *The information contained in this email and any attachment is privileged and confidential law enforcement information. If you have received this email in error, please call 978-451-3700 immediately. Thank you.*

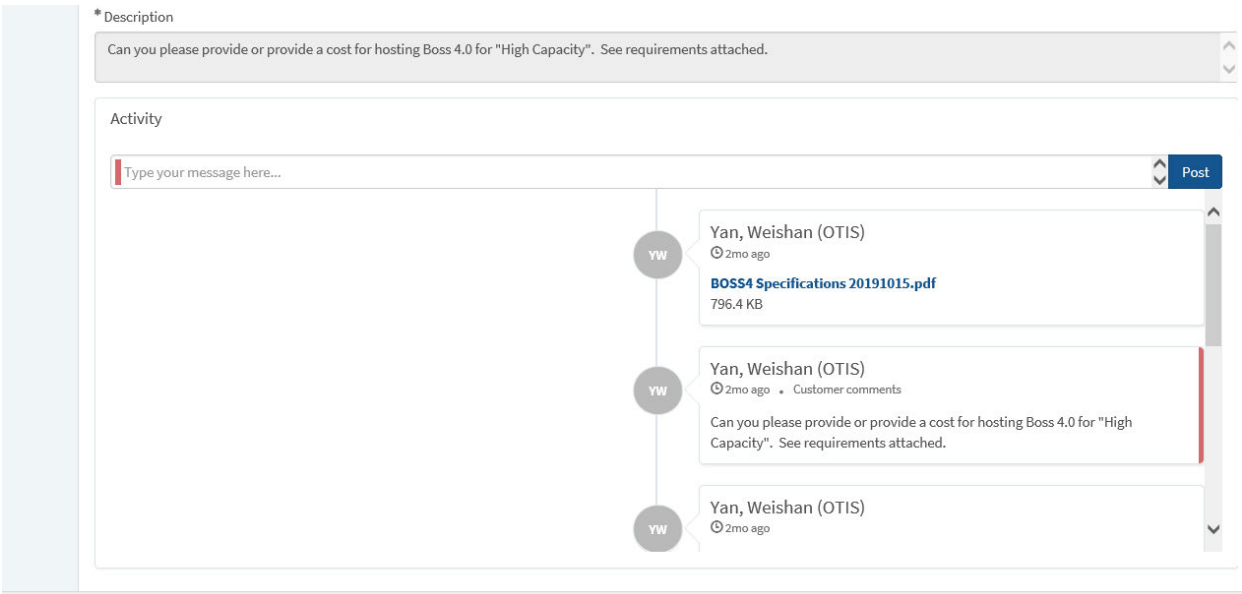
From: Slater, James (CHS)
To: Egnitz, Brian (POL)
Cc: Quinn, Dermot (POL)
Subject: RE: BOSS update
Date: Tuesday, March 3, 2020 8:16:18 PM
Attachments: image001.png
image002.png

Thanks, Brian…I'll get back to you folks tomorrow.

Jim

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Tuesday, March 3, 2020 16:14
To: Slater, James (CHS) <james.slater@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: FW: BOSS update

Specs attached. See ticket INC0318850



From: Peter Crary [mailto:pcrary@neology.net]
Sent: Tuesday, January 14, 2020 1:34 PM
To: Egnitz, Brian (POL); John Tedona
Subject: RE: BOSS update

No, attached are the current server specs.

-Peter Crary
Global R&D Director, ANPR/ALPR
(858) 391-0260 x1153 (d)
(865) 386-3821 (m)

The information contained in this communication is confidential and intended only for the use of the recipient named and may also be legally privileged. If you are not the intended recipient (named addressee), you are hereby notified that any dissemination, distribution, copying or making use of this communication, or any of its contents, is strictly prohibited. Please notify the sender immediately by email and delete the original message and any copy of it from your computer system. The integrity, security of and absence of viruses in this message cannot be guaranteed on the internet. The sender therefore does not accept liability for any errors or omissions in the contents of this message, nor any damage caused, which arise as a result of e-mail transmission.

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Tuesday, 14 January, 2020 05:07
To: Peter Crary <pcrary@neology.net>; John Tedona <jtedona@neology.net>
Subject: FW: BOSS update

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Are this still current for Boss 4.0?

From: Egnitz, Brian (POL)
Sent: Tuesday, March 12, 2019 4:14 PM
To: Stockwell, Matt (EPS); Mitchell, Timothy (EPS)
Subject: RE: BOSS update

From: Stockwell, Matt (EPS)
Sent: Tuesday, March 12, 2019 4:14 PM
To: Egnitz, Brian (POL); Mitchell, Timothy (EPS)
Subject: RE: BOSS update

Hi Brian –

If there was an attachment or additional details on the sizing they did not come through via e-mail.

Matt

From: Egnitz, Brian (POL)
Sent: Tuesday, March 12, 2019 3:04 PM

To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Stockwell, Matt (EPS) <matt.stockwell@mass.gov>
Subject: FW: BOSS update

FYI

From: John Tedona [mailto:jtedona@neology.net]
Sent: Tuesday, March 12, 2019 11:00 AM
To: Egnitz, Brian (POL)
Cc: Michael Roth
Subject: RE: BOSS update

Brian,

Here's the recommended sizing criteria for the application and database servers. With more fixed cameras pushing data to BOSS it's highly recommended you keep this sizing criteria in mind.

John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Tuesday, March 12, 2019 10:49 AM
To: Michael Roth <mroth@neology.net>
Cc: Peter Crary <pcrary@neology.net>; Israel Padilla <ipadilla@neology.mx>; Michell Itallekzi Garcia Garcia <colaborador6@neopartners.mx>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; John Tedona <jtedona@neology.net>; PIPS Technology Support <support@pipstechnology.com>; Quinn, Dermot (POL) <dermot.quinn@state.ma.us>; Clarke, Shannon (EPS) <shannon.clarke@state.ma.us>
Subject: RE: BOSS update

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Thanks Mike, Ive sent that to the tech. here is the license key. I saw the 5 concurrent number in the boss log folder

---

From: Michael Roth [mailto:mroth@neology.net]
Sent: Tuesday, March 12, 2019 10:33 AM
To: Egnitz, Brian (POL); Peter Crary; Israel Padilla; Michell Itallekzi Garcia Garcia; Mitchell, Timothy (EPS); John Tedona; PIPS Technology Support; Quinn, Dermot (POL); Clarke, Shannon (EPS)
Subject: RE: BOSS update

Can you send me screen shoot of the licenses.

That error occurs when using other browser than IE.

1. Prerequisites needed to successful install of BossUI client, the below settings pertain to OS where client is being installed.
    a. "Active Scripting" needs to be enabled in Windows "Internet Options"- "Security"- "Internet"- "Custom level". (This setting is for Bing maps to function).
    b. Can you add http:// address to "Local Intranet" in Intranet Zones Sites. (This can be taken out after installation as it is only needed for deployment).

2. Internet Explorer must be use.

Michael B. Roth
ALPR Technician
O: 858.391.0260 Ext. 1234
C: 513.767.7610
mroth@neology.net
A Business
www.pipstechnology.com

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Tuesday, March 12, 2019 7:06 AM
To: Peter Crary <pcrary@neology.net>; Michael Roth <mroth@neology.net>; Israel Padilla <ipadilla@neology.mx>; Michell Itallekzi Garcia Garcia <colaborador6@neopartners.mx>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; John Tedona <jtedona@neology.net>; PIPS Technology Support <support@pipstechnology.com>; Quinn, Dermot (POL) <dermot.quinn@state.ma.us>; Clarke, Shannon (EPS) <shannon.clarke@state.ma.us>
Subject: RE: BOSS update

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

I addition, I believe we may need a new license file. The logs say "5 concurrent" licenses available.

From: Egnitz, Brian (POL)
Sent: Tuesday, March 12, 2019 6:43 AM
To: Peter Crary; Michael Roth; Israel Padilla; Michell Itallekzi Garcia Garcia; Mitchell, Timothy (EPS); John Tedona; PIPS Technology Support; Quinn, Dermot (POL); Clarke, Shannon (EPS)
Subject: Fwd: BOSS update

Hi guys,

Is there an updated client? This on appears to be calling the Spanish version of dot net, it's also not using the updated version already installed. Do you have one that is properly signed too???

Begin forwarded message:

> **From:** "Ghasemi, Kiarash (POL)" <Kiarash.Ghasemi@pol.state.ma.us>
> **Date:** March 11, 2019 at 10:35:38 PM EDT
> **To:** "Egnitz, Brian (POL)" <brian.egnitz@pol.state.ma.us>, "Sullivan, Margaret (POL)" <Margaret.Sullivan@pol.state.ma.us>
> **Cc:** "Quinn, Dermot (POL)" <dermot.quinn@pol.state.ma.us>, "Kelly, Edward (POL)" <Edward.Kelly@pol.state.ma.us>, "Hernandez, Oscar (POL)" <Oscar.Hernandez@pol.state.ma.us>, "Weldon, Stephen (POL)" <Stephen.Weldon@pol.State.MA.US>, "Griffin, Daniel (POL)" <daniel.griffin@MassMail.State.MA.US>

Subject: RE: BOSS update

Hi Brian,

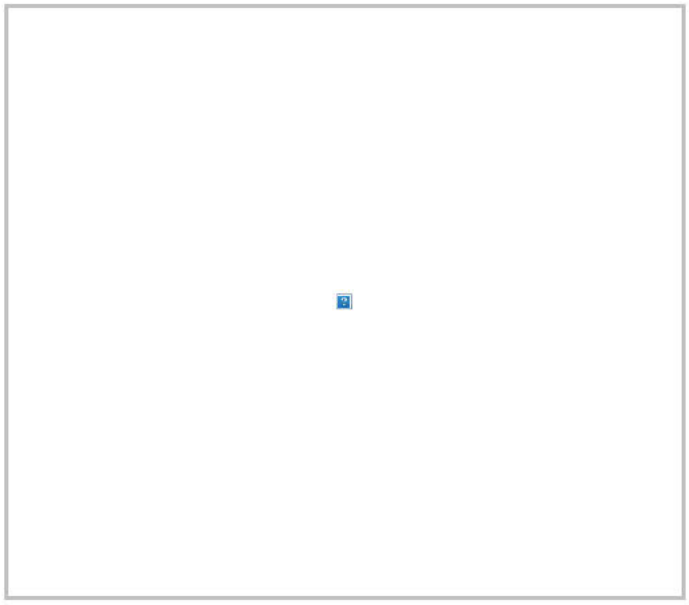
Before this update, On computers that needed access to LPR reporting, we have a copied a folder called "SA Client" and "SA.UI" within that folder, we create a shortcut to that file and that eliminated installation of any program.

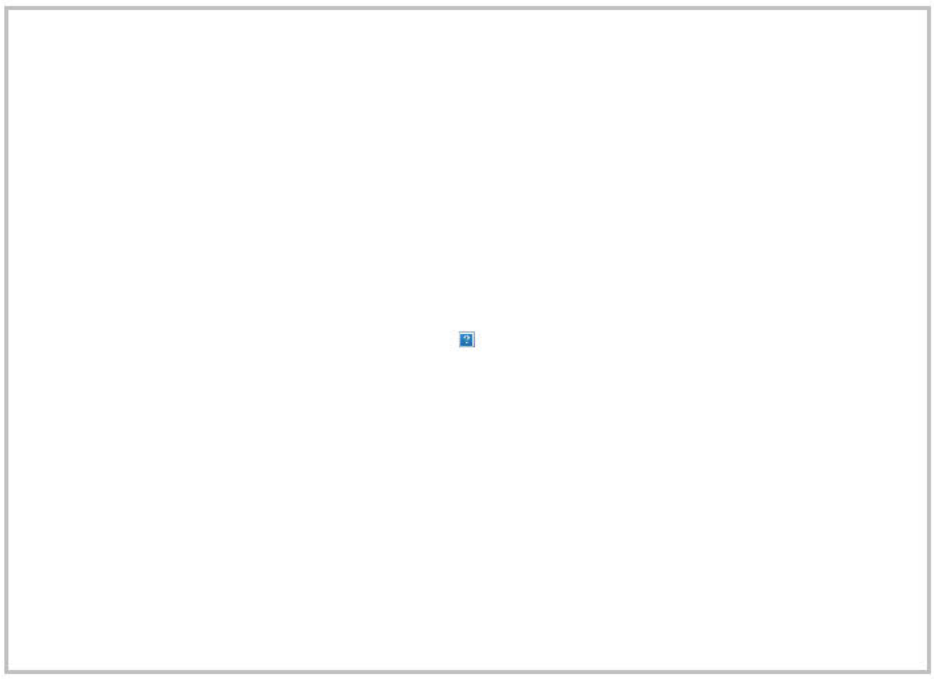
But I have tried the link that you have provided us and I'm getting an error message in Spanish during the installation! (Please see below) What I get from it, it need .Net. 4.5.2 but my computer already has 4.7 installed on it. I also tried to install it on Watchcenter computers and I got the same error message in Spanish and .Net 4.5.2 wont install on top of the current version of 4.7

Also translation of other part of the error message is that:

"The Microsoft .NET Framework 4.5.2 installation is not supported on this operating system. Please contact the administrator."

I have CC Lt. Griffin on this email, since he has done many installation of the old one too and all his stations are also effected too.





Error de comprobación de los requisitos previos del componente del sistema Microsoft .NET Framework 4.5.2 (x86 y x64) con el siguiente mensaje:
"La instalación de Microsoft .NET Framework 4.5.2 no se admite en este sistema operativo. Póngase en contacto con el administrador."

Vea el archivo de registro de la instalación que se encuentra en 'C:\Users\MJACKS~1\AppData\Local\Temp\VSD1947.tmp\install.log' para obtener más información.

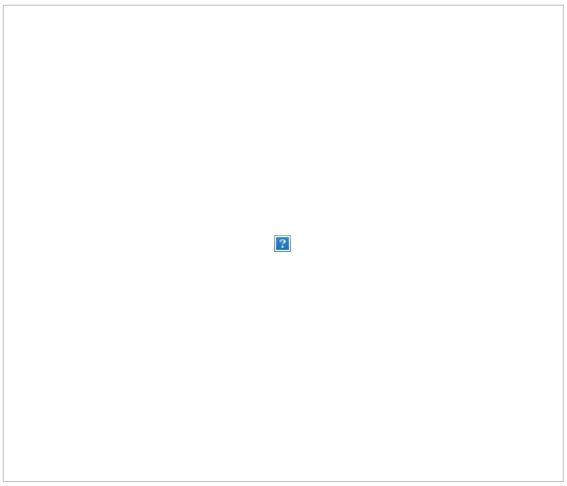
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Monday, March 11, 2019 9:58 PM
To: Sullivan, Margaret (POL) <Margaret.Sullivan@pol.state.ma.us>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Kelly, Edward (POL) <Edward.Kelly@pol.state.ma.us>; Hernandez, Oscar (POL) <Oscar.Hernandez@pol.state.ma.us>; Weldon, Stephen (POL) <Stephen.Weldon@pol.State.MA.US>; Ghasemi, Kiarash (POL) <Kiarash.Ghasemi@pol.state.ma.us>
Subject: BOSS update

Hi Peg,

The BOSS ALPR application has been updated in case you get some calls regarding ALPR. The client can be updated using the url below if it doesn't do it automatically. Configure IP and port as below.

-Brian

http://[redacted]9988/publish.htm



Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
Phone: 978-451-3710 (Maynard) 508-988-7302 (GHQ)
Email: Brian.Egnitz@massmail.state.ma.us
Monday - Friday, 8 to 4

CONFIDENTIALITY NOTICE: *The information contained in this email and any attachment is privileged and confidential law enforcement information. If you have received this email in error, please call 978-451-3700 immediately. Thank you.*

From: [A. Jones v. Jones (POL)]
To: [E-911 A. Jones (POL)]
Subject: FW: Case Law Update - ALPRs on Bourne/Sagamore Bridges not a search
Date: Tuesday, April 21, 2020 10:33:39 PM
Attachments: Outlook-Sunset.png

Thanks. Good read. Throw my hands up is we have to starting writing for LPR s and Pole Cams in the future.

Trooper Jason P. Abramoski #3528
Massachusetts State Police
DHS - C.I.N.R.E.T
326 W Grove St, Middleboro, MA 02346
508-468-0502

On Apr 21, 2020, at 2 11 PM, Rudolph, James (POL) <James.Rudolph@pol.state.ma.us> wrote

Case Law update.

Win for the good guys. Defense tried to mirror the Connolly case and suggest a S/W needed to check ALPRs. Court said no. But this could change if a case relied more heavily on ALPR info. Interesting read.

-rudy

RESPECTFULLY
LIEUTENANT JAMES R. RUDOLPH #2786
450 RAYNHAM ROAD, TAUNTON, MA 02780
508.824.2112
<OUTLOOK-PERSNUWB.PNG>

From: Grant Marguerite (NFK) <Marguerite.Grant@MassMail.State.MA.US>
Sent: Friday, April 17, 2020 5:24 PM



Chiefs,
Commonwealth v. McCarthy (SJC 12750)← click on that link to see the case
In this case the SJC ruled that police tracking D's car using 4 automatic license plate readers (ALPRs) at both ends of the Bourne and Sagamore Bridges was too limited to amount to a constitutional "search." The SJC declined to say exactly how detailed digital surveillance would have to be to constitute a search leaving that issue for future cases.

State Police maintain ALPRs including ones at both ends of the Bourne and Sagamore Bridges. (p.3) The ALPRs photograph vehicles' license plates; that data along with the date and time of the sighting is retained by GOPPS for a year. (p.3-4) Authorized users including police may put a license plate number on a "hot list" and receive an alert if that plate is sighted; reasons to put someone on the "hot list" include not only criminal investigations but also Amber alerts missing persons and BOLO alerts. (p. 3 25 n.13)

Through surveillance controlled buys and information from 4 CIs Barnstable police suspected that the co-D was se ling heroin out of his house in Barnstable. (p.4) Police saw a black Hyundai driven by D visit there briefly so they suspected that D was the co-D's supplier. Police put the Hyundai's license plate number on the State Police ALPR "hot list" so that they'd be notified whenever the Hyundai crossed one of the bridges. (p.5) After getting an alert that the Hyundai had crossed onto the Cape police followed both the Hyundai and the co-D to the buy location on a quiet residential street where D and co-D met for about 30 seconds but police could not see a physical exchange. (p.5) From the ALPR data police generated a spreadsheet showing that in mid-winter the Hyundai had crossed the bridges dozens of times sometimes more than once a day adding to police suspicion that D was the heroin supplier. (p.5-6) When police got a second alert that the Hyundai had crossed onto the Cape they again followed D and co-D to the buy location and saw a 30-second meeting but could not see any exchange. This time police stopped both cars handcuffed both co-D and D and read them Miranda. On co-D police found heroin; on D police found 2 cell phones and cash. (p.6-7) At the station police repeatedly told D he was "not under arrest." and D made statements.

D moved to suppress the ALPR data his statements and evidence obtained from the stop. A Superior Court judge found that the moment of arrest was when D and co-D were handcuffed at the scene of the traffic stop but denied the motion to suppress. (p.33) The SJC upheld the denial.

Limits and expectation of privacy in digital surveillance At some length the SJC discussed the constitutional issues raised by digital surveillance. (p.7-29) Police conduct amounts to a search if: (1) it intrudes on a D's expectation of privacy and (2) society is willing to recognize the expectation of privacy as reasonable. Here the SJC ruled D did have an expectation of privacy because D and co-D chose a buy location in a quiet residential area. (p.8 n.5) As to what expectation of privacy society recognizes as reasonable with regard to digital surveillance the SJC was guided by historical understandings of what was an unreasonable search and seizure when the U.S. and Mass. Constitutions were adopted in the late 1700s in reaction to redicals' rummaging without restraint through colonists' homes. (p.8-10) New technologies like ALPRs raise difficult legal issues because they are easier and less expensive for police than traditional surveillance can be done secretly and permit police to search back in time for a vehicle's movements even before po ice suspicion arose. (p.12-14) Society does not recognize as reasonable an expectation of privacy in what someone knowingly exposes" to public view like a license plate – which by statute must be "displayed conspicuously." (p.15-16 n.8) In older cases involving less advanced technology courts have held that a D did not have an expectation of privacy in contents of a phone conversation in a phone booth or a radio beeper" tracking a single journey. (p14-17) But technology like ALPRs GPS and CSLI are different because they may give police a **mosaic** of information where each piece may be public but when viewed together they create a picture that implicates someone's privacy interests like their political re ligious or sexual associations. (p.17-21) The SJC was concerned that with enough ALPRs police could track someone's location everywhere which would be "creepy." (p.21) Exigent circumstances would likely justify using an ALPR in a situation involving an Amber alert or missing person. (p.21 n.12) The D urged the SJC to consider not just these four ALPRs on the Bourne and Sagamore Bridges but the hundreds of ALPRs across Massachusetts; the SJC declined to do so because that evidence is not in the record of this case. (p.24) The **limited number of cameras** here and their placements on the bridges was not enough to give D an expectation of privacy that society would recognize as reasonable. (p.28) The SJC declined to say how much digital surveillance would give such an expectation and admitted that its unwillingness to do so "**may bring some interim confusion**" until further cases develop the law on this issue. (p.28 n.15) Chief Justice Gants wrote a separate concurrence suggesting that one thing the SJC could do is to require police who want to search a vast amount of digital data to apply for a court order supported by an affidavit showing reasonable suspicion to do so. (concurrence p.3) This would be like a 5W but with a lower standard than PC.

Written policy The SJC rejected D's argument that Barnstable PD should have had a written policy about ALPRs and the MSP policy on which Barnstable relied was not specific enough. (p.30) Written policies are required to justify certain exceptions to the SW requirement (like inventory searches and sobriety checkpoints) – they do not apply to the threshold question whether a search occurred in the first place. (p.31)

Miranda issues At the station police repeatedly told D that D was "not under arrest." But the motion judge found that the moment of arrest was when police handcuffed D at the traffic stop. (p.33) D argued that his statements should be suppressed because police tel ing him he was not under arrest amounted to "deceit or trickery" to get D to confess. The motion judge and the SJC rejected that argument saying that even if telling D he was not under arrest amounted to deceit or trickery it was just one factor to be used in determining voluntariness.

Bottom line: Police use of ALPRs at limited locations is not a constitutional search – but we don't know how many locations it'd have to be to amount to one. Using an ALPR in **exigent circumstances** like an Amber Alert is likely OK. Local police don't need a written policy to use ALPRs maintained by MSP. After a D has been handcuffed police should not tell D that D is "not under arrest" – po ice will likely be accused later of deceit and trickery.

A thought: There are news stories online that cell phones may be used to do contact tracing for people exposed to COVID-19. If lots of people willingly agree to let their cell phone data be used to track their whereabouts would that ever change courts' view of what society recognizes as a reasonable expectation of privacy? At some point if members of the public come to expect that they're being tracked should police be allowed to use that evidence too? Or at the very least should there be a jury instruction explaining that police have less access to the data than other entities (like software companies or public health agencies)?

As always email me with any questions. Wash your hands!

Marguerite

Marguerite T. Grant
General Counsel – Director of Training
Office of Norfolk District Attorney Michael W. Morrissey
45 Shawmut Road
Canton, MA 02021
781-830-4820

From: Telford, Erik (POL)
To: Rudolph, James (POL); Grace, Marguerite (POL); Abramoski, Jason (POL); Santos, John (POL); Lavoie, Marc (POL)
Subject: Comm v. McCarthy - ALPRs on Bourne/Sagamore Bridges not a "search"
Date: Tuesday, April 21, 2020 2:20:09 PM
Attachments: Ct rule Commv.pdf

Thank you!

Respectfully,

Lieutenant Erik V. Telford #2934
Massachusetts State Police
Division of Investigative Services
Gang Unit
Cell 7818312058
Email erik.telford@pol.state.ma.us

From: Rudolph James (POL) <James.Rudolph@pol.state.ma.us>
Sent: Tuesday, April 21, 2020 2:11:43 PM
To: Dunn Scott (POL) <Scott.Dunn@pol.state.ma.us>; Long Richard (POL) <richard.long@pol.state.ma.us>; Abramoski Jason (POL) <jason.abramoski@pol.state.ma.us>; Santos John (POL) <john.santos@pol.state.ma.us>; Telford Erik (POL) <erik.telford@pol.state.ma.us>; Lavoie Marc (POL) <marc.lavoie@pol.state.ma.us>
Subject: Comm v. McCarthy - ALPRs on Bourne/Sagamore Bridges not a "search"

Case Law update.

Win for the good guys. Defense tried to mirror the Connolly case and suggest a S/W needed to check ALPRs. Court said no. But this could change if a case relied more heavily on ALPR info. Interesting read.

-rudy

RESPECTFULLY
LIEUTENANT JAMES D. RUDOLPH #2786
MASSACHUSETTS STATE POLICE
600 WORCESTER ROAD, FRAMINGHAM, MA 01702
508-820-2122

From: Grant Marguerite (NFK) <Marguerite.Grant@MassMail.State.MA.US>
Sent: Friday, April 17, 2020 5:33 PM



Chiefs

Commonwealth v. McCarthy (SJC 12750) ← click on that link to see the case
In this case the SJC ruled that police tracking D's car using it automatic license plate readers (ALPRs) at both ends of the Bourne and Sagamore Bridges was too limited to amount to a constitutional "search." The SJC declined to say exactly how detailed digital surveillance would have to be to constitute a search leaving that issue for future cases.

State Po ice maintain ALPRs including ones at both ends of the Bourne and Sagamore Bridges. (p.3) The ALPRs photograph vehicles' license plates; that data along with the date and time of the sighting is retained by EOPPS for a year. (p.3-4) Authorized users including police may put a license plate number on a "hot list " and receive an alert if that plate is sighted; reasons to put someone on the "hot list" include not only criminal investigations but also Amber alerts missing persons and BOLO alerts. (p. 2 25, n.13)

Through surveillance controlled buys and information from 4 Cis Barnstable police suspected that the co-D was selling heroin out of his house in Barnstable. (p.4) Police saw a black Hyundai driven by D visit there briefly so they suspected that D was the co-D's supplier. Police put the Hyundai's license plate number on the State Police ALPR "hot list " so that they'd be notified whenever the Hyundai crossed one of the bridges. (p.5) After getting an alert that the Hyundai had crossed onto the Cape police followed both the Hyundai and the co-D to the buy location on a quiet residential street where D and co-D met for about 30 seconds but police could not see a physical exchange. (p.5) From the ALPR data police generated a spreadsheet showing that in mid-winter the Hyundai had crossed the bridges dozens of times sometimes more than once a day adding to police suspicion that D was the heroin supplier. (p.5-6) When police got a second alert that the Hyundai had crossed onto the Cape they again followed D and co-D to the buy location and saw a 30-second meeting but could not see any exchange. This time police stopped both cars handcuffed both co-D and D and read them Miranda. On co-D police found heroin; on D police found 2 cell phones and cash. (p.6-7) At the station police repeatedly told D he was "not under arrest " and D made statements.

D moved to suppress the ALPR data his statements and evidence obtained from the stop. A Superior Court judge found that the moment of arrest was when D and co-D were handcuffed at the scene of the traffic stop but denied the motion to suppress. (p.33) The SJC upheld the denial.

ALPRs and expectation of privacy in digital surveillance: At some length the SJC discussed the constitutional issues raised by digital surveillance. (p.7-29) Police conduct amounts to a search if: (1) it intrudes on a D's expectation of privacy and (2) society is willing to recognize the expectation of privacy as reasonable. Here the SJC ruled D did have an expectation of privacy because D and co-D chose a buy location in a quiet residential area. (p.8 n.5) As to what expectation of privacy society recognizes as reasonable with regard to digital surveillance the SJC was guided by historical understandings of what was an unreasonable search and seizure when the U.S. and Mass. Constitutions were adopted in the late 1700s in reaction to redcoats' rummaging without restraint through colonists' homes. (p.8-10) New technologies like ALPRs raise difficult legal issues because they are easier and less expensive for police than traditional surveillance can be done secretly and permit police to search back in time for a vehicle's movements even before police suspicion arose. (p.12-14) Society does not recognize as reasonable an expectation of privacy in what someone "knowingly exposes" to public view like a license plate – which by statute must be "displayed conspicuously." (p.15-16 & n.8) In older cases involving less advanced technology courts have held that a D did not have an expectation of privacy in contents of a phone conversation in a phone booth or a radio beeper" tracking a single journey. (p14-17) But technology like ALPRs GPS and CSLI are different because they may give police a **mosaic** of information where each piece may be public but when viewed together they create a picture that implicates someone's privacy interests like their political religious or sexual associations. (p.17-21) The SJC was concerned that with enough ALPRs police could track someone's location everywhere which would be "creepy." (p.21) Exigent circumstances would likely justify using an ALPR in a situation involving an Amber alert or missing person. (p.25 n.13) The D urged the SJC to consider not just these four ALPRs on the Bourne and Sagamore Bridges but the hundreds of ALPRs across Massachusetts; the SJC declined to do so because that evidence is not in the record of this case. (p.26) The **limited number of cameras** here and their placements on the bridges was not enough to give D an expectation of privacy that society would recognize as reasonable. (p.28) The SJC declined to say how much digital surveillance would give such an expectation and admitted that its unwillingness to do so **"may bring some interim confusion"** until further cases develop the law on this issue. (p.28 n.15) Chief Justice Gants wrote a separate concurrence suggesting that one thing the SJC could do is to require police who want to search a vast amount of digital data to apply for a court order supported by an affidavit showing reasonable suspicion to do so. (concurrence p.3) This would be like a SW but with a lower standard than PC.

Written policy: The SJC rejected D's argument that Barnstable PD should have had a written policy about ALPRs and the MSP policy on which Barnstable relied was not specific enough. (p.30) Written policies are required to justify certain exceptions to the SW requirement (like inventory searches and sobriety checkpoints) – they do not apply to the threshold question whether a search occurred in the first place. (p.31)

Miranda issues: At the station police repeatedly told D that D was "not under arrest." But the motion judge found that the moment of arrest was when police handcuffed D at the traffic stop. (p.33) D argued that his statements should be suppressed because police telling him he was not under arrest amounted to "deceit or trickery" to get D to confess. The motion judge and the SJC rejected that argument saying that even if telling D he was not under arrest amounted to deceit or trickery it was just one factor to be used in determining voluntariness.

Bottom line: Police use of ALPRs at limited locations is not a constitutional search – but we don't know how many locations it'd have to be to amount to one. Using an ALPR in **exigent circumstances** like an Amber Alert is likely OK. Local police don't need a written policy to use ALPRs maintained by MSP. After a D has been handcuffed police should not tell D that D is "not under arrest" – police will likely be accused later of deceit and trickery.

A thought: There are news stories online that cell phones may be used to do contact tracing for people exposed to COVID-19. If lots of people willingly agree to let their cell phone data be used to track their whereabouts would that ever change courts' view of what society recognizes as a reasonable expectation of privacy? At some point if members of the pub ic come to expect that they're being tracked should police be allowed to use that evidence too? Or at the very least should there be a jury instruction explaining that police have less access to the data than other entities (like software companies or public health agencies)?

As always email me with any questions. Wash your hands!

Marguerite

Marguerite T. Grace
General Counsel + Director of Training
Office of Norfolk District Attorney Michael W. Morrissey
45 Shawmut Road
Canton, MA 02021
781-830-4820

From: [E. Jed. D. Sawyer, ESQ.]
To: [E. Jed. D. Sawyer, ESQ.]
Subject: Fwd: Comm. v. McCarthy - ALPRs on Bourne/Sagamore Bridges not a search
Date: Wednesday, April 22, 2020 11:33:33 AM
Attachments: Outlook-iconbqfl.png

Ha! No doubt.

RESPECTFULLY,
LIEUTENANT JAMES D. RUDOLPH #2786
[redacted]
508-820-2373

From: Abramoski Jason (POL) <jason.abramoski@pol.state.ma.us>
Sent: Tuesday, April 21, 2020 9:33 PM
To: Rudolph James (POL) <James.Rudolph@pol.state.ma.us>
Subject: Re: Comm v. McCarthy - ALPRs on Bourne/Sagamore Bridges not a "search"

Thanks. Good read. Throw my hands up is we have to starting writing for LPR s and Pole Cams in the future.

Trooper Jason P. Abramoski #3528
Massachusetts State Police
DHS - C.I.N.R.E.T
326 W Grove St. Middleboro, MA 02346
508-468-0502

On Apr 21, 2020, at 2:11 PM, Rudolph, James (POL) <James.Rudolph@pol.state.ma.us> wrote:

Case Law update.

Win for the good guys. Defense tried to mirror the Connolly case and suggest a S/W needed to check ALPRs. Court said no. But this could change if a case relied more heavily on ALPR info. Interesting read.

-rudy

RESPECTFULLY
LIEUTENANT JAMES D. RUDOLPH #2786
[redacted]
508-820-2373
<OUTLOOK-FE3BWUWL.PNG>

From: Grant Marguerite (NFK) <Marguerite.Grant@MassMail.State.MA.US>
Sent: Friday, April 17, 2020 5:19 PM



Chiefs,
Commonwealth v. McCarthy (SJC-12750)← click on that link to see the case
In this case the SJC ruled that police tracking D's car using 4 automatic license plate readers (ALPRs) at both ends of the Bourne and Sagamore Bridges was too limited to amount to a constitutional "search." The SJC declined to say exactly how detailed digital surveillance would have to be to constitute a search leaving that issue for future cases.

State Police maintain ALPRs including ones at both ends of the Bourne and Sagamore Bridges. (p.3) The ALPRs photograph vehicles' license plates; that data along with the date and time of the sighting is retained by EOPPS for a year. (p.3-4) Authorized users including police may put a license plate number on a "hot list" and receive an alert if that plate is sighted; reasons to put someone on the "hot list" include not only criminal investigations but also Amber alerts missing persons and BOLO alerts. (p. 2 21 n.13)

Through surveillance controlled buys and information from 4 Cis Barnstable police suspected that the co-D was se ling heroin out of his house in Barnstable. (p.4) Police saw a black Hyundai driven by D visit there briefly so they suspected that D was the co-D's supplier. Police put the Hyundai's license plate number on the State Police ALPR "hot list " so that they'd be notified whenever the Hyundai crossed one of the bridges. (p.5) After getting an alert that the Hyundai had crossed onto the Cape police followed both the Hyundai and the co-D to the buy location on a quiet residential street where D and co-D met for about 30 seconds but police could not see a physical exchange. (p.5) From the ALPR data police generated a spreadsheet showing that in mid-winter the Hyundai had crossed the bridges dozens of times sometimes more than once a day adding to police suspicion that D was the heroin supplier. (p.5-6) When police got a second alert that the Hyundai had crossed onto the Cape they again followed D and co-D to the buy location and saw a 30-second meeting but could not see any exchange. This time police stopped both cars handcuffed both co-D and D and read them Miranda. On co-D police found heroin; on D police found 2 cell phones and cash. (p.6-7) At the station police repeatedly told D he was "not under arrest " and D made statements.

D moved to suppress the ALPR data his statements and evidence obtained from the stop. A Superior Court judge found that the moment of arrest was when D and co-D were handcuffed at the scene of the traffic stop but denied the motion to suppress. (p.23) The SJC upheld the denial.

ALPRs and expectation of privacy in digital surveillance: At some length the SJC discussed the constitutional issues raised by digital surveillance. (p.7-29) Police conduct amounts to a search if: (1) it intrudes on a D's expectation of privacy and (2) society is willing to recognize the expectation of privacy as reasonable. Here the SJC ruled D did have an expectation of privacy because D and co-D chose a buy location in a quiet residential area. (p.8 n.5) As to what expectation of privacy society recognizes as reasonable with regard to digital surveillance the SJC was guided by historical understandings of what was an unreasonable search and seizure when the U.S. and Mass. Constitutions were adopted in the late 1700s in reaction to redcoats' rummaging without restraint through colonists' homes. (p.8-10) New technologies like ALPRs raise difficult legal issues because they are easier and less expensive for police than traditional surveillance can be done secretly and permit police to search back in time for a vehicle's movements even before police suspicion arose. (p.12-14) Society does not recognize as reasonable an expectation of privacy in what someone knowingly exposes" to public view like a license plate – which by statute must be "displayed conspicuously." (p.15-16 & n.8) In older cases involving less advanced technology courts have held that a D did not have an expectation of privacy in contents of a phone conversation in a phone booth or a radio beeper" tracking a single journey. (p14-17) But technology like ALPRs GPS and CSLI are different because they may give police a **mosaic** of information where each piece may be public but when viewed together they create a picture that implicates someone's privacy interests like their political re ligious or sexual associations. (p.17-21) The SJC was concerned that with enough ALPRs police could track someone's location everywhere which would be "creepy." (p.25) Exigent circumstances would likely justify using an ALPR in a situation involving an Amber alert or missing person. (p.25 n.13) The D urged the SJC to consider not just these four ALPRs on the Bourne and Sagamore Bridges but the hundreds of ALPRs across Massachusetts; the SJC declined to do so because that evidence is not in the record of this case. (p.26) The **limited number of cameras** here and their placements on the bridges was not enough to give D an expectation of privacy that society would recognize as reasonable. (p.28) The SJC declined to say how much digital surveillance would give such an expectation and admitted that its unwillingness to do so "**may bring some interim confusion**" until further cases develop the law on this issue. (p.28 n.15) Chief Justice Gants wrote a separate concurrence suggesting that one thing the SJC could do is to require police who want to search a vast amount of digital data to apply for a court order supported by an affidavit showing reasonable suspicion to do so. (concurrence p.3) This would be like a SW but with a lower standard than PC.

Written policy: The SJC rejected D's argument that Barnstable PD should have had a written policy about ALPRs and the MSP policy on which Barnstable relied was not specific enough. (p.30) Written policies are required to justify certain exceptions to the SW requirement (like inventory searches and sobriety checkpoints) – they do not apply to the threshold question whether a search occurred in the first place. (p.31)

Miranda issues: At the station police repeatedly told D that D was "not under arrest." But the motion judge found that the moment of arrest was when police handcuffed D at the traffic stop. (p.32) D argued that his statements should be suppressed because police tel ling him he was not under arrest amounted to "deceit or trickery" to get D to confess. The motion judge and the SJC rejected that argument saying that even if telling D he was not under arrest amounted to deceit or trickery it was just one factor to be used in determining voluntariness.

Bottom line: Police use of ALPRs at limited locations is not a constitutional search – but we don't know how many locations it'd have to be to amount to one. Using an ALPR in **exigent circumstances** like an Amber Alert is likely OK. Local police don't need a written policy to use ALPRs maintained by MSP. After a D has been handcuffed police should not tell D that D is "not under arrest" – po ice will likely be accused later of deceit and trickery.

A thought: There are news stories online that cell phones may be used to do contact tracing for people exposed to COVID-19. If lots of people willingly agree to let their cell phone data be used to track their whereabouts would that ever change courts' view of what society recognizes as a reasonable expectation of privacy? At some point if members of the public come to expect that they're being tracked should police be allowed to use that evidence too? Or at the very least should there be a jury instruction explaining that police have less access to the data than other entities (like software companies or public health agencies)?

As always email me with any questions. Wash your hands!

Marguerite

Marguerite T. Grant
General Counsel – Director of Training
Office of Norfolk District Attorney Michael W. Morrissey
45 Shawmut Road
Canton, MA 02021
781-830-4820

To:	Bennett, Marcy (POL)
Subject:	RE: INC0316723 : LPR Install on Windows 10 PC"s Recently Upgraded from Windows 7
Date:	Tuesday, March 17, 2020 4:08:06 PM
Attachments:	CFC On Call Guide.pdf

From: Bennett, Marcy (POL) <Marcy.Bennett@pol.state.ma.us>
Sent: Tuesday, March 17, 2020 4:06 PM
To: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Subject: RE: INC0316723 : LPR Install on Windows 10 PC's Recently Upgraded from Windows 7

Hi. Any idea what the passwords are for the gmx accounts?

From: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Sent: Tuesday, March 17, 2020 3:56 PM
To: Bennett, Marcy (POL) <Marcy.Bennett@pol.state.ma.us>
Subject: RE: INC0316723 : LPR Install on Windows 10 PC's Recently Upgraded from Windows 7

From: Bennett, Marcy (POL) <Marcy.Bennett@pol.state.ma.us>
Sent: Tuesday, March 17, 2020 3:53 PM
To: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Subject: RE: INC0316723 : LPR Install on Windows 10 PC's Recently Upgraded from Windows 7

Hi. Can you send me the fake facebook account? Thank you!

From: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Sent: Tuesday, March 17, 2020 3:06 PM
To: Bennett, Marcy (POL) <Marcy.Bennett@pol.state.ma.us>
Cc: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Subject: RE: INC0316723 : LPR Install on Windows 10 PC's Recently Upgraded from Windows 7

Bender can walk you through it, or reach out to Kia, he's here

---

From: Bennett, Marcy (POL) <Marcy.Bennett@pol.state.ma.us>
Sent: Tuesday, March 17, 2020 2:58 PM
To: Wilkerson, Diane A. (EOTSS) <diane.a.wilkerson@mass.gov>
Cc: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Subject: RE: INC0316723 : LPR Install on Windows 10 PC's Recently Upgraded from Windows 7

Hi. I need to map the m drive to my laptop. Is there instructions in the watch or something you can email me? Thanks.

From: Wilkerson, Diane A. (EOTSS) <diane.a.wilkerson@mass.gov>
Sent: Tuesday, March 17, 2020 10:55 AM
To: Bennett, Marcy (POL) <Marcy.Bennett@pol.state.ma.us>
Subject: Fwd: INC0316723 : LPR Install on Windows 10 PC's Recently Upgraded from Windows 7

FYI

Diane Wilkerson
Deskside Support Southeast

326 West Grove Street, Middleboro, MA 02346
Office: (508) 923-4036
diane.a.wilkerson@mass.gov| www.mass.gov/eotss
Executive Office of Technology Services and Security (EOTSS)
EOTSS provides secure and quality digital information, services, and tools to constituents and service providers when and where they need them.

Begin forwarded message:

> **From:** "Ghasemi, Kiarash (EOTSS)" <Kiarash.Ghasemi2@mass.gov>
> **Date:** January 15, 2020 at 8:54:14 AM EST
> **To:** "Henderson, Phillip (POL)" <Phillip.Henderson@pol.state.ma.us>
> **Cc:** "Wilkerson, Diane A. (EOTSS)" <diane.a.wilkerson@mass.gov>,
> "Henderson, Phillip W. (EOTSS)" <Phillip.W.Henderson@mass.gov>
> **Subject: RE: INC0316723 : LPR Install on Windows 10 PC's Recently Upgraded from Windows 7**
>
> Please run the following link from IE11
>
> http://[redacted]9988/publish.htm

Kiarash Ghasemi | **System Analyst III**
Executive Office of Technology Services and Security (EOTSS)
MA State Police Headquarters
470 Worcester Road
Framingham, MA 01701
Office: (508) 988-7486 |
Kiarash.Ghasem2@Mass.Gov | **www.mass.gov/eotss**

Please update your address book with my new email address..

Executive Office of Technology Services and Security (EOTSS)

EOTSS provides secure and quality digital information, services, and tools
to constituents and service providers when and where they need them.

From: Ghasemi, Kiarash (EOTSS)
Sent: Wednesday, January 15, 2020 6:40 AM
To: Henderson, Phillip (POL) <Phillip.Henderson@pol.state.ma.us>
Cc: Wilkerson, Diane A. (EOTSS) <diane.a.wilkerson@mass.gov>; Henderson, Phillip W. (EOTSS) <Phillip.W.Henderson@mass.gov>
Subject: RE: INC0316723 : LPR Install on Windows 10 PC's Recently Upgraded from Windows 7

Sorry for the delay, I will send u the new link today.

Kiarash Ghasemi | System Analyst III
MA State Police Headquarters
470 Worcester Road
Framingham, MA 01701
Office: (508) 988-7486 |
Kiarash.Ghasem2@Mass.Gov | www.mass.gov/eotss

Executive Office of Technology Services and Security (EOTSS)
EOTSS provides secure and quality digital information, services, and tools
to constituents and service providers when and where they need them.

-------- Original message --------
From: "Henderson, Phillip (POL)" <Phillip.Henderson@pol.state.ma.us>
Date: 1/14/20 9:13 AM (GMT-05:00)
To: "Ghasemi, Kiarash (EOTSS)" <Kiarash.Ghasemi2@mass.gov>
Cc: "Wilkerson, Diane A. (EOTSS)" <diane.a.wilkerson@mass.gov>, "Henderson, Phillip W. (EOTSS)" <Phillip.W.Henderson@mass.gov>
Subject: INC0316723 : LPR Install on Windows 10 PC's Recently Upgraded from Windows 7

Kia,

I have multiple PC's (@5) at Cape and Islands CPAC that were recently upgraded from Windows 7 to Windows 10 by C&I IT. The previously installed and operational LPR software no longer works.

Issue covered under INC0316723.

Please advise if there are corrective steps that need to be taken.

Thanks,
Phillip

To:	Bennett, Marcy (POL)
Subject:	RE: INC0316723 : LPR Install on Windows 10 PC"s Recently Upgraded from Windows 7
Date:	Tuesday, March 17, 2020 4:08:06 PM
Attachments:	CFC On Call Guide.pdf

From: Bennett, Marcy (POL) <Marcy.Bennett@pol.state.ma.us>
Sent: Tuesday, March 17, 2020 4:06 PM
To: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Subject: RE: INC0316723 : LPR Install on Windows 10 PC's Recently Upgraded from Windows 7

Hi. Any idea what the passwords are for the gmx accounts?

From: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Sent: Tuesday, March 17, 2020 3:56 PM
To: Bennett, Marcy (POL) <Marcy.Bennett@pol.state.ma.us>
Subject: RE: INC0316723 : LPR Install on Windows 10 PC's Recently Upgraded from Windows 7

From: Bennett, Marcy (POL) <Marcy.Bennett@pol.state.ma.us>
Sent: Tuesday, March 17, 2020 3:53 PM
To: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Subject: RE: INC0316723 : LPR Install on Windows 10 PC's Recently Upgraded from Windows 7

Hi. Can you send me the fake facebook account? Thank you!

From: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Sent: Tuesday, March 17, 2020 3:06 PM
To: Bennett, Marcy (POL) <Marcy.Bennett@pol.state.ma.us>
Cc: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Subject: RE: INC0316723 : LPR Install on Windows 10 PC's Recently Upgraded from Windows 7

Bender can walk you through it, or reach out to Kia, he's here

---

From: Bennett, Marcy (POL) <Marcy.Bennett@pol.state.ma.us>
Sent: Tuesday, March 17, 2020 2:58 PM
To: Wilkerson, Diane A. (EOTSS) <diane.a.wilkerson@mass.gov>
Cc: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Subject: RE: INC0316723 : LPR Install on Windows 10 PC's Recently Upgraded from Windows 7

Hi. I need to map the m drive to my laptop. Is there instructions in the watch or something you can email me? Thanks.

From: Wilkerson, Diane A. (EOTSS) <diane.a.wilkerson@mass.gov>
Sent: Tuesday, March 17, 2020 10:55 AM
To: Bennett, Marcy (POL) <Marcy.Bennett@pol.state.ma.us>
Subject: Fwd: INC0316723 : LPR Install on Windows 10 PC's Recently Upgraded from Windows 7

FYI

Diane Wilkerson
Deskside Support Southeast

326 West Grove Street, Middleboro, MA 02346
Office: (508) 923-4036
diane.a.wilkerson@mass.gov| www.mass.gov/eotss
Executive Office of Technology Services and Security (EOTSS)
EOTSS provides secure and quality digital information, services, and tools to constituents and service providers when and where they need them.

Begin forwarded message:

> **From:** "Ghasemi, Kiarash (EOTSS)" <Kiarash.Ghasemi2@mass.gov>
> **Date:** January 15, 2020 at 8:54:14 AM EST
> **To:** "Henderson, Phillip (POL)" <Phillip.Henderson@pol.state.ma.us>
> **Cc:** "Wilkerson, Diane A. (EOTSS)" <diane.a.wilkerson@mass.gov>,
> "Henderson, Phillip W. (EOTSS)" <Phillip.W.Henderson@mass.gov>
> **Subject: RE: INC0316723 : LPR Install on Windows 10 PC's Recently Upgraded from Windows 7**
>
> Please run the following link from IE11
>
> http://[redacted]9988/publish.htm

Kiarash Ghasemi | **System Analyst III**
Executive Office of Technology Services and Security (EOTSS)
MA State Police Headquarters
470 Worcester Road
Framingham, MA 01701
Office: (508) 988-7486 |
Kiarash.Ghasem2@Mass.Gov | **www.mass.gov/eotss**

Please update your address book with my new email address..

Executive Office of Technology Services and Security (EOTSS)

EOTSS provides secure and quality digital information, services, and tools
to constituents and service providers when and where they need them.

From: Ghasemi, Kiarash (EOTSS)
Sent: Wednesday, January 15, 2020 6:40 AM
To: Henderson, Phillip (POL) <Phillip.Henderson@pol.state.ma.us>
Cc: Wilkerson, Diane A. (EOTSS) <diane.a.wilkerson@mass.gov>; Henderson, Phillip W. (EOTSS) <Phillip.W.Henderson@mass.gov>
Subject: RE: INC0316723 : LPR Install on Windows 10 PC's Recently Upgraded from Windows 7

Sorry for the delay, I will send u the new link today.

Kiarash Ghasemi | System Analyst III
MA State Police Headquarters
470 Worcester Road
Framingham, MA 01701
Office: (508) 988-7486 |
Kiarash.Ghasem2@Mass.Gov | www.mass.gov/eotss

Executive Office of Technology Services and Security (EOTSS)
EOTSS provides secure and quality digital information, services, and tools
to constituents and service providers when and where they need them.

-------- Original message --------
From: "Henderson, Phillip (POL)" <Phillip.Henderson@pol.state.ma.us>
Date: 1/14/20 9:13 AM (GMT-05:00)
To: "Ghasemi, Kiarash (EOTSS)" <Kiarash.Ghasemi2@mass.gov>
Cc: "Wilkerson, Diane A. (EOTSS)" <diane.a.wilkerson@mass.gov>,
"Henderson, Phillip W. (EOTSS)" <Phillip.W.Henderson@mass.gov>
Subject: INC0316723 : LPR Install on Windows 10 PC's Recently Upgraded from Windows 7

Kia,

I have multiple PC's (@5) at Cape and Islands CPAC that were recently upgraded from Windows 7 to Windows 10 by C&I IT. The previously installed and operational LPR software no longer works.

Issue covered under INC0316723.

Please advise if there are corrective steps that need to be taken.

Thanks,
Phillip

From: Brooks, Brian (POL)
To: Bennett, Marcy (POL)
Subject: RE: INC0316723 : LPR Install on Windows 10 PC"s Recently Upgraded from Windows 7
Date: Tuesday, March 17, 2020 4:09:00 PM
Attachments: CFC On Call Guide.pdf

This is all I got

From: Bennett, Marcy (POL) <Marcy.Bennett@pol.state.ma.us>
Sent: Tuesday, March 17, 2020 4:06 PM
To: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Subject: RE: INC0316723 : LPR Install on Windows 10 PC's Recently Upgraded from Windows 7

Hi. Any idea what the passwords are for the gmx accounts?

From: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Sent: Tuesday, March 17, 2020 3:56 PM
To: Bennett, Marcy (POL) <Marcy.Bennett@pol.state.ma.us>
Subject: RE: INC0316723 : LPR Install on Windows 10 PC's Recently Upgraded from Windows 7

From: Bennett, Marcy (POL) <Marcy.Bennett@pol.state.ma.us>
Sent: Tuesday, March 17, 2020 3:53 PM
To: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Subject: RE: INC0316723 : LPR Install on Windows 10 PC's Recently Upgraded from Windows 7

Hi. Can you send me the fake facebook account? Thank you!

From: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Sent: Tuesday, March 17, 2020 3:06 PM
To: Bennett, Marcy (POL) <Marcy.Bennett@pol.state.ma.us>
Cc: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Subject: RE: INC0316723 : LPR Install on Windows 10 PC's Recently Upgraded from Windows 7

Bender can walk you through it, or reach out to Kia, he’s here

---

From: Bennett, Marcy (POL) <Marcy.Bennett@pol.state.ma.us>
Sent: Tuesday, March 17, 2020 2:58 PM
To: Wilkerson, Diane A. (EOTSS) <diane.a.wilkerson@mass.gov>
Cc: Brooks, Brian (POL) <brian.brooks@pol.state.ma.us>
Subject: RE: INC0316723 : LPR Install on Windows 10 PC's Recently Upgraded from Windows 7

Hi. I need to map the m drive to my laptop. Is there instructions in the watch or something you can email me? Thanks.

From: Wilkerson, Diane A. (EOTSS) <diane.a.wilkerson@mass.gov>
Sent: Tuesday, March 17, 2020 10:55 AM
To: Bennett, Marcy (POL) <Marcy.Bennett@pol.state.ma.us>
Subject: Fwd: INC0316723 : LPR Install on Windows 10 PC's Recently Upgraded from Windows 7

FYI

Diane Wilkerson
Deskside Support Southeast

326 West Grove Street, Middleboro, MA 02346
Office: (508) 923-4036
diane.a.wilkerson@mass.gov| www.mass.gov/eotss
Executive Office of Technology Services and Security (EOTSS)
EOTSS provides secure and quality digital information, services, and tools to constituents and service providers when and where they need them.

Begin forwarded message:

> **From:** "Ghasemi, Kiarash (EOTSS)" <Kiarash.Ghasemi2@mass.gov>
> **Date:** January 15, 2020 at 8:54:14 AM EST
> **To:** "Henderson, Phillip (POL)" <Phillip.Henderson@pol.state.ma.us>
> **Cc:** "Wilkerson, Diane A. (EOTSS)" <diane.a.wilkerson@mass.gov>,
> "Henderson, Phillip W. (EOTSS)" <Phillip.W.Henderson@mass.gov>
> **Subject: RE: INC0316723 : LPR Install on Windows 10 PC's Recently Upgraded from Windows 7**
>
> Please run the following link from IE11
>
> http://[redacted]9988/publish.htm

Kiarash Ghasemi | **System Analyst III**
Executive Office of Technology Services and Security (EOTSS)
MA State Police Headquarters
470 Worcester Road
Framingham, MA 01701
Office: (508) 988-7486 |
Kiarash.Ghasem2@Mass.Gov | **www.mass.gov/eotss**

Please update your address book with my new email address..

Executive Office of Technology Services and Security (EOTSS)
EOTSS provides secure and quality digital information, services, and tools
to constituents and service providers when and where they need them.

From: Ghasemi, Kiarash (EOTSS)
Sent: Wednesday, January 15, 2020 6:40 AM
To: Henderson, Phillip (POL) <Phillip.Henderson@pol.state.ma.us>
Cc: Wilkerson, Diane A. (EOTSS) <diane.a.wilkerson@mass.gov>; Henderson, Phillip W. (EOTSS) <Phillip.W.Henderson@mass.gov>
Subject: RE: INC0316723 : LPR Install on Windows 10 PC's Recently Upgraded from Windows 7

Sorry for the delay, I will send u the new link today.

Kiarash Ghasemi | System Analyst III
MA State Police Headquarters
470 Worcester Road
Framingham, MA 01701
Office: (508) 988-7486 |
Kiarash.Ghasem2@Mass.Gov | www.mass.gov/eotss

Executive Office of Technology Services and Security (EOTSS)
EOTSS provides secure and quality digital information, services, and tools
to constituents and service providers when and where they need them.

-------- Original message --------
From: "Henderson, Phillip (POL)" <Phillip.Henderson@pol.state.ma.us>
Date: 1/14/20 9:13 AM (GMT-05:00)
To: "Ghasemi, Kiarash (EOTSS)" <Kiarash.Ghasemi2@mass.gov>
Cc: "Wilkerson, Diane A. (EOTSS)" <diane.a.wilkerson@mass.gov>,
"Henderson, Phillip W. (EOTSS)" <Phillip.W.Henderson@mass.gov>
Subject: INC0316723 : LPR Install on Windows 10 PC's Recently Upgraded from Windows 7

Kia,

I have multiple PC's (@5) at Cape and Islands CPAC that were recently upgraded from Windows 7 to Windows 10 by C&I IT. The previously installed and operational LPR software no longer works.

Issue covered under INC0316723.

From: Mills, Melissa (POL)
To: Rivera Morgan, Awilda (POL)
Subject: RE: IT Returns
Date: Friday, May 29, 2020 12:57:00 PM
Attachments: Copy of IT Property Returns FY2020.xlsx

This is great. I tweaked two minor things (closed a parenthesis and replaced "I" with "Awilda")
Question- how will step 10 take place (verify SP255)

Melissa M. Mills
Compliance Quality Assurance Manager
508.820.2687 – office
melissa.mills@pol.state.ma.us

This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may include privileged or otherwise confidential information. Any unauthorized review, use, forwarding, printing, copying, disclosure or distribution is strictly prohibited. If you received this message in error, or have reason to believe you are not authorized to receive it, please notify me and promptly delete this message and attachments. This email, including any attachments, could possibly contain viruses. The receiver assumes all responsibility for checking and deleting any potential viruses.

From: Rivera Morgan, Awilda (POL) <Awilda.RiveraMorgan@pol.state.ma.us>
Sent: Friday, May 29, 2020 12:31 PM
To: Mills, Melissa (POL) <Melissa.Mills@pol.state.ma.us>
Subject: IT Returns

See the process tab and let me know if something does not make sense.

Respectfully,

Awilda Rivera Morgan
Director of Compliance
Division of Administrative Services
Massachusetts State Police
470 Worcester Road
Framingham, Massachusetts 01702

508-820-2346 – work direct
508-782-0665 – work cell
508-820-2359 –fax number
awilda.riveramorgan@pol.state.ma.us

This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may include privileged or otherwise confidential information. Any unauthorized review, use, forwarding, printing, copying, disclosure or distribution is strictly prohibited. If you received this message in error, or have reason to believe you are not authorized to receive it, please notify me and promptly delete this message and attachments. This email, including any attachments, could possibly contain viruses. The receiver assumes all responsibility for checking and deleting any potential viruses.

To: Rivera Morgan, Awilda (POL)
Subject: RE: IT Returns
Date: Friday, May 29, 2020 12:57:10 PM
Attachments: Copy of IT Property Returns FY2020.xlsx

This is great. I tweaked two minor things (closed a parenthesis and replaced "I" with "Awilda")
Question- how will step 10 take place (verify SP255)

Melissa M. Mills
Compliance Quality Assurance Manager
508.820.2687 – office
melissa.mills@pol.state.ma.us

This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may include privileged or otherwise confidential information. Any unauthorized review, use, forwarding, printing, copying, disclosure or distribution is strictly prohibited. If you received this message in error, or have reason to believe you are not authorized to receive it, please notify me and promptly delete this message and attachments. This email, including any attachments, could possibly contain viruses. The receiver assumes all responsibility for checking and deleting any potential viruses.

From: Rivera Morgan, Awilda (POL) <Awilda.RiveraMorgan@pol.state.ma.us>
Sent: Friday, May 29, 2020 12:31 PM
To: Mills, Melissa (POL) <Melissa.Mills@pol.state.ma.us>
Subject: IT Returns

See the process tab and let me know if something does not make sense.

Respectfully,

Awilda Rivera Morgan
Director of Compliance
Division of Administrative Services
Massachusetts State Police
470 Worcester Road
Framingham, Massachusetts 01702

508-820-2346 – work direct
508-782-0665 – work cell
508-820-2359 –fax number
awilda.riveramorgan@pol.state.ma.us

This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may include privileged or otherwise confidential information. Any unauthorized review, use, forwarding, printing, copying, disclosure or distribution is strictly prohibited. If you received this message in error, or have reason to believe you are not authorized to receive it, please notify me and promptly delete this message and attachments. This email, including any attachments, could possibly contain viruses. The receiver assumes all responsibility for checking and deleting any potential viruses.

From: Miller, Dianne (POL)
To: Firlit, Deborah (OGR)
Subject: RE: Latest word versions
Date: Monday, June 1, 2020 12:17:00 PM
Attachments: ISAEPSFY20SCHKPOL20C $1200000 thru 9.15.2019.doc
FFY20SCHK Amendment Indirect Rate.docx
ISAEPSFY20STEPPOL20B $200K 11-14-19.doc
Amended Attachment B Indirect.docx
ISAEPSFY20YDRSPOL20A $30000 thru 9.15.2020.doc
FFY20YDRS CARRY FORWARD-AMENDMENT INDIRECT RATE ATTACHMENT B.docx
image001.png

Good afternoon Deb,
Attached are the most current ISA's and attachment B's.

Thanks

Dianne Miller
Accountant IV
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
(508) 820-2143

The preceding email message (including any attachments) contains information that may be confidential, may be protected by the attorney-client or other applicable privileges, or may constitute non-public information. It is intended to be conveyed only to the designated recipient(s) named above. If you are not an intended recipient of this message, please notify the sender by replying to this message and then delete all copies of it from your computer system. Any use, dissemination, distribution, or reproduction of this message by unintended recipients is not authorized and may be unlawful.

From: Firlit, Deborah (OGR)
Sent: Monday, June 01, 2020 9:00 AM
To: Miller, Dianne (POL)
Subject: Latest word versions

Dianne,
Can you send me the latest word versions of the ISAs that had the budget amendments made to them?
Sob Chkpt
STEP
Young Drivers

Thanks.
deb

Deborah Firlit
Program Coordinator
Office of Grants & Research, Highway Safety Division
Ten Park Plaza, Suite 3720-A, Boston, MA 02116
T: 617-725-3356 F: 617-725-0260
Deborah.Firlit@mass.gov

From: Mason, Christopher (POL)
To: Quinn, Dermot (POL)
Cc: Warmington, Scott (POL)
Subject: Re: LPR
Date: Monday, February 10, 2020 10:07:34 AM
Attachments: image001.png
image002.png
image003.png
image004.png
image005.png
image006.png

Sir,

This looks good. Thank you.

Colonel Christopher Mason
Superintendent
Massachusetts State Police

On Feb 10, 2020, at 9:34 AM, Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us> wrote:

Sirs,

Are you ok with this email? I would like to send to EOPSS and EOTSS and Massport teams.

Respectfully,

DJQ

Good Morning,

I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.

Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.

Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as "BOSS" and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport's cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.

MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.

I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.

To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.

I can't overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security's technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.

Respectfully,

Lieutenant Colonel Dermot J. Quinn #1765

Division Commander
Division of Homeland Security & Preparedness
Massachusetts State Police

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, January 17, 2020 1:10 PM
To: Slater, James (CHS) <james.slater@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>; Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; John Tedona <jtedona@neology.net>; Chute, Alexander <AChute@massport.com>; Peter Crary <pcrary@neology.net>; Michalski, Maria (EPS) <maria.michalski@mass.gov>
Subject: RE: MassPort LPR Cameras

Hi Jim,

BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.

-Brian

From: Egnitz, Brian (POL)
Sent: Monday, January 6, 2020 1:33 PM
To: Slater, James (CHS)
Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter Crary
Subject: RE: MassPort LPR Cameras

Hi Jim,

We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?

Thanks Brian

From: John Tedona [mailto:jtedona@neology.net]
Sent: Monday, December 9, 2019 4:55 PM
To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); Slater, James (CHS)
Subject: RE: MassPort LPR Cameras

Alex,

I can be available most anytime tomorrow for a call.

Regards,

John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: Chute, Alexander <AChute@massport.com>
Sent: Monday, December 9, 2019 4:38 PM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; John Tedona <jtedona@neology.net>; Peter Crary <pcrary@neology.net>
Cc: Guerriero, Robert (MASSIT) <robert.guerriero@state.ma.us>; Peek, Brian T. (EOTSS) <brian.t.peek@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Slater III, James F (CHS) <james.slater@state.ma.us>
Subject: RE: MassPort LPR Cameras

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Hello All,

I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.

Respectfully,

~Alex

<image002.png>

Alexander B. Chute
Program Manager, Public Safety Systems
Massachusetts Port Authority
Cell: [redacted]
Office: 617.568.5942
achute@massport.com

WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Monday, November 18, 2019 3:26 PM
To: John Tedona (jtedona@neology.net); pcrary@neology.net
Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
Subject: RE: MassPort LPR Cameras

Hi John, Peter

Any issues with moving Massports cameras to the Chelsea DB?

Using the Boss calculator, I estimate that we would need 9-10 TB of storage.

The current app server
<image003.png>

Current DB server

<image004.png>

<image005.png>

Our current reads by month for about 66 active cameras

Year	Month	Day	Month Name	Reads Count
2019	11	1	November	495,113
2019	11	2	November	472,907
2019	11	3	November	384,409
2019	11	4	November	411,440
2019	11	5	November	434,085
2019	11	6	November	495,537
2019	11	7	November	444,123
2019	11	8	November	542,492
2019	11	9	November	443,463
2019	11	10	November	389,514
2019	11	11	November	362,548
2019	11	12	November	236,539

From: Chute, Alexander [mailto:AChute@massport.com]
Sent: Wednesday, November 13, 2019 2:49 PM
To: Egnitz, Brian (POL)
Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
Subject: RE: MassPort LPR Cameras

These stats are from the 18 active cameras we have in the system for this month:

<image006.png>

~Alex

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Tuesday, November 12, 2019 5:28 PM
To: Chute, Alexander
Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
Subject: RE: MassPort LPR Cameras

Hi Alex,

Can you please provide the updated reads per day? Previously you were interested in sharing 6 cameras at approximately 75,000 reads per day.

Here is the P492 confi I mentioned.

Set host to boss [redacted]
Set image [redacted]
Set number of [redacted]
Set Ping interval [redacted]
Set udp ping [redacted]
Set ping wait time [redacted]
Set security [redacted]

I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.

-Brian

From: Chute, Alexander [mailto:AChute@massport.com]
Sent: Tuesday, November 12, 2019 2:08 PM
To: Egnitz, Brian (POL)
Subject: MassPort LPR Cameras

Brian,

Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the Troop F building. I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the roadway cameras are fed to 2 primary network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have 18 cameras in production, with another 19 scheduled to come online within the next two months. I anticipate this number growing to approximately 50 fixed cameras within our campus over the next year. Let me know what you think the appropriate next steps would be.

Respectfully,

~Alex

<image002.png>

Alexander B. Chute
Program Manager, Public Safety Systems
Massachusetts Port Authority
Cell: [redacted]
Office: 617.568.5942
achute@massport.com

WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

Lieutenant Colonel Dermot J. Quinn #1765
Division Commander
Division of Investigative Services
Massachusetts State Police
<image001.png>

From: Brian Kruger
To: Egnitz, Brian (POL)
Cc: Rhonda Fromm
Subject: RE: LRP network ideas?
Date: Tuesday, January 7, 2020 10:10:04 AM
Attachments: image001.png

Brian,
We have dropped three builds in the last 2 weeks out there. They are still having connection code issues with the debug code in place. I am expecting to have another build either today or tomorrow. The last one was deployed yesterday.

Regards,

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Tuesday, January 7, 2020 7:11 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Rhonda Fromm <rfromm@forensiclogic.com>
Subject: Re: LRP network ideas?

How are we making out on RMV?

> On Dec 6, 2019, at 11:31 AM, Brian Kruger <bkruger@forensiclogic.com> wrote:
>
> Billy,
> Please let the group know when this will be available. I will work with John to get it deployed and tested as soon as we have it released.
>
> Regards,
>
> <image001.png>
> **Brian Kruger**
> Operations and Support Manager
> **Forensic Logic / COPLINK**
> Office: 520.367.2775

Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Tuesday, November 26, 2019 1:17 PM
To: 'Ouellette, John (EPS)' <john.ouellette@state.ma.us>; 'Egnitz, Brian (POL)' <brian.egnitz@state.ma.us>; Samson Dunatunga <mdunatunga@forensiclogic.com>; Billy Moore <bmoore@forensiclogic.com>
Cc: 'Dunne, Michaela (CHS)' <michaela.dunne@state.ma.us>; 'Dunn-CHS, William (CHS)' <william.dunn-chs@state.ma.us>; 'Mitchell, Timothy (EPS)' <timothy.mitchell@state.ma.us>; 'Ramsay, Christopher (EPS)' <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

John,
Thank you for the information on the call this afternoon.

Samson/Billy,
We need to add some additional debug code into our service so we can see the full communication path and what is being sent and received. John is also in the process to check and make sure their three servers can reach back into our 184.171 on port 6060. I have also reattached the IP wireshark I did this morning.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Tuesday, November 26, 2019 8:29 AM
To: Ouellette, John (EPS) <john.ouellette@state.ma.us>; Egnitz, Brian (POL)

<brian.egnitz@state.ma.us>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

John,
Give me a few minutes and I will give you a call. Here is the CSV file from wireshark. I had to repull it. I don't see any actually log details in our tomcat instance. In the wireshark though I see a bunch of event code errors like below:

Event: <Unknown eventcode 72>, <Unknown eventcode 111>, <Unknown eventcode 116>, <Unknown eventcode 121>, <Unknown eventcode 110>, <Unknown eventcode 45>, <Unknown eventcode 112>, <Unknown eventcode 110>, <Unknown eventcode 114>, <Unknown eventcode 115>, <Unknown eventcode 47>, <Unknown eventcode 110>, <Unknown eventcode 111>, <Unknown eventcode 118>, <Unknown eventcode 110>, <Unknown eventcode 111>, <Unknown eventcode 47>, ColormapNotify, <Unknown eventcode 97>, <Unknown eventcode 120>, <Unknown eventcode 58>, <Unknown eventcode 46>, <Unknown eventcode 104>, <Unknown eventcode 46>, <Unknown eventcode 117>, <Unknown eventcode 97>, <Unknown eventcode 47>, <Unknown eventcode 62>, <Unknown eventcode 114>, <Unknown eventcode 114>, <Unknown eventcode 82>, <Unknown eventcode 120>, <Unknown eventcode 101>, MappingNotify, <Unknown eventcode 109>, <Unknown eventcode 98>, <Unknown eventcode 47>, <Unknown eventcode 119>, <Unknown eventcode 62>, <Unknown eventcode 114>, ColormapNotify, <Unknown eventcode 62>, <Unknown eventcode 115>, MappingNotify, <Unknown eventcode 110>

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Tuesday, November 26, 2019 7:29 AM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Brian Kruger <bkruger@forensiclogic.com>

Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Hey Brian,

You can call me at 617-660-4775

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Monday, November 25, 2019 7:53 PM
To: Brian Kruger <bkruger@forensiclogic.com>; Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: Re: LRP network ideas?

Does it make sense to schedule a call and work through it in real time?

> On Nov 22, 2019, at 4:00 PM, Ouellette, John (EPS) <john.ouellette@mass.gov> wrote:
>
> Hi Brian,
>
> I do not see any requests for your ORI. Can you review the acknowledgements that the broker sends back as a return value? There may be error information in there.
>
> John Ouellette | Massachusetts Executive Office of Public Safety and Security
> Office of Technology and Information Services
> Enterprise Application and Database Services
> Application Support and Management
> 200 Arlington Street Suite 2200
> Chelsea, MA 02150
> john.ouellette@state.ma.us | http://www.mass.gov/eops
>
> ---
>
> **From:** Brian Kruger <bkruger@forensiclogic.com>

Sent: Friday, November 22, 2019 3:47 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

John,
Can you check again and see if there is a request coming into the .154 server. I ran a packet capture and I do see data sent from the .171 to the .154 server.

<image001.png>

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 22, 2019 12:26 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

I'm not sure if 224.154 is a load balancer. I don't believe it is though. It doesn't matter though, that is where you will send requests. You will receive a synchronous response called an acknowledgement. That will let you know if your request was accepted or rejected.

Later, an asynchronous response will be sent from 170.154.224.155 or 170.154.224.156 to your web service.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 22, 2019 2:19 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
The 154 address is a load balancer for the services correct. As far as I know there should be no blocked traffic to the .171 but let me include Chris and Tim on this thread.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 22, 2019 9:36 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL)

<brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

I didn't find any submitted requests.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Ouellette, John (EPS)
Sent: Friday, November 22, 2019 11:34 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

I can check.

The broker will send responses from 170.154.224.155 or 170.154.224.156 on port 6060. Make sure you are allowing that traffic.

When you send in a request you will receive an xml document as the return value. The documents lists if the request was accepted and if it wasn't, why it wasn't. You should be checking those.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 22, 2019 11:28 AM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Ouellette, John (EPS) <john.ouellette@mass.gov>

Subject: RE: LRP network ideas?

Bill,
I have the service send back a no data found so it looks like we are connecting. Can you check your logs to see if our request actually made it into your system.

I am sending the following test cycle from the 170.154.224.82 web server to our FR server

http://[redacted]6060/CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=S32935254

Just so everybody is clear, this the is the connection path

170.154.224.82 → [redacted] port 6060 → [redacted] port 6060

Return path

[redacted] → [redacted] port 6060 → 170.154.224.82

Log of request:

2019-11-22 11:16:13,982 main DEBUG LoggerContext[name=MassLPRServlet, org.apache.logging.log4j.core.LoggerContext@59303963] started OK with configuration org.apache.logging.log4j.core.config.properties.PropertiesConfiguration@61e86192.
2019-11-22 11:16:13,982 main DEBUG Log4jServletContextListener ensuring that Log4j starts up properly.
2019-11-22 11:16:13,982 main DEBUG Log4jServletFilter initialized.
driversLicense=S32935254
remote host=170.154.224.82
remote port=60194
remote addr=170.154.224.82
scheme =http
scheme =HTTP/1.1
local addr =[redacted]
local name =EPS-CLFACEMATCH
context path = /CHSBReceiver
Init parameter1 =Value1
Current UUID : f3837e1f-0e40-4af6-8587-203e99240d92
javax.xml.bind.JAXBElement@227d5180
Request UUID: [redacted]f3837e1f-0e40-4af6-8587-203e99240d92

Rest response file contains:
no data found.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Thursday, November 21, 2019 2:11 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Ouellette, John (EPS) <john.ouellette@state.ma.us>
Subject: RE: LRP network ideas?

Thanks Bill!

It looks like we are close on this.

-Brian

From: Dunn-CHS, William (CHS)
Sent: Tuesday, November 19, 2019 7:50 AM
To: Brian Kruger; Ouellette, John (EPS)
Cc: Dunne, Michaela (CHS); Egnitz, Brian (POL); Dunn-CHS, William (CHS)
Subject: RE: LRP network ideas?

I think I see what might be part of the problem.

The R1 is either OLN or SSN, you can not send both at the same time.

There is No TEST SSN inquiry, use someone from MSP who is working on your project or if you have a developer who is from MA
The TEST OLN is S32935254

From: Brian Kruger [mailto:bkruger@forensiclogic.com]
Sent: Monday, November 18, 2019 6:33 PM

To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
Dev confirmed they are sending XML in the request. Do you have a valid License number in the test data I can try.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 15, 2019 11:16 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

The broker is a web service. You need to create a client to connect. Requests are made by sending in an xml document.

Did I forget to send you the broker documentation? Let me know.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 1:10 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
I ran two queries through IE I don't see an acknowledge me in the logs. Below is what I am seeing. Do we have a valid Lic number that is in the system I can try, or valid SSN.

My test URLs are:"
http://[G.L. c. 4.sec. 7.cl.26 (n)(security)]6060/CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=987654321

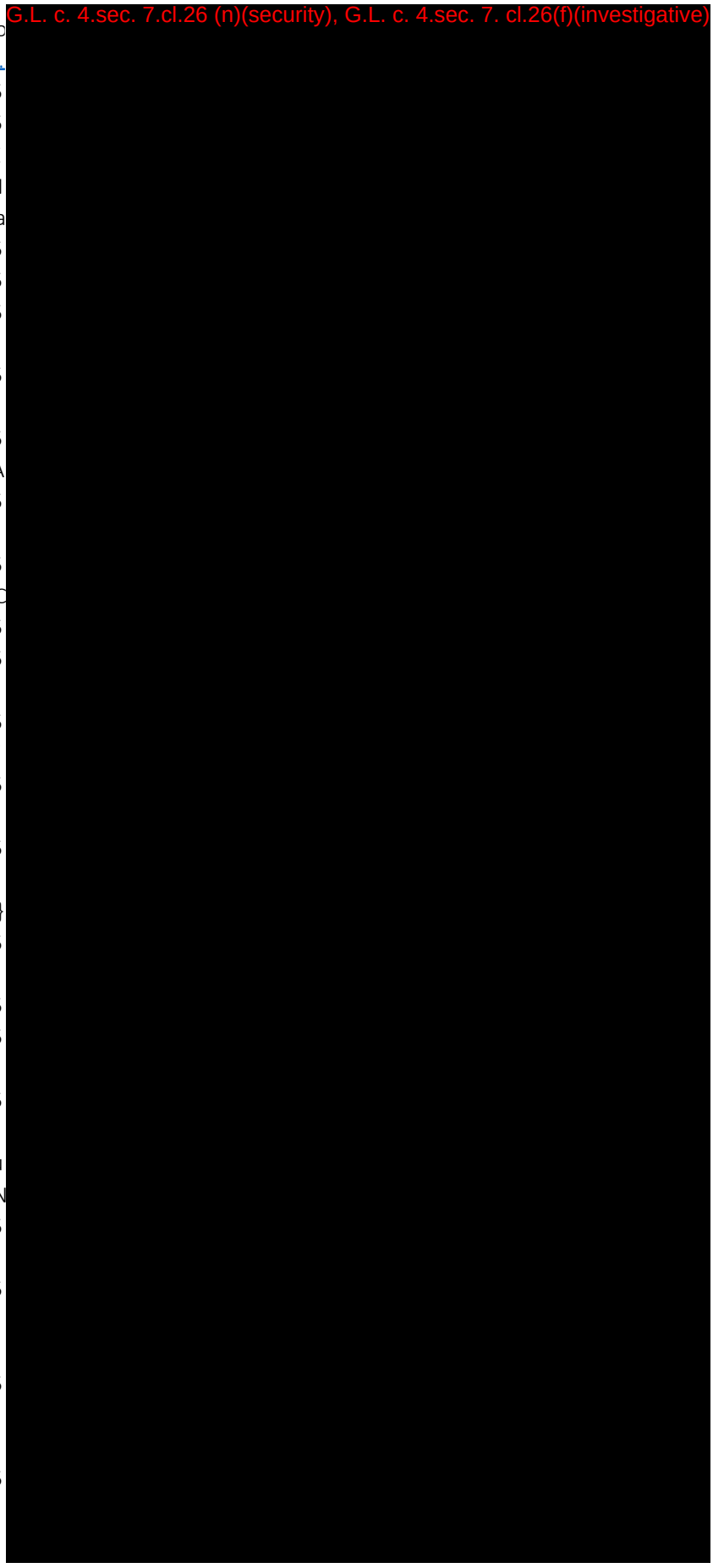
http://[G.L. c. 4.sec. 7.cl.26 (n)(security)]6060/CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=987654321

In my access log I see a 200:

[G.L. c. 4.sec. 7.cl.26 (n)(security)] - - [15/Nov/2019:13:02:50 -0500] "GET /CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=987654321 HTTP/1.1" 200 -
[G.L. c. 4.sec. 7.cl.26 (n)(security)] - - [15/Nov/2019:13:03:05 -0500] "GET /CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=987654321 HTTP/1.1" 200 –

In my log stdout log I see this:

[G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)]



configuratio
org.apache.
2019-11-15
2019-11-15
language: E
[nashorn, N
class: jdk.na
2019-11-15
2019-11-15
2019-11-15
class=org.a
2019-11-15
plugins
2019-11-15
value="C:\A
2019-11-15
class=org.a
2019-11-15
{filename=C
2019-11-15
2019-11-15
class=org.a
2019-11-15
level="null"
2019-11-15
class=org.a
2019-11-15
level="DEB
{RollingFile}
2019-11-15
class=org.a
2019-11-15
2019-11-15
class=org.a
2019-11-15
%C{1.} [%t]
Replace=nu
noConsoleN
2019-11-15
plugins
2019-11-15
Plugin[nam
class=org.a
2019-11-15
TimeBased
maxRando
2019-11-15
Plugin[nam
class=org.a

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)



[redacted]

org.apache.lo[redacted]949edcb30
initialized
2019-11-15 1[redacted]
org.apache.lo[redacted]949edcb30
2019-11-15 1[redacted]
org.apache.lo[redacted]949edcb30
OK.
2019-11-15 1[redacted]ager
SYSTEM_OUT[redacted]
2019-11-15 1[redacted]r
SYSTEM_OUT[redacted]
2019-11-15 1[redacted]ed with
status true
2019-11-15 1[redacted]
org.apache.lo[redacted]
2019-11-15 1[redacted]
org.apache.lo[redacted]
2019-11-15 1[redacted]
org.apache.lo[redacted]ctor
2019-11-15 1[redacted]
org.apache.lo[redacted]e=mass.servlet.images
2019-11-15 1[redacted]
org.apache.lo[redacted]ame=DefaultConsole-
2
2019-11-15 1[redacted]
org.apache.lo[redacted]ame=RollingFile
2019-11-15 1[redacted]
org.apache.lo[redacted]
timestamps.
2019-11-15 1[redacted]vlet,
org.apache.lo[redacted]
configuration
org.apache.lo[redacted]949edcb30.
2019-11-15 1[redacted]ing that
Log4j starts u[redacted]
2019-11-15 1[redacted]
driversLicense=987654321
remote host=[redacted]
remote port=62034
remote addr=[redacted]
scheme =http
scheme =HTTP/1.1
local addr =[redacted]
local name =EPS-CLFACEMATCH
context path = /CHSBReceiver
Init parameter1 =Value1

remote host not allowed. ignoring request.
driversLicense=987654321
remote host=[redacted]
remote port=62034
remote addr=[redacted]
scheme =http
scheme =HTTP/1.1
local addr =[redacted]
local name =EPS-CLFACEMATCH
context path = /CHSBReceiver
Init parameter1 =Value1
remote host not allowed. ignoring request.

My stderr log

[redacted]

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

15-Nov-
org.apac
Dcatalin
15-Nov-
org.apac
Dcatalin
15-Nov-
org.apac
Dignore.
15-Nov-
org.apac
Djava.io.
15-Nov-
org.apac
Djava.uti
15-Nov-
org.apac
Djava.uti
9.0.14\c
15-Nov-
org.apac
exit
15-Nov-
org.apac
abort
15-Nov-
org.apac
Xms128
15-Nov-
org.apac
Xmx102
15-Nov-
org.apac
Apache
15-Nov-
org.apac
[true], s
15-Nov-
org.apac
configur
15-Nov-
org.apac
initialize
15-Nov-
Initializin
15-Nov-
Initializin
15-Nov-
Server in

15-Nov-2
org.apach
15-Nov-2
org.apach
[Apache T
15-Nov-2
org.apach
archive [D
15-Nov-2
com.sun.x
JAX-WS se
15-Nov-2
org.apach
TLDs yet c
list of JAR
unneeded
time.
15-Nov-2
com.sun.x
WSSERVL
15-Nov-2
org.apach
applicatio
9.0.14\we
15-Nov-2
org.apach
archive [D
15-Nov-2
org.apach
TLDs yet c
list of JAR
unneeded
time.
15-Nov-2
org.apach
applicatio
9.0.14\we
15-Nov-2
org.apach
applicatio
15-Nov-2
org.apach
TLDs yet c
list of JAR
unneeded
time.
15-Nov-2
org.apach

[redacted]

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

time.
15-N
org.a
appli
finish
15-N
Starti
15-N
Starti
15-N
Serve

Rega

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 15, 2019 9:54 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hey Brian,

When you send in a request, the return to that call is an acknowledgement. That is an xml document that will state if your request was accepted or not; and if it is not, what the reason is.

Are you seeing any acknowledgements?

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services

Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 11:49 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
According to dev the message that is coming back: remote host not allowed. ignoring request. They are stating is a response from your system telling us we are not allowed. Is there anyway you and I can get on the phone, I can try and send some responses and see if you see anything in your log files. I am wondering if they are forming the response to you correctly.

As for the WSDL this is what I see from the 184.171 server.

<image003.png>

Full W G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)
<?xml
- <wsd
xmlns:
xmlns:
xmlns:
xmlns:
target
- <wsd
- <xsd:
xmlns:
attribu
target
<xsd:e
<xsd:e
<xsd:e
<xsd:e
</xsd:
</wsdl
- <wsd
<wsdl:
</wsdl
- <wsd

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

[redacted]

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603

bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 15, 2019 9:36 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

If you are able to telnet, then you should be able to send in a request.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 11:06 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
This is all from the 184.171 server.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com

www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 15, 2019 8:41 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Are you doing the ping and telnet from G.L. c. 4.sec. 7.cl.26 (n)(security)

Your error message from earlier seems to be your network not allowing the access.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 10:37 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
I am reaching out to the G.L. c. 4.sec. 7.cl.26 (n)(security) on port 6060. I can ping the IP and also hit the port.
<image004.png>

<image005.png>

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager

Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 15, 2019 8:26 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

What is the ip address you are trying to connect to?
Are you able to ping that machine?

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 10:22 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

Brian,
Thank you for checking in, sorry for the delay. I had the email together but it was in my draft. I tested the connection again today.

John,

I am still getting the remote Host not allowed. This is the error below:

2019-11-15 10:15:45,808 main DEBUG Log4jServletFilter initialized.
driversLicense=987654321
remote host=[redacted]
remote port=61799
remote addr=[redacted]
scheme =http
scheme =HTTP/1.1
local addr =[redacted]
local name =EPS-CLFACEMATCH
context path = /CHSBReceiver
Init parameter1 =Value1
remote host not allowed. ignoring request.

Regards,



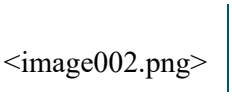
Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Friday, November 8, 2019 1:17 PM
To: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

John,
Thank you, I will work on testing the connection and let you know the results. According to Dev the other queries we will be running on the R1 and RI.

Regards,



Brian Kruger
Operations and Support Manager

Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 8, 2019 12:18 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

I have added your configuration on the test broker for R1 and RI.
Are there more queries/transactions you'd like to test? Michaela may have requirements for other queries.

The ORI is MAMSPF022
Your requests come from [redacted] and responses will be sent back to http://[redacted]6060/CHSBReceiver/CHSBService

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Ouellette, John (EPS)
Sent: Tuesday, November 5, 2019 12:54 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>
Subject: RE: LRP network ideas?

Hi Brian,

I think Bill needs to have more information on your project to assign an ORI to use

on the test broker.
Is there a project name on your side?

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Monday, November 4, 2019 3:30 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
Any luck on this.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Tuesday, October 22, 2019 12:32 PM
To: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Subject: RE: LRP network ideas?

John,
Yea we should be sending the XML packet with the service that we have created. Do you know if that IP is natted to [redacted] The server that we have our service on is the [redacted] Face match server. I don't have any servers in the 170.154.226.x IP range unless it is getting natted somehow.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Tuesday, October 22, 2019 12:21 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hay Brian,

That won't work. The broker accepts an xml document containing the request, as well as other information.
Attached is a sample R1 request.

By the way, I have your requests coming from 170.154.226.47

In order to get responses, you need a web service on your end to receive the responses and I'll need to configure it on the broker side.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Monday, October 21, 2019 5:04 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
Can you provide me with a DL that should work. From the .82 server this is what we are running:

http://[redacted]6060/CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=987654321

I just need to update the drivers license number and hopefully it will work

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Tuesday, September 24, 2019 8:07 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

So, just R1 and RI?

I'll start configuring the test broker.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Tuesday, September 24, 2019 10:59 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
For the queries that we will using this is what I got back from Dev… let me know if this helps

…Attachments\CJISBroker_2016-03-24[13247].zip\CJISBroker_2016-03-24\CJISBroker\transactions\queries\rmv\r1\xml

…Attachments\CJISBroker_2016-03-24[13247].zip\CJISBroker_2016-03-24\CJISBroker\transactions\queries\rmv\ri\xml

The rest is correct, for testing the ORI list will grow once we go to production.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Tuesday, September 24, 2019 6:39 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hi Brian,

I haven't added your configuration to the test broker yet. Can you confirm the following:
For broker connections, we need the following:
IP Address for request: [redacted]
URL for responses: http://[redacted]6060/CHSBReceiver/CHSBService
ORI: MAMSP0000
Queries: I need the list of queries/transactions you will be testing

You will submit to http://[redacted]6060/CJISService This call will return a synchronous acknowledgment.

Responses will come back from 170.154.224.155 or 170.154.224.156 on port 6060. You need to return a synchronous acknowledgement for each response.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200

Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Monday, September 23, 2019 7:53 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
I have deployed a new package, but I see this in the log.

2019-09-23 19:48:37,297 main DEBUG Registering MBean org.apache.logging.log4j2:type=MassLPRServlet,component=Appenders,name=RollingFile
2019-09-23 19:48:37,304 main DEBUG org.apache.logging.log4j.core.util.SystemClock does not support precise timestamps.
2019-09-23 19:48:37,305 main DEBUG LoggerContext[name=MassLPRServlet, org.apache.logging.log4j.core.LoggerContext@2180e789] started OK with configuration org.apache.logging.log4j.core.config.properties.PropertiesConfiguration@5e9bbd9d.
2019-09-23 19:48:37,307 main DEBUG Log4jServletContextListener ensuring that Log4j starts up properly.
2019-09-23 19:48:37,309 main DEBUG Log4jServletFilter initialized.
driversLicense=987654321
remote host=0:0:0:0:0:0:0:1
remote port=65146
remote addr=0:0:0:0:0:0:0:1
scheme =http
scheme =HTTP/1.1
local addr =0:0:0:0:0:0:0:1
local name =EPS-CLFACEMATCH
context path = /CHSBReceiver
Init parameter1 =Value1
remote host not allowed. ignoring request.

can you check and make sure this machine has access:

EPS-CLFACEMATCH
Connection-specific DNS Suffix . :
IPv4 Address. . . . . : [redacted]
Subnet Mask . . . . . : 255.255.255.128
Default Gateway . . . . . : 170.154.184.129

C:\Users\msp_user>
Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, September 6, 2019 6:15 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hey Brian,

I'm not sure what is in the test system either. I believe a dl of 987654321 will work; at least it used to.
Try to find something in test CJISWeb.

Remember that all queries will send in an xml document and will receive a return acknowledgement stating success or failure. If the request failed, the reason will be in the acknowledgement.

At a later time, seconds or less, the response will be returned to your web service. You must return an acknowledgement to that also to let the system know that the response was received and the next response can be sent.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Thursday, September 5, 2019 5:17 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
Not yet, I don't know what is in the test system… are they actually dls or fake ones.

Our query against our service is going to look something like, that will translate to yours.

http://[redacted]6060/CHSBReceiver/CHSBService?ori=REM000001&username=TEST&ssn=123123123&driversLicense=AZ67676767

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Thursday, September 5, 2019 1:09 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Have you tried your DL and SSN?

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Thursday, September 5, 2019 2:36 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
Do you have a sample DL and ssn, we can try passing through the service to see if we can pull an image. According to dev we are just utilizing the XML out of R1 and

Ri.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, August 9, 2019 7:04 AM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Brian Kruger <bkruger@forensiclogic.com>; Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

All of the broker queries use the same method and accept an xml document. The contents of the xml direct what action the system should take. I have attached documentation for the broker. It's a 5 MB zip file.

If you can't accept zip files or 5 MB files let me know how to send the file.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, August 9, 2019 9:39 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Brian Kruger

<bkruger@forensiclogic.com>; Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>
Subject: Re: LRP network ideas?

Thanks John, I'll defer to Brian Kruger to respond regarding where he's sending the query. Are you able to answer his question below?

"

> I can pull back the WSDL but want to send an image request to it to see if it actually pulls the image. I am looking for something like /GetPhoto?dl_num=20180061903&ss_num=2&type=M, the actually call method

"

On Aug 9, 2019, at 9:04 AM, Ouellette, John (EPS) <john.ouellette@mass.gov> wrote:

> Hi Brian,
>
> For broker connections to test, we need the following:
> IP Address for request: [redacted]
> URL for responses:
> http://[redacted]6060/CHSBReceiver/CHSBService
> ORI: MAMSP0000
> Queries:
>
> Can you confirm this information and send the list of queries you would like to run?
> Please remember that this system would only be used for test. Another system would need to be used when you move to production.
>
> John Ouellette | Massachusetts Executive Office of Public Safety and Security
> Office of Technology and Information Services
> Enterprise Application and Database Services
> Application Support and Management
> 200 Arlington Street Suite 2200
> Chelsea, MA 02150
> john.ouellette@state.ma.us | http://www.mass.gov/eops
>
> ---

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, August 9, 2019 8:54 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Ouellette, John (EPS) <john.ouellette@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>
Subject: Re: LRP network ideas?

Hi Brian,

are we testing on this yet?

On Jul 22, 2019, at 1:37 PM, Brian Kruger <bkruger@forensiclogic.com> wrote:

> Tim,
> Attached is the full list of agencies and ORI that we currently have in the admin DB.
>
> Regards,
>
> <image001.png>
>
> **Brian Kruger**
> Operations and Support Manager
> **Forensic Logic / COPLINK**
> 520.488.1603
> bkruger@forensiclogic.com
> www.forensiclogic.com
>
> ***CONFIDENTIALITY:*** *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*
>
> ---
>
> **From:** Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
> **Sent:** Monday, July 22, 2019 8:37 AM
> **To:** Brian Kruger <bkruger@forensiclogic.com>
> **Cc:** Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Ouellette, John (EPS) <john.ouellette@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
> **Subject:** RE: LRP network ideas?
>
> Any update on this from dev, do you still need a

sample RI url? Can you make sure you are also sending the CopLink user name in the UserID parameter.

Tks, Brian

From: Brian Kruger [mailto:bkruger@forensiclogic.com]
Sent: Thursday, July 18, 2019 5:19 PM
To: Mitchell, Timothy (EPS)
Cc: Ramsay, Christopher (EPS); Egnitz, Brian (POL); Ouellette, John (EPS)
Subject: RE: LRP network ideas?

Tim,
I am still pending an answer back from dev on how they are going to pull the ORI. For now can we use `MAMSP0000`. `That is actually in our systems as MSP.`

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
Sent: Tuesday, July 16, 2019 4:07 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Ouellette, John (EPS) <john.ouellette@state.ma.us>
Subject: RE: LRP network ideas?

Brian
What is the ORI that you are using for this setup? There is some configuration work that needs to be done on the broker side to allow your service to run transactions.

Thanks
Tim

Timothy Mitchell
Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise and Field Services Support Division
Public Safety Data Center
200 Arlington St., Suite 2200
Chelsea, MA 02150
(P) 617.660.4665
(F) 617.884.4601
(E) timothy.mitchell@state.ma.us
http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Monday, July 15, 2019 7:05 PM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

Folks,
For the RMV pull, does anybody have an example image we can try and run through. All the connectivity looks good, I have tried a few ways to pull an image without success.

Our service http://[redacted]6060/CHSBReceiver/CHSBService?wsdl refers to http://[redacted]6060/CJISService?wsdl

I can pull back the WSDL but want to send an image request to it to see if it actually pulls the image. I am looking for something like /GetPhoto?dl_num=20180061903&ss_num=2&type=M, the actually call method

To pull back the WSDL
<?xml version="1.0" encoding="UTF-8" ?>

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

[redacted]

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
Sent: Wednesday, May 8, 2019 5:52 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: Re: LRP network ideas?

Brian
Can you test the connectivity again?
Thanks

Sent from my iPhone

On May 7, 2019, at 10:43 AM, Brian Kruger <bkruger@forensiclogic.com> wrote:

> Tim,
> Thank you sir, sorry this fell off my radar. I was working on reallocation for Dan.
>
> Regards,
>
> <image001.png>
>
> **Brian Kruger**
> Operations and Support Manager
> **Forensic Logic / COPLINK**
> 520.488.1603
> bkruger@forensiclogic.com
> www.forensiclogic.com
>
> ***CONFIDENTIALITY:*** *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*
>
> ---
>
> **From:** Mitchell, Timothy (EPS)

<timothy.mitchell@state.ma.us>
Sent: Tuesday, May 7, 2019 7:42 AM
To: Brian Kruger <bkruger@forensiclogic.com>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Brian
Yes you will need to run the transactions across to the test server first and DCJIS will need to approve it before you can run to the production server. I will check out the firewall rules today and let you know.
Thanks

Timothy Mitchell
Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise and Field Services Support Division
Public Safety Data Center
200 Arlington St., Suite 2200
Chelsea, MA 02150
(P) 617.660.4665
(F) 617.884.4601
(E) timothy.mitchell@state.ma.us
http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Tuesday, May 07, 2019 10:40 AM
To: Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

Chris,

I am guessing test first, that way we can validate the broker, unless the route is setup already for production and I can switch it out to that.

Brian E.,
Your thoughts?

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Sent: Tuesday, May 7, 2019 7:18 AM
To: Brian Kruger <bkruger@forensiclogic.com>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Brian,

[redacted] is the TEST cjis broker system. Is the test system what you're looking to use?

-Chris

Christopher Ramsay | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information

Services
Division of Enterprise & Field Services
Support | Enterprise Systems

200 Arlington St. Suite 2200
Chelsea, MA 02150
p. 617.660.4720 | f. 617.660.4613
christopher.ramsay@mass.gov |
http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Tuesday, May 7, 2019 1:49 AM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

Tim,
I was checking the cjis broker service and I can't get to the [G.L. c. 4.sec. 7.cl.26 (n)(security)] on 6060 from the FR server at [G.L. c. 4.sec. 7.cl.26 (n)(security)] I was going through old email and just checking the status of the connections. The [G.L. c. 4.sec. 7.cl.26 (n)(security)] is what I received from Dev. Let me know if this is not correct.

<image003.jpg>

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and*

delete this e-mail from your system.

From: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
Sent: Friday, March 1, 2019 1:28 PM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Brian Kruger <bkruger@forensiclogic.com>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Hi folks
The CJIS broker transactions will need to use port 6060 as that is what they have been configured for in the past.

We have discussed the LPR port request and we think that going with a higher port seems to be more acceptable to EOTSS to allow through their public access firewall. Would port 56446 (https) work? We will need to open a ticket with EOTSS to have them allow this port through.

Thanks

Timothy Mitchell
Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise and Field Services Support Division
Public Safety Data Center
200 Arlington St., Suite 2200
Chelsea, MA 02150
(P) 617.660.4665
(F) 617.884.4601
(E) timothy.mitchell@state.ma.us
http://www.mass.gov/eops

From: Egnitz, Brian (POL)
Sent: Friday, March 01, 2019 12:44 PM
To: Mitchell, Timothy (EPS)

<timothy.mitchell@mass.gov>; Brian Kruger <bkruger@forensiclogic.com>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

Hi Tim,

I spoke with Brian Kruger and he wants the RI image CJIS Broker return to go to the same port as the ALPR image results, are there any issues with that? If not, is your team picking the port or is CopLink? I've included his email request. It sounds like they want to use the same web service to simplify the two integrations (LPR & RMV Images).

Tks, Brian

From: Mitchell, Timothy (EPS)
Sent: Friday, February 15, 2019 9:39 AM
To: Brian Kruger; Egnitz, Brian (POL); Ramsay, Christopher (EPS)
Subject: RE: LRP network ideas?

Brian
We are in receipt and reviewing on this side. I will get back to you next week.
Thanks

Timothy Mitchell
Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise and Field Services Support Division
Public Safety Data Center
200 Arlington St., Suite 2200
Chelsea, MA 02150
(P) 617.660.4665
(F) 617.884.4601
(E) timothy.mitchell@state.ma.us
http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Tuesday, February 12, 2019 2:46 PM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

Tim,
Here you go.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
Sent: Tuesday, February 12, 2019 8:19 AM
To: Brian Kruger <bkruger@forensiclogic.com>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian
Did you send over a diagram for review? If yes, can you resend as I can't come across it? We need to review this before

providing any additional ports.
Thanks

Timothy Mitchell
Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise and Field Services Support Division
Public Safety Data Center
200 Arlington St., Suite 2200
Chelsea, MA 02150
(P) 617.660.4665
(F) 617.884.4601
(E) timothy.mitchell@state.ma.us
http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Tuesday, February 12, 2019 12:00 AM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

Tim/Brian,
We are ready to start up the LPR ingest again, however I still need to assign a port to Tomcat on the FR server that will be accessible from both application servers. Is there any port range that we can shoot for. I would like to get the LPR data flowing as soon as possible.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603

bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Thursday, February 7, 2019 1:47 PM
To: 'Mitchell, Timothy (EPS)' <timothy.mitchell@state.ma.us>; 'Egnitz, Brian (POL)' <brian.egnitz@state.ma.us>; 'Ramsay, Christopher (EPS)' <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Tim,
Do you have any ports you send me that would be allowed for the connection from the app servers. I can update the diagram for approval that will work on the FR server. I will need two, one for Tomcat and one for LEXSR TR.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Thursday, February 7, 2019 8:50 AM
To: 'Mitchell, Timothy (EPS)' <timothy.mitchell@state.ma.us>; 'Egnitz, Brian (POL)' <brian.egnitz@state.ma.us>; 'Ramsay, Christopher (EPS)' <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Tim/Brian,
I was thinking last night and would actually like to move the new Image service to the FR server([redacted]). We have a route in place already from both PAA and Internal web to that server. I would just need to know what port to run tomcat on. This would also work for the Thompson Reuters adapter as well. Let me know what you guys think.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Monday, February 4, 2019 11:17 AM
To: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>

Subject: LRP network ideas?

Brian/Tim,
Nick is almost done with the new LPR service that will remove the images from the database and have a tomcat app that host the images for a return to the UI.
What I need to know:

1. The Migration will sit on the migration server and needs access to the LPR database to pull out the metadata and create the URL for the Image links.
2. The new service is going to be hosted in Tomcat, so this service will need access to the LPR database for images and both application servers need to be able to query this tomcat instance. I just need to know where to put it, I can host it on both severs or if we can set it up on the internal server and have a firewall rule that will allow the DMZ server to talk to the internal server. Let me know if you would like to have a call on this. I have attached a rough network diagram for visual reference.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

<MSP agency ORI.xlsx>

From: Fonitz, Brian (POL)
To: Brian Kruger
Subject: Re: LRP network ideas?
Date: Thursday, February 20, 2020 10:29:14 AM
Attachments: image001.png

There isn't one that I'm aware of.

On Feb 20, 2020, at 9:47 AM, Brian Kruger <bkruger@forensiclogic.com> wrote:

Brian,
This is the last email from John. It looks like we are missing a XSD file for the name space. I reached out just on the side to xfact to see if they have the XSD but haven't heard back.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Wednesday, February 12, 2020 8:37 AM
To: Samson Dunatunga <mdunatunga@forensiclogic.com>
Cc: Billy Moore <bmoore@forensiclogic.com>; Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hi Samson,

All of the xsd files are in the package and that is the only dev package we have.
Some of these namespaces were developed some time ago and are still in use.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Samson Dunatunga <mdunatunga@forensiclogic.com>
Sent: Tuesday, February 11, 2020 11:23 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Billy Moore <bmoore@forensiclogic.com>; Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Got all three packages extracted. I still don't see the XSD file for http://www.xfact.com/schemas/eopss/dcjis/cjx/3.0
I see XSD file (CJISBroker_2016-03-24.zip\CJISBroker_2016-03-24\CJISBroker\transactions\core\xsd\dcjis\1.0\dcjis.xsd) for http://www.xfact.com/schemas/eopss/dcjis/1.0 within the package CJISBroker_2016-03-24.zip

Do you have any other dev packages that includes above XSD files?
Thanks,
-Samson

From: Ouellette, John (EPS)
Sent: Tuesday, February 11, 2020 6:37 AM
To: Samson Dunatunga
Cc: Billy Moore; Brian Kruger
Subject: RE: LRP network ideas?

HI Samson,

Attached are the dev packages. They are zipped up, let me know if you don't get them.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Samson Dunatunga <mdunatunga@forensiclogic.com>
Sent: Monday, February 10, 2020 4:11 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>; Brian Kruger <bkruger@forensiclogic.com>
Cc: Billy Moore <bmoore@forensiclogic.com>
Subject: RE: LRP network ideas?

Hi John,
Thank you for the reply. The sample you have attached is a bit different from the sample I have. Where can I get the development package with the sample file you sent? It looks like I have been using an older implementation development package to generate the request. I don't have any class files related to dcjis schema in the development package I have.

Thanks,
-Samson

From: Ouellette, John (EPS)
Sent: Friday, February 7, 2020 2:39 PM
To: Samson Dunatunga; Brian Kruger
Cc: Billy Moore
Subject: RE: LRP network ideas?

Your namespaces should be:
xmlns:dcjis="http://www.xfact.com/schemas/eopss/dcjis/1.0" xmlns:cjx="http://www.xfact.com/schemas/eopss/dcjis/cjx/3.0"
xmlns:j="http://www.it.ojp.gov/jxdm/3.0"
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance

Attached is a sample R1 request.

John Ouellette | Massachusetts Executive Office of Public Safety and Security

Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Samson Dunatunga <mdunatunga@forensiclogic.com>
Sent: Friday, February 7, 2020 4:26 PM
To: Brian Kruger <bkruger@forensiclogic.com>; Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Billy Moore <bmoore@forensiclogic.com>
Subject: RE: LRP network ideas?

Hi John,
I compared the XML we are sending with the sample XML in the development package. I don't see any structural differences in them, but we are still getting reply indicating XML is not valid. Any help you can provide is appreciated.
Here is the XML we are sending for transaction type R1.
Thanks,
-Samson

---request begin----

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns1:CJISRequestTransaction xmlns:ns2="http://www.it.ojp.gov/jxdm/3.0" xmlns:ns1="http://www.xfact.com/schemas/chsb/cjis/2.0">
  <ns1:CJISRequestHeader>
    <ns1:UUID>S.L. c. 4 sec. 7 cl. 26</ns1:UUID>
    <ns1:CreateDateTime>2020-02-07T16:08:03.123-05:00</ns1:CreateDateTime>
    <ns1:TransactionSource>COPLINK</ns1:TransactionSource>
    <ns1:UserID>TEST</ns1:UserID>
    <ns2:OrganizationORIID>
      <ns2:ID>MAMSP0000</ns2:ID>
    </ns2:OrganizationORIID>
    <ns1:TimeToLive>unlimited</ns1:TimeToLive>
    <ns1:SchemaVersion>2.0</ns1:SchemaVersion>
    <ns1:ApplicationVersion>2.0</ns1:ApplicationVersion>
    <ns1:ResponseMechanism>Wait</ns1:ResponseMechanism>
    <ns1:RespondTo>http://S.L. c. 4 sec. 7 cl. 26:6060/CHSBReceiver/CHSBService</ns1:RespondTo>
    <ns1:CJISUserID>
      <ns2:ID>TEST</ns2:ID>
    </ns1:CJISUserID>
    <ns1:CJISUserPassword>password</ns1:CJISUserPassword>
    <ns1:CJISQueryAuthorizer>
      <ns2:PersonFullName>Joe Authorizer</ns2:PersonFullName>
    </ns1:CJISQueryAuthorizer>
    <ns1:CJISQueryOperator>
      <ns2:PersonFullName>Jane Authorizer</ns2:PersonFullName>
    </ns1:CJISQueryOperator>
    <ns1:CJISQueryRequester>
      <ns2:PersonFullName>Jane Requester</ns2:PersonFullName>
    </ns1:CJISQueryRequester>
    <ns1:CJISQueryPurposeCode>C</ns1:CJISQueryPurposeCode>
  </ns1:CJISRequestHeader>
  <ns1:CJISRequestBody>
    <ns1:R1QueryInput>
      <ns1:CJISMessageKey>R1</ns1:CJISMessageKey>
      <ns2:DriverAuthorization xsi:type="ns1:DriverAuthorizationType" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <ns2:DriverAuthorizationID>
          <ns2:ID>532935254</ns2:ID>
        </ns2:DriverAuthorizationID>
      </ns2:DriverAuthorization>
    </ns1:R1QueryInput>
  </ns1:CJISRequestBody>
</ns1:CJISRequestTransaction>
```

--- request end ----

Here is the sample XML provided to us.

```
<?xml version="1.0" encoding="UTF-8"?>
<cjx:CJISRequestTransaction xmlns:cjx="http://www.xfact.com/schemas/chsb/cjis/2.0" xmlns:j="http://www.it.ojp.gov/jxdm/3.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <cjx:CJISRequestHeader>
    <cjx:UUID>192.168.0.18/1237228378953.1.12</cjx:UUID>
    <cjx:CreateDateTime>2009-03-16T14:32:58-04:00</cjx:CreateDateTime>
    <cjx:TransactionSource>192.168.1.137 / CHSB</cjx:TransactionSource>
    <cjx:UserID>joe_user</cjx:UserID>
    <j:OrganizationORIID>
      <j:ID>MACJIS0M0</j:ID>
    </j:OrganizationORIID>
    <cjx:DeviceAddress></cjx:DeviceAddress>
    <cjx:UserContexts></cjx:UserContexts>
    <cjx:TimeToLive>unlimited</cjx:TimeToLive>
    <cjx:SchemaVersion>2.0</cjx:SchemaVersion>
    <cjx:ApplicationVersion>2.0</cjx:ApplicationVersion>
    <cjx:ResponseMechanism>Wait</cjx:ResponseMechanism>
    <cjx:RespondTo>http://192.168.0.30:6060/public/CHSBService.asmx</cjx:RespondTo>
    <cjx:CJISUserID>
      <j:ID>cjis_user</j:ID>
    </cjx:CJISUserID>
    <cjx:CJISUserPassword>password</cjx:CJISUserPassword>
    <cjx:CJISQueryAuthorizer>
      <j:PersonFullName>Joe Authorizer</j:PersonFullName>
    </cjx:CJISQueryAuthorizer>
    <cjx:CJISQueryOperator>
      <j:PersonFullName>Jane Operator</j:PersonFullName>
    </cjx:CJISQueryOperator>
    <cjx:CJISQueryRequester>
      <j:PersonFullName>Jane Requester</j:PersonFullName>
    </cjx:CJISQueryRequester>
    <cjx:CJISQueryPurposeCode>C</cjx:CJISQueryPurposeCode>
  </cjx:CJISRequestHeader>
  <cjx:CJISRequestBody>
    <cjx:R1QueryInput>
      <cjx:CJISMessageKey>R1</cjx:CJISMessageKey>
      <j:DriverAuthorization xsi:type="cjx:DriverAuthorizationType">
        <j:DriverAuthorizationID>
          <j:ID>900000035</j:ID>
        </j:DriverAuthorizationID>
      </j:DriverAuthorization>
    </cjx:R1QueryInput>
  </cjx:CJISRequestBody>
</cjx:CJISRequestTransaction>
```

Here is the reply we got for the XML we sent.

imagebroker.ImageBrokerREST.getEncodedImage result of service call: <?xml version="1.0" encoding="UTF-8"?>
<dcjis:DataExchange xmlns:dcjis="http://www.xfact.com/schemas/eopss/dcjis/1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><dcjis:Acknowledgment><dcjis:AcknowledgmentHeader>
<dcjis:UUID>ERROR</dcjis:UUID><dcjis:CreateDateTime>2020-02-07T16:08:18-0500</dcjis:CreateDateTime><dcjis:TransactionSource>ERROR</dcjis:TransactionSource>
<dcjis:TransactionMessageKey>ERROR</dcjis:TransactionMessageKey><dcjis:TransactionOrganizationID><dcjis:ID>ERROR</dcjis:ID></dcjis:TransactionOrganizationID><dcjis:UserContexts /><dcjis:DeviceAddress />
<dcjis:SchemaVersion>1.0</dcjis:SchemaVersion><dcjis:ApplicationVersion>2.0</dcjis:ApplicationVersion><dcjis:CJISUserID><dcjis:ID>ERROR</dcjis:ID></dcjis:CJISUserID><dcjis:CJISUserPassword>ERROR</dcjis:CJISUserPassword>
<dcjis:CJISQueryAuthorizer><dcjis:PersonFullName>ERROR</dcjis:PersonFullName></dcjis:CJISQueryAuthorizer><dcjis:CJISQueryOperator><dcjis:PersonFullName>ERROR</dcjis:PersonFullName></dcjis:CJISQueryOperator>
<dcjis:CJISQueryRequester><dcjis:PersonFullName>ERROR</dcjis:PersonFullName></dcjis:CJISQueryRequester><dcjis:CJISQueryPurposeCode>ERROR</dcjis:CJISQueryPurposeCode><dcjis:Transaction>
<dcjis:TransactionStatus>-903</dcjis:TransactionStatus><dcjis:TransactionDescription>Transaction failed schema validation</dcjis:TransactionDescription></dcjis:Transaction></dcjis:AcknowledgmentHeader>
<dcjis:AcknowledgmentBody /></dcjis:Acknowledgment></dcjis:DataExchange>

From: Brian Kruger
Sent: Tuesday, January 28, 2020 3:23 PM
To: Ouellette, John (EPS); Samson Dunatunga
Subject: RE: LRP network ideas?

Samson,
Did you get what you needed?

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Thursday, January 23, 2020 9:25 AM
To: Samson Dunatunga <mdunatunga@forensiclogic.com>
Cc: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hi Samson,

Do you have the dev package? There are example xml documents in there.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Samson Dunatunga <mdunatunga@forensiclogic.com>
Sent: Thursday, January 23, 2020 11:00 AM
To: Brian Kruger <bkruger@forensiclogic.com>; Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
Here is the XML sent from our server to retrieve relevant data. The CJISMessageKey is set to R1. The response we got indicates the XML sent is invalid. Can you point me to what is not valid in the XML? By the way, I checked the XML syntax with an online XML validation tool which indicates the syntax is good.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns1:CJISRequestTransaction xmlns:ns2="http://www.it.ojp.gov/jxdm/3.0" xmlns:ns1="http://www.xfact.com/schemas/chsb/cjis/2.0">
   <ns1:CJISRequestHeader>
      <ns1:UUID>S.L.c. 4.sec. 7.cl.c[redacted]87fc738-d2fa-4b4f-8841-067b2d85e636</ns1:UUID>
      <ns1:CreateDateTime>2020-01-22T10:47:23.216-05:00</ns1:CreateDateTime>
      <ns1:TransactionSource>COPLINK</ns1:TransactionSource>
      <ns1:UserID>TEST</ns1:UserID>
      <ns2:OrganizationORIID>
         <ns2:ID>MAMSP0000</ns2:ID>
      </ns2:OrganizationORIID>
      <ns1:TimeToLive>unlimited</ns1:TimeToLive>
      <ns1:SchemaVersion>2.0</ns1:SchemaVersion>
      <ns1:ApplicationVersion>2.0</ns1:ApplicationVersion>
      <ns1:ResponseMechanism>Wait</ns1:ResponseMechanism>
      <ns1:RespondTo>http://S.L.c. 4.sec. 7.cl.7[redacted]6060/CHSBReceiver/CHSBService</ns1:RespondTo>
      <ns1:CJISUserID>
         <ns2:ID>TEST</ns2:ID>
      </ns1:CJISUserID>
      <ns1:CJISUserPassword>password</ns1:CJISUserPassword>
      <ns1:CJISQueryAuthorizer>
         <ns2:PersonFullName>Joe Authorizer</ns2:PersonFullName>
      </ns1:CJISQueryAuthorizer>
      <ns1:CJISQueryOperator>
         <ns2:PersonFullName>Jane Authorizer</ns2:PersonFullName>
      </ns1:CJISQueryOperator>
      <ns1:CJISQueryRequester>
         <ns2:PersonFullName>Jane Requester</ns2:PersonFullName>
      </ns1:CJISQueryRequester>
      <ns1:CJISQueryPurposeCode>C</ns1:CJISQueryPurposeCode>
   </ns1:CJISRequestHeader>
   <ns1:CJISRequestBody>
      <ns1:R1QueryInput>
         <ns1:CJISMessageKey>R1</ns1:CJISMessageKey>
         <ns2:DriverAuthorization xsi:type="ns1:DriverAuthorizationType" ns2:id="S32935254" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"/>
      </ns1:R1QueryInput>
   </ns1:CJISRequestBody>
</ns1:CJISRequestTransaction>
```

Thank you,
-Samson

From: Brian Kruger
Sent: Wednesday, January 22, 2020 1:39 PM
To: Ouellette, John (EPS); Samson Dunatunga
Subject: RE: LRP network ideas?

John,
I am adding Samson on this thread.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Wednesday, January 22, 2020 1:35 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hi Brian,

The only namespaces I can find are:
xmlns:dcjis="http://www.xfact.com/schemas/eopss/dcjis/1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:cjx="http://www.xfact.com/schemas/eopss/dcjis/cjx/3.0"
xmlns:j="http://www.it.ojp.gov/jxdm/3.0">

Which message key are you trying to run?

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Wednesday, January 22, 2020 2:57 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
I have been putting out new versions of our Broker on this build Samson noticed that we are using xml namespace 2.0 which doesn't work. Do you know what version we should be running.

From: Samson Dunatunga <mdunatunga@forensiclogic.com>
Sent: Wednesday, January 22, 2020 11:28 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE:

Looks like the XML namespace xmlns:ns1="http://www.xfact.com/schemas/chsb/cjis/2.0"
is no longer available. Can you find out what we are supposed to use?

Thanks,
-Samson

From: Brian Kruger
Sent: Wednesday, January 22, 2020 8:56 AM
To: Samson Dunatunga
Subject:

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

2020-01-2
22-Jan-20
22-Jan-20
22-Jan-20

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

<dcjis:CJISQueryAuthorizer><dcjis:PersonFullName>ERROR</dcjis:PersonFullName></dcjis:CJISQueryAuthorizer><dcjis:CJISQueryOperator><dcjis:PersonFullName>ERROR</dcjis:PersonFullName></dcjis:CJISQueryOperator>
<dcjis:CJISQueryRequester><dcjis:PersonFullName>ERROR</dcjis:PersonFullName></dcjis:CJISQueryRequester><dcjis:CJISQueryPurposeCode>ERROR</dcjis:CJISQueryPurposeCode><dcjis:Transaction>
<dcjis:TransactionStatus>-903</dcjis:TransactionStatus><dcjis:TransactionDescription>Transaction failed schema validation</dcjis:TransactionDescription></dcjis:Transaction></dcjis:AcknowledgmentHeader>
<dcjis:AcknowledgmentBody /></dcjis:Acknowledgment></dcjis:DataExchange>

Regards,

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, December 6, 2019 9:45 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hey Brian,

Can we change the subject to Broker?
LPR is the license plate reader.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, December 6, 2019 11:31 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Samson Dunatunga <mdunatunga@forensiclogic.com>; Billy Moore <bmoore@forensiclogic.com>; Rhonda Fromm <rfromm@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

Billy,
Please let the group know when this will be available. I will work with John to get it deployed and tested as soon as we have it released.

Regards,

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Tuesday, November 26, 2019 1:17 PM
To: 'Ouellette, John (EPS)' <john.ouellette@state.ma.us>; 'Egnitz, Brian (POL)' <brian.egnitz@state.ma.us>; Samson Dunatunga <mdunatunga@forensiclogic.com>; Billy Moore <bmoore@forensiclogic.com>
Cc: 'Dunne, Michaela (CHS)' <michaela.dunne@state.ma.us>; 'Dunn-CHS, William (CHS)' <william.dunn-chs@state.ma.us>; 'Mitchell, Timothy (EPS)' <timothy.mitchell@state.ma.us>; 'Ramsay, Christopher (EPS)' <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

John,
Thank you for the information on the call this afternoon.

Samson/Billy,
We need to add some additional debug code into our service so we can see the full communication path and what is being sent and received. John is also in the process to check and make sure their three servers can reach back into our 184.171 on port 6060. I have also reattached the IP wireshark I did this morning.

Regards,

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Tuesday, November 26, 2019 8:29 AM
To: Ouellette, John (EPS) <john.ouellette@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

John,
Give me a few minutes and I will give you a call. Here is the CSV file from wireshark. I had to repull it. I don't see any actually log details in our tomcat instance. In the wireshark though I see a bunch of event code errors like below:

Event: <Unknown eventcode 72>, <Unknown eventcode 111>, <Unknown eventcode 116>, <Unknown eventcode 121>, <Unknown eventcode 110>, <Unknown eventcode 45>, <Unknown eventcode 112>, <Unknown eventcode 110>, <Unknown eventcode 114>, <Unknown eventcode 115>, <Unknown eventcode 47>, <Unknown eventcode 110>, <Unknown eventcode 111>, <Unknown eventcode 118>, <Unknown eventcode 110>, <Unknown eventcode 111>, <Unknown eventcode 47>, ColormapNotify, <Unknown eventcode 97>, <Unknown eventcode 120>, <Unknown eventcode 58>, <Unknown eventcode 46>, <Unknown eventcode 104>, <Unknown eventcode 46>, <Unknown eventcode 117>, <Unknown eventcode 97>, <Unknown eventcode 47>, <Unknown eventcode 62>, <Unknown eventcode 114>, <Unknown eventcode 114>, <Unknown eventcode 82>, <Unknown eventcode 120>, <Unknown

eventcode 101>, MappingNotify, <Unknown eventcode 109>, <Unknown eventcode 98>, <Unknown eventcode 47>, <Unknown eventcode 119>, <Unknown eventcode 62>, <Unknown eventcode 114>, ColormapNotify, <Unknown eventcode 62>, <Unknown eventcode 115>, MappingNotify, <Unknown eventcode 110>

Regards,

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Tuesday, November 26, 2019 7:29 AM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Hey Brian,

You can call me at 617-660-4775

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Monday, November 25, 2019 7:53 PM
To: Brian Kruger <bkruger@forensiclogic.com>; Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: Re: LRP network ideas?

Does it make sense to schedule a call and work through it in real time?

> On Nov 22, 2019, at 4:00 PM, Ouellette, John (EPS) <john.ouellette@mass.gov> wrote:
>
> Hi Brian,
>
> I do not see any requests for your ORI. Can you review the acknowledgements that the broker sends back as a return value? There may be error information in there.
>
> John Ouellette | Massachusetts Executive Office of Public Safety and Security
> Office of Technology and Information Services
> Enterprise Application and Database Services
> Application Support and Management
> 200 Arlington Street Suite 2200
> Chelsea, MA 02150
> john.ouellette@state.ma.us | http://www.mass.gov/eops
>
> ---
>
> **From:** Brian Kruger <bkruger@forensiclogic.com>
> **Sent:** Friday, November 22, 2019 3:47 PM
> **To:** Ouellette, John (EPS) <john.ouellette@mass.gov>
> **Cc:** Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
> **Subject:** RE: LRP network ideas?
>
> John,
> Can you check again and see if there is a request coming into the .154 server. I ran a packet capture and I do see data sent from the .171 to the .154 server.
>
> <image001.png>
>
> Regards,
>
>
>
> **Brian Kruger**
> Operations and Support Manager
> **Forensic Logic / COPLINK**
> Office: 520.367.2775
> Mobile: 520.488.1603
> bkruger@forensiclogic.com
> www.forensiclogic.com
>
> ***CONFIDENTIALITY:*** *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*
>
> ---
>
> **From:** Ouellette, John (EPS) <john.ouellette@state.ma.us>
> **Sent:** Friday, November 22, 2019 12:26 PM
> **To:** Brian Kruger <bkruger@forensiclogic.com>
> **Cc:** Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
> **Subject:** RE: LRP network ideas?
>
> Hi Brian,
>
> I'm not sure if 224.154 is a load balancer. I don't believe it is though. It doesn't matter though, that is where you will send requests. You will receive a synchronous response called an acknowledgement. That will let you know if your request was accepted or rejected.
>
> Later, an asynchronous response will be sent from 170.154.224.155 or 170.154.224.156 to your web service.
>
> John Ouellette | Massachusetts Executive Office of Public Safety and Security
> Office of Technology and Information Services
> Enterprise Application and Database Services

Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 22, 2019 2:19 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
The 154 address is a load balancer for the services correct. As far as I know there should be no blocked traffic to the .171 but let me include Chris and Tim on this thread.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 22, 2019 9:36 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

I didn't find any submitted requests.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Ouellette, John (EPS)
Sent: Friday, November 22, 2019 11:34 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

I can check.

The broker will send responses from 170.154.224.155 or 170.154.224.156 on port 6060. Make sure you are allowing that traffic.

When you send in a request you will receive an xml document as the return value. The documents lists if the request was accepted and if it wasn't, why it wasn't. You should be checking those.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 22, 2019 11:28 AM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

Bill,
I have the service send back a no data found so it looks like we are connecting. Can you check your logs to see if our request actually made it into your system.

I am sending the following test cycle from the 170.154.224.82 web server to our FR server

http://[redacted]6060/CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=S32935254

Just so everybody is clear, this the is the connection path

170.154.224.82 → [redacted]port 6060 → [redacted]port 6060

Return path

[redacted]→[redacted]port 6060 → 170.154.224.82

Log of request:

2019-11-22 11:16:13,982 main DEBUG LoggerContext[name=MassLPRServlet, org.apache.logging.log4j.core.LoggerContext@59303963] started OK with configuration org.apache.logging.log4j.core.config.properties.PropertiesConfiguration@61e86192.
2019-11-22 11:16:13,982 main DEBUG Log4jServletContextListener ensuring that Log4j starts up properly.
2019-11-22 11:16:13,982 main DEBUG Log4jServletFilter initialized.
driversLicense=S32935254
remote host=170.154.224.82
remote port=60194
remote addr=170.154.224.82
scheme =http
scheme =HTTP/1.1
local addr =[redacted]
local name =EPS-CLFACEMATCH
context path = /CHSBReceiver
Init parameter1 =Value1
Current UUID : f3837e1f-0e40-4af6-8587-203e99240d92
javax.xml.bind.JAXBElement@227d5180

Request UUID:[redacted]f3837e1f-0e40-4af6-8587-203e99240d92

Rest response file contains:
no data found.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Thursday, November 21, 2019 2:11 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Ouellette, John (EPS) <john.ouellette@state.ma.us>
Subject: RE: LRP network ideas?

Thanks Bill!

It looks like we are close on this.

-Brian

From: Dunn-CHS, William (CHS)
Sent: Tuesday, November 19, 2019 7:50 AM
To: Brian Kruger; Ouellette, John (EPS)
Cc: Dunne, Michaela (CHS); Egnitz, Brian (POL); Dunn-CHS, William (CHS)
Subject: RE: LRP network ideas?

I think I see what might be part of the problem.

The R1 is either OLN or SSN, you can not send both at the same time.

There is No TEST SSN inquiry, use someone from MSP who is working on your project or if you have a developer who is from MA
The TEST OLN is S32935254

From: Brian Kruger [mailto:bkruger@forensiclogic.com]
Sent: Monday, November 18, 2019 6:33 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
Dev confirmed they are sending XML in the request. Do you have a valid License number in the test data I can try.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 15, 2019 11:16 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

The broker is a web service. You need to create a client to connect. Requests are made by sending in an xml document.

Did I forget to send you the broker documentation? Let me know.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 1:10 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
I ran two queries through IE I don't see an acknowledge me in the logs. Below is what I am seeing. Do we have a valid Lic number that is in the system I can try, or valid SSN.

My test URLs are:"
http://[redacted]6060/CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=987654321

http://[redacted]6060/CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=987654321

In my access log I see a 200:

G.L. c. 4.sec. 7.cl.2- - [15/Nov/2019:13:02:50 -0500] "GET /CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=987654321 HTTP/1.1" 200 -
G.L. c. 4.sec. 7.cl.2- - [15/Nov/2019:13:03:05 -0500] "GET /CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=987654321 HTTP/1.1" 200 –

In my log stdout log I see this:

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
org.apache.loggi
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0 AScript,
ecmascript], fact
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0 ll)
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0 ptions="null",
disableAnsi="nul
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0 tern="null",
Configuration(Pr
2019-11-15 13:0
2019-11-15 13:0 ="null",
Policies(Compos
DefaultRollover
bufferedIo="null
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
SizeBasedTrigger
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

15-Nov-201
15-Nov-201
15-Nov-201

phone, I can try and send some responses and see if you see anything in your log files. I am wondering if they are forming the response to you correctly.

As for the WSDL this is what I see from the 184.171 server.

<image003.png>

Full WSDL

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

```
<?xml version="1.0" enc
- <wsdl:definitions xmln                                                    "http://server.service.cjis.xfact.com/"
xmlns:soap="http://sch                                                     getNamespace="http://server.service.cjis.xfact.com/">
- <wsdl:types>
- <xsd:schema xmlns:xsd                                                    efault="unqualified" elementFormDefault="qualified"
targetNamespace="http
<xsd:element name="st
<xsd:element name="st
<xsd:element name="st
<xsd:element name="st
</xsd:schema>
</wsdl:types>
- <wsdl:message name=
<wsdl:part element="tn
</wsdl:message>
- <wsdl:message name=
<wsdl:part element="tn
</wsdl:message>
<wsdl:message name="
+ <wsdl:message name=
<wsdl:part element="tn
</wsdl:message>
- <wsdl:message name=
<wsdl:part element="tn
</wsdl:message>
- <wsdl:message name=
<wsdl:part element="tn
</wsdl:message>
- <wsdl:message name=
<wsdl:part element="tn
</wsdl:message>
- <wsdl:message name=
<wsdl:part element="tn
</wsdl:message>
- <wsdl:portType name=
- <wsdl:operation name
<wsdl:input message="t
<wsdl:output message=
</wsdl:operation>
- <wsdl:operation name
<wsdl:input message="t
<wsdl:output message=
</wsdl:operation>
- <wsdl:operation name
<wsdl:input message="t
<wsdl:output message=
</wsdl:operation>
- <wsdl:operation name
<wsdl:input message="t
<wsdl:output message=
</wsdl:operation>
</wsdl:portType>
- <wsdl:binding name="
<soap:binding style="do
- <wsdl:operation name
<soap:operation soapAc
- <wsdl:input name="pr
<soap:body use="literal
</wsdl:input>
- <wsdl:output name="p
<soap:body use="literal
</wsdl:output>
</wsdl:operation>
- <wsdl:operation name
<soap:operation soapAc
- <wsdl:input name="ve
<soap:body use="literal
</wsdl:input>
- <wsdl:output name="v
<soap:body use="literal
</wsdl:output>
</wsdl:operation>
- <wsdl:operation name
<soap:operation soapAc
- <wsdl:input name="pr
<soap:body use="literal
</wsdl:input>
- <wsdl:output name="p
<soap:body use="literal
</wsdl:output>
</wsdl:operation>
- <wsdl:operation name
<soap:operation soapAc
- <wsdl:input name="pr
<soap:body use="literal
</wsdl:input>
- <wsdl:output name="p
<soap:body use="literal
</wsdl:output>
</wsdl:operation>
</wsdl:binding>
- <wsdl:service name="C
- <wsdl:port binding="tn
<soap:address location=
</wsdl:port>
</wsdl:service>
</wsdl:definitions>
```

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 15, 2019 9:36 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

If you are able to telnet, then you should be able to send in a request.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 11:06 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
This is all from the 184.171 server.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 15, 2019 8:41 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Are you doing the ping and telnet from G.L. c. 4.sec. 7.cl.26

Your error message from earlier seems to be your network not allowing the access.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 10:37 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
I am reaching out to the G.L. c. 4.sec. 7.cl.26 on port 6060. I can ping the IP and also hit the port.
<image004.png>

<image005.png>

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 15, 2019 8:26 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

What is the ip address you are trying to connect to?
Are you able to ping that machine?

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 10:22 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

Brian,
Thank you for checking in, sorry for the delay. I had the email together but it was in my draft. I tested the connection again today.

John,
I am still getting the remote Host not allowed. This is the error below:

2019-11-15 10:15:45,808 main DEBUG Log4jServletFilter initialized.
driversLicense=987654321
remote host=[redacted]
remote port=61799
remote addr=[redacted]
scheme =http
scheme =HTTP/1.1
local addr =[redacted]
local name =EPS-CLFACEMATCH
context path = /CHSBReceiver
Init parameter1 =Value1
remote host not allowed. ignoring request.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Friday, November 8, 2019 1:17 PM
To: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

John,
Thank you, I will work on testing the connection and let you know the results. According to Dev the other queries we will be running on the R1 and RI.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 8, 2019 12:18 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

I have added your configuration on the test broker for R1 and RI.
Are there more queries/transactions you'd like to test? Michaela may have requirements for other queries.

The ORI is MAMSPF022
Your requests come from [redacted] and responses will be sent back to http://[redacted]:6060/CHSBReceiver/CHSBService

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Ouellette, John (EPS)
Sent: Tuesday, November 5, 2019 12:54 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>
Subject: RE: LRP network ideas?

Hi Brian,

I think Bill needs to have more information on your project to assign an ORI to use on the test broker.

Is there a project name on your side?

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Monday, November 4, 2019 3:30 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
Any luck on this.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Tuesday, October 22, 2019 12:32 PM
To: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Subject: RE: LRP network ideas?

John,
Yea we should be sending the XML packet with the service that we have created. Do you know if that IP is natted to [redacted] The server that we have our service on is the [redacted]Face match server. I don't have any servers in the 170.154.226.x IP range unless it is getting natted somehow.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Tuesday, October 22, 2019 12:21 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hay Brian,

That won't work. The broker accepts an xml document containing the request, as well as other information.
Attached is a sample R1 request.

By the way, I have your requests coming from 170.154.226.47

In order to get responses, you need a web service on your end to receive the responses and I'll need to configure it on the broker side.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Monday, October 21, 2019 5:04 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
Can you provide me with a DL that should work. From the .82 server this is what we are running:

http:/[redacted]6060/CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=987654321

I just need to update the drivers license number and hopefully it will work

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Tuesday, September 24, 2019 8:07 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

So, just R1 and RI?

I'll start configuring the test broker.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Tuesday, September 24, 2019 10:59 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
For the queries that we will using this is what I got back from Dev… let me know if this helps

…Attachments\CJISBroker_2016-03-24[13247].zip\CJISBroker_2016-03-24\CJISBroker\transactions\queries\rmv\r1\xml

…Attachments\CJISBroker_2016-03-24[13247].zip\CJISBroker_2016-03-24\CJISBroker\transactions\queries\rmv\ri\xml

The rest is correct, for testing the ORI list will grow once we go to production.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Tuesday, September 24, 2019 6:39 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hi Brian,

I haven't added your configuration to the test broker yet. Can you confirm the following:
For broker connections, we need the following:
IP Address for requests: [redacted]
URL for responses: http://[redacted]:6060/CHSBReceiver/CHSBService
ORI: MAMSP0000
Queries: I need the list of queries/transactions you will be testing

You will submit to http://[redacted]:6060/CJISService This call will return a synchronous acknowledgment.

Responses will come back from 170.154.224.155 or 170.154.224.156 on port 6060. You need to return a synchronous acknowledgement for each response.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Monday, September 23, 2019 7:53 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
I have deployed a new package, but I see this in the log.

2019-09-23 19:48:37,297 main DEBUG Registering MBean org.apache.logging.log4j2:type=MassLPRServlet,component=Appenders,name=RollingFile
2019-09-23 19:48:37,304 main DEBUG org.apache.logging.log4j.core.util.SystemClock does not support precise timestamps.
2019-09-23 19:48:37,305 main DEBUG LoggerContext[name=MassLPRServlet, org.apache.logging.log4j.core.LoggerContext@2180e789] started OK with configuration org.apache.logging.log4j.core.config.properties.PropertiesConfiguration@5e9bbd9d.
2019-09-23 19:48:37,307 main DEBUG Log4jServletContextListener ensuring that Log4j starts up properly.
2019-09-23 19:48:37,309 main DEBUG Log4jServletFilter initialized.
driversLicense=987654321
remote host=0:0:0:0:0:0:0:1
remote port=65146
remote addr=0:0:0:0:0:0:0:1
scheme =http
scheme =HTTP/1.1
local addr =0:0:0:0:0:0:0:1
local name =EPS-CLFACEMATCH
context path = /CHSBReceiver
Init parameter1 =Value1
remote host not allowed. ignoring request.

can you check and make sure this machine has access:

EPS-CLFACEMATCH
Connection-specific DNS Suffix . :
IPv4 Address. . . . . : [redacted]
Subnet Mask . . . . . : 255.255.255.128
Default Gateway . . . . . : 170.154.184.129

C:\Users\msp_user>
Regards,

<image002.png>

Brian Kruger
Operations and Support Manager

Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, September 6, 2019 6:15 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hey Brian,

I'm not sure what is in the test system either. I believe a dl of 987654321 will work; at least it used to.
Try to find something in test CJISWeb.

Remember that all queries will send in an xml document and will receive a return acknowledgement stating success or failure. If the request failed, the reason will be in the acknowledgement.

At a later time, seconds or less, the response will be returned to your web service. You must return an acknowledgement to that also to let the system know that the response was received and the next response can be sent.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Thursday, September 5, 2019 5:17 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
Not yet, I don't know what is in the test system… are they actually dls or fake ones.

Our query against our service is going to look something like, that will translate to yours.

http://[redacted]6060/CHSBReceiver/CHSBService?ori=REM000001&username=TEST&ssn=123123123&driversLicense=AZ67676767

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Thursday, September 5, 2019 1:09 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Have you tried your DL and SSN?

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Thursday, September 5, 2019 2:36 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
Do you have a sample DL and ssn, we can try passing through the service to see if we can pull an image. According to dev we are just utilizing the XML out of R1 and Ri.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, August 9, 2019 7:04 AM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Brian Kruger <bkruger@forensiclogic.com>; Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

All of the broker queries use the same method and accept an xml document. The contents of the xml direct what action the system should take. I have attached documentation for the broker. It's a 5 MB zip file.

If you can't accept zip files or 5 MB files let me know how to send the file.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, August 9, 2019 9:39 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Brian Kruger <bkruger@forensiclogic.com>; Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>
Subject: Re: LRP network ideas?

Thanks John, I'll defer to Brian Kruger to respond regarding where he's sending the query. Are you able to answer his question below?

"

> I can pull back the WSDL but want to send an image request to it to see if it actually pulls the image. I am looking for something like /GetPhoto?dl_num=20180061903&ss_num=2&type=M, the actually call method

"

On Aug 9, 2019, at 9:04 AM, Ouellette, John (EPS) <john.ouellette@mass.gov> wrote:

> Hi Brian,
>
> For broker connections to test, we need the following:
> IP Address for request: [redacted]
> URL for responses: http://[redacted]6060/CHSBReceiver/CHSBService
> ORI: MAMSP0000
> Queries:
>
> Can you confirm this information and send the list of queries you would like to run?
> Please remember that this system would only be used for test. Another system would need to be used when you move to production.
>
> John Ouellette | Massachusetts Executive Office of Public Safety and Security
> Office of Technology and Information Services
> Enterprise Application and Database Services
> Application Support and Management
> 200 Arlington Street Suite 2200
> Chelsea, MA 02150
> john.ouellette@state.ma.us | http://www.mass.gov/eops
>
> ---
>
> **From:** Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Sent:** Friday, August 9, 2019 8:54 AM
> **To:** Brian Kruger <bkruger@forensiclogic.com>
> **Cc:** Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Ouellette, John (EPS) <john.ouellette@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>
> **Subject:** Re: LRP network ideas?
>
> Hi Brian,
>
> are we testing on this yet?
>
> On Jul 22, 2019, at 1:37 PM, Brian Kruger <bkruger@forensiclogic.com> wrote:
>
> > Tim,
> > Attached is the full list of agencies and ORI that we currently have in the admin DB.
> >
> > Regards,
> >
> > <image001.png>
> > **Brian Kruger**
> > Operations and Support Manager
> > **Forensic Logic / COPLINK**
> > 520.488.1603
> > bkruger@forensiclogic.com
> > www.forensiclogic.com
> >
> > ***CONFIDENTIALITY:*** *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*
>
> ---
>
> **From:** Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
> **Sent:** Monday, July 22, 2019 8:37 AM
> **To:** Brian Kruger <bkruger@forensiclogic.com>
> **Cc:** Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Ouellette, John (EPS) <john.ouellette@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
> **Subject:** RE: LRP network ideas?
>
> Any update on this from dev, do you still need a sample RI url? Can you make sure you are also sending the CopLink user name in the UserID parameter.
>
> Tks, Brian
>
> ---
>
> **From:** Brian Kruger [mailto:bkruger@forensiclogic.com]
> **Sent:** Thursday, July 18, 2019 5:19 PM
> **To:** Mitchell, Timothy (EPS)
> **Cc:** Ramsay, Christopher (EPS); Egnitz, Brian (POL); Ouellette, John (EPS)
> **Subject:** RE: LRP network ideas?
>
> Tim,
> I am still pending an answer back from dev on how they are going to pull the ORI. For now can we use `MAMSP0000. That is actually in our systems as MSP.`
>
> Regards,
>
> <image001.png>
> **Brian Kruger**
> Operations and Support Manager
> **Forensic Logic / COPLINK**
> 520.488.1603
> bkruger@forensiclogic.com
> www.forensiclogic.com
>
> ***CONFIDENTIALITY:*** *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
Sent: Tuesday, July 16, 2019 4:07 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Ouellette, John (EPS) <john.ouellette@state.ma.us>
Subject: RE: LRP network ideas?

Brian
What is the ORI that you are using for this setup? There is some configuration work that needs to be done on the broker side to allow your service to run transactions.
Thanks
Tim

Timothy Mitchell
Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise and Field Services Support Division
Public Safety Data Center
200 Arlington St., Suite 2200
Chelsea, MA 02150
(P) 617.660.4665
(F) 617.884.4601
(E) timothy.mitchell@state.ma.us
http://www.mass.gov/eops

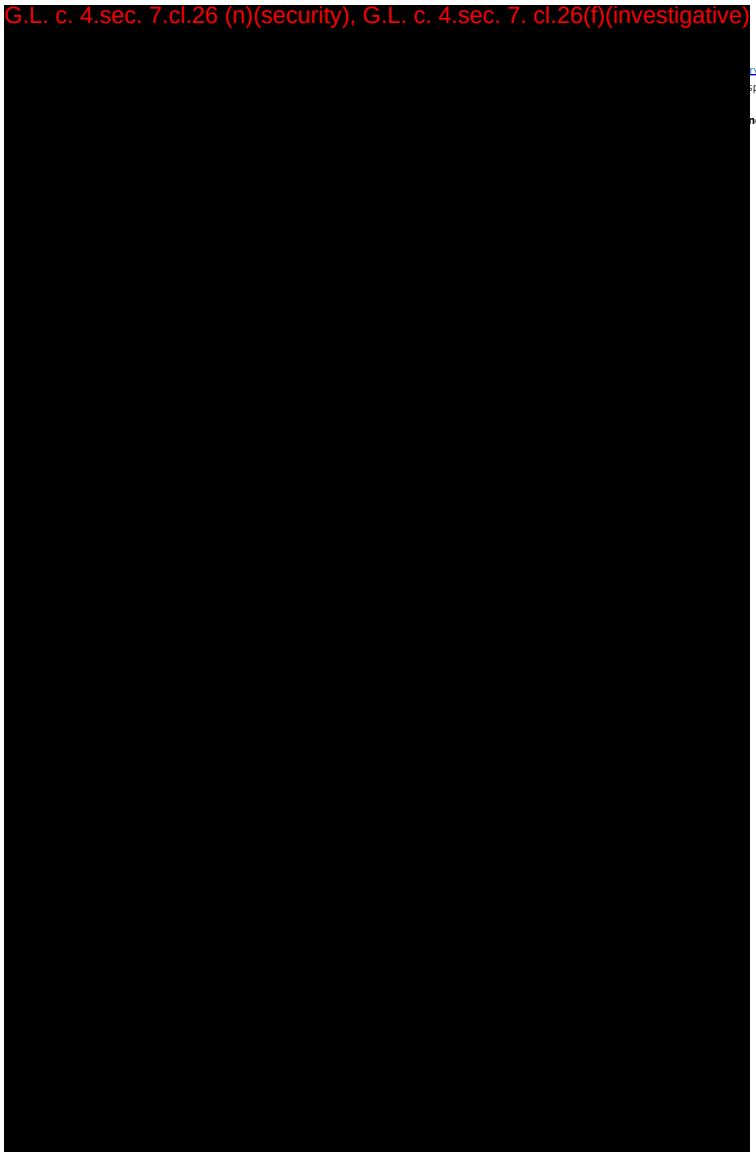
From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Monday, July 15, 2019 7:05 PM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

Folks,
For the RMV pull, does anybody have an example image we can try and run through. All the connectivity looks good, I have tried a few ways to pull an image without success.

Our service
http://G.L. c. 4.sec. 7.cl.26 6060/CHSBReceiver/CHSBService?wsdl refers to http://G.L. c. 4.sec. 7.cl.26 6060/CJISService?wsdl

I can pull back the WSDL but want to send an image request to it to see if it actually pulls the image. I am looking for something like /GetPhoto?dl_num=20180061903&ss_num=2&type=M, the actually call method

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)



rver.service.cjis.xfact.com/"
space="**http://server.service.cjis.xfact.com/**">

nqualified" elementFormDefault="**qualified**"

[redacted] G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
Sent: Wednesday, May 8, 2019 5:52 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: Re: LRP network ideas?

Brian
Can you test the connectivity again?
Thanks

Sent from my iPhone

On May 7, 2019, at 10:43 AM, Brian Kruger <bkruger@forensiclogic.com> wrote:

> Tim,
> Thank you sir, sorry this fell off my radar. I was working on reallocation for Dan.
>
> Regards,
>
> <image001.png>
>
> **Brian Kruger**
> Operations and Support Manager
> **Forensic Logic / COPLINK**
> 520.488.1603
> bkruger@forensiclogic.com
> www.forensiclogic.com
>
> ***CONFIDENTIALITY:*** *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*
>
> ---
>
> **From:** Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
> **Sent:** Tuesday, May 7, 2019 7:42 AM
> **To:** Brian Kruger <bkruger@forensiclogic.com>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
> **Subject:** RE: LRP network ideas?
>
> Brian
> Yes you will need to run the transactions across to the test server first and DCJIS will need to approve it before you can run to the production server. I will check out the firewall rules today and let you know.
> Thanks
>
> Timothy Mitchell
> Massachusetts Executive Office of Public Safety and Security
> Office of Technology and Information Services
> Enterprise and Field Services Support Division
> Public Safety Data Center
> 200 Arlington St., Suite 2200
> Chelsea, MA 02150
> (P) 617.660.4665
> (F) 617.884.4601
> (E) timothy.mitchell@state.ma.us
> http://www.mass.gov/eops
>
> ---
>
> **From:** Brian Kruger <bkruger@forensiclogic.com>
> **Sent:** Tuesday, May 07, 2019 10:40 AM
> **To:** Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Subject:** RE: LRP network ideas?
>
> Chris,
> I am guessing test first, that way we can validate the broker, unless the route is setup already for production and I can switch it out to that.

Brian E.,
Your thoughts?

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Sent: Tuesday, May 7, 2019 7:18 AM
To: Brian Kruger <bkruger@forensiclogic.com>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Brian,

G.L. c. 4.sec. 7.cl.2is the TEST cjis broker system. Is the test system what you're looking to use?

-Chris

Christopher Ramsay | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Division of Enterprise & Field Services Support | Enterprise Systems

200 Arlington St. Suite 2200
Chelsea, MA 02150
p. 617.660.4720 | f. 617.660.4613
christopher.ramsay@mass.gov | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Tuesday, May 7, 2019 1:49 AM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

Tim,
I was checking the cjis broker service and I can't get to theG.L. c. 4.sec. 7.cl.2on 6060 from the FR server atG.L. c. 4.sec. 7.cl.2 I was going through old email and just checking the status of the connections. TheG.L. c. 4.sec. 7.cl.2is what I received from Dev. Let me know if this is not correct.

<image003.jpg>

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
Sent: Friday, March 1, 2019 1:28 PM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Brian Kruger <bkruger@forensiclogic.com>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Hi folks
The CJIS broker transactions will need to use port 6060 as that is what they have been configured for in the past.

We have discussed the LPR port request and we think that going with a higher port seems to be more acceptable to EOTSS to allow through their public access firewall. Would port 56446 (https) work? We will need to open a ticket with EOTSS to have them allow this port through.

Thanks

Timothy Mitchell
Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise and Field Services Support Division
Public Safety Data Center
200 Arlington St., Suite 2200
Chelsea, MA 02150
(P) 617.660.4665
(F) 617.884.4601
(E) timothy.mitchell@state.ma.us
http://www.mass.gov/eops

From: Egnitz, Brian (POL)
Sent: Friday, March 01, 2019 12:44 PM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Brian Kruger <bkruger@forensiclogic.com>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

Hi Tim,

I spoke with Brian Kruger and he wants the RI image CJIS Broker return to go to the same port as the ALPR image results, are there any issues with that? If not, is your team picking the port or is CopLink? I've included his email request. It sounds like they want to use the same web service to simplify the two integrations (LPR & RMV Images).

Tks, Brian

From: Mitchell, Timothy (EPS)
Sent: Friday, February 15, 2019 9:39 AM
To: Brian Kruger; Egnitz, Brian (POL); Ramsay, Christopher (EPS)
Subject: RE: LRP network ideas?

Brian
We are in receipt and reviewing on this side. I will get back to you next week.

Thanks

Timothy Mitchell
Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise and Field Services Support Division
Public Safety Data Center
200 Arlington St., Suite 2200
Chelsea, MA 02150
(P) 617.660.4665
(F) 617.884.4601
(E) timothy.mitchell@state.ma.us
http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Tuesday, February 12, 2019 2:46 PM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

Tim,
Here you go.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
Sent: Tuesday, February 12, 2019 8:19 AM
To: Brian Kruger <bkruger@forensiclogic.com>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian
Did you send over a diagram for review? If yes, can you resend as I can't come across it? We need to review this before providing any additional ports.
Thanks

Timothy Mitchell
Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise and Field Services Support Division
Public Safety Data Center
200 Arlington St., Suite 2200
Chelsea, MA 02150
(P) 617.660.4665
(F) 617.884.4601
(E) timothy.mitchell@state.ma.us
http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Tuesday, February 12, 2019 12:00 AM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

Tim/Brian,
We are ready to start up the LPR ingest again, however I still need to assign a port to Tomcat on the FR server that will be accessible from both application servers. Is there any port range that we can shoot for. I would like to get the LPR data flowing as soon as possible.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Thursday, February 7, 2019 1:47 PM
To: 'Mitchell, Timothy (EPS)' <timothy.mitchell@state.ma.us>; 'Egnitz, Brian (POL)' <brian.egnitz@state.ma.us>; 'Ramsay, Christopher (EPS)' <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Tim,
Do you have any ports you send me that would be allowed for the connection from the app servers. I can update the diagram for approval that will work on the FR server. I will need two, one for Tomcat and one for LEXSR TR.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Thursday, February 7, 2019 8:50 AM
To: 'Mitchell, Timothy (EPS)' <timothy.mitchell@state.ma.us>; 'Egnitz, Brian (POL)' <brian.egnitz@state.ma.us>; 'Ramsay, Christopher (EPS)' <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Tim/Brian,
I was thinking last night and would actually like to move the new Image service to the FR server S.L. c. 4 sec. 7 cl 26We have a route in place already from both PAA and Internal web to that server. I would just need to know what port to run tomcat on. This would also work for the Thompson Reuters adapter as well. Let me know what you guys think.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Monday, February 4, 2019 11:17 AM
To: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: LRP network ideas?

Brian/Tim,
Nick is almost done with the new LPR service that will remove the images from the database and have a tomcat app that host the images for a return to the UI. What I need to know:

<!--
[if !supportLists]-->-->1.<!--[endif]-->-->The Migration will sit on the migration server and needs access to the LPR database to pull out the metadata and create the URL for the Image links.
<!--[if !supportLists]-->-->2.<!--[endif]-->-->The new service is going to be hosted in Tomcat, so this service will need access to the LPR database for images and both application servers need to be able to

query this tomcat instance. I just need to know where to put it, I can host it on both severs or if we can set it up on the internal server and have a firewall rule that will allow the DMZ server to talk to the internal server. Let me know if you would like to have a call on this. I have attached a rough network diagram for visual reference.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

<MSP agency ORI.xlsx>

From: Smith, Eleanor (POL)
To: Thibault, Amy (POL)
Subject: RE: MA Crimenet
Date: Monday, October 19, 2020 4:52:47 PM
Attachments: Chris Neville - ems.docx

These are super comprehensive. I only had one minor thing – added in blue, but not sure if it is even worth mentioning. But aside from that you had everything I had and more. I also put a note in where I took down a different stat, so maybe we confirm with him.

Thanks!

From: Thibault, Amy (POL)
Sent: Monday, October 19, 2020 3:40 PM
To: Smith, Eleanor (POL) <Eleanor.Smith@pol.state.ma.us>
Subject: RE: MA Crimenet

From: Smith, Eleanor (POL)
Sent: Monday, October 19, 2020 3:39 PM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Subject: RE: MA Crimenet

Mine are handwritten, might be easier for me to plug them into yours…

From: Thibault, Amy (POL)
Sent: Monday, October 19, 2020 3:28 PM
To: Smith, Eleanor (POL) <Eleanor.Smith@pol.state.ma.us>
Subject: MA Crimenet

I just went through my Chris Neville notes. I know youre really busy with the assessment. Do you want to send me yours to combine them? I want to get them up the chain ASAP.

From: Thibault, Amy (POL)
To: Smith, Eleanor (POL)
Subject: RE: MA Crimenet
Date: Monday, October 19, 2020 3:40:00 PM
Attachments: Chris Neville.docx

From: Smith, Eleanor (POL)
Sent: Monday, October 19, 2020 3:39 PM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Subject: RE: MA Crimenet

Mine are handwritten, might be easier for me to plug them into yours…

From: Thibault, Amy (POL)
Sent: Monday, October 19, 2020 3:28 PM
To: Smith, Eleanor (POL) <Eleanor.Smith@pol.state.ma.us>
Subject: MA Crimenet

I just went through my Chris Neville notes. I know youre really busy with the assessment. Do you want to send me yours to combine them? I want to get them up the chain ASAP.

From: Smith, Eleanor (POL)
To: Thibault, Amy (POL)
Subject: RE: MA Crimenet
Date: Monday, December 7, 2020 3:04:08 PM
Attachments: MA Crimenet TO FROM.doc

Suggested edits attached☺ Looks good!

From: Thibault, Amy (POL)
Sent: Monday, December 7, 2020 2:29 PM
To: Smith, Eleanor (POL) <Eleanor.Smith@pol.state.ma.us>
Subject: MA Crimenet

DO you have time to read this and see if I am missing anything or there are any grammar/spelling issues? I'd like to send it up today.

Respectfully,

Amy Thibault
Intelligence Services Manager
MA State Police
Intelligence Services Unit
Commonwealth Fusion Center
Main Number: 508-820-2233
Desk: 978-451-3717
amy.thibault@pol.state.ma.us

From:	Brooks, Brian (POL)
To:	Lenti, Jeffrey (POL); Mauer, Ryan (POL)
Cc:	Chalmers, Traylen (POL)
Subject:	RE: MA DOT Toll stanchion Inquiry
Date:	Thursday, September 3, 2020 12:53:00 PM
Attachments:	700cmr7.pdf

Ryan, our requests are limited to emergency or exigent circumstances, I'm sorry but you will have to go to DOT directly, please see attached 700 CMR 7.05 (8)

From: Lenti, Jeffrey (POL) <[redacted]pol.state.ma.us>
Sent: Thursday, September 3, 2020 11:52 AM
To: Mauer, Ryan (POL) <ryan.mauer@pol.state.ma.us>
Cc: Chalmers, Traylen (POL) <traylen.chalmers@pol.state.ma.us>; Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>
Subject: Re: MA DOT Toll stanchion Inquiry

Ryan,

I'm in at 1500 today but I'm forwarding this to the Fusion "In" box and the day shift can start working on it.

Jeff

> On Sep 3, 2020, at 10:34 AM, Mauer, Ryan (POL) <ryan.mauer@pol.state.ma.us> wrote:
>
> Hey Lt,
>
> We have a home invasion case (Aciss #2020-103-101) which occurred in Washington (yes the middle of nowhere) that we are jointly working with the Cheshire Barracks. The incident occurred on March 15, 2020. Through CDR results we are able to ascertain that the suspect travelled EB on the pike after the incident. We do NOT have a vehicle description or plate of the target vehicle. We were able to narrow down that the suspect likely passed under the **Blandford toll stanchion EB** between:
>
> **March 15, 2020**
> - 2203-2209 hours
>
> Do you know if DOT will require a search warrant for vehicle images and plate numbers of those that passed under the stanchion during that time?
>
> Thanks,

Ryan Mauer
Berkshire SPDU
413-281-8143

To: Peek, Brian (POL)
Cc: Guerriero, Robert (EOTSS); Quinn, Dermot (POL)
Subject: RE: MassPort ALPR
Date: Friday, April 17, 2020 6:37:30 AM
Attachments: image001.png

Hi Brian,

As you are aware

From: Peek, Brian (POL)
Sent: Thursday, February 28, 2019 9:37 AM
To: Egnitz, Brian (POL)
Cc: Mitchell, Timothy (EPS); Guerriero, Robert (EOTSS)
Subject: RE: MassPort ALPR

Morning Brian,

We will need the proposal and design created by you and your project team.

If you have any questions please let me know,

Thanks
bp

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Wednesday, February 27, 2019 9:57 AM
To: Peek, Brian (POL) <brian.peek@pol.state.ma.us>
Cc: Cronin, Tim (POL) <Tim.Cronin@pol.state.ma.us>; Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>
Subject: RE: MassPort ALPR

Sounds good, who is responsible for the proposal and diagram? And what do you need from my end?

-Brian

From: Peek, Brian (POL)
Sent: Wednesday, February 27, 2019 8:55 AM
To: Egnitz, Brian (POL)
Cc: Cronin, Tim (POL); Guerriero, Robert (EOTSS)
Subject: RE: MassPort ALPR

Morning Brian,

We should discuss how this traffic would be routed to the watch center at GHQ. We would need a proposal, diagram and then approved by TSS security.

I am free tomorrow if you want to talk.

Thanks
Brian

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Tuesday, February 26, 2019 5:08 PM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; AChute@massport.com
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Warmington, Scott (POL) <Scott.Warmington@pol.state.ma.us>; Peek, Brian (POL) <brian.peek@pol.state.ma.us>
Subject: RE: MassPort ALPR

Any thoughts on sharing the client with the watch? I'm still waiting on a quote from the vendor to split the feeds at the camera.

-Brian

From: Egnitz, Brian (POL)
Sent: Friday, February 8, 2019 11:30 AM
To: Mitchell, Timothy (EPS); AChute@massport.com
Cc: Quinn, Dermot (POL); Warmington, Scott (POL); Peek, Brian (POL)
Subject: RE: MassPort ALPR

Hi guys,

I spoke to Neology's Global R&D Director. He should have an answer Monday as to the technical approach.

-Brian

From: Mitchell, Timothy (EPS)
Sent: Friday, January 18, 2019 9:57 AM
To: Egnitz, Brian (POL)
Cc: AChute@massport.com; Peek, Brian (POL)
Subject: RE: MassPort ALPR

I can do Wednesday after 2:30pm or anytime on Thursday before 2:30pm.

Thanks

Timothy Mitchell
Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise and Field Services Support Division

Public Safety Data Center
200 Arlington St., Suite 2200
Chelsea, MA 02150
(P) 617.660.4665
(F) 617.884.4601
(E) timothy.mitchell@state.ma.us
http://www.mass.gov/eops

From: Egnitz, Brian (POL)
Sent: Friday, January 18, 2019 9:41 AM
To: Mitchell, Timothy (EPS)
Cc: AChute@massport.com; Peek, Brian (POL)
Subject: RE: MassPort ALPR

I've sent out a meeting invite. Peek is unable to attend. Please advise if there is a different date/time

---

From: Mitchell, Timothy (EPS)
Sent: Thursday, January 17, 2019 3:53 PM
To: Egnitz, Brian (POL)
Cc: AChute@massport.com; Peek, Brian (POL)
Subject: RE: MassPort ALPR

Hi Brian
Yes, I am available for a call next week. I have time on Tuesday morning if you folks are free.
Thanks
Tim

Timothy Mitchell
Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise and Field Services Support Division
Public Safety Data Center
200 Arlington St., Suite 2200
Chelsea, MA 02150
(P) 617.660.4665
(F) 617.884.4601
(E) timothy.mitchell@state.ma.us
http://www.mass.gov/eops

From: Egnitz, Brian (POL)
Sent: Wednesday, January 09, 2019 3:07 PM
To: Mitchell, Timothy (EPS)
Cc: AChute@massport.com; Peek, Brian (POL)
Subject: Fwd: MassPort ALPR

Hi Tim,

I'd like to revive this initiative are you available to meet and discuss?

Thanks, Brian

Begin forwarded message:

From: "Chute, Alexander" <AChute@massport.com>
Date: February 13, 2018 at 3:36:43 PM EST
To: "Egnitz, Brian (POL)" <brian.egnitz@massmail.state.ma.us>
Subject: RE: MassPort ALPR

Thank you for making the introductions. I got a call while I was out last week and am just getting caught up, but should hopefully have this taken care of soon. I also got your voicemail about using a cellular based modem, and agree with you about the ease of setup if I can't get my other idea to pan out.

Thanks again!

~Alex

From: Egnitz, Brian (POL) [mailto:brian.egnitz@MassMail.State.MA.US]
Sent: Monday, February 05, 2018 10:54 AM
To: Chute, Alexander
Cc: Quinn, Dermot (POL); Hughes, Sean M. (EOTSS)
Subject: RE: MassPort ALPR

Hi Alex,

I think the best POC would be Sean Hughes at EOTSS. Please see below for his contact information. His team should be able to provide the IPs and Ports to facilitate the connectivity to the LPR system. Once connected, we can assist with the hotlists or configuration on the application side.

Sean M. Hughes
Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Assistant Secretariat Chief Information Officer
200 Arlington Street, Suite 2200
Chelsea, MA 02150
Phone 617.660.4620
Toll Free 844.868.4620
Fax 617.884.4601
sean.hughes@mass.gov

http://www.mass.gov/eops

-Brian

Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
Phone: 978-451-3710 (Maynard) 508-988-7216 (GHQ)
Email: Brian.Egnitz@massmail.state.ma.us
Monday - Friday, 8 to 4

CONFIDENTIALITY NOTICE: *The information contained in this email and any attachment is privileged and confidential law enforcement information. If you have received this email in error, please call 978-451-3700 immediately. Thank you.*

From: Chute, Alexander [mailto:AChute@massport.com]
Sent: Wednesday, January 31, 2018 8:05 AM
To: Egnitz, Brian (POL)
Subject: MassPort ALPR

Hi Brian,

I hope this finds you well. We spoke a while ago about the various options for the fixed ALPR cameras here at MassPort and I have been asked to migrate their reporting over to the state system. Would you be the appropriate contact to help start this process, or would you be able to direct me to the right person? Let me know if you have a minute to discuss. Thank you for your time.

Respectfully,

~Alex

Alexander B. Chute
Program Manager, Public Safety Systems
Massachusetts Port Authority
Cell: [redacted]
Office: 617.568.5942
achute@massport.com

WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

From: Silva, Kyra (POL)
To: Sullivan, Margaret (POL)
Subject: RE: MassPort LPR Cameras
Date: Thursday, April 16, 2020 3:00:03 PM
Attachments: SierraQuoteForMassPort.pdf

Hi Peg,

Was this submitted to for processing?

Thank you

-----Original Message-----
From: Egnitz, Brian (POL)
Sent: Thursday, April 09, 2020 4:06 PM
To: Silva, Kyra (POL)
Subject: FW: MassPort LPR Cameras

Hi Kyra,

Can you please see below and attached. Let me know if you have any questions.

Thanks, Brian

-----Original Message-----
From: Quinn, Dermot (POL)
Sent: Thursday, April 9, 2020 2:00 PM
To: Egnitz, Brian (POL)
Cc: Warren, Rosemary (POL)
Subject: RE: MassPort LPR Cameras

This is to allow the Massport ALPR cameras to write to thestate ALPR server in Chelsea. Approved at DHS. Please forward to Kyra Silva in Fiscal for funding.

Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division of Homeland Security & Preparedness Massachusetts State Police

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Thursday, April 9, 2020 1:58 PM
To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: RE: MassPort LPR Cameras

Do you know if this was moved on? We need it for the MassPort modem project.

-----Original Message-----
From: Egnitz, Brian (POL)
Sent: Tuesday, March 10, 2020 10:52 AM
To: Quinn, Dermot (POL)
Subject: FW: MassPort LPR Cameras

Hi LTC.,

Can we order this equipment for the MassPort project?

Thanks, Brian

-----Original Message-----
From: Slater, James (CHS)
Sent: Tuesday, March 10, 2020 10:26 AM
To: Egnitz, Brian (POL)
Subject: RE: MassPort LPR Cameras

Hi, Brian!

This needs to go through MSP fiscal. They need to enter the purchase in OPAS.

Jim

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Tuesday, March 10, 2020 08:06
To: Slater, James (CHS) <james.slater@mass.gov>
Subject: RE: MassPort LPR Cameras

Is this something you can order or does it need to go through MSP?

-----Original Message-----
From: Slater, James (CHS)
Sent: Monday, March 9, 2020 10:36 AM
To: Egnitz, Brian (POL)
Subject: RE: MassPort LPR Cameras

Thanks, Brian...I will check with TSS.

Jim

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Monday, March 9, 2020 10:29
To: Slater, James (CHS) <james.slater@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: RE: MassPort LPR Cameras

Thanks Jim,

I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need 6 sierra wireless AC adapters and 12 antennas. I have reached out to BCM for a quote.

I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.

I plan to cut one sector (5-6 cameras per sector) over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?

-Brian

-----Original Message-----
From: Slater, James (CHS)
Sent: Friday, March 6, 2020 1:43 PM
To: Egnitz, Brian (POL)
Cc: Quinn, Dermot (POL)
Subject: RE: MassPort LPR Cameras

Hi, Brian!

I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.

So, assuming you move forward with this, who would actually make this happen?

Thanks.

Jim

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Wednesday, March 4, 2020 17:53
To: Slater, James (CHS) <james.slater@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: Re: MassPort LPR Cameras

Hi Jim,

Regarding the Massport cameras; in the early days of AVL we installed 39 Sierra wireless modem‘s in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don’t we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn’t have to do any firewall work either because they have a 166. and communicate like all of the MDT‘s . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.

We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.

Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.

> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>
> Thank you sir
>
> Major Charles W. Atchison III
> Troop F Commander
> Massachusetts State Police
> Director of Aviation Security
> 2 Service Road
> East Boston, Ma 02128
> Office: 617-568-7555
> Cell: 508-[redacted]
>
>

> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>
> All,
> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>
> Thanks
>
> CW
>
> From: Quinn, Dermot (POL)
> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
> Sent: Monday, February 10, 2020 10:31 AM
> To: Egnitz, Brian (POL)
> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
> Slater, James (CHS)
> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
> Robert (EOTSS)
> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
> Warmington, Scott (POL)
> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
> .us>>; Peek, Brian T. (EOTSS)
> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
> Timothy (EPS)
> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
> Michalski, Maria (EPS)
> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
> Christopher (POL)
> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
> Hughes, Sean M. (EOTSS)
> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
> Atchison, Charles (POL)
> <catchison@massport.com<mailto:catchison@massport.com>>
> Subject: RE: MassPort LPR Cameras
>
> Good Morning,
>
> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>
> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>
> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and

application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>
> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>
> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>
> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>
> I can’t overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security’s technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>
> Respectfully,
>
>
> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
> of Homeland Security & Preparedness Massachusetts State Police
> <image006.png>
>
>
>
>
> From: Egnitz, Brian (POL)
> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
> Sent: Friday, January 17, 2020 1:10 PM
> To: Slater, James (CHS)
> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
> Cc: Quinn, Dermot (POL)
> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
> Guerriero, Robert (EOTSS)
> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
> Brian T. (EOTSS)
> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
> Timothy (EPS)
> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
> Maria (EPS)
> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
> Subject: RE: MassPort LPR Cameras
>
> Hi Jim,

>
> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>
> -Brian
>
>
> From: Egnitz, Brian (POL)
> Sent: Monday, January 6, 2020 1:33 PM
> To: Slater, James (CHS)
> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
> Crary
> Subject: RE: MassPort LPR Cameras
>
> Hi Jim,
>
> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>
> Thanks Brian
>
>
> From: John Tedona [mailto:jtedona@neology.net]
> Sent: Monday, December 9, 2019 4:55 PM
> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS); Slater, James (CHS)
> Subject: RE: MassPort LPR Cameras
>
> Alex,
>
> I can be available most anytime tomorrow for a call.
>
>
> Regards,
>
> John Tedona
> PIPS TECHNOLOGY - A Neology Business
> Sales Manager
> 12760 Danielson Ct. Suite A
> Poway, CA 92064
> Phone: 201-841-6237
> Email: jtedona@neology.net<mailto:jtedona@neology.net>
> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ
> U2sB_fmM6g&e=>
>
>
> From: Chute, Alexander

> <AChute@massport.com<mailto:AChute@massport.com>>
> Sent: Monday, December 9, 2019 4:38 PM
> To: Egnitz, Brian (POL)
> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
> <pcrary@neology.net<mailto:pcrary@neology.net>>
> Cc: Guerriero, Robert (MASSIT)
> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
> Peek, Brian T. (EOTSS)
> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
> Timothy (EPS)
> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
> Slater III, James F (CHS)
> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
> Subject: RE: MassPort LPR Cameras
>
> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>
> Hello All,
>
> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>
> Respectfully,
>
> ~Alex
>
>
> <image007.png>
>
> Alexander B. Chute
> Program Manager, Public Safety Systems Massachusetts Port Authority
> Cell: [redacted]
> Office: 617.568.5942
> achute@massport.com<mailto:achute@massport.com>
>
> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>
>
>
> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
> Sent: Monday, November 18, 2019 3:26 PM
> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
> pcrary@neology.net<mailto:pcrary@neology.net>
> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
> Subject: RE: MassPort LPR Cameras
>
> Hi John, Peter
>

> Any issues with moving Massports cameras to the Chelsea DB?
>
> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>
> The current app server
> <image008.png>
>
> Current DB server
>
> <image009.png>
> <image010.png>
>
> Our current reads by month for about 66 active cameras
>
> Year
>
> Month
>
> Day
>
> Month Name
>
> Reads Count
>
> 2019
>
> 11
>
> 1
>
> November
>
> 495,113
>
> 2019
>
> 11
>
> 2
>
> November
>
> 472,907
>
> 2019
>
> 11
>
> 3
>
> November
>
> 384,409
>
> 2019
>
> 11

>
> 4
>
> November
>
> 411,440
>
> 2019
>
> 11
>
> 5
>
> November
>
> 434,085
>
> 2019
>
> 11
>
> 6
>
> November
>
> 495,537
>
> 2019
>
> 11
>
> 7
>
> November
>
> 444,123
>
> 2019
>
> 11
>
> 8
>
> November
>
> 542,492
>
> 2019
>
> 11
>
> 9
>
> November
>
> 443,463
>

> 2019
>
> 11
>
> 10
>
> November
>
> 389,514
>
> 2019
>
> 11
>
> 11
>
> November
>
> 362,548
>
> 2019
>
> 11
>
> 12
>
> November
>
> 236,539
>
>
>
>
>
> From: Chute, Alexander [mailto:AChute@massport.com]
> Sent: Wednesday, November 13, 2019 2:49 PM
> To: Egnitz, Brian (POL)
> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS)
> Subject: RE: MassPort LPR Cameras
>
> These stats are from the 18 active cameras we have in the system for this month:
>
> <image011.png>
>
> ~Alex
>
>
> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
> Sent: Tuesday, November 12, 2019 5:28 PM
> To: Chute, Alexander
> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS)
> Subject: RE: MassPort LPR Cameras
>
> Hi Alex,
>

> Can you please provide the updated reads per day? Previously you were interested in sharing 6 cameras at approximately 75,000 reads per day.
>
> Here is the P492 confi I mentioned.
>
> Set host to boss [redacted]
> Set image [redacted]
> Set number of [redacted]
> Set Ping interval [redacted]
> Set udp ping [redacted]
> Set ping wait time [redacted]
> Set security [redacted]
>
> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>
> -Brian
>
>
>
> From: Chute, Alexander [mailto:AChute@massport.com]
> Sent: Tuesday, November 12, 2019 2:08 PM
> To: Egnitz, Brian (POL)
> Subject: MassPort LPR Cameras
>
> Brian,
>
> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the Troop F building. I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the roadway cameras are fed to 2 primary network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have 18 cameras in production, with another 19 scheduled to come online within the next two months. I anticipate this number growing to approximately 50 fixed cameras within our campus over the next year. Let me know what you think the appropriate next steps would be.
>
> Respectfully,
>
> ~Alex
>
> <image007.png>
>
> Alexander B. Chute
> Program Manager, Public Safety Systems Massachusetts Port Authority
> Cell: [redacted]
> Office: 617.568.5942
> achute@massport.com<mailto:achute@massport.com>
>
> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>

From: Egnitz, Brian (POL)
To: Quinn, Dermot (POL)
Subject: RE: MassPort LPR Cameras
Date: Thursday, April 9, 2020 1:57:00 PM
Attachments: SierraQuoteForMassPort.pdf

Do you know if this was moved on? We need it for the MassPort modem project.

-----Original Message-----
From: Egnitz, Brian (POL)
Sent: Tuesday, March 10, 2020 10:52 AM
To: Quinn, Dermot (POL)
Subject: FW: MassPort LPR Cameras

Hi LTC.,

Can we order this equipment for the MassPort project?

Thanks, Brian

-----Original Message-----
From: Slater, James (CHS)
Sent: Tuesday, March 10, 2020 10:26 AM
To: Egnitz, Brian (POL)
Subject: RE: MassPort LPR Cameras

Hi, Brian!

This needs to go through MSP fiscal. They need to enter the purchase in OPAS.

Jim

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Tuesday, March 10, 2020 08:06
To: Slater, James (CHS) <james.slater@mass.gov>
Subject: RE: MassPort LPR Cameras

Is this something you can order or does it need to go through MSP?

-----Original Message-----
From: Slater, James (CHS)
Sent: Monday, March 9, 2020 10:36 AM
To: Egnitz, Brian (POL)
Subject: RE: MassPort LPR Cameras

Thanks, Brian...I will check with TSS.

Jim

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Monday, March 9, 2020 10:29
To: Slater, James (CHS) <james.slater@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>

Subject: RE: MassPort LPR Cameras

Thanks Jim,

I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need 6 sierra wireless AC adapters and 12 antennas. I have reached out to BCM for a quote.

I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.

I plan to cut one sector (5-6 cameras per sector) over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?

-Brian

-----Original Message-----
From: Slater, James (CHS)
Sent: Friday, March 6, 2020 1:43 PM
To: Egnitz, Brian (POL)
Cc: Quinn, Dermot (POL)
Subject: RE: MassPort LPR Cameras

Hi, Brian!

I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.

So, assuming you move forward with this, who would actually make this happen?

Thanks.

Jim

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Wednesday, March 4, 2020 17:53
To: Slater, James (CHS) <james.slater@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: Re: MassPort LPR Cameras

Hi Jim,

Regarding the Massport cameras; in the early days of AVL we installed 39 Sierra wireless modem‘s in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don’t we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn’t have to do any firewall work either because they have a 166. and communicate like all of the MDT‘s . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.

We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.

Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.

> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>
> Thank you sir
>
> Major Charles W. Atchison III
> Troop F Commander
> Massachusetts State Police
> Director of Aviation Security
> 2 Service Road
> East Boston, Ma 02128
> Office: 617-568-7555
> Cell: 508-[redacted]
>
>
> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>
> All,
> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>
> Thanks
>
> CW
>
> From: Quinn, Dermot (POL)
> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
> Sent: Monday, February 10, 2020 10:31 AM
> To: Egnitz, Brian (POL)
> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
> Slater, James (CHS)
> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
> Robert (EOTSS)
> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
> Warmington, Scott (POL)
> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
> .us>>; Peek, Brian T. (EOTSS)
> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
> Timothy (EPS)
> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
> Michalski, Maria (EPS)
> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
> Christopher (POL)
> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
> Hughes, Sean M. (EOTSS)
> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
> Atchison, Charles (POL)
> <catchison@massport.com<mailto:catchison@massport.com>>
> Subject: RE: MassPort LPR Cameras
>

> Good Morning,
>
> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>
> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>
> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>
> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>
> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>
> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>
> I can’t overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security’s technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>
> Respectfully,
>
>
> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
> of Homeland Security & Preparedness Massachusetts State Police
> <image006.png>
>
>
>
>
> From: Egnitz, Brian (POL)
> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
> Sent: Friday, January 17, 2020 1:10 PM
> To: Slater, James (CHS)
> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
> Cc: Quinn, Dermot (POL)

> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
> Guerriero, Robert (EOTSS)
> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
> Brian T. (EOTSS)
> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
> Timothy (EPS)
> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
> Maria (EPS)
> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
> Subject: RE: MassPort LPR Cameras
>
> Hi Jim,
>
> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>
> -Brian
>
>
> From: Egnitz, Brian (POL)
> Sent: Monday, January 6, 2020 1:33 PM
> To: Slater, James (CHS)
> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
> Crary
> Subject: RE: MassPort LPR Cameras
>
> Hi Jim,
>
> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>
> Thanks Brian
>
>
> From: John Tedona [mailto:jtedona@neology.net]
> Sent: Monday, December 9, 2019 4:55 PM
> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS); Slater, James (CHS)
> Subject: RE: MassPort LPR Cameras
>
> Alex,
>
> I can be available most anytime tomorrow for a call.
>
>
> Regards,
>
> John Tedona
> PIPS TECHNOLOGY - A Neology Business

> Sales Manager
> 12760 Danielson Ct. Suite A
> Poway, CA 92064
> Phone: 201-841-6237
> Email: jtedona@neology.net<mailto:jtedona@neology.net>
> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ
> U2sB_fmM6g&e=>
>
>
> From: Chute, Alexander
> <AChute@massport.com<mailto:AChute@massport.com>>
> Sent: Monday, December 9, 2019 4:38 PM
> To: Egnitz, Brian (POL)
> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
> <pcrary@neology.net<mailto:pcrary@neology.net>>
> Cc: Guerriero, Robert (MASSIT)
> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
> Peek, Brian T. (EOTSS)
> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
> Timothy (EPS)
> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
> Slater III, James F (CHS)
> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
> Subject: RE: MassPort LPR Cameras
>
> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>
> Hello All,
>
> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>
> Respectfully,
>
> ~Alex
>
>
> <image007.png>
>
> Alexander B. Chute
> Program Manager, Public Safety Systems Massachusetts Port Authority
> Cell: [redacted]
> Office: 617.568.5942
> achute@massport.com<mailto:achute@massport.com>
>
> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or

the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>
>
>
> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
> Sent: Monday, November 18, 2019 3:26 PM
> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
> pcrary@neology.net<mailto:pcrary@neology.net>
> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
> Subject: RE: MassPort LPR Cameras
>
> Hi John, Peter
>
> Any issues with moving Massports cameras to the Chelsea DB?
>
> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>
> The current app server
> <image008.png>
>
> Current DB server
>
> <image009.png>
> <image010.png>
>
> Our current reads by month for about 66 active cameras
>
> Year
>
> Month
>
> Day
>
> Month Name
>
> Reads Count
>
> 2019
>
> 11
>
> 1
>
> November
>
> 495,113
>
> 2019
>
> 11
>
> 2
>
> November
>

> 472,907
>
> 2019
>
> 11
>
> 3
>
> November
>
> 384,409
>
> 2019
>
> 11
>
> 4
>
> November
>
> 411,440
>
> 2019
>
> 11
>
> 5
>
> November
>
> 434,085
>
> 2019
>
> 11
>
> 6
>
> November
>
> 495,537
>
> 2019
>
> 11
>
> 7
>
> November
>
> 444,123
>
> 2019
>
> 11
>
> 8

>
> November
>
> 542,492
>
> 2019
>
> 11
>
> 9
>
> November
>
> 443,463
>
> 2019
>
> 11
>
> 10
>
> November
>
> 389,514
>
> 2019
>
> 11
>
> 11
>
> November
>
> 362,548
>
> 2019
>
> 11
>
> 12
>
> November
>
> 236,539
>
>
>
>
>
> From: Chute, Alexander [mailto:AChute@massport.com]
> Sent: Wednesday, November 13, 2019 2:49 PM
> To: Egnitz, Brian (POL)
> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS)
> Subject: RE: MassPort LPR Cameras
>
> These stats are from the 18 active cameras we have in the system for this month:

>
> <image011.png>
>
> ~Alex
>
>
> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
> Sent: Tuesday, November 12, 2019 5:28 PM
> To: Chute, Alexander
> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS)
> Subject: RE: MassPort LPR Cameras
>
> Hi Alex,
>
> Can you please provide the updated reads per day? Previously you were interested in sharing 6 cameras at approximately 75,000 reads per day.
>
> Here is the P492 confi I mentioned.
>
> Set host to boss G.L. c. 4.sec. 7.cl.26 (n)(security) G
> Set image G.L. c. 4.sec. 7.cl.26
> Set number of G.L. c. 4.sec. 7.cl.26 (n)(sec
> Set Ping interval G.L. c. 4.se
> Set udp ping G.L. c. 4.sec. 7.cl.26
> Set ping wait time G.L. c. 4.sec. 7.c
> Set security G.L. c. 4.sec. 7.cl.26
>
> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>
> -Brian
>
>
>
> From: Chute, Alexander [mailto:AChute@massport.com]
> Sent: Tuesday, November 12, 2019 2:08 PM
> To: Egnitz, Brian (POL)
> Subject: MassPort LPR Cameras
>
> Brian,
>
> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the Troop F building. I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the roadway cameras are fed to 2 primary network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have 18 cameras in production, with another 19 scheduled to come online within the next two months. I anticipate this number growing to approximately 50 fixed cameras within our campus over the next year. Let me know what you think the appropriate next steps would be.
>
> Respectfully,
>
> ~Alex

>
> <image007.png>
>
> Alexander B. Chute
> Program Manager, Public Safety Systems Massachusetts Port Authority
> Cell: [redacted]
> Office: 617.568.5942
> achute@massport.com<mailto:achute@massport.com>
>
> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>

From: Egnitz, Brian (POL)
To: Quinn, Dermot (POL)
Subject: RE: MassPort LPR Cameras
Date: Tuesday, March 31, 2020 8:12:00 AM
Attachments: SierraQuoteForMassPort.pdf

Do you know if this was moved on? We need it for the MassPort modem project.

-----Original Message-----
From: Egnitz, Brian (POL)
Sent: Tuesday, March 10, 2020 10:52 AM
To: Quinn, Dermot (POL)
Subject: FW: MassPort LPR Cameras

Hi LTC.,

Can we order this equipment for the MassPort project?

Thanks, Brian

-----Original Message-----
From: Slater, James (CHS)
Sent: Tuesday, March 10, 2020 10:26 AM
To: Egnitz, Brian (POL)
Subject: RE: MassPort LPR Cameras

Hi, Brian!

This needs to go through MSP fiscal. They need to enter the purchase in OPAS.

Jim

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Tuesday, March 10, 2020 08:06
To: Slater, James (CHS) <james.slater@mass.gov>
Subject: RE: MassPort LPR Cameras

Is this something you can order or does it need to go through MSP?

-----Original Message-----
From: Slater, James (CHS)
Sent: Monday, March 9, 2020 10:36 AM
To: Egnitz, Brian (POL)
Subject: RE: MassPort LPR Cameras

Thanks, Brian...I will check with TSS.

Jim

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Monday, March 9, 2020 10:29
To: Slater, James (CHS) <james.slater@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>

Subject: RE: MassPort LPR Cameras

Thanks Jim,

I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need 6 sierra wireless AC adapters and 12 antennas. I have reached out to BCM for a quote.

I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.

I plan to cut one sector (5-6 cameras per sector) over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?

-Brian

-----Original Message-----
From: Slater, James (CHS)
Sent: Friday, March 6, 2020 1:43 PM
To: Egnitz, Brian (POL)
Cc: Quinn, Dermot (POL)
Subject: RE: MassPort LPR Cameras

Hi, Brian!

I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.

So, assuming you move forward with this, who would actually make this happen?

Thanks.

Jim

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Wednesday, March 4, 2020 17:53
To: Slater, James (CHS) <james.slater@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: Re: MassPort LPR Cameras

Hi Jim,

Regarding the Massport cameras; in the early days of AVL we installed 39 Sierra wireless modem‘s in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don’t we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn’t have to do any firewall work either because they have a 166. and communicate like all of the MDT‘s . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.

We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.

Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.

> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>
> Thank you sir
>
> Major Charles W. Atchison III
> Troop F Commander
> Massachusetts State Police
> Director of Aviation Security
> 2 Service Road
> East Boston, Ma 02128
> Office: 617-568-7555
> Cell: 508-[redacted]
>
>
> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>
> All,
> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>
> Thanks
>
> CW
>
> From: Quinn, Dermot (POL)
> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
> Sent: Monday, February 10, 2020 10:31 AM
> To: Egnitz, Brian (POL)
> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
> Slater, James (CHS)
> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
> Robert (EOTSS)
> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
> Warmington, Scott (POL)
> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
> .us>>; Peek, Brian T. (EOTSS)
> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
> Timothy (EPS)
> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
> Michalski, Maria (EPS)
> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
> Christopher (POL)
> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
> Hughes, Sean M. (EOTSS)
> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
> Atchison, Charles (POL)
> <catchison@massport.com<mailto:catchison@massport.com>>
> Subject: RE: MassPort LPR Cameras
>

> Good Morning,
>
> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>
> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>
> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>
> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>
> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>
> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>
> I can’t overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security’s technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>
> Respectfully,
>
>
> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
> of Homeland Security & Preparedness Massachusetts State Police
> <image006.png>
>
>
>
>
> From: Egnitz, Brian (POL)
> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
> Sent: Friday, January 17, 2020 1:10 PM
> To: Slater, James (CHS)
> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
> Cc: Quinn, Dermot (POL)

> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
> Guerriero, Robert (EOTSS)
> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
> Brian T. (EOTSS)
> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
> Timothy (EPS)
> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
> Maria (EPS)
> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
> Subject: RE: MassPort LPR Cameras
>
> Hi Jim,
>
> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>
> -Brian
>
>
> From: Egnitz, Brian (POL)
> Sent: Monday, January 6, 2020 1:33 PM
> To: Slater, James (CHS)
> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
> Crary
> Subject: RE: MassPort LPR Cameras
>
> Hi Jim,
>
> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>
> Thanks Brian
>
>
> From: John Tedona [mailto:jtedona@neology.net]
> Sent: Monday, December 9, 2019 4:55 PM
> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS); Slater, James (CHS)
> Subject: RE: MassPort LPR Cameras
>
> Alex,
>
> I can be available most anytime tomorrow for a call.
>
>
> Regards,
>
> John Tedona
> PIPS TECHNOLOGY - A Neology Business

> Sales Manager
> 12760 Danielson Ct. Suite A
> Poway, CA 92064
> Phone: 201-841-6237
> Email: jtedona@neology.net<mailto:jtedona@neology.net>
> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ
> U2sB_fmM6g&e=>
>
>
> From: Chute, Alexander
> <AChute@massport.com<mailto:AChute@massport.com>>
> Sent: Monday, December 9, 2019 4:38 PM
> To: Egnitz, Brian (POL)
> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
> <pcrary@neology.net<mailto:pcrary@neology.net>>
> Cc: Guerriero, Robert (MASSIT)
> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
> Peek, Brian T. (EOTSS)
> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
> Timothy (EPS)
> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
> Slater III, James F (CHS)
> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
> Subject: RE: MassPort LPR Cameras
>
> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>
> Hello All,
>
> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>
> Respectfully,
>
> ~Alex
>
>
> <image007.png>
>
> Alexander B. Chute
> Program Manager, Public Safety Systems Massachusetts Port Authority
> Cell: [redacted]
> Office: 617.568.5942
> achute@massport.com<mailto:achute@massport.com>
>
> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or

the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>
>
>
> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
> Sent: Monday, November 18, 2019 3:26 PM
> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
> pcrary@neology.net<mailto:pcrary@neology.net>
> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
> Subject: RE: MassPort LPR Cameras
>
> Hi John, Peter
>
> Any issues with moving Massports cameras to the Chelsea DB?
>
> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>
> The current app server
> <image008.png>
>
> Current DB server
>
> <image009.png>
> <image010.png>
>
> Our current reads by month for about 66 active cameras
>
> Year
>
> Month
>
> Day
>
> Month Name
>
> Reads Count
>
> 2019
>
> 11
>
> 1
>
> November
>
> 495,113
>
> 2019
>
> 11
>
> 2
>
> November
>

> 472,907
>
> 2019
>
> 11
>
> 3
>
> November
>
> 384,409
>
> 2019
>
> 11
>
> 4
>
> November
>
> 411,440
>
> 2019
>
> 11
>
> 5
>
> November
>
> 434,085
>
> 2019
>
> 11
>
> 6
>
> November
>
> 495,537
>
> 2019
>
> 11
>
> 7
>
> November
>
> 444,123
>
> 2019
>
> 11
>
> 8

>
> November
>
> 542,492
>
> 2019
>
> 11
>
> 9
>
> November
>
> 443,463
>
> 2019
>
> 11
>
> 10
>
> November
>
> 389,514
>
> 2019
>
> 11
>
> 11
>
> November
>
> 362,548
>
> 2019
>
> 11
>
> 12
>
> November
>
> 236,539
>
>
>
>
>
> From: Chute, Alexander [mailto:AChute@massport.com]
> Sent: Wednesday, November 13, 2019 2:49 PM
> To: Egnitz, Brian (POL)
> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS)
> Subject: RE: MassPort LPR Cameras
>
> These stats are from the 18 active cameras we have in the system for this month:

>
> <image011.png>
>
> ~Alex
>
>
> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
> Sent: Tuesday, November 12, 2019 5:28 PM
> To: Chute, Alexander
> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS)
> Subject: RE: MassPort LPR Cameras
>
> Hi Alex,
>
> Can you please provide the updated reads per day? Previously you were interested in sharing 6 cameras at approximately 75,000 reads per day.
>
> Here is the P492 confi I mentioned.
>
> Set host to boss [redacted]
> Set image [redacted]
> Set number of [redacted]
> Set Ping interval [redacted]
> Set udp ping [redacted]
> Set ping wait time [redacted]
> Set security [redacted]
>
> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>
> -Brian
>
>
>
> From: Chute, Alexander [mailto:AChute@massport.com]
> Sent: Tuesday, November 12, 2019 2:08 PM
> To: Egnitz, Brian (POL)
> Subject: MassPort LPR Cameras
>
> Brian,
>
> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the Troop F building. I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the roadway cameras are fed to 2 primary network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have 18 cameras in production, with another 19 scheduled to come online within the next two months. I anticipate this number growing to approximately 50 fixed cameras within our campus over the next year. Let me know what you think the appropriate next steps would be.
>
> Respectfully,
>
> ~Alex

>
> <image007.png>
>
> Alexander B. Chute
> Program Manager, Public Safety Systems Massachusetts Port Authority
> Cell: [redacted]
> Office: 617.568.5942
> achute@massport.com<mailto:achute@massport.com>
>
> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>

From: Egnitz, Brian (POL)
To: Slater, James (CHS)
Subject: RE: MassPort LPR Cameras
Date: Tuesday, March 10, 2020 8:06:00 AM
Attachments: SierraQuoteForMassPort.pdf

Is this something you can order or does it need to go through MSP?

-----Original Message-----
From: Slater, James (CHS)
Sent: Monday, March 9, 2020 10:36 AM
To: Egnitz, Brian (POL)
Subject: RE: MassPort LPR Cameras

Thanks, Brian...I will check with TSS.

Jim

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Monday, March 9, 2020 10:29
To: Slater, James (CHS) <james.slater@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: RE: MassPort LPR Cameras

Thanks Jim,

I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need 6 sierra wireless AC adapters and 12 antennas. I have reached out to BCM for a quote.

I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.

I plan to cut one sector (5-6 cameras per sector) over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?

-Brian

-----Original Message-----
From: Slater, James (CHS)
Sent: Friday, March 6, 2020 1:43 PM
To: Egnitz, Brian (POL)
Cc: Quinn, Dermot (POL)
Subject: RE: MassPort LPR Cameras

Hi, Brian!

I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.

So, assuming you move forward with this, who would actually make this happen?

Thanks.

Jim

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Wednesday, March 4, 2020 17:53
To: Slater, James (CHS) <james.slater@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: Re: MassPort LPR Cameras

Hi Jim,

Regarding the Massport cameras; in the early days of AVL we installed 39 Sierra wireless modem‘s in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don’t we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn’t have to do any firewall work either because they have a 166. and communicate like all of the MDT‘s . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.

We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.

Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.

> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>
> Thank you sir
>
> Major Charles W. Atchison III
> Troop F Commander
> Massachusetts State Police
> Director of Aviation Security
> 2 Service Road
> East Boston, Ma 02128
> Office: 617-568-7555
> Cell: 508-[redacted]
>
>
> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>
> All,
> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>
> Thanks
>
> CW
>
> From: Quinn, Dermot (POL)
> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
> Sent: Monday, February 10, 2020 10:31 AM
> To: Egnitz, Brian (POL)
> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
> Slater, James (CHS)

> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
> Robert (EOTSS)
> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
> Warmington, Scott (POL)
> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
> .us>>; Peek, Brian T. (EOTSS)
> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
> Timothy (EPS)
> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
> Michalski, Maria (EPS)
> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
> Christopher (POL)
> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
> Hughes, Sean M. (EOTSS)
> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
> Atchison, Charles (POL)
> <catchison@massport.com<mailto:catchison@massport.com>>
> Subject: RE: MassPort LPR Cameras
>
> Good Morning,
>
> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>
> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>
> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>
> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>
> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>
> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of

our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>
> I can't overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security's technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>
> Respectfully,
>
>
> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
> of Homeland Security & Preparedness Massachusetts State Police
> <image006.png>
>
>
>
>
> From: Egnitz, Brian (POL)
> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
> Sent: Friday, January 17, 2020 1:10 PM
> To: Slater, James (CHS)
> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
> Cc: Quinn, Dermot (POL)
> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
> Guerriero, Robert (EOTSS)
> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
> Brian T. (EOTSS)
> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
> Timothy (EPS)
> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
> Maria (EPS)
> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
> Subject: RE: MassPort LPR Cameras
>
> Hi Jim,
>
> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>
> -Brian
>
>
> From: Egnitz, Brian (POL)
> Sent: Monday, January 6, 2020 1:33 PM
> To: Slater, James (CHS)
> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
> Crary
> Subject: RE: MassPort LPR Cameras
>
> Hi Jim,
>

> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>
> Thanks Brian
>
>
> From: John Tedona [mailto:jtedona@neology.net]
> Sent: Monday, December 9, 2019 4:55 PM
> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS); Slater, James (CHS)
> Subject: RE: MassPort LPR Cameras
>
> Alex,
>
> I can be available most anytime tomorrow for a call.
>
>
> Regards,
>
> John Tedona
> PIPS TECHNOLOGY - A Neology Business
> Sales Manager
> 12760 Danielson Ct. Suite A
> Poway, CA 92064
> Phone: 201-841-6237
> Email: jtedona@neology.net<mailto:jtedona@neology.net>
> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ
> U2sB_fmM6g&e=>
>
>
> From: Chute, Alexander
> <AChute@massport.com<mailto:AChute@massport.com>>
> Sent: Monday, December 9, 2019 4:38 PM
> To: Egnitz, Brian (POL)
> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
> <pcrary@neology.net<mailto:pcrary@neology.net>>
> Cc: Guerriero, Robert (MASSIT)
> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
> Peek, Brian T. (EOTSS)
> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
> Timothy (EPS)
> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
> Slater III, James F (CHS)
> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
> Subject: RE: MassPort LPR Cameras
>
> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless

you recognize the sender and know the content is safe.
>
> Hello All,
>
> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>
> Respectfully,
>
> ~Alex
>
>
> <image007.png>
>
> Alexander B. Chute
> Program Manager, Public Safety Systems Massachusetts Port Authority
> Cell: [redacted]
> Office: 617.568.5942
> achute@massport.com<mailto:achute@massport.com>
>
> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>
>
>
> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
> Sent: Monday, November 18, 2019 3:26 PM
> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
> pcrary@neology.net<mailto:pcrary@neology.net>
> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
> Subject: RE: MassPort LPR Cameras
>
> Hi John, Peter
>
> Any issues with moving Massports cameras to the Chelsea DB?
>
> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>
> The current app server
> <image008.png>
>
> Current DB server
>
> <image009.png>
> <image010.png>
>
> Our current reads by month for about 66 active cameras
>
> Year
>
> Month

>
> Day
>
> Month Name
>
> Reads Count
>
> 2019
>
> 11
>
> 1
>
> November
>
> 495,113
>
> 2019
>
> 11
>
> 2
>
> November
>
> 472,907
>
> 2019
>
> 11
>
> 3
>
> November
>
> 384,409
>
> 2019
>
> 11
>
> 4
>
> November
>
> 411,440
>
> 2019
>
> 11
>
> 5
>
> November
>
> 434,085
>

> 2019
>
> 11
>
> 6
>
> November
>
> 495,537
>
> 2019
>
> 11
>
> 7
>
> November
>
> 444,123
>
> 2019
>
> 11
>
> 8
>
> November
>
> 542,492
>
> 2019
>
> 11
>
> 9
>
> November
>
> 443,463
>
> 2019
>
> 11
>
> 10
>
> November
>
> 389,514
>
> 2019
>
> 11
>
> 11
>
> November

>
> 362,548
>
> 2019
>
> 11
>
> 12
>
> November
>
> 236,539
>
>
>
>
>
> From: Chute, Alexander [mailto:AChute@massport.com]
> Sent: Wednesday, November 13, 2019 2:49 PM
> To: Egnitz, Brian (POL)
> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS)
> Subject: RE: MassPort LPR Cameras
>
> These stats are from the 18 active cameras we have in the system for this month:
>
> <image011.png>
>
> ~Alex
>
>
> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
> Sent: Tuesday, November 12, 2019 5:28 PM
> To: Chute, Alexander
> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
> Timothy (EPS)
> Subject: RE: MassPort LPR Cameras
>
> Hi Alex,
>
> Can you please provide the updated reads per day? Previously you were interested in sharing 6 cameras at approximately 75,000 reads per day.
>
> Here is the P492 confi I mentioned.
>
> Set host to boss [redacted]
> Set image [redacted]
> Set number of [redacted]
> Set Ping interval [redacted]
> Set udp ping [redacted]
> Set ping wait time [redacted]
> Set security [redacted]
>
> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.

>
> -Brian
>
>
>
> From: Chute, Alexander [mailto:AChute@massport.com]
> Sent: Tuesday, November 12, 2019 2:08 PM
> To: Egnitz, Brian (POL)
> Subject: MassPort LPR Cameras
>
> Brian,
>
> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the Troop F building. I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the roadway cameras are fed to 2 primary network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have 18 cameras in production, with another 19 scheduled to come online within the next two months. I anticipate this number growing to approximately 50 fixed cameras within our campus over the next year. Let me know what you think the appropriate next steps would be.
>
> Respectfully,
>
> ~Alex
>
> <image007.png>
>
> Alexander B. Chute
> Program Manager, Public Safety Systems Massachusetts Port Authority
> Cell: [redacted]
> Office: 617.568.5942
> achute@massport.com<mailto:achute@massport.com>
>
> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>

From: Wood, Curtis (EOTSS)
To: Quinn, Dermot (POL); Egnitz, Brian (POL); Slater, James (CHS); Guerriero, Robert (EOTSS); Warmington, Scott (POL); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Michalski, Maria (EPS); Mason, Christopher (POL); Hughes, Sean M. (EOTSS); Peter Crary; Shaw, Harold; Ball, Richard (POL); Atchison, Charles (POL)
Subject: RE: MassPort LPR Cameras
Date: Tuesday, February 11, 2020 11:28:45 AM
Attachments: image006.png
image007.png
image008.png
image009.png
image010.png
image011.png

All,
Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.

Thanks

CW

From: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Sent: Monday, February 10, 2020 10:31 AM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Slater, James (CHS) <james.slater@mass.gov>; Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>; Warmington, Scott (POL) <Scott.Warmington@pol.state.ma.us>; Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; John Tedona <jtedona@neology.net>; Chute, Alexander <AChute@massport.com>; Michalski, Maria (EPS) <maria.michalski@mass.gov>; Mason, Christopher (POL) <Chris.Mason@pol.state.ma.us>; Hughes, Sean M. (EOTSS) <sean.hughes@mass.gov>; Peter Crary <pcrary@neology.net>; Wood, Curtis (EOTSS) <curtis.wood@mass.gov>; Shaw, Harold <HShaw@massport.com>; Ball, Richard (POL) <Richard.Ball@pol.state.ma.us>; Atchison, Charles (POL) <catchison@massport.com>
Subject: RE: MassPort LPR Cameras

Good Morning,

I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.

Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.

Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.

MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.

I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.

To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.

I can’t overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security’s technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.

Respectfully,

Lieutenant Colonel Dermot J. Quinn #1765
Division Commander
Division of Homeland Security & Preparedness
Massachusetts State Police

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, January 17, 2020 1:10 PM
To: Slater, James (CHS) <james.slater@mass.gov>

Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>; Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; John Tedona <jtedona@neology.net>; Chute, Alexander <AChute@massport.com>; Peter Crary <pcrary@neology.net>; Michalski, Maria (EPS) <maria.michalski@mass.gov>
Subject: RE: MassPort LPR Cameras

Hi Jim,

BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.

-Brian

From: Egnitz, Brian (POL)
Sent: Monday, January 6, 2020 1:33 PM
To: Slater, James (CHS)
Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter Crary
Subject: RE: MassPort LPR Cameras

Hi Jim,

We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?

Thanks Brian

From: John Tedona [mailto:jtedona@neology.net]
Sent: Monday, December 9, 2019 4:55 PM
To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); Slater, James (CHS)
Subject: RE: MassPort LPR Cameras

Alex,

I can be available most anytime tomorrow for a call.

Regards,

John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: Chute, Alexander <AChute@massport.com>
Sent: Monday, December 9, 2019 4:38 PM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; John Tedona <jtedona@neology.net>; Peter Crary <pcrary@neology.net>
Cc: Guerriero, Robert (MASSIT) <robert.guerriero@state.ma.us>; Peek, Brian T. (EOTSS) <brian.t.peek@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Slater III, James F (CHS) <james.slater@state.ma.us>
Subject: RE: MassPort LPR Cameras

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Hello All,

I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.

Respectfully,

~Alex

Alexander B. Chute

Program Manager, Public Safety Systems
Massachusetts Port Authority
Cell: [redacted]
Office: 617.568.5942
achute@massport.com

WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

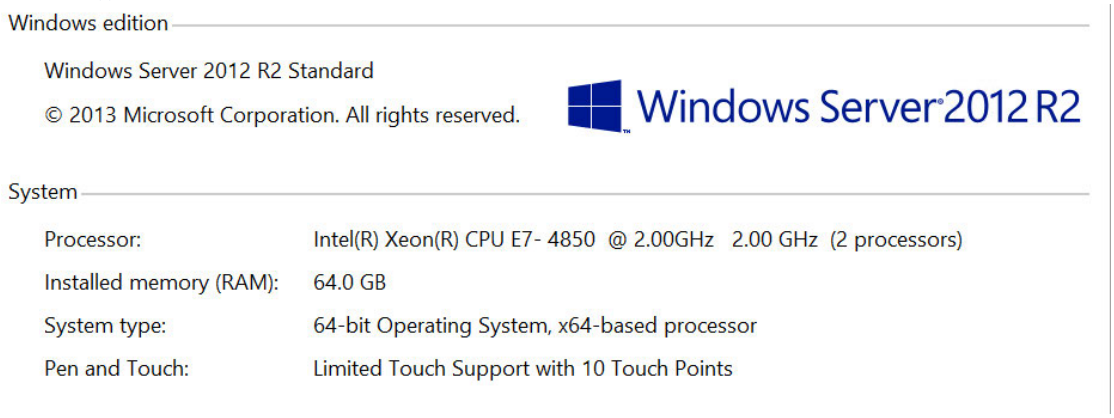
From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Monday, November 18, 2019 3:26 PM
To: John Tedona (jtedona@neology.net); pcrary@neology.net
Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
Subject: RE: MassPort LPR Cameras

Hi John, Peter

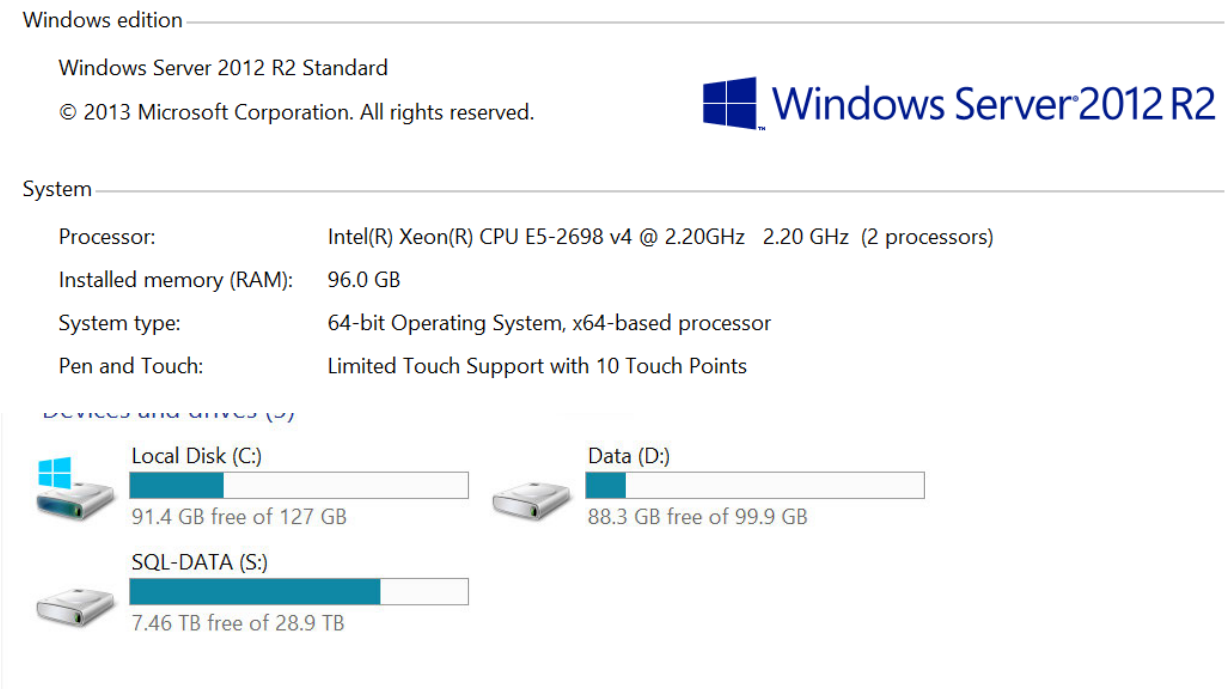
Any issues with moving Massports cameras to the Chelsea DB?

Using the Boss calculator, I estimate that we would need 9-10 TB of storage.

The current app server



Current DB server



Our current reads by month for about 66 active cameras

Year	Month	Day	Month Name	Reads Count
2019	11	1	November	495,113
2019	11	2	November	472,907
2019	11	3	November	384,409
2019	11	4	November	411,440
2019	11	5	November	434,085
2019	11	6	November	495,537
2019	11	7	November	444,123
2019	11	8	November	542,492
2019	11	9	November	443,463
2019	11	10	November	389,514
2019	11	11	November	362,548
2019	11	12	November	236,539

From: Chute, Alexander [mailto:AChute@massport.com]
Sent: Wednesday, November 13, 2019 2:49 PM
To: Egnitz, Brian (POL)
Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
Subject: RE: MassPort LPR Cameras

These stats are from the 18 active cameras we have in the system for this month:

Month	Day	Total Scans
⊟ November		
	1	169551
	2	115486
	3	169178
	4	201136
	5	162319
	6	171825
	7	192996
	8	202159
	9	136410
	10	165834
	11	193613
	12	183947

~Alex

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Tuesday, November 12, 2019 5:28 PM
To: Chute, Alexander
Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
Subject: RE: MassPort LPR Cameras

Hi Alex,

Can you please provide the updated reads per day? Previously you were interested in sharing 6 cameras at approximately 75,000 reads per day.

Here is the P492 confi I mentioned.

Set host to boss [redacted]
Set image [redacted]
Set number of [redacted]
Set Ping interval [redacted]
Set udp ping [redacted]
Set ping wait time [redacted]
Set security [redacted]

I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.

For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.

-Brian

From: Chute, Alexander [mailto:AChute@massport.com]
Sent: Tuesday, November 12, 2019 2:08 PM
To: Egnitz, Brian (POL)
Subject: MassPort LPR Cameras

Brian,

Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the Troop F building. I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the roadway cameras are fed to 2 primary network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have 18 cameras in production, with another 19 scheduled to come online within the next two months. I anticipate this number growing to approximately 50 fixed cameras within our campus over the next year. Let me know what you think the appropriate next steps would be.

Respectfully,

~Alex

Alexander B. Chute
Program Manager, Public Safety Systems
Massachusetts Port Authority
Cell: [redacted]
Office: 617.568.5942
achute@massport.com

WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

From: Chen, Kwang
To: Shaw, Harold; Quinn, Dermot (POL); Egnitz, Brian (POL); Slater, James (CHS); Guerriero, Robert (EOTSS); Warmington, Scott (POL); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Michalski, Maria (EPS); Mason, Christopher (POL); Hughes, Sean M. (EOTSS); Peter Crary; Wood, Curtis (EOTSS); Ball, Richard (POL); Atchison, Charles (POL); Haverty, Robert
Subject: RE: MassPort LPR Cameras
Date: Monday, February 10, 2020 12:55:08 PM
Attachments: image002.png
image003.png
image004.png
image005.png
image006.png
image007.png

Team – We will fully support MSP in the transition of LPR data to the DCJIS BOSS server in Chelsea when the timing is appropriate.

Kwang

Information Technology
Massachusetts Port Authority
One Harborside Drive, Suite 200S
East Boston, MA 02128-2909

617.568.5939
kchen@massport.com

From: Shaw, Harold <HShaw@massport.com>
Sent: Monday, February 10, 2020 11:26 AM
To: Quinn, Dermot (POL) <dermot.quinn@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Slater, James (CHS) <james.slater@state.ma.us>; Guerriero, Robert (MASSIT) <robert.guerriero@state.ma.us>; Warmington, Scott (POL) <scott.warmington@state.ma.us>; Peek, Brian T (MASSIT) <brian.t.peek@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; John Tedona <jtedona@neology.net>; Chute, Alexander <AChute@massport.com>; Michalski, Maria (EPS) <maria.michalski@state.ma.us>; Mason, Chris (POL) <chris.mason@state.ma.us>; Hughes, Sean (MASSIT) <sean.hughes@state.ma.us>; Peter Crary <pcrary@neology.net>; Wood, Curtis (EOTSS) <curtis.wood@state.ma.us>; Richard Ball <Richard.Ball@state.ma.us>; Atchison, Charles W <CAtchison@massport.com>; Chen, Kwang <KChen@massport.com>; Haverty, Robert <RHaverty@massport.com>
Subject: RE: MassPort LPR Cameras

LTC Quinn,

From my perspective, you've clearly laid out the issues at hand. I couldn't agree more with your characterization of the significance that ALPR technology plays as part of the layered security at Logan, but I also understand the greater benefits of integrating these systems to best support MSP and LE efforts across the greater Commonwealth. As we know, ALPR plays an important role in both proactive and reactive investigations, and the value of finding the best mechanism to integrate not only makes sense, promotes better use of the technology, but ultimately better protects a system put in-place specifically for law enforcement purposes. For all intense and purposes, having a separate "stand alone" system at Logan is inefficient, especially when the primary end users at Logan are from MSP Troop F.

I know there have been a number of discussions on this matter, and I believe finding a viable solution is important to all stakeholders. I've included Massport's CIO Kwang Chen and Bob Haverty, Director of IT – Aviation Systems, into the discussion to share any thoughts they may have from a Massport IT perspective.

Thanks

Hank

From: Quinn, Dermot (POL) <dermot.quinn@state.ma.us>
Sent: Monday, February 10, 2020 10:31 AM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Slater, James (CHS) <james.slater@state.ma.us>; Guerriero, Robert (MASSIT) <robert.guerriero@state.ma.us>; Warmington, Scott (POL) <scott.warmington@state.ma.us>; Peek, Brian T (MASSIT) <brian.t.peek@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; John Tedona <jtedona@neology.net>; Chute, Alexander <AChute@massport.com>; Michalski, Maria (EPS) <maria.michalski@state.ma.us>; Mason, Chris (POL) <chris.mason@state.ma.us>; Hughes, Sean (MASSIT) <sean.hughes@state.ma.us>; Peter Crary <pcrary@neology.net>; Wood, Curtis (EOTSS) <curtis.wood@state.ma.us>; Shaw, Harold <HShaw@massport.com>; Richard Ball <Richard.Ball@state.ma.us>; Atchison, Charles W <CAtchison@massport.com>
Subject: RE: MassPort LPR Cameras

Good Morning,

I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.

Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.

Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as "BOSS" and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport's cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.

MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.

I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.

To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.

I can't overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security's technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.

Respectfully,

Lieutenant Colonel Dermot J. Quinn #1765
Division Commander
Division of Homeland Security & Preparedness
Massachusetts State Police

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, January 17, 2020 1:10 PM
To: Slater, James (CHS) <james.slater@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>; Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; John Tedona <jtedona@neology.net>; Chute, Alexander <AChute@massport.com>; Peter Crary <pcrary@neology.net>; Michalski, Maria (EPS) <maria.michalski@mass.gov>
Subject: RE: MassPort LPR Cameras

Hi Jim,

BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.

-Brian

From: Egnitz, Brian (POL)
Sent: Monday, January 6, 2020 1:33 PM
To: Slater, James (CHS)
Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter Crary
Subject: RE: MassPort LPR Cameras

Hi Jim,

We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?

Thanks Brian

From: John Tedona [mailto:jtedona@neology.net]
Sent: Monday, December 9, 2019 4:55 PM
To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); Slater, James (CHS)
Subject: RE: MassPort LPR Cameras

Alex,

I can be available most anytime tomorrow for a call.

Regards,

John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager
12760 Danielson Ct. Suite A

Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: Chute, Alexander <AChute@massport.com>
Sent: Monday, December 9, 2019 4:38 PM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; John Tedona <jtedona@neology.net>; Peter Crary <pcrary@neology.net>
Cc: Guerriero, Robert (MASSIT) <robert.guerriero@state.ma.us>; Peek, Brian T. (EOTSS) <brian.t.peek@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Slater III, James F (CHS) <james.slater@state.ma.us>
Subject: RE: MassPort LPR Cameras

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Hello All,

I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.

Respectfully,

~Alex

Alexander B. Chute
Program Manager, Public Safety Systems
Massachusetts Port Authority
Cell: [redacted]
Office: 617.568.5942
achute@massport.com

WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

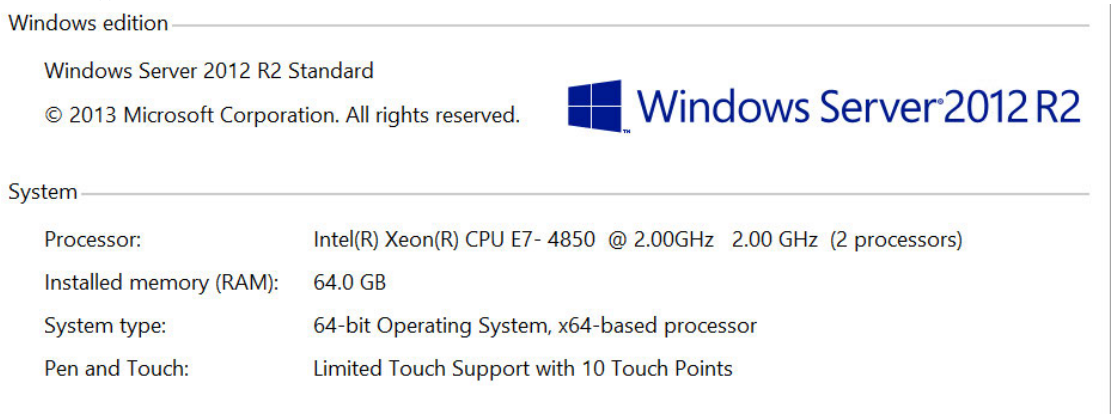
From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Monday, November 18, 2019 3:26 PM
To: John Tedona (jtedona@neology.net); pcrary@neology.net
Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
Subject: RE: MassPort LPR Cameras

Hi John, Peter

Any issues with moving Massports cameras to the Chelsea DB?

Using the Boss calculator, I estimate that we would need 9-10 TB of storage.

The current app server



Current DB server

Windows edition

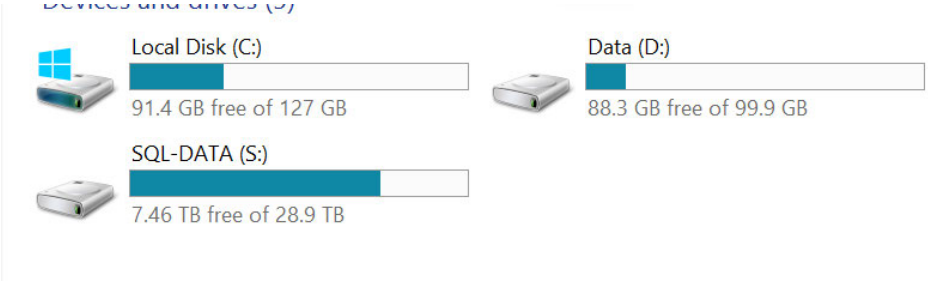
Windows Server 2012 R2 Standard

© 2013 Microsoft Corporation. All rights reserved.

Windows Server 2012 R2

System

Processor:	Intel(R) Xeon(R) CPU E5-2698 v4 @ 2.20GHz 2.20 GHz (2 processors)
Installed memory (RAM):	96.0 GB
System type:	64-bit Operating System, x64-based processor
Pen and Touch:	Limited Touch Support with 10 Touch Points



Our current reads by month for about 66 active cameras

Year	Month	Day	Month Name	Reads Count
2019	11	1	November	495,113
2019	11	2	November	472,907
2019	11	3	November	384,409
2019	11	4	November	411,440
2019	11	5	November	434,085
2019	11	6	November	495,537
2019	11	7	November	444,123
2019	11	8	November	542,492
2019	11	9	November	443,463
2019	11	10	November	389,514
2019	11	11	November	362,548
2019	11	12	November	236,539

From: Chute, Alexander [mailto:AChute@massport.com]
Sent: Wednesday, November 13, 2019 2:49 PM
To: Egnitz, Brian (POL)
Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
Subject: RE: MassPort LPR Cameras

These stats are from the 18 active cameras we have in the system for this month:

Month	Day	Total Scans
⊟ November		
	1	169551
	2	115486
	3	169178
	4	201136
	5	162319
	6	171825
	7	192996
	8	202159
	9	136410
	10	165834
	11	193613
	12	183947

~Alex

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Tuesday, November 12, 2019 5:28 PM
To: Chute, Alexander
Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
Subject: RE: MassPort LPR Cameras

Hi Alex,

Can you please provide the updated reads per day? Previously you were interested in sharing 6 cameras at approximately 75,000 reads per day.

Here is the P492 confi I mentioned.

Set host to boss G.L. c. 4.sec. 7.cl.26 (n)
Set image G.L. c. 4.sec. 7
Set number of G.L. c. 4.sec. 7.cl.2
Set Ping interval G.L. c. 4
Set udp ping G.L. c. 4.sec. 7
Set ping wait time G.L. c. 4.sec
Set security G.L. c. 4.sec. 7

I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.

-Brian

From: Chute, Alexander [mailto:AChute@massport.com]
Sent: Tuesday, November 12, 2019 2:08 PM
To: Egnitz, Brian (POL)
Subject: MassPort LPR Cameras

Brian,

Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the Troop F building. I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the roadway cameras are fed to 2 primary network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have 18 cameras in production, with another 19 scheduled to come online within the next two months. I anticipate this number growing to approximately 50 fixed cameras within our campus over the next year. Let me know what you think the appropriate next steps would be.

Respectfully,

~Alex

Alexander B. Chute
Program Manager, Public Safety Systems
Massachusetts Port Authority
Cell: G.L. c. 4.sec. 7.cl.26
Office: 617.568.5942

achute@massport.com

WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

From: Shaw, Harold
To: Quinn, Dermot (POL); Egnitz, Brian (POL); Slater, James (CHS); Guerriero, Robert (EOTSS); Warmington, Scott (POL); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Michalski, Maria (EPS); Mason, Christopher (POL); Hughes, Sean M. (EOTSS); Peter Crary; Wood, Curtis (EOTSS); Ball, Richard (POL); Atchison, Charles (POL); Chen, Kwang; Haverty, Robert
Subject: RE: MassPort LPR Cameras
Date: Monday, February 10, 2020 11:25:45 AM
Attachments: image006.png
image007.png
image008.png
image009.png
image010.png
image011.png

LTC Quinn,

From my perspective, you've clearly laid out the issues at hand. I couldn't agree more with your characterization of the significance that ALPR technology plays as part of the layered security at Logan, but I also understand the greater benefits of integrating these systems to best support MSP and LE efforts across the greater Commonwealth. As we know, ALPR plays an important role in both proactive and reactive investigations, and the value of finding the best mechanism to integrate not only makes sense, promotes better use of the technology, but ultimately better protects a system put in-place specifically for law enforcement purposes. For all intense and purposes, having a separate "stand alone" system at Logan is inefficient, especially when the primary end users at Logan are from MSP Troop F.

I know there have been a number of discussions on this matter, and I believe finding a viable solution is important to all stakeholders. I've included Massport's CIO Kwang Chen and Bob Haverty, Director of IT – Aviation Systems, into the discussion to share any thoughts they may have from a Massport IT perspective.

Thanks

Hank

From: Quinn, Dermot (POL) <dermot.quinn@state.ma.us>
Sent: Monday, February 10, 2020 10:31 AM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Slater, James (CHS) <james.slater@state.ma.us>; Guerriero, Robert (MASSIT) <robert.guerriero@state.ma.us>; Warmington, Scott (POL) <scott.warmington@state.ma.us>; Peek, Brian T (MASSIT) <brian.t.peek@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; John Tedona <jtedona@neology.net>; Chute, Alexander <AChute@massport.com>; Michalski, Maria (EPS) <maria.michalski@state.ma.us>; Mason, Chris (POL) <chris.mason@state.ma.us>; Hughes, Sean (MASSIT) <sean.hughes@state.ma.us>; Peter Crary <pcrary@neology.net>; Wood, Curtis (EOTSS) <curtis.wood@state.ma.us>; Shaw, Harold <HShaw@massport.com>; Richard Ball <Richard.Ball@state.ma.us>; Atchison, Charles W <CAtchison@massport.com>
Subject: RE: MassPort LPR Cameras

Good Morning,

I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.

Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.

Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as "BOSS" and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport's cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.

MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.

I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.

To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.

I can't overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security's technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.

Respectfully,

Lieutenant Colonel Dermot J. Quinn #1765
Division Commander
Division of Homeland Security & Preparedness
Massachusetts State Police

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, January 17, 2020 1:10 PM
To: Slater, James (CHS) <james.slater@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>; Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; John Tedona <jtedona@neology.net>; Chute, Alexander <AChute@massport.com>; Peter Crary <pcrary@neology.net>; Michalski, Maria (EPS) <maria.michalski@mass.gov>
Subject: RE: MassPort LPR Cameras

Hi Jim,

BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.

-Brian

From: Egnitz, Brian (POL)
Sent: Monday, January 6, 2020 1:33 PM
To: Slater, James (CHS)
Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter Crary
Subject: RE: MassPort LPR Cameras

Hi Jim,

We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?

Thanks Brian

From: John Tedona [mailto:jtedona@neology.net]
Sent: Monday, December 9, 2019 4:55 PM
To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); Slater, James (CHS)
Subject: RE: MassPort LPR Cameras

Alex,

I can be available most anytime tomorrow for a call.

Regards,

John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: Chute, Alexander <AChute@massport.com>
Sent: Monday, December 9, 2019 4:38 PM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; John Tedona <jtedona@neology.net>; Peter Crary <pcrary@neology.net>
Cc: Guerriero, Robert (MASSIT) <robert.guerriero@state.ma.us>; Peek, Brian T. (EOTSS) <brian.t.peek@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Slater III, James F (CHS) <james.slater@state.ma.us>
Subject: RE: MassPort LPR Cameras

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Hello All,

I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call

to discuss the details.

Respectfully,

~Alex

Alexander B. Chute
Program Manager, Public Safety Systems
Massachusetts Port Authority
Cell: [redacted]
Office: 617.568.5942
achute@massport.com

WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Monday, November 18, 2019 3:26 PM
To: John Tedona (jtedona@neology.net); pcrary@neology.net
Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
Subject: RE: MassPort LPR Cameras

Hi John, Peter

Any issues with moving Massports cameras to the Chelsea DB?

Using the Boss calculator, I estimate that we would need 9-10 TB of storage.

The current app server

Windows edition

Windows Server 2012 R2 Standard

© 2013 Microsoft Corporation. All rights reserved.

Windows Server 2012 R2

System

Processor:	Intel(R) Xeon(R) CPU E7- 4850 @ 2.00GHz 2.00 GHz (2 processors)
Installed memory (RAM):	64.0 GB
System type:	64-bit Operating System, x64-based processor
Pen and Touch:	Limited Touch Support with 10 Touch Points

Current DB server

Windows edition

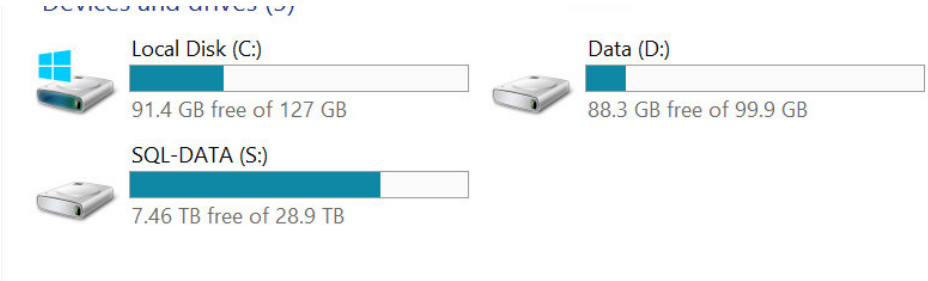
Windows Server 2012 R2 Standard

© 2013 Microsoft Corporation. All rights reserved.

Windows Server 2012 R2

System

Processor:	Intel(R) Xeon(R) CPU E5-2698 v4 @ 2.20GHz 2.20 GHz (2 processors)
Installed memory (RAM):	96.0 GB
System type:	64-bit Operating System, x64-based processor
Pen and Touch:	Limited Touch Support with 10 Touch Points



Our current reads by month for about 66 active cameras

Year	Month	Day	Month Name	Reads Count
2019	11	1	November	495,113
2019	11	2	November	472,907
2019	11	3	November	384,409
2019	11	4	November	411,440
2019	11	5	November	434,085
2019	11	6	November	495,537
2019	11	7	November	444,123
2019	11	8	November	542,492
2019	11	9	November	443,463
2019	11	10	November	389,514
2019	11	11	November	362,548
2019	11	12	November	236,539

From: Chute, Alexander [mailto:AChute@massport.com]
Sent: Wednesday, November 13, 2019 2:49 PM
To: Egnitz, Brian (POL)
Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
Subject: RE: MassPort LPR Cameras

These stats are from the 18 active cameras we have in the system for this month:

Month	Day	Total Scans
⊟ November		
	1	169551
	2	115486
	3	169178
	4	201136
	5	162319
	6	171825
	7	192996
	8	202159
	9	136410
	10	165834
	11	193613
	12	183947

~Alex

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Tuesday, November 12, 2019 5:28 PM
To: Chute, Alexander
Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
Subject: RE: MassPort LPR Cameras

Hi Alex,

Can you please provide the updated reads per day? Previously you were interested in sharing 6 cameras at approximately 75,000 reads per day.

Here is the P492 confi I mentioned.

Set host to boss [redacted]
Set image [redacted]
Set number of [redacted]
Set Ping interval [redacted]
Set udp ping [redacted]
Set ping wait time [redacted]
Set security [redacted]

I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.

-Brian

From: Chute, Alexander [mailto:AChute@massport.com]
Sent: Tuesday, November 12, 2019 2:08 PM
To: Egnitz, Brian (POL)
Subject: MassPort LPR Cameras

Brian,

Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the Troop F building. I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the roadway cameras are fed to 2 primary network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have 18 cameras in production, with another 19 scheduled to come online within the next two months. I anticipate this number growing to approximately 50 fixed cameras within our campus over the next year. Let me know what you think the appropriate next steps would be.

Respectfully,

~Alex

Alexander B. Chute
Program Manager, Public Safety Systems
Massachusetts Port Authority
Cell: [redacted]
Office: 617.568.5942
achute@massport.com

WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

From: Quinn, Dermot (POL)
To: Egnitz, Brian (POL); Slater, James (CHS); Guerriero, Robert (EOTSS); Warmington, Scott (POL); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Michalski, Maria (EPS); Mason, Christopher (POL); Hughes, Sean M. (EOTSS); Peter Crary; Wood, Curtis (EOTSS); Shaw, Harold; Ball, Richard (POL); Atchison, Charles (POL)
Subject: RE: MassPort LPR Cameras
Date: Monday, February 10, 2020 10:31:07 AM
Attachments: image001.png
image002.png
image003.png
image004.png
image005.png
image006.png

Good Morning,

I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.

Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.

Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.

MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.

I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.

To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.

I can’t overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security’s technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.

Respectfully,

Lieutenant Colonel Dermot J. Quinn #1765
Division Commander
Division of Homeland Security & Preparedness
Massachusetts State Police

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, January 17, 2020 1:10 PM
To: Slater, James (CHS) <james.slater@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>; Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; John Tedona <jtedona@neology.net>; Chute, Alexander <AChute@massport.com>; Peter Crary <pcrary@neology.net>; Michalski, Maria (EPS) <maria.michalski@mass.gov>
Subject: RE: MassPort LPR Cameras

Hi Jim,

BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system’s software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.

-Brian

From: Egnitz, Brian (POL)
Sent: Monday, January 6, 2020 1:33 PM
To: Slater, James (CHS)
Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter Crary
Subject: RE: MassPort LPR Cameras

Hi Jim,

We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?

Thanks Brian

From: John Tedona [mailto:jtedona@neology.net]
Sent: Monday, December 9, 2019 4:55 PM
To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); Slater, James (CHS)
Subject: RE: MassPort LPR Cameras

Alex,

I can be available most anytime tomorrow for a call.

Regards,

John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: Chute, Alexander <AChute@massport.com>
Sent: Monday, December 9, 2019 4:38 PM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; John Tedona <jtedona@neology.net>; Peter Crary <pcrary@neology.net>
Cc: Guerriero, Robert (MASSIT) <robert.guerriero@state.ma.us>; Peek, Brian T. (EOTSS) <brian.t.peek@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Slater III, James F (CHS) <james.slater@state.ma.us>
Subject: RE: MassPort LPR Cameras

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Hello All,

I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.

Respectfully,

~Alex

Alexander B. Chute
Program Manager, Public Safety Systems
Massachusetts Port Authority
Cell: [redacted]
Office: 617.568.5942
achute@massport.com

WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Monday, November 18, 2019 3:26 PM
To: John Tedona (jtedona@neology.net); pcrary@neology.net
Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
Subject: RE: MassPort LPR Cameras

Hi John, Peter

Any issues with moving Massports cameras to the Chelsea DB?

Using the Boss calculator, I estimate that we would need 9-10 TB of storage.

The current app server

Windows edition

Windows Server 2012 R2 Standard

© 2013 Microsoft Corporation. All rights reserved.

Windows Server 2012 R2

System

Processor:	Intel(R) Xeon(R) CPU E7- 4850 @ 2.00GHz 2.00 GHz (2 processors)
Installed memory (RAM):	64.0 GB
System type:	64-bit Operating System, x64-based processor
Pen and Touch:	Limited Touch Support with 10 Touch Points

Current DB server

Windows edition

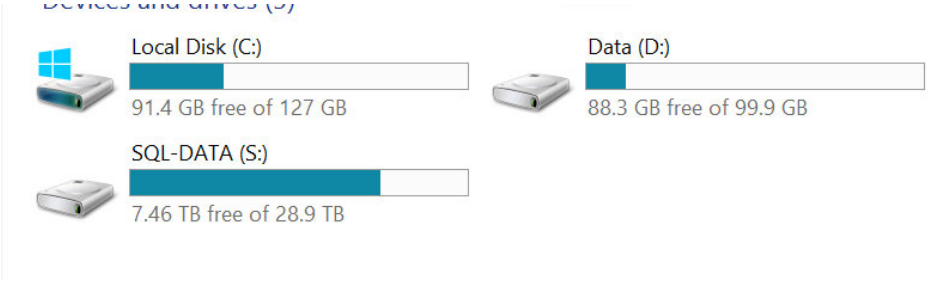
Windows Server 2012 R2 Standard

© 2013 Microsoft Corporation. All rights reserved.

Windows Server 2012 R2

System

Processor:	Intel(R) Xeon(R) CPU E5-2698 v4 @ 2.20GHz 2.20 GHz (2 processors)
Installed memory (RAM):	96.0 GB
System type:	64-bit Operating System, x64-based processor
Pen and Touch:	Limited Touch Support with 10 Touch Points



Our current reads by month for about 66 active cameras

Year	Month	Day	Month Name	Reads Count
2019	11	1	November	495,113
2019	11	2	November	472,907
2019	11	3	November	384,409
2019	11	4	November	411,440
2019	11	5	November	434,085
2019	11	6	November	495,537
2019	11	7	November	444,123
2019	11	8	November	542,492

2019	11	9	November	443,463
2019	11	10	November	389,514
2019	11	11	November	362,548
2019	11	12	November	236,539

From: Chute, Alexander [mailto:AChute@massport.com]
Sent: Wednesday, November 13, 2019 2:49 PM
To: Egnitz, Brian (POL)
Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
Subject: RE: MassPort LPR Cameras

These stats are from the 18 active cameras we have in the system for this month:

Month	Day	Total Scans
⊟ November		
	1	169551
	2	115486
	3	169178
	4	201136
	5	162319
	6	171825
	7	192996
	8	202159
	9	136410
	10	165834
	11	193613
	12	183947

~Alex

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Tuesday, November 12, 2019 5:28 PM
To: Chute, Alexander
Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
Subject: RE: MassPort LPR Cameras

Hi Alex,

Can you please provide the updated reads per day? Previously you were interested in sharing 6 cameras at approximately 75,000 reads per day.

Here is the P492 confi I mentioned.

Set host to boss [redacted]
Set image [redacted]
Set number of [redacted]
Set Ping interval [redacted]
Set udp ping [redacted]
Set ping wait time [redacted]
Set security [redacted]

I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.

-Brian

From: Chute, Alexander [mailto:AChute@massport.com]
Sent: Tuesday, November 12, 2019 2:08 PM
To: Egnitz, Brian (POL)
Subject: MassPort LPR Cameras

Brian,

Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the Troop F building. I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the roadway cameras are fed to 2 primary network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations.

Currently we have 18 cameras in production, with another 19 scheduled to come online within the next two months. I anticipate this number growing to approximately 50 fixed cameras within our campus over the next year. Let me know what you think the appropriate next steps would be.

Respectfully,

~Alex

Alexander B. Chute
Program Manager, Public Safety Systems
Massachusetts Port Authority
Cell: [redacted]
Office: 617.568.5942
achute@massport.com

WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

From: Mason, Christopher (POL)
To: Wood, Curtis (EOTSS)
Subject: Re: MassPort LPR Cameras
Date: Tuesday, February 11, 2020 11:59:27 AM
Attachments: image006.png
image007.png
image008.png
image009.png
image010.png
image011.png

Thank you.

Colonel Christopher Mason
Superintendent
Massachusetts State Police

On Feb 11, 2020, at 11:28 AM, Wood, Curtis (EOTSS) <curtis.wood@mass.gov> wrote:

All,
Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.

Thanks

CW

From: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Sent: Monday, February 10, 2020 10:31 AM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Slater, James (CHS) <james.slater@mass.gov>; Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>; Warmington, Scott (POL) <Scott.Warmington@pol.state.ma.us>; Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; John Tedona <jtedona@neology.net>; Chute, Alexander <AChute@massport.com>; Michalski, Maria (EPS) <maria.michalski@mass.gov>; Mason, Christopher (POL) <Chris.Mason@pol.state.ma.us>; Hughes, Sean M. (EOTSS) <sean.hughes@mass.gov>; Peter Crary <pcrary@neology.net>; Wood, Curtis (EOTSS) <curtis.wood@mass.gov>; Shaw, Harold <HShaw@massport.com>; Ball, Richard (POL) <Richard.Ball@pol.state.ma.us>; Atchison, Charles (POL) <catchison@massport.com>
Subject: RE: MassPort LPR Cameras

Good Morning,

I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.

Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.

Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.

MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.

I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.

To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.

I can’t overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR

data from Massport facilities would be a significant addition to the MSP Division of Homeland Security's technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.

Respectfully,

Lieutenant Colonel Dermot J. Quinn #1765
Division Commander
Division of Homeland Security & Preparedness
Massachusetts State Police
<image006.png>

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, January 17, 2020 1:10 PM
To: Slater, James (CHS) <james.slater@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>; Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; John Tedona <jtedona@neology.net>; Chute, Alexander <AChute@massport.com>; Peter Crary <pcrary@neology.net>; Michalski, Maria (EPS) <maria.michalski@mass.gov>
Subject: RE: MassPort LPR Cameras

Hi Jim,

BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.

-Brian

From: Egnitz, Brian (POL)
Sent: Monday, January 6, 2020 1:33 PM
To: Slater, James (CHS)
Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter Crary
Subject: RE: MassPort LPR Cameras

Hi Jim,

We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR

server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?

Thanks Brian

From: John Tedona [mailto:jtedona@neology.net]
Sent: Monday, December 9, 2019 4:55 PM
To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); Slater, James (CHS)
Subject: RE: MassPort LPR Cameras

Alex,

I can be available most anytime tomorrow for a call.

Regards,

John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: Chute, Alexander <AChute@massport.com>
Sent: Monday, December 9, 2019 4:38 PM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; John Tedona <jtedona@neology.net>; Peter Crary <pcrary@neology.net>
Cc: Guerriero, Robert (MASSIT) <robert.guerriero@state.ma.us>; Peek, Brian T. (EOTSS) <brian.t.peek@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Slater III, James F (CHS) <james.slater@state.ma.us>
Subject: RE: MassPort LPR Cameras

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Hello All,

I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.

Respectfully,

~Alex

<image007.png>

Alexander B. Chute
Program Manager, Public Safety Systems
Massachusetts Port Authority
Cell: [redacted]
Office: 617.568.5942
achute@massport.com

WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Monday, November 18, 2019 3:26 PM
To: John Tedona (jtedona@neology.net); pcrary@neology.net
Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
Subject: RE: MassPort LPR Cameras

Hi John, Peter

Any issues with moving Massports cameras to the Chelsea DB?

Using the Boss calculator, I estimate that we would need 9-10 TB of storage.

The current app server

<image008.png>

Current DB server

<image009.png>

<image010.png>

Our current reads by month for about 66 active cameras

Year	Month	Day	Month Name	Reads Count
2019	11	1	November	495,113
2019	11	2	November	472,907
2019	11	3	November	384,409
2019	11	4	November	411,440
2019	11	5	November	434,085
2019	11	6	November	495,537
2019	11	7	November	444,123
2019	11	8	November	542,492
2019	11	9	November	443,463
2019	11	10	November	389,514
2019	11	11	November	362,548
2019	11	12	November	236,539

From: Chute, Alexander [mailto:AChute@massport.com]
Sent: Wednesday, November 13, 2019 2:49 PM
To: Egnitz, Brian (POL)
Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
Subject: RE: MassPort LPR Cameras

These stats are from the 18 active cameras we have in the system for this month:

<image011.png>

~Alex

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Tuesday, November 12, 2019 5:28 PM
To: Chute, Alexander
Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
Subject: RE: MassPort LPR Cameras

Hi Alex,

Can you please provide the updated reads per day? Previously you were interested in sharing 6 cameras at approximately 75,000 reads per day.

Here is the P492 confi I mentioned.

Set host to boss [redacted]
Set image [redacted]
Set number of [redacted]
Set Ping interval [redacted]
Set udp ping [redacted]
Set ping wait time [redacted]
Set security [redacted]

I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.

-Brian

From: Chute, Alexander [mailto:AChute@massport.com]
Sent: Tuesday, November 12, 2019 2:08 PM
To: Egnitz, Brian (POL)
Subject: MassPort LPR Cameras

Brian,

Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the Troop F building. I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to

and cut the entire LPR network at MassPort over to EOPSS. Most of the roadway cameras are fed to 2 primary network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have 18 cameras in production, with another 19 scheduled to come online within the next two months. I anticipate this number growing to approximately 50 fixed cameras within our campus over the next year. Let me know what you think the appropriate next steps would be.

Respectfully,

~Alex

Alexander B. Chute
Program Manager, Public Safety Systems
Massachusetts Port Authority
Cell: [redacted]
Office: 617.568.5942
achute@massport.com

WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

From: Egnitz, Brian (POL)
To: Slater, James (CHS)
Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter Crary; Michalski, Maria (EPS)
Subject: RE: MassPort LPR Cameras
Date: Friday, January 17, 2020 1:09:00 PM
Attachments: New Solutions and End-Of-Life Announcement.msg
image001.png
image002.png
image003.png
image004.png
image005.png

Hi Jim,

BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.

-Brian

From: Egnitz, Brian (POL)
Sent: Monday, January 6, 2020 1:33 PM
To: Slater, James (CHS)
Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter Crary
Subject: RE: MassPort LPR Cameras

Hi Jim,

We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?

Thanks Brian

From: John Tedona [mailto:jtedona@neology.net]
Sent: Monday, December 9, 2019 4:55 PM
To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); Slater, James (CHS)
Subject: RE: MassPort LPR Cameras

Alex,

I can be available most anytime tomorrow for a call.

Regards,

John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: Chute, Alexander <AChute@massport.com>
Sent: Monday, December 9, 2019 4:38 PM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; John Tedona <jtedona@neology.net>; Peter Crary <pcrary@neology.net>
Cc: Guerriero, Robert (MASSIT) <robert.guerriero@state.ma.us>; Peek, Brian T. (EOTSS) <brian.t.peek@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Slater III, James F (CHS) <james.slater@state.ma.us>
Subject: RE: MassPort LPR Cameras

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Hello All,

I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.

Respectfully,

~Alex

Alexander B. Chute
Program Manager, Public Safety Systems
Massachusetts Port Authority
Cell: [redacted]
Office: 617.568.5942
achute@massport.com

WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Monday, November 18, 2019 3:26 PM
To: John Tedona (jtedona@neology.net); pcrary@neology.net
Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
Subject: RE: MassPort LPR Cameras

Hi John, Peter

Any issues with moving Massports cameras to the Chelsea DB?

Using the Boss calculator, I estimate that we would need 9-10 TB of storage.

The current app server

Windows edition

Windows Server 2012 R2 Standard

© 2013 Microsoft Corporation. All rights reserved.

Windows Server 2012 R2

System

Processor:	Intel(R) Xeon(R) CPU E7- 4850 @ 2.00GHz 2.00 GHz (2 processors)
Installed memory (RAM):	64.0 GB
System type:	64-bit Operating System, x64-based processor
Pen and Touch:	Limited Touch Support with 10 Touch Points

Current DB server

Windows edition

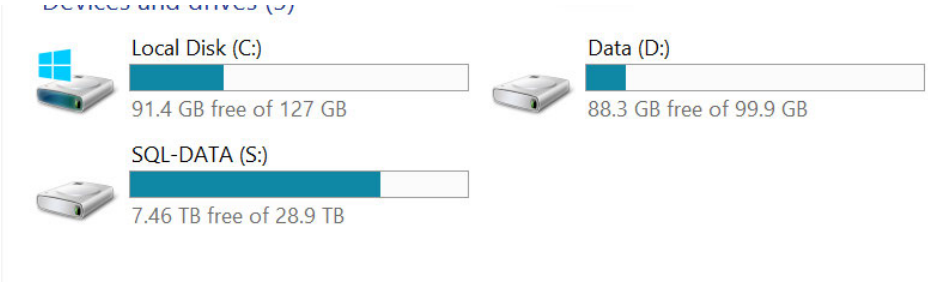
Windows Server 2012 R2 Standard

© 2013 Microsoft Corporation. All rights reserved.

Windows Server 2012 R2

System

Processor:	Intel(R) Xeon(R) CPU E5-2698 v4 @ 2.20GHz 2.20 GHz (2 processors)
Installed memory (RAM):	96.0 GB
System type:	64-bit Operating System, x64-based processor
Pen and Touch:	Limited Touch Support with 10 Touch Points



Our current reads by month for about 66 active cameras

Year	Month	Day	Month Name	Reads Count
2019	11	1	November	495,113
2019	11	2	November	472,907
2019	11	3	November	384,409
2019	11	4	November	411,440
2019	11	5	November	434,085
2019	11	6	November	495,537
2019	11	7	November	444,123
2019	11	8	November	542,492
2019	11	9	November	443,463
2019	11	10	November	389,514
2019	11	11	November	362,548
2019	11	12	November	236,539

From: Chute, Alexander [mailto:AChute@massport.com]
Sent: Wednesday, November 13, 2019 2:49 PM
To: Egnitz, Brian (POL)
Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
Subject: RE: MassPort LPR Cameras

These stats are from the 18 active cameras we have in the system for this month:

Month	Day	Total Scans
⊟ November		
	1	169551
	2	115486
	3	169178
	4	201136
	5	162319
	6	171825
	7	192996
	8	202159
	9	136410
	10	165834
	11	193613
	12	183947

~Alex

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Tuesday, November 12, 2019 5:28 PM
To: Chute, Alexander
Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
Subject: RE: MassPort LPR Cameras

Hi Alex,

Can you please provide the updated reads per day? Previously you were interested in sharing 6 cameras at approximately 75,000 reads per day.

Here is the P492 confi I mentioned.

Set host to boss [redacted]
Set image [redacted]
Set number of [redacted]
Set Ping interval [redacted]
Set udp ping [redacted]
Set ping wait time [redacted]
Set security [redacted]

I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.

-Brian

From: Chute, Alexander [mailto:AChute@massport.com]
Sent: Tuesday, November 12, 2019 2:08 PM
To: Egnitz, Brian (POL)
Subject: MassPort LPR Cameras

Brian,

Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the Troop F building. I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the roadway cameras are fed to 2 primary network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have 18 cameras in production, with another 19 scheduled to come online within the next two months. I anticipate this number growing to approximately 50 fixed cameras within our campus over the next year. Let me know what you think the appropriate next steps would be.

Respectfully,

~Alex

Alexander B. Chute
Program Manager, Public Safety Systems
Massachusetts Port Authority
Cell: [redacted]
Office: 617.568.5942
achute@massport.com

WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

From: Atchison, Charles W
To: Wood, Curtis (EOTSS)
Cc: Quinn, Dermot (POL); Egnitz, Brian (POL); Slater, James (CHS); Guerriero, Robert (EOTSS); Warmington, Scott (POL); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Michalski, Maria (EPS); Mason, Christopher (POL); Hughes, Sean M. (EOTSS); Peter Crary; Shaw, Harold; Ball, Richard (POL)
Subject: Re: MassPort LPR Cameras
Date: Tuesday, February 11, 2020 11:35:26 AM
Attachments: image006.png
image007.png
image008.png
image009.png
image010.png
image011.png

Thank you sir

Major Charles W. Atchison III
Troop F Commander
Massachusetts State Police
Director of Aviation Security
2 Service Road
East Boston, Ma 02128
Office: 617-568-7555
Cell: 508[redacted]

On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT) <curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:

All,
Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.

Thanks

CW

From: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
Sent: Monday, February 10, 2020 10:31 AM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>; Slater, James (CHS) <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Warmington, Scott (POL) <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma.us>>; Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute, Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Michalski, Maria (EPS) <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason, Christopher (POL) <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>; Hughes, Sean M. (EOTSS) <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS) <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL) <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>; Atchison, Charles (POL) <catchison@massport.com<mailto:catchison@massport.com>>
Subject: RE: MassPort LPR Cameras

Good Morning,

I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.

Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.

Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as "BOSS" and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport's cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.

MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.

I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.

To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.

I can't overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security's technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.

Respectfully,

Lieutenant Colonel Dermot J. Quinn #1765
Division Commander
Division of Homeland Security & Preparedness
Massachusetts State Police
<image006.png>

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
Sent: Friday, January 17, 2020 1:10 PM
To: Slater, James (CHS) <james.slater@mass.gov<mailto:james.slater@mass.gov>>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>; Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute, Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski, Maria (EPS) <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
Subject: RE: MassPort LPR Cameras

Hi Jim,

BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.

-Brian

From: Egnitz, Brian (POL)
Sent: Monday, January 6, 2020 1:33 PM
To: Slater, James (CHS)
Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter Crary
Subject: RE: MassPort LPR Cameras

Hi Jim,

We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?

Thanks Brian

From: John Tedona [mailto:jtedona@neology.net]
Sent: Monday, December 9, 2019 4:55 PM
To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); Slater, James (CHS)
Subject: RE: MassPort LPR Cameras

Alex,

I can be available most anytime tomorrow for a call.

Regards,

John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net<mailto:jtedona@neology.net>
PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http-

3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FNEWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJbaP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJU2sB_fmM6g&e=>

From: Chute, Alexander <AChute@massport.com<mailto:AChute@massport.com>>
Sent: Monday, December 9, 2019 4:38 PM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary <pcrary@neology.net<mailto:pcrary@neology.net>>
Cc: Guerriero, Robert (MASSIT) <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>; Peek, Brian T. (EOTSS) <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>; Slater III, James F (CHS) <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
Subject: RE: MassPort LPR Cameras

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Hello All,

I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.

Respectfully,

~Alex

<image007.png>

Alexander B. Chute
Program Manager, Public Safety Systems
Massachusetts Port Authority
Cell: [redacted]
Office: 617.568.5942
achute@massport.com<mailto:achute@massport.com>

WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Monday, November 18, 2019 3:26 PM
To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>); pcrary@neology.net<mailto:pcrary@neology.net>
Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
Subject: RE: MassPort LPR Cameras

Hi John, Peter

Any issues with moving Massports cameras to the Chelsea DB?

Using the Boss calculator, I estimate that we would need 9-10 TB of storage.

The current app server
<image008.png>

Current DB server

<image009.png>
<image010.png>

Our current reads by month for about 66 active cameras

Year

Month

Day

Month Name

Reads Count

2019

11

1

November

495,113

2019

11

2

November

472,907

2019

11

3

November

384,409

2019

11

4

November

411,440

2019

11

5

November

434,085

2019

11

6

November

495,537

2019

11

7

November

444,123

2019

11

8

November

542,492

2019

11

9

November

443,463

2019

11

10

November

389,514

2019

11

11

November

362,548

2019

11

12

November

236,539

From: Chute, Alexander [mailto:AChute@massport.com]
Sent: Wednesday, November 13, 2019 2:49 PM
To: Egnitz, Brian (POL)
Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
Subject: RE: MassPort LPR Cameras

These stats are from the 18 active cameras we have in the system for this month:

<image011.png>

~Alex

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Tuesday, November 12, 2019 5:28 PM
To: Chute, Alexander
Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
Subject: RE: MassPort LPR Cameras

Hi Alex,

Can you please provide the updated reads per day? Previously you were interested in sharing 6 cameras at approximately 75,000 reads per day.

Here is the P492 confi I mentioned.

Set host to boss G.L. c. 4.sec. 7
Set image G.L. c. 4
Set number of G.L. c. 4.sec.
Set Ping interval G.L. c.
Set udp ping G.L. c. 4
Set ping wait time G.L. c. 4
Set security G.L. c. 4

I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.

-Brian

From: Chute, Alexander [mailto:AChute@massport.com]
Sent: Tuesday, November 12, 2019 2:08 PM
To: Egnitz, Brian (POL)
Subject: MassPort LPR Cameras

Brian,

Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the Troop F building. I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the roadway cameras are fed to 2 primary network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have 18 cameras in production, with another 19 scheduled to come online within the next two months. I anticipate this number growing to approximately 50 fixed cameras within our campus over the next year. Let me know what you think the appropriate next steps would be.

Respectfully,

~Alex

<image007.png>

Alexander B. Chute
Program Manager, Public Safety Systems
Massachusetts Port Authority
Cell: G.L. c. 4.sec.
Office: 617.568.5942
achute@massport.com<mailto:achute@massport.com>

WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

From: Atchison, Charles W
To: Chen, Kwang
Cc: Shaw, Harold; Quinn, Dermot (POL); Egnitz, Brian (POL); Slater, James (CHS); Guerriero, Robert (EOTSS); Warmington, Scott (POL); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Michalski, Maria (EPS); Mason, Christopher (POL); Hughes, Sean M. (EOTSS); Peter Crary; Wood, Curtis (EOTSS); Ball, Richard (POL); Haverty, Robert
Subject: Re: MassPort LPR Cameras
Date: Monday, February 10, 2020 1:29:08 PM
Attachments: image002.png
image003.png
image004.png
image005.png
image006.png
image007.png

Thank you sir

Major Charles W. Atchison III
Troop F Commander
Massachusetts State Police
Director of Aviation Security
2 Service Road
East Boston, Ma 02128
Office: 617-568-7555
Cell: 508-[redacted]

On Feb 10, 2020, at 12:54 PM, Chen, Kwang <KChen@massport.com<mailto:KChen@massport.com>> wrote:

Team – We will fully support MSP in the transition of LPR data to the DCJIS BOSS server in Chelsea when the timing is appropriate.

Kwang

<image008.jpg>
Information Technology
Massachusetts Port Authority
One Harborside Drive, Suite 200S
East Boston, MA 02128-2909

617.568.5939
kchen@massport.com<mailto:kchen@massport.com>

From: Shaw, Harold <HShaw@massport.com<mailto:HShaw@massport.com>>
Sent: Monday, February 10, 2020 11:26 AM
To: Quinn, Dermot (POL) <dermot.quinn@state.ma.us<mailto:dermot.quinn@state.ma.us>>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; Slater, James (CHS) <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>; Guerriero, Robert (MASSIT) <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>; Warmington, Scott (POL) <scott.warmington@state.ma.us<mailto:scott.warmington@state.ma.us>>; Peek, Brian T (MASSIT) <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>; John Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute, Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Michalski, Maria (EPS) <maria.michalski@state.ma.us<mailto:maria.michalski@state.ma.us>>; Mason, Chris (POL) <chris.mason@state.ma.us<mailto:chris.mason@state.ma.us>>; Hughes, Sean (MASSIT) <sean.hughes@state.ma.us<mailto:sean.hughes@state.ma.us>>; Peter Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS) <curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>>; Richard Ball <Richard.Ball@state.ma.us<mailto:Richard.Ball@state.ma.us>>; Atchison, Charles W <CAtchison@massport.com<mailto:CAtchison@massport.com>>; Chen, Kwang <KChen@massport.com<mailto:KChen@massport.com>>; Haverty, Robert <RHaverty@massport.com<mailto:RHaverty@massport.com>>
Subject: RE: MassPort LPR Cameras

LTC Quinn,

From my perspective, you've clearly laid out the issues at hand. I couldn't agree more with your characterization of the significance that ALPR technology plays as part of the layered security at Logan, but I also understand the greater benefits of integrating these systems to best support MSP and LE efforts across the greater Commonwealth. As we know, ALPR plays an important role in both proactive and reactive investigations, and the value of finding the best mechanism to integrate not only makes sense, promotes better use of the technology, but ultimately better protects a system put in-place specifically for law enforcement purposes. For all intense and purposes, having a separate "stand alone" system at Logan is inefficient, especially when the primary end users at Logan are from MSP Troop F.

I know there have been a number of discussions on this matter, and I believe finding a viable solution is important to all stakeholders. I've included Massport's CIO Kwang Chen and Bob Haverty, Director of IT – Aviation Systems, into the discussion to share any thoughts they may have from a Massport IT perspective.

Thanks

Hank

From: Quinn, Dermot (POL) <dermot.quinn@state.ma.us<mailto:dermot.quinn@state.ma.us>>
Sent: Monday, February 10, 2020 10:31 AM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; Slater, James (CHS) <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>; Guerriero, Robert (MASSIT)

<robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>; Warmington, Scott (POL)
<scott.warmington@state.ma.us<mailto:scott.warmington@state.ma.us>>; Peek, Brian T (MASSIT)
<brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell, Timothy (EPS)
<timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>; John Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute, Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Michalski, Maria (EPS)
<maria.michalski@state.ma.us<mailto:maria.michalski@state.ma.us>>; Mason, Chris (POL) <chris.mason@state.ma.us<mailto:chris.mason@state.ma.us>>; Hughes, Sean (MASSIT) <sean.hughes@state.ma.us<mailto:sean.hughes@state.ma.us>>; Peter Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS) <curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>>; Shaw, Harold
<HShaw@massport.com<mailto:HShaw@massport.com>>; Richard Ball <Richard.Ball@state.ma.us<mailto:Richard.Ball@state.ma.us>>; Atchison, Charles W <CAtchison@massport.com<mailto:CAtchison@massport.com>>
Subject: RE: MassPort LPR Cameras

Good Morning,

I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.

Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.

Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as "BOSS" and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport's cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.

MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.

I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.

To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.

I can't overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security's technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.

Respectfully,

Lieutenant Colonel Dermot J. Quinn #1765
Division Commander
Division of Homeland Security & Preparedness
Massachusetts State Police
<image002.png>

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
Sent: Friday, January 17, 2020 1:10 PM
To: Slater, James (CHS) <james.slater@mass.gov<mailto:james.slater@mass.gov>>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>; Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek, Brian T. (EOTSS)
<Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute, Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski, Maria (EPS) <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
Subject: RE: MassPort LPR Cameras

Hi Jim,

BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.

-Brian

From: Egnitz, Brian (POL)
Sent: Monday, January 6, 2020 1:33 PM
To: Slater, James (CHS)

Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter Crary
Subject: RE: MassPort LPR Cameras

Hi Jim,

We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?

Thanks Brian

From: John Tedona [mailto:jtedona@neology.net]
Sent: Monday, December 9, 2019 4:55 PM
To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); Slater, James (CHS)
Subject: RE: MassPort LPR Cameras

Alex,

I can be available most anytime tomorrow for a call.

Regards,

John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net<mailto:jtedona@neology.net>
PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http-3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FNEWIHnzbfZimE&r=89OIO8SaE5lJ_8vwaRRPUGu7CJmo6iYQfe-UT7KUAAs&m=gh-21xF1hRXShV16i1HF7Pnk_3Av_MpUANsafRkNSbg&s=ITcz4YzGL1G4Oef62jrbEWRWlUZtOvZzzpKmSQaQQYE&e=>

From: Chute, Alexander <AChute@massport.com<mailto:AChute@massport.com>>
Sent: Monday, December 9, 2019 4:38 PM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary <pcrary@neology.net<mailto:pcrary@neology.net>>
Cc: Guerriero, Robert (MASSIT) <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>; Peek, Brian T. (EOTSS) <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>; Slater III, James F (CHS) <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
Subject: RE: MassPort LPR Cameras

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Hello All,

I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.

Respectfully,

~Alex

<image003.png>

Alexander B. Chute
Program Manager, Public Safety Systems
Massachusetts Port Authority
Cell: [redacted]
Office: 617.568.5942
achute@massport.com<mailto:achute@massport.com>

WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Monday, November 18, 2019 3:26 PM
To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>); pcrary@neology.net<mailto:pcrary@neology.net>
Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
Subject: RE: MassPort LPR Cameras

Hi John, Peter

Any issues with moving Massports cameras to the Chelsea DB?

Using the Boss calculator, I estimate that we would need 9-10 TB of storage.

The current app server
<image004.png>

Current DB server

<image005.png>
<image006.png>

Our current reads by month for about 66 active cameras

Year

Month

Day

Month Name

Reads Count

2019

11

1

November

495,113

2019

11

2

November

472,907

2019

11

3

November

384,409

2019

11

4

November

411,440

2019

11

5

November

434,085

2019

11

6

November

495,537

2019

11

7

November

444,123

2019

11

8

November

542,492

2019

11

9

November

443,463

2019

11

10

November

389,514

2019

11

11

November

362,548

2019

11

12

November

236,539

From: Chute, Alexander [mailto:AChute@massport.com]
Sent: Wednesday, November 13, 2019 2:49 PM
To: Egnitz, Brian (POL)
Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
Subject: RE: MassPort LPR Cameras

These stats are from the 18 active cameras we have in the system for this month:

<image007.png>

~Alex

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Tuesday, November 12, 2019 5:28 PM
To: Chute, Alexander
Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
Subject: RE: MassPort LPR Cameras

Hi Alex,

Can you please provide the updated reads per day? Previously you were interested in sharing 6 cameras at approximately 75,000 reads per day.

Here is the P492 confi I mentioned.

Set host to boss [redacted]
Set image [redacted]
Set number of [redacted]
Set Ping interval [redacted]
Set udp ping [redacted]
Set ping wait time [redacted]
Set security [redacted]

I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.

-Brian

From: Chute, Alexander [mailto:AChute@massport.com]
Sent: Tuesday, November 12, 2019 2:08 PM
To: Egnitz, Brian (POL)
Subject: MassPort LPR Cameras

Brian,

Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the Troop F building. I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the roadway cameras are fed to 2 primary network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have 18 cameras in production, with another 19 scheduled to come online within the next two months. I anticipate this number growing to approximately 50 fixed cameras within our campus over the next year. Let me know what you think the appropriate next steps would be.

Respectfully,

~Alex

<image003.png>

Alexander B. Chute
Program Manager, Public Safety Systems
Massachusetts Port Authority
Cell: [redacted]
Office: 617.568.5942
achute@massport.com<mailto:achute@massport.com>

WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

From: Egnitz, Brian (POL)
To: Peek, Brian T. (EOTSS)
Cc: Guerriero, Robert (EOTSS); Mitchell, Timothy P. (EOTSS)
Subject: RE: Massport
Date: Wednesday, February 12, 2020 9:30:00 AM
Attachments: RE MassPort LPR Cameras.msg

Sure;

Stakeholders are users of ALPR, MSP, and Public Safety Agencies and MassPort.

The Goal is to get the current and new ALPR MassPort cameras redirected to the EOPSS boss server

Deliverables are when reads are coming into the database and the application is stable

Current Environment is MassPort submitting reads to their own BOSS internal server.

Attached is the thread history.

-Brian

From: Peek, Brian T. (EOTSS)
Sent: Wednesday, February 12, 2020 8:38 AM
To: Egnitz, Brian (POL)
Cc: Guerriero, Robert (EOTSS); Mitchell, Timothy P. (EOTSS)
Subject: Massport

Morning Brian,

Can we get a high level overview of this Project:

- Stakeholders
- Goals
- Define Deliverables
- Current Environment

There will be a Project Manager assigned so we would like to have some information to present him\her.

thanks

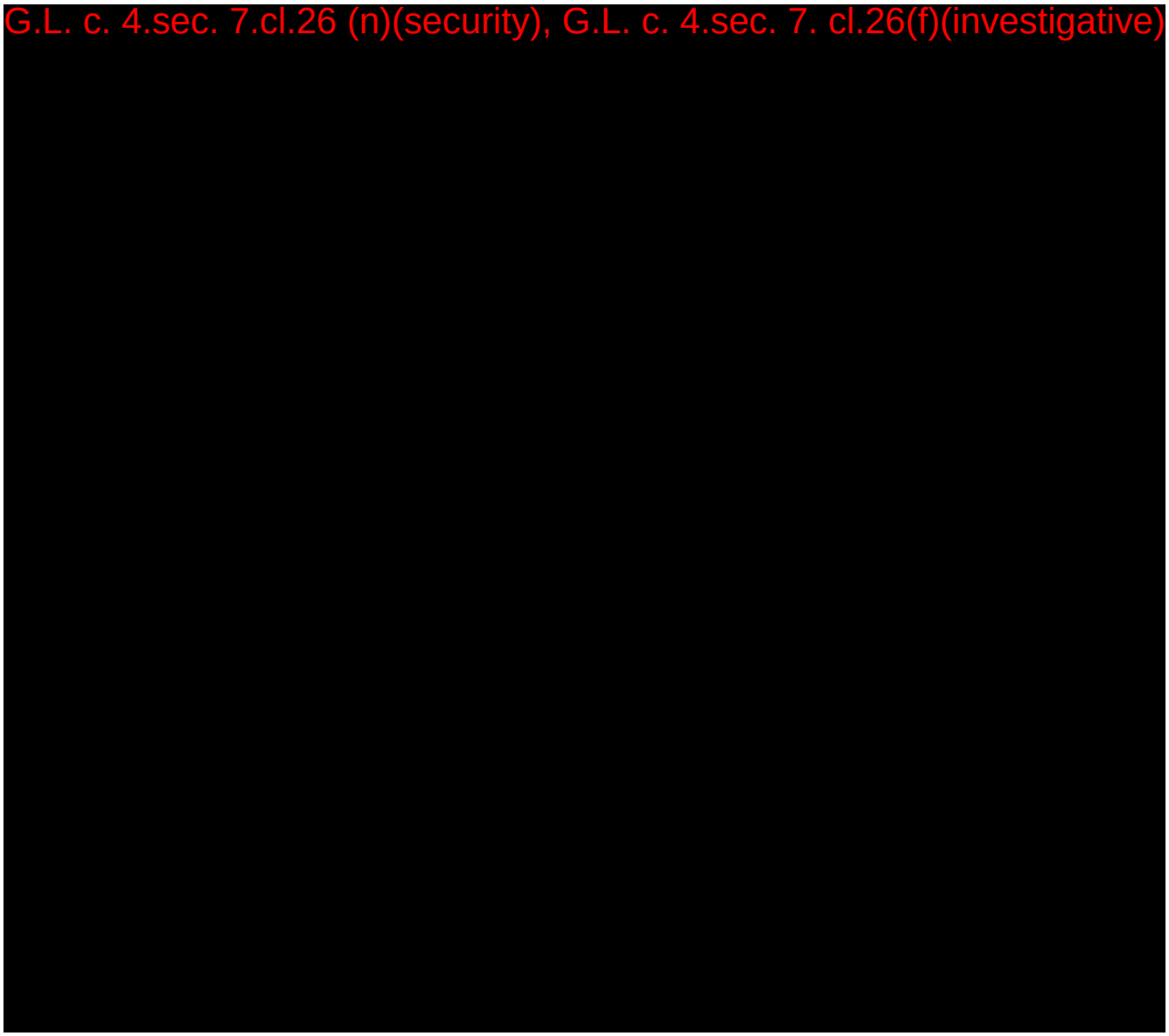
Brian Peek | Massachusetts Executive Office of Technical Services and Security
Network Services/WAN
Phone: 508.922.2740
brian.t.peek@mass.gov | www.mass.gov/eotss

From: Egnitz, Brian (POL)
To: Gilmore, Joey; Alves, Joe; Sillsby, Blane; Quinn, Michael
Cc: Haverty, Robert; Harney, Michael; Quinn, Dermot (POL); Crouse, David (POL)
Subject: RE: MSP LPR
Date: Tuesday, May 5, 2020 2:13:00 PM
Attachments: image001.png
image002.png
image003.png
image004.png
image005.png
image006.png

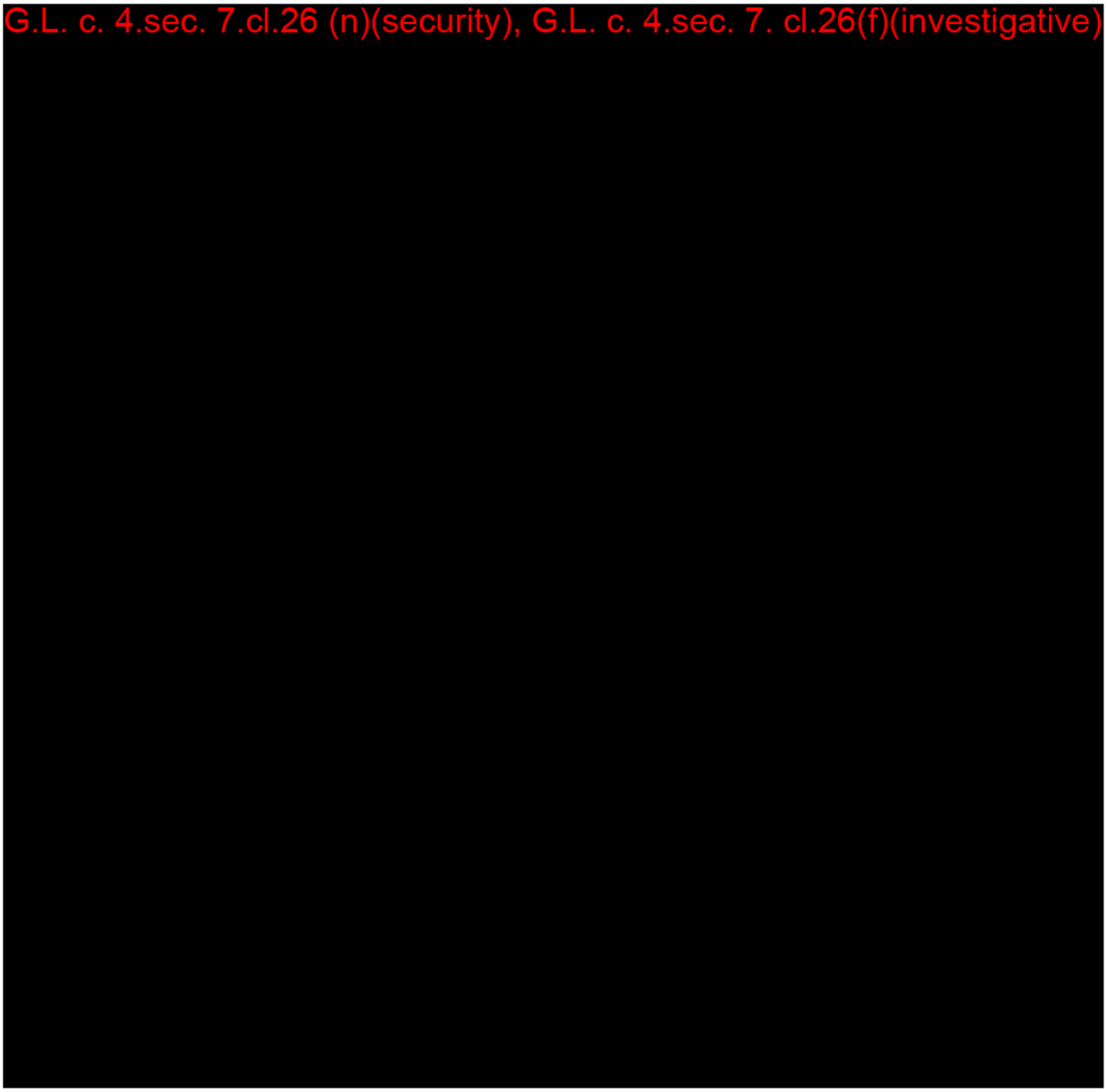
Hi Guys,

Quick update: The 6 modems have been removed, firmware updated and firewalls checked to the EOPSS BOSS server. Below are the devices, I have confirmed the accuracy and they are ready to go. Joe and I plan to meet tomorrow @ 10 to cut over a site.

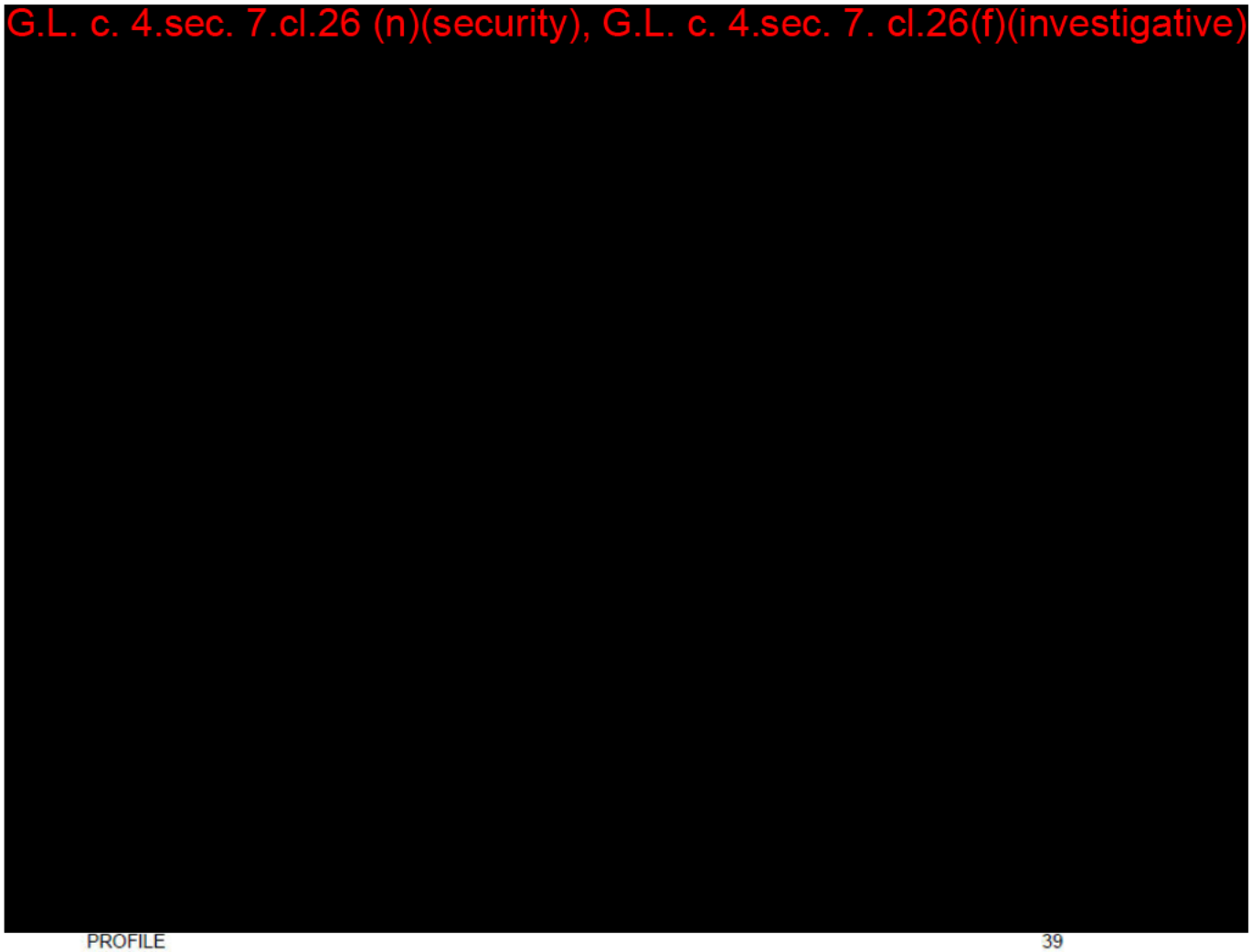
-Brian



Kit # 11 MAS05 - MA State Police/EOPSS 40 Kits



Kit # 7 MAS05 - MA State Police/EOPSS 40 Kits

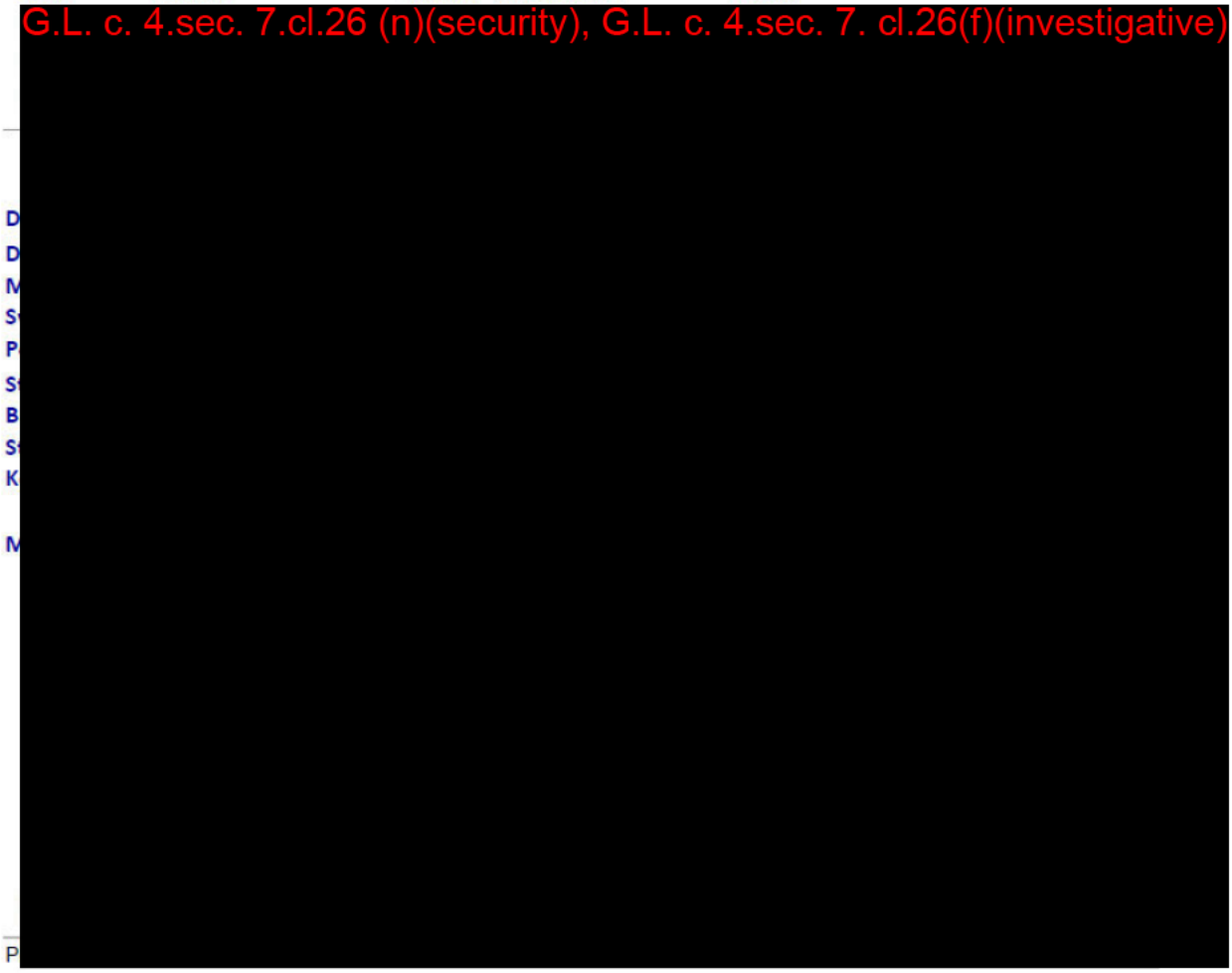


PROFILE 39

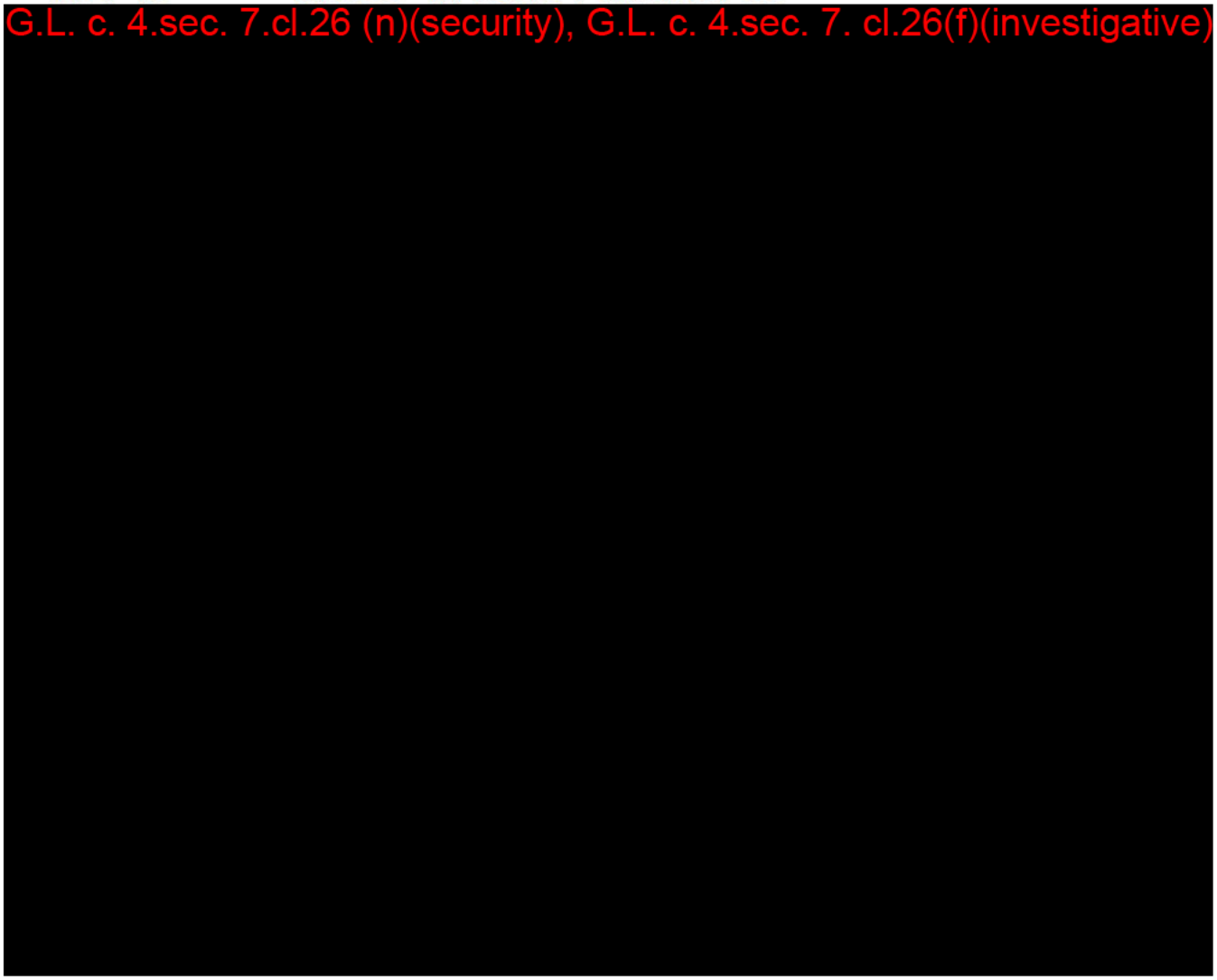
Kit # 13 MAS05 - MA State Police/EOPSS 40 Kits

City: Boston Admin: Al Bob Dave Team:

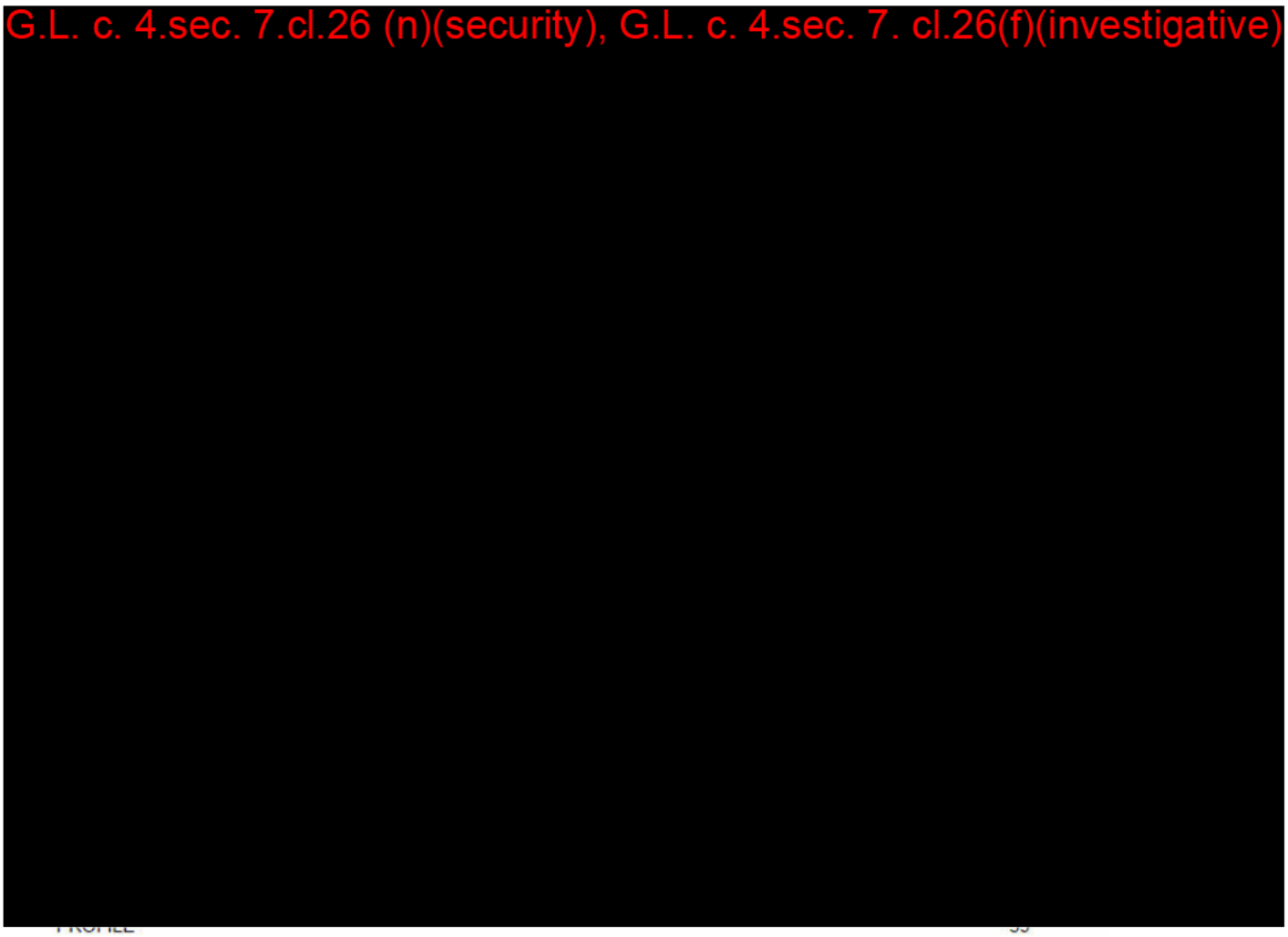
G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)



Kit # 10 MAS05 - MA State Police/EOPSS 40 Kits



Kit # 16 MAS05 - MA State Police/EOPSS 40 Kits



From: Gilmore, Joey [mailto:JGilmore@massport.com]
Sent: Monday, May 4, 2020 9:41 AM
To: Egnitz, Brian (POL); Alves, Joe; Sillsby, Blane; Quinn, Michael
Cc: Haverty, Robert; Harney, Michael
Subject: RE: MSP LPR

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Joe,
Later today Brian will send over the actual IMEI numbers that they are using for this project. Once received, can you please confirm if they are unlimited data plans?

Brian,
Joe Alves is in onsite Wednesday and Friday. He said the camera box near the Hilton is accessible without road closure and would make a good first install. Can you please reach out to him to arrange a time for Wednesday? Joe's cell number is G.L. c. 4.sec. 7.cl.26 (n)(secur

Thank you,
Joey Gilmore
Manager - IT Security Systems
Information Technology
Massachusetts Port Authority

One Harborside Drive, Suite 200S
East Boston, MA 02128-2909
Tel: 617-568-5915
Cell: G.L. c. 4.sec. 7.cl.26 (n)(se

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Thursday, April 23, 2020 10:30 AM
To: Gilmore, Joey <JGilmore@massport.com>; Alves, Joe <JAlves@massport.com>; Sillsby, Blane <BSillsby@massport.com>; Quinn, Michael <MQuinn@massport.com>
Cc: Haverty, Robert <RHaverty@massport.com>; Harney, Michael <MHarney@massport.com>
Subject: RE: MSP LPR

-----Original Appointment-----
From: Gilmore, Joey [mailto:JGilmore@massport.com]
Sent: Wednesday, April 22, 2020 11:35 AM
To: Gilmore, Joey; Alves, Joe; Sillsby, Blane; Quinn, Michael; Egnitz, Brian (POL)
Cc: Haverty, Robert; Harney, Michael
Subject: MSP LPR
When: Thursday, April 23, 2020 10:00 AM-11:00 AM (UTC-05:00) Eastern Time (US & Canada).
Where: https://global.gotomeeting.com/join/500426357

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Hi Guys,

This meeting is to discuss the method of bringing Logan LPR cameras to the EOPSS network.

This is the last status update from Chute before he left:

"Currently MassPort has G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative) After several iterations of the system architecture, it has been decided that the path of least resistance is to employ commercial carrier service on the MSP MPLS to the CJIS Datacenter in Chelsea. MSP is working to procure the necessary power adapter and antenna equipment while also identifying accounts and equipment that can be re-purposed for this project. If/when it is feasible for this system to be networked through terrestrial means, MassPort has the switch infrastructure in place to make a direct connection to the EOPSS network at Building 11 (Troop F Headquarters). I hope this gives a brief overview of where we are at, and please do not hesitate to reach out to me via my personal contact information if any questions come up."

MPA - MSP
Thu, Apr 23, 2020 10:00 AM - 11:30 AM (EDT)

Please join my meeting from your computer, tablet or smartphone.
https://global.gotomeeting.com/join/500426357

This meeting is locked with a password : MPAMSP-APR23

You can also dial in using your phone.
United States: +1 (571) 317-3122

Access Code: 500-426-357

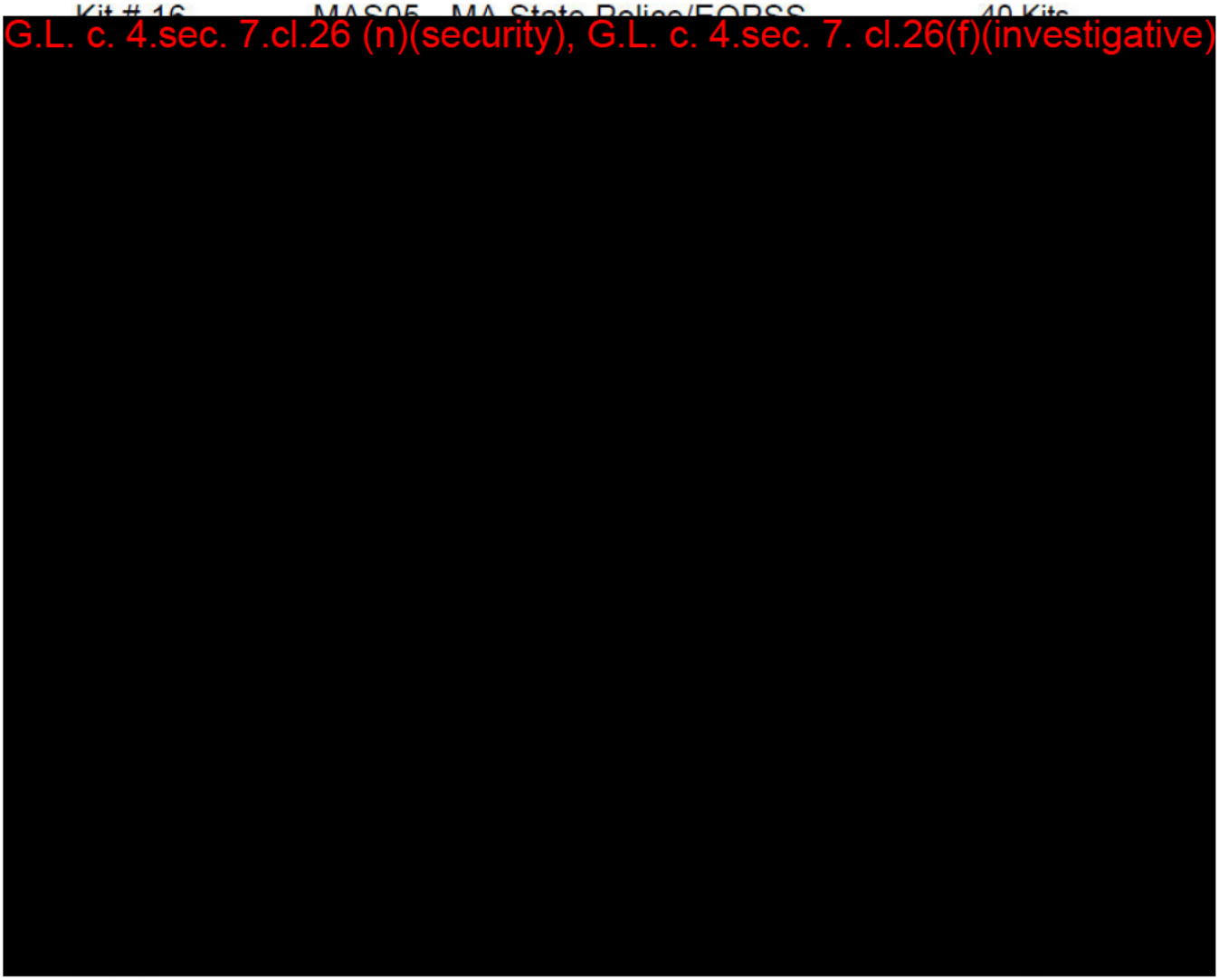
New to GoToMeeting? Get the app now and be ready when your first meeting starts:
https://global.gotomeeting.com/install/500426357

Thank you,

Joey Gilmore

Manager - IT Security Systems
Information Technology
Massachusetts Port Authority
One Harborside Drive, Suite 200S
East Boston, MA 02128-2909
Tel: 617-568-5915
Cell: [redacted]

Kit # 16 MAS05 - MA State Police/FORSS 40 Kits



From: Gilmore, Joey [mailto:JGilmore@massport.com]
Sent: Monday, May 4, 2020 9:41 AM
To: Egnitz, Brian (POL); Alves, Joe; Sillsby, Blane; Quinn, Michael
Cc: Haverty, Robert; Harney, Michael
Subject: RE: MSP LPR

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Joe,
Later today Brian will send over the actual IMEI numbers that they are using for this project. Once received, can you please confirm if they are unlimited data plans?

Brian,
Joe Alves is in onsite Wednesday and Friday. He said the camera box near the Hilton is accessible without road closure and would make a good first install. Can you please reach out to him to arrange a time for Wednesday? Joe's cell number is 7[G.L. c. 4.sec. 7.cl.26 (n)(se

Thank you,
Joey Gilmore
Manager - IT Security Systems
Information Technology
Massachusetts Port Authority

One Harborside Drive, Suite 200S
East Boston, MA 02128-2909
Tel: 617-568-5915
Cell [G.L. c. 4.sec. 7.cl.26 (n)(sec

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Thursday, April 23, 2020 10:30 AM
To: Gilmore, Joey <JGilmore@massport.com>; Alves, Joe <JAlves@massport.com>; Sillsby, Blane <BSillsby@massport.com>; Quinn, Michael <MQuinn@massport.com>
Cc: Haverty, Robert <RHaverty@massport.com>; Harney, Michael <MHarney@massport.com>
Subject: RE: MSP LPR

-----Original Appointment-----
From: Gilmore, Joey [mailto:JGilmore@massport.com]
Sent: Wednesday, April 22, 2020 11:35 AM
To: Gilmore, Joey; Alves, Joe; Sillsby, Blane; Quinn, Michael; Egnitz, Brian (POL)
Cc: Haverty, Robert; Harney, Michael
Subject: MSP LPR
When: Thursday, April 23, 2020 10:00 AM-11:00 AM (UTC-05:00) Eastern Time (US & Canada).
Where: https://global.gotomeeting.com/join/500426357

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Hi Guys,

This meeting is to discuss the method of bringing Logan LPR cameras to the EOPSS network.

This is the last status update from Chute before he left:

"[G.L. c. 4.sec. 7.cl.26 (n)([G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)] After several iterations of the system architecture, it has been decided that the path of least resistance is to employ commercial carrier service on the MSP MPLS to the CJIS Datacenter in Chelsea. MSP is working to procure the necessary power adapter and antenna equipment while also identifying accounts and equipment that can be re-purposed for this project. If/when it is feasible for this system to be networked through terrestrial means, MassPort has the switch infrastructure in place to make a direct connection to the EOPSS network at Building 11 (Troop F Headquarters). I hope this gives a brief overview of where we are at, and please do not hesitate to reach out to me via my personal contact information if any questions come up."

MPA - MSP
Thu, Apr 23, 2020 10:00 AM - 11:30 AM (EDT)

Please join my meeting from your computer, tablet or smartphone.
https://global.gotomeeting.com/join/500426357

This meeting is locked with a password : MPAMSP-APR23

You can also dial in using your phone.
United States: +1 (571) 317-3122

Access Code: 500-426-357

New to GoToMeeting? Get the app now and be ready when your first meeting starts:
https://global.gotomeeting.com/install/500426357

Thank you,

Joey Gilmore

Manager - IT Security Systems
Information Technology
Massachusetts Port Authority
One Harborside Drive, Suite 200S
East Boston, MA 02128-2909
Tel: 617-568-5915
Cell: [redacted]

From: Egnitz, Brian (POL)
To: Gilmore, Joey; Alves, Joe; Haverty, Robert
Cc: Harney, Michael
Subject: RE: MSP LPR
Date: Tuesday, June 16, 2020 3:07:00 PM
Attachments: image001.png

3 sites and 7 cameras are complete and have been cut over. 1 camera was unresponsive on 1A. 2 sites remain and require a detail to complete.

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

From: Gilmore, Joey [mailto:JGilmore@massport.com]
Sent: Tuesday, June 16, 2020 11:22 AM
To: Egnitz, Brian (POL); Alves, Joe; Haverty, Robert
Cc: Harney, Michael
Subject: RE: MSP LPR
Importance: High

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Hello Brian,

Can you please let me know how many of the camera sites have been cut over to EOPSS? Also how many total cameras.

Thank you,
Joey Gilmore
Manager - IT Security Systems
Information Technology
Massachusetts Port Authority
One Harborside Drive, Suite 200S
East Boston, MA 02128-2909
Tel: 617-568-5915
Cell: 617 G.L. c. 4.sec

From: Gilmore, Joey
Sent: Monday, May 4, 2020 9:41 AM
To: 'Egnitz, Brian (POL)' <brian.egnitz@state.ma.us>; Alves, Joe <JAlves@massport.com>; Sillsby, Blane <BSillsby@massport.com>; Quinn, Michael <MQuinn@massport.com>
Cc: Haverty, Robert <RHaverty@massport.com>; Harney, Michael <MHarney@massport.com>
Subject: RE: MSP LPR

Joe,
Later today Brian will send over the actual IMEI numbers that they are using for this project. Once received, can you please confirm if they are unlimited data plans?

Brian,
Joe Alves is in onsite Wednesday and Friday. He said the camera box near the Hilton is accessible without road closure and would make a good first install. Can you please reach out to him to arrange a time for Wednesday? Joe's cell number is 781-426-6944.

Thank you,
Joey Gilmore
Manager - IT Security Systems
Information Technology
Massachusetts Port Authority
One Harborside Drive, Suite 200S
East Boston, MA 02128-2909
Tel: 617-568-5915
Cell: 617 G.L. c. 4.sec

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Thursday, April 23, 2020 10:30 AM
To: Gilmore, Joey <JGilmore@massport.com>; Alves, Joe <JAlves@massport.com>; Sillsby, Blane <BSillsby@massport.com>; Quinn, Michael <MQuinn@massport.com>
Cc: Haverty, Robert <RHaverty@massport.com>; Harney, Michael <MHarney@massport.com>
Subject: RE: MSP LPR

-----Original Appointment-----
From: Gilmore, Joey [mailto:JGilmore@massport.com]
Sent: Wednesday, April 22, 2020 11:35 AM
To: Gilmore, Joey; Alves, Joe; Sillsby, Blane; Quinn, Michael; Egnitz, Brian (POL)

Cc: Haverty, Robert; Harney, Michael
Subject: MSP LPR
When: Thursday, April 23, 2020 10:00 AM-11:00 AM (UTC-05:00) Eastern Time (US & Canada).
Where: https://global.gotomeeting.com/join/500426357

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Hi Guys,

This meeting is to discuss the method of bringing Logan LPR cameras to the EOPSS network.

This is the last status update from Chute before he left:

"Currently MassPort has [redacted] After several iterations of the system architecture, it has been decided that the path of least resistance is to employ commercial carrier service on the MSP MPLS to the CJIS Datacenter in Chelsea. MSP is working to procure the necessary power adapter and antenna equipment while also identifying accounts and equipment that can be re-purposed for this project. If/when it is feasible for this system to be networked through terrestrial means, MassPort has the switch infrastructure in place to make a direct connection to the EOPSS network at Building 11 (Troop F Headquarters). I hope this gives a brief overview of where we are at, and please do not hesitate to reach out to me via my personal contact information if any questions come up."

MPA - MSP
Thu, Apr 23, 2020 10:00 AM - 11:30 AM (EDT)

Please join my meeting from your computer, tablet or smartphone.
https://global.gotomeeting.com/join/500426357

This meeting is locked with a password : MPAMSP-APR23

You can also dial in using your phone.
United States: +1 (571) 317-3122

Access Code: 500-426-357

New to GoToMeeting? Get the app now and be ready when your first meeting starts:
https://global.gotomeeting.com/install/500426357

Thank you,

Joey Gilmore

Manager - IT Security Systems
Information Technology
Massachusetts Port Authority
One Harborside Drive, Suite 200S
East Boston, MA 02128-2909
Tel: 617-568-5915
Cell: 617-[redacted]

The information contained in this communication, including any attachments, is confidential and is intended only for the use of the recipient(s) named above. If the reader of this message is not an intended recipient, you are notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you receive this communication in error, please notify the sender immediately, and delete the communication, any attachments, and all copies.

From: Peter Crary
To: Egnitz, Brian (POL)
Cc: John Tedona
Subject: RE: P492 & P392+ Patch
Date: Wednesday, December 30, 2020 11:20:45 AM
Attachments: image005.png
pips_382392_manualp392papp_4_9_11308.pdf

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Brian,

Attached is the manual that goes over the NTP changes. It's pretty technical and will require using Toolkit to configure.

-Peter Crary
Global R&D Director, ANPR/ALPR
(865) 386-3821 (m)

The information contained in this communication is confidential and intended only for the use of the recipient named and may also be legally privileged. If you are not the intended recipient (named addressee), you are hereby notified that any dissemination, distribution, copying or making use of this communication, or any of its contents, is strictly prohibited. Please notify the sender immediately by email and delete the original message and any copy of it from your computer system. The integrity, security of and absence of viruses in this message cannot be guaranteed on the internet. The sender therefore does not accept liability for any errors or omissions in the contents of this message, nor any damage caused, which arise as a result of e-mail transmission.

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Wednesday, 30 December, 2020 07:19
To: Peter Crary <pcrary@neology.net>
Subject: RE: P492 & P392+ Patch
Importance: High

Thanks Peter,

Is the watermark configuration on by default?

Can I also get the updated 525 or watermark setting?

-Brian

From: Peter Crary <pcrary@neology.net>
Sent: Tuesday, December 29, 2020 3:07 PM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: P492 & P392+ Patch

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Brian,

See attachment.

PIPS TECHNOLOGY
A NEOLOGY Business

Peter R. Crary
Global R&D Director, ANPR/ALPR
pcrary@pipstechnology.com

Customer Support & Sales: (833) PIPS-LPR or (833) 747-7577

The information contained in this communication is confidential and intended only for the use of the recipient named and may also be legally privileged. If you are not the intended recipient (named addressee), you are hereby notified that any dissemination, distribution, copying or making use of this communication, or any of its contents, is strictly prohibited. Please notify the sender immediately by email and delete the original message and any copy of it from your computer system. The integrity, security of and absence of viruses in this message cannot be guaranteed on the internet. The sender therefore does not accept liability for any errors or omissions in the contents of this message, nor any damage caused, which arise as a result of e-mail transmission.

From: Alford, Pamela (NFK)
To: NFK-DL-ADA-District-ct; NFK-DL-ADA-Superior-ct
Cc: Morrissey, Michael (NFK); Antoine, Romere (POL)
Subject: SJC- Com. v. McCarthy- Constitutional ramifications of automatic license plate readers (ALPRs)
Date: Thursday, April 16, 2020 10:54:59 AM
Attachments: e12750.pdf

Today, the SJC addressed whether automatic license plate readers (ALPRs) implicated a person's reasonable expectation of privacy. In addressing the facts of the case before them, involving cameras on the Bourne and Sagamore bridges, they concluded it did not due to the limited extent and use of ALPR data in that case. The Court allowed; however, that in some cases where greater information was taken, an analysis focusing on "the extent to which a substantial picture of the defendant's public movements are revealed by the surveillance," that such information may implicate constitutional protections (pp. 21-26).

From: Alford, Pamela (NFK)
To: NFK-DL-ADA-District-ct; NFK-DL-ADA-Superior-ct; Morrissey, Michael (NFK); Antoine, Romere (POL)
Subject: SJC- Com. v. Mora- Long-term usage of pole cameras constitute search under Art. 14
Date: Thursday, August 6, 2020 10:33:17 AM
Attachments: p12890.pdf

Today, the SJC found that the usuage of pole cameras on a defendant's residence for a continual two month period constitutes a search under Art. 14. They declined to decide whether a lesser period of pole camera usage or usage not directed toward a home, would implicate the same reasonable expectation of privacy. They found that because this was a new rule the case should be remanded to the Superior Court to allow the Commonwealth to attempt to demonstrate that there was probable cause for the search.

Anyone who has a pole camera case should read this opinion. If there are any questions, please reach out.

From: Sweeney, Elizabeth (CPI)
To: Mason, Christopher (POL)
Subject: SJC McCarthy Bridge Cam Decision
Date: Thursday, April 16, 2020 10:38:33 AM
Attachments: McCarthy Bridge Cam decision.pdf

Good morning Colonel Mason,
The SJC issued its opinion in the McCarthy cape bridges ALPR case today, which we met and discussed in August. Opinion is in the link below and a PDF attachment. The SJC declined to suppress the ALPR camera evidence, great news. I have not read the entire opinion yet- 40 pages- but I wanted to forward it to you quickly. They give some guidance on how the "limited" use of cameras is permissible in this case, but widespread camera tracking (like a cellphone) would cause concern. This is the holding:

3. Conclusion. While we recognize that the widespread use of ALPRs in the Commonwealth could implicate constitutional protections against unreasonable searches, the limited use of the technology in this case does not.

Thank you to MSP, especially Brian Egnitz, who met with me and answered all my many questions about the plate readers. It helped immensely.

I will have my cellphone on me today if you have any questions. 508-826-7458.
Thank you,
Elizabeth Sweeney

From: Reporter of Decisions - Supreme Judicial Court of Mass. <sjcreporter@sjc.state.ma.us>
Sent: Thursday, April 16, 2020 10:08 AM
To: Sweeney, Elizabeth (CPI)
Subject: All Criminal

All Criminal

April 16, 2020

Commonwealth v. McCarthy (SJC 12750)

Reporter of Decisions - Supreme Judicial Court of Mass,
1 Pemberton Square, Suite 2500, Boston, MA 02108

SafeUnsubscribe™ esweeney@massmail.state.ma.us

Forward this email | Update Profile | About our service provider
Sent by sjcreporter@sjc.state.ma.us in collaboration with

Constant Contact



Try email marketing for free today!

From: kloving@groups.io on behalf of Klingenberg, Brianne via groups.io
To: kloving@groups.io
Subject: [kloving] ALPR
Date: Wednesday, December 9, 2020 11:28:57 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Good Morning All!

Is anyone aware of an ALPR (License plate reader) system that would date back pretty far? I have a missing person MIA since 2007 and an associated vehicle without any hits on an NCIC Offline search.

Thanks!

Detective Brianne Klingenberg #2226
Santa Clara County Sheriff's Office – Investigations Division
Missing Persons, Juvenile Crimes, Child Abuse (E/B)
55 West Younger Avenue; San Jose, CA 95110
408-808-4539 / 408-808-4545 Fax

Groups.io Links:

You receive all messages sent to this group.

View/Reply Online (#16759) | Reply To Group | Reply To Sender | Mute This Topic | New Topic
Your Subscription | Contact Group Owner | Unsubscribe [john.conron@state.ma.us]

From: kloving@groups.io on behalf of Klingenberg, Brianne via groups.io
To: kloving@groups.io
Subject: [kloving] ALPR
Date: Wednesday, December 9, 2020 11:28:56 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Good Morning All!

Is anyone aware of an ALPR (License plate reader) system that would date back pretty far? I have a missing person MIA since 2007 and an associated vehicle without any hits on an NCIC Offline search.

Thanks!

Detective Brianne Klingenberg #2226
Santa Clara County Sheriff's Office – Investigations Division
Missing Persons, Juvenile Crimes, Child Abuse (E/B)
55 West Younger Avenue; San Jose, CA 95110
408-808-4539 / 408-808-4545 Fax

Groups.io Links:

You receive all messages sent to this group.

View/Reply Online (#16759) | Reply To Group | Reply To Sender | Mute This Topic | New Topic
Your Subscription | Contact Group Owner | Unsubscribe [william.j.desantis@state.ma.us]

From: kloving@groups.io on behalf of Klingenberg, Brianne
To: kloving@groups.io
Subject: [kloving] ALPR
Date: Wednesday, December 9, 2020 11:28:54 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Good Morning All!

Is anyone aware of an ALPR (License plate reader) system that would date back pretty far? I have a missing person MIA since 2007 and an associated vehicle without any hits on an NCIC Offline search.

Thanks!

Detective Brianne Klingenberg #2226
Santa Clara County Sheriff's Office – Investigations Division
Missing Persons, Juvenile Crimes, Child Abuse (E/B)
55 West Younger Avenue; San Jose, CA 95110
408-808-4539 / 408-808-4545 Fax

Groups.io Links:

You receive all messages sent to this group.

View/Reply Online (#16759) | Reply To Group | Reply To Sender | Mute This Topic | New Topic
Your Subscription | Contact Group Owner | Unsubscribe
[christopher.macdonald@pol.state.ma.us]

From: kloving@groups.io on behalf of Klingenberg, Brianne via groups.io
To: kloving@groups.io
Subject: [kloving] ALPR
Date: Wednesday, December 9, 2020 11:28:52 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Good Morning All!

Is anyone aware of an ALPR (License plate reader) system that would date back pretty far? I have a missing person MIA since 2007 and an associated vehicle without any hits on an NCIC Offline search.

Thanks!

Detective Brianne Klingenberg #2226
Santa Clara County Sheriff's Office – Investigations Division
Missing Persons, Juvenile Crimes, Child Abuse (E/B)
55 West Younger Avenue; San Jose, CA 95110
408-808-4539 / 408-808-4545 Fax

Groups.io Links:

You receive all messages sent to this group.

View/Reply Online (#16759) | Reply To Group | Reply To Sender | Mute This Topic | New Topic
Your Subscription | Contact Group Owner | Unsubscribe [thomas.forest@state.ma.us]

From: kloving@groups.io on behalf of Klingenberg, Brianne
To: kloving@groups.io
Subject: [kloving] ALPR
Date: Wednesday, December 9, 2020 11:29:17 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Good Morning All!

Is anyone aware of an ALPR (License plate reader) system that would date back pretty far? I have a missing person MIA since 2007 and an associated vehicle without any hits on an NCIC Offline search.

Thanks!

Detective Brianne Klingenberg #2226
Santa Clara County Sheriff's Office – Investigations Division
Missing Persons, Juvenile Crimes, Child Abuse (E/B)
55 West Younger Avenue; San Jose, CA 95110
408-808-4539 / 408-808-4545 Fax

Groups.io Links:

You receive all messages sent to this group.

View/Reply Online (#16759) | Reply To Group | Reply To Sender | Mute This Topic | New Topic
Your Subscription | Contact Group Owner | Unsubscribe [edward.keefe@pol.state.ma.us]

From: Motorola Solutions
To: McCarthy, Steven (POL)
Subject: [Webinar] Automated License Plate Detection Technology
Date: Thursday, February 13, 2020 2:08:04 PM

Register now
View Online

WEBINAR: AUTOMATED LICENSE PLATE DETECTION TECHNOLOGY

REGISTER NOW

banner

97% of car thieves commit additional crimes, oftentimes with the stolen vehicle.

Actively detecting license plates can alert officers to

WEBINAR INFORMATION

vehicles of interest, potentially interrupting a string of crimes.

The **WatchGuard 4RE Mobile ALPR Solution** uses vehicle license plate detection during traffic stops to provide real-time, in-vehicle actionable intelligence. This results in increased patrol officer safety, proactive crime interruption, and more leads delivered to investigators to solve more cases.

Join WatchGuard, a recent Motorola Solutions acquisition, for an informative webinar. **RSVP now** to learn how you can bring actionable intelligence to your patrol officers.

RSVP NOW

Detect License Plates with WatchGuard In-Car Camera System

Register for one of the following webinar dates:

March 2, 12:00 - 1:00 PM CST
March 9, 12:00 - 1:00 PM CST

REGISTER

Can't make it live? Register anyway and we'll send you a recorded version once the webinar is complete.

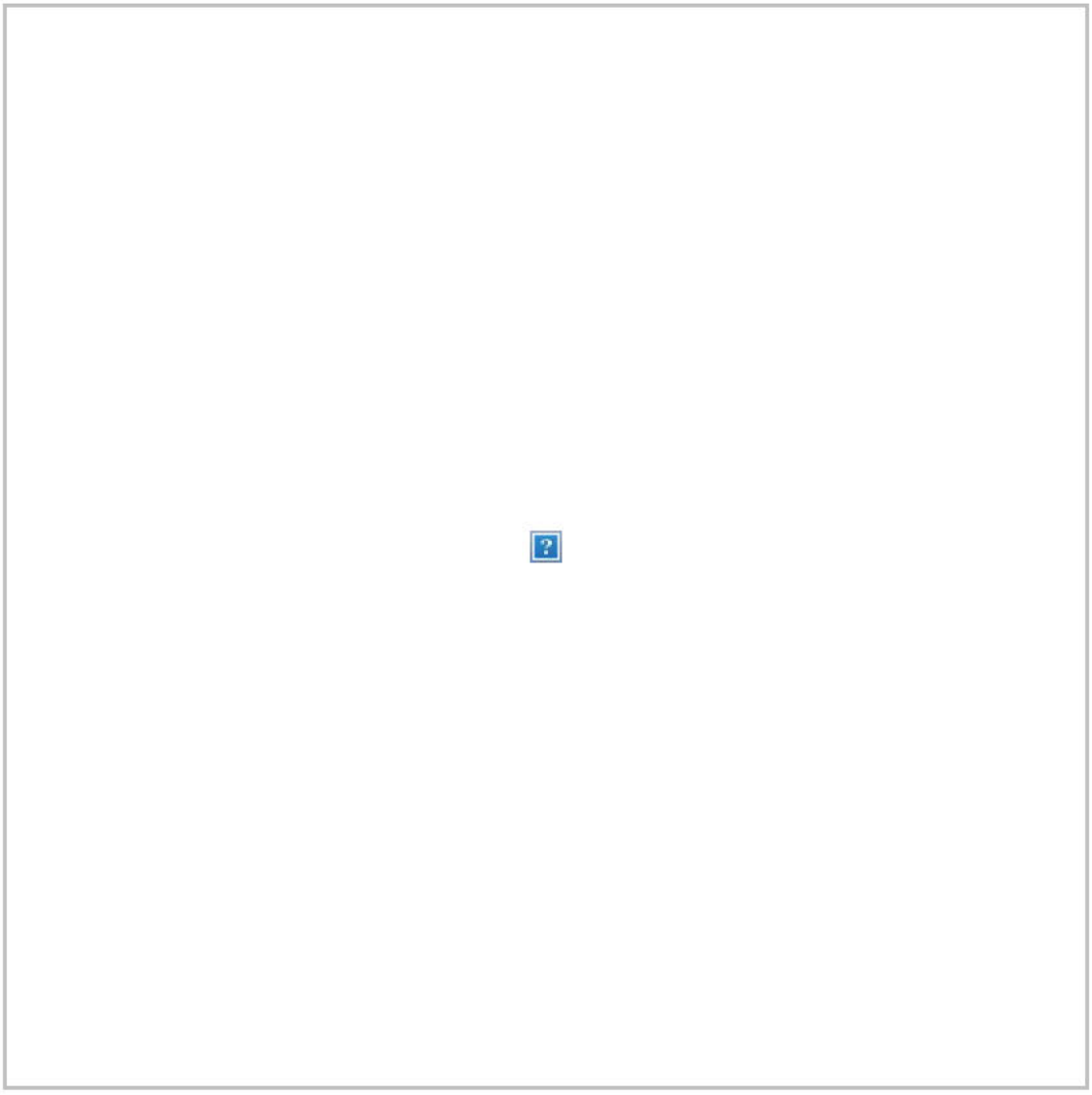
Read and Subscribe to our Blog >

Follow Us:

Motorola Solutions values your privacy. See our Privacy Policy and Terms of Use. You can manage your communication preferences or unsubscribe at any time. You may also write to Motorola Solutions, Inc., Attention: Privacy Compliance Program, P.O. Box 59263, Schaumburg, IL USA 60159-0263 or email privacy1@motorolasolutions.com.

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license.All other trademarks are the property of their respective owners. © 2020 Motorola Solutions, Inc. All rights reserved.

From: Luke Normington
To: Griffin, Daniel (POL)
Subject: 2020 Vision - PIPS Technology Update
Date: Wednesday, January 29, 2020 9:25:00 AM



Dear DanGriffin,

As we step into a new year, and decade, we wanted to take a moment to thank you for your continued loyalty and use of the PIPS Technology by Neology solutions. We are incredibly grateful of the customers, re-sellers and partners who, over the last years have remained loyal and supported us in our vision of “Driving Detection Innovation”. Each day we strive to make a difference in supporting you to achieve your goals, solve your challenges and achieve your mission.

2019 was a major year for us as we finalized significant elements of the overhaul of our products and solutions, culminating with the release of BOSS 4 in the fall, alongside brand new Fixed and Mobile ALPR solutions. Click to find the latest reminders in relation to our products and software versions to ensure you are getting the most out of your Neology products and solutions.

The year ahead is primed to be an exciting one! At Neology we firmly believe that the development doesn't stop – we have almost 30% of our workforce working specifically in the product development area of our business in order to constantly evolve our solutions, improve performance and add new features. We have some exciting additions to the portfolio which are imminent that will provide not only performance improvements to the existing solutions but also provide the ability for greater interoperability across the Law Enforcement ALPR market in the US more generally. We believe that you retaining the control and ownership of your data is paramount and we continue to respect that as we always have whilst supporting those customers who choose to share and provide secure, trusted data sharing between neighbors and friends.

We are always keen to hear your feedback – if there are any elements of our services, solutions or products which you would like to feedback on, please don't hesitate to get in touch with me so I can provide personal attention to both positive and negative feedback. Email me here

Thank you for your continued support – we look forward to serving you in 2020 and beyond.

Best Regards,
Luke & the PIPS Technology team

Copyright © 2020 Neology, All rights reserved.

Our mailing address is:
13520 Evening Creek Dr. E. #460,
San Diego, CA 92128

This email was sent to daniel.griffin@state.ma.us
why did I get this? unsubscribe from this list update subscription preferences
Neology · 6801 N Capital of Texas Hwy # 220B · Austin, TX 78731-1780 · USA

From: communications@aamva.org
To: Mason, Christopher (POL)
Subject: AAMVA Special Alert - License Plate Standard
Date: Wednesday, October 21, 2020 6:40:33 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

October 21, 2020

InTheNewsBanner.jpg

Newly Published!
License Plate Standard - Edition 2

Including Best Practices for Managing Vanity and Specialty License Plate Programs

License plates quickly identify motor vehicles and vehicle registrant information and are most effective when they are designed to optimize legibility to the human eye as well as for license plate readers (LPRs). License plates serve one common purpose: to identify motor vehicles. The ability of motor vehicle agency (MVA) employees, law enforcement, and citizens to quickly and easily identify license plate numbers (consisting of alpha and/or numeric characters) is fundamental to accurate vehicle registration data creation, maintenance, and retrieval. The adoption of the standards within Chapters 1 through 5 streamlines the license plate retrieval processes within MVAs and improves the exchange of license plate data and information between jurisdictions. Alignment with these standards also supports highway safety and increases revenue collection, which are dependent on accurate license plate identification, such as toll collection, restricted lane access, and parking regulations. License plate recognition, by human eye and LPR, is critical to serving these purposes.

In addition, license plates play a central role in preventing and solving crimes. Every day across North America, crimes are prevented or solved through the identification of license plates. It is difficult to quantify the missed opportunities that occur to prevent or solve a crime because a license plate was misread by either the human eye or by LPR, but testing has documented that misreads occur. Adoption of the license plate standard contained in this document will minimize the risk of such misreads.

AAMVA's License Plate Standard - Edition 2 was developed to support a jurisdiction's ability to produce license plates that enhance accurate license plate identification while not limiting a jurisdiction's flexibility for innovation and allowing for multiple license plate designs. It is designed for full-size license plates issued by jurisdictions; portions of it may not apply to smaller license plates typically issued to motorcycles and other similar vehicles. AAMVA recommends jurisdictions involve law enforcement, tolling authorities, and other stakeholders they deem appropriate when developing new license plate designs.

Sections Include:

- Chapter 1: Administrative
- Chapter 2: Design

Appendices Include:

- Appendix A: Definitions
- Appendix B: Temporary License Plate and

Chapter 3: Manufacture
- Chapter 4: Temporary License Plates **NEW!**
- Chapter 5: Alternative Vehicle License Plate Displays **NEW!**
- Chapter 6: Best Practices for Managing Vanity License Plate Programs **NEW!**
- Chapter 7: Best Practices for Managing Specialty License Plate Programs **NEW!**

Temporary Registration Exemplars: Rhode Island
- Appendix C: Sample Handout (for sponsors): Specialty License Plate Specifications
- Appendix D: Example of a Specialty License Plate Agreement
- Appendix E: AAMVA Improving ALPR Effectiveness through Uniform License Plate Design and Manufacture Best Practices Guide
- Appendix F: AAMVA 2020 License Plate Standard Working Group Roster

---

New License Plate Verification Program

To assist jurisdictions in determining if their license plates meet these standards, AAMVA offers the License Plate Verification Program (LPVP). The LPVP provides jurisdictions, at no cost, the opportunity to submit up to four license plates during each AAMVA fiscal year for comparison to the 2020 AAMVA License Plate Standard. A written report will be generated outlining where the submitted license plate does, and does not, align with the standard.

LPV_Form_3_1713123.png

To participate in the License Plate Verification Program, AAMVA jurisdiction members must ship the plate(s) they wish to submit for verification, along with a completed submission form, to the AAMVA Project Manager (PM), Brian Ursino. The PM will collect plates from submitting jurisdictions and ship in bulk to Element, Inc., approximately every 60-days. Element, Inc. will provide analysis reports to the AAMVA PM within 30-days of receiving the plate(s). The AAMVA PM will forward those reports to the submitting jurisdictions. The examined license plates will be returned to the submitting jurisdiction if their return is requested. Otherwise, they will become part of AAMVA's sample license plate inventory. For additional information contact Brian Ursino, Director, Law Enforcement Programs

---

For more standards, best practices, guidelines, whitepapers, and interim reports, please visit our website.

This email was developed and distributed by the American Association of Motor Vehicle Administrators (AAMVA). Click to unsubscribe or manage your subscriptions.

4401 Wilson Boulevard, Suite 700, Arlington, VA 22203

From: WatchGuard
To: McCarthy, Steven (POL)
Subject: Add LPR Technology to Your In-Car Camera System
Date: Tuesday, May 5, 2020 1:37:48 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Not rendering correctly? View this email as a web page here.



Add LPR Technology to Your In-Car Camera System

Officers on patrol are often within close proximity to vehicles that have been associated with crimes, high-risk individuals, missing persons, and abducted children, but they aren't aware of it because they don't always have the information.

Adding LPR to your in-car video system provides access to actionable intelligence via

real-time alerts. WatchGuard in-car video systems are already the technology and industry leader, but adding Vigilant LPR capabilities allow them to do even more. Now, you can use your in-car camera technology as an LPR system without compromising the functionality of the existing system.

The result? Faster response times, interruption of crime, and lives saved. All while spending less.



WatchGuard Video
415 E Exchange Parkway
Allen, TX 75002
USA

You received this email because you are subscribed to Products from WatchGuard Video.

Update your email preferences to choose the types of emails you receive.

Unsubscribe from all future emails

From: Gallagher, David (POL)
To: Babbin, Timothy (AGO)
Subject: ALPR Accounts
Date: Monday, August 17, 2020 7:44:12 PM

DLT Babbin,

Sgt. Tirella reached out and requested I set up ALPR accounts for the following:

DLT Timothy Babbin #2120 *****
Lt. Michael Ahern #2486
Lt. Walter Foley #3110
Lt. Steven Connolly #2719 *****
Lt. Joseph Ross #2264
Lt. Michelle Sutherland #2466
Sgt. Michael Leo #2887
Sgt. Maura McCarthy #2759
Sgt. Patrick Johnson #3128
Sgt. Matthew Hannigan #3281
Sgt. Thomas Mahon #3146
Tpr. John MacDonald #3143
Tpr. Loming Chan #0741 *****
Tpr. Robert Noonan #3327
Tpr. Jose Cuevas #3237
Tpr. Carly Rose #3347
Tpr. Robert Soldani #3879
Tpr. Daniel Nunes #3674 *****
Tpr. Erin McLaughlin #3655
Tpr. Kevin Flynn #3791
Tpr. Christopher Andrade #3738 *****
Tpr. Martin Concannon #3409
Tpr. Shawn Murphy #3481
Tpr. Joshua Rucho #3704
Tpr. Nicholas Pellegrino #3684
Tpr. Shawn LeBlanc #3015
Tpr. Steven Grasso #3803
Tpr. Julio Barbosa #4074

***** Indicates that there is already account created.

I will send a separate email with user guide / link to download software.

Logon will be [redacted]

Initial password will be [redacted] [redacted] [redacted]!

They can change it after initial login.

If you can designate a single POC to address any issues, that would be greatly appreciated.

Lt's and Sgt's have advanced access. Tprs. have basic access.

Please let me know if you need any further assistance.

Respectfully,

David M. Gallagher
Major, Massachusetts State Police
Special Operations
508-820-2162
David.Gallagher3@MassMail.state.ma.us

From: Egnitz, Brian (POL)
To: Guerriero, Robert (EOTSS)
Cc: Quinn, Dermot (POL); Hughes, Sean M. (EOTSS); Slater, James (CHS); Crouse, David (POL); Peek, Brian T. (EOTSS)
Subject: ALPR Cameras
Date: Friday, April 17, 2020 6:56:00 AM

Hi Rob,

As you are probably aware the MassPort project to migrate their ALPR Cameras over to the MSP is moving forward over Verizon Wireless. We have identified modems, data plans and purchased the accessories needed for the project and hope to begin cutting over in the next 2-3 weeks.

I wanted to run something by you and the team to review; we just completed the Sierra MP70 VPN project with IPC and it went well (thanks for your teams help - BTW). Do you want to use the same approach (OneNetwork) for these ALPRS? I think it would give us the same functionality originally discussed by pushing the traffic over MassPorts network back to the core, but we would run it over Verizon.

A couple of thoughts;

This could be a good long term approach for all ALPRs we are hosting, we've begun to standardized on MP70s

This could give us much needed remote access to the cameras

If we moved to the Neology Hosted solution, we could do a split tunnel and pipe the traffic straight over the internet, but only allow remote management via the tunnel.

IPC was the prime on the sierra project and work would be minimal to expand, we also want to begin leveraging them more for our other wire/ covert/camera networks we run down the road (when Jim decides to retire).

If MassPort wants us off Verizon (since they are paying for the data plans), they could get us a straight internet route and connect to the MP70 (Our MP70 establishes internet via a LAN Port, Wifi and Cell, all establishing the VPN tunnel after connection).

Let me know what you think and if you want to get on a call to discuss. Otherwise, we can just get MassPort done with the normal static plan.

Thanks, Brian

Brian Egnitz

Commonwealth Fusion Center

Massachusetts State Police

Phone: 978-451-3710 (Maynard) 508-988-7302 (GHQ)

Email: Brian.Egnitz@massmail.state.ma.us

Monday - Friday, 8 to 4

CONFIDENTIALITY NOTICE: *The information contained in this email and any attachment is privileged and confidential law enforcement information. If you have received this email in error, please call 978-451-3700 immediately. Thank you.*

From: Egnitz, Brian (POL)
To: Guerriero, Robert (EOTSS)
Cc: Quinn, Dermot (POL); Hughes, Sean M. (EOTSS); Crouse, David (POL); Peek, Brian T. (EOTSS)
Subject: ALPR Cameras
Date: Friday, April 17, 2020 6:55:00 AM

Hi Rob,

As you are probably aware the MassPort project to migrate their ALPR Cameras over to the MSP is moving forward over Verizon Wireless. We have identified modems, data plans and purchased the accessories needed for the project and hope to begin cutting over in the next 2-3 weeks.

I wanted to run something by you and the team to review; we just completed the Sierra MP70 VPN project with IPC and it went well (thanks for your teams help - BTW). Do you want to use the same approach (OneNetwork) for these ALPRS? I think it would give us the same functionality originally discussed by pushing the traffic over MassPorts network back to the core, but we would run it over Verizon.

A couple of thoughts;

This could be a good long term approach for all ALPRs we are hosting, we've begun to standardized on MP70s

This could give us much needed remote access to the cameras

If we moved to the Neology Hosted solution, we could do a split tunnel and pipe the traffic straight over the internet, but only allow remote management via the tunnel.

IPC was the prime on the sierra project and work would be minimal to expand, we also want to begin leveraging them more for our other wire/ covert/camera networks we run down the road (when Jim decides to retire).

If MassPort wants us off Verizon (since they are paying for the data plans), they could get us a straight internet route and connect to the MP70 (Our MP70 establishes internet via a LAN Port, Wifi and Cell, all establishing the VPN tunnel after connection).

Let me know what you think and if you want to get on a call to discuss. Otherwise, we can just get MassPort done with the normal static plan.

Thanks, Brian

Brian Egnitz

Commonwealth Fusion Center

Massachusetts State Police

Phone: 978-451-3710 (Maynard) 508-988-7302 (GHQ)

Email: Brian.Egnitz@massmail.state.ma.us

Monday - Friday, 8 to 4

CONFIDENTIALITY NOTICE: *The information contained in this email and any attachment is privileged and confidential law enforcement information. If you have received this email in error, please call 978-451-3700 immediately. Thank you.*

To: Guerriero, Robert (EOTSS)
Cc: Quinn, Dermot (POL); Hughes, Sean M. (EOTSS); Crouse, David (POL); Peek, Brian T. (EOTSS)
Subject: ALPR Cameras
Date: Friday, April 17, 2020 6:52:28 AM

Hi Rob,

As you are probably aware the MassPort project to migrate their ALPR Cameras over to the MSP is moving forward over Verizon Wireless. We have identified modems, data plans and purchased the accessories needed for the project and hope to begin cutting over in the next 2-3 weeks.

I wanted to run something by you and the team to review; we just completed the Sierra MP70 VPN project with IPC and it went well (thanks for your teams help - BTW). Do you want to use the same approach (OneNetwork) for these ALPRS? I think it would give us the same functionality originally discussed by pushing the traffic over MassPorts network back to the core, but we would run it over Verizon.

A couple of thoughts;

This could be a good long term approach for all ALPRs we are hosting, we've begun to standardized on MP70s

This could give us much needed remote access to the cameras

If we moved to the Neology Hosted solution, we could do a split tunnel and pipe the traffic straight over the internet, but only allow remote management via the tunnel.

IPC was the prime on the sierra project and work would be minimal to expand, we also want to begin leveraging them more for our other covert/camera networks we run down the road.

If MassPort wants us off Verizon (since they are paying for the data plans), they could get us a straight internet route and connect to the MP70 (Our MP70 establishes internet via a LAN Port, Wifi and Cell, all establishing the VPN tunnel after connection).

Let me know if you want to get on a call to discuss.

Thanks, Brian

From: McCarthy, Daniel (AGO)
To: Bender, Sean (POL); Barton, Shannan (POL)
Subject: ALPR use upheld by Supreme Judicial Court
Date: Thursday, April 16, 2020 11:09:27 AM

---

https://www.mass.gov/files/documents/2020/04/16/e12750.pdf

Dan McCarthy
Sr. Intelligence Analyst, Enterprise, Major, and Cyber Crimes Division
Office of the Attorney General
One Ashburton Place, 19th Floor
Boston, MA 02108
Office: (617) 963-2505

From: Kevin Coughlin
To: Quinn, Dermot (POL)
Cc: McCarthy, Steven (POL); Jim DOWLING; Chris Perez; Steve Teese
Subject: ALPR Webinar tomorrow
Date: Monday, June 15, 2020 5:25:54 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Good evening Colonel Quinn. I'm not sure if you are interested in this or not, but it is timely. Dep. Chief Scott Whittemore from Wellesley is one of the platform speakers on the ALPR Webinar taking place tomorrow. They are long time Vigilant customers and superusers. They have also rolled out the Vigilant ALPR with WatchGuard 4RE integration. He is a big fan. Just in case you are interested.

From: **FBI National Academy Associates, Inc.** <do-not-reply@fbinaa.org>
Date: Wed, May 6, 2020 at 6:36 AM
Subject: TRAINING WEBINAR: Engage the Community by Leveraging License Plate Recognition Technology
To: <lauren.mora@motorolasolutions.com>



As the adoption of advanced video and analytics technology grows, so does the imperative that is applied in collaborative efforts to co-produce public safety programs with communities. At its core, public safety relies on a partnership between law enforcement and community, one that is built on a basis of trust and transparency. In which data, and the technology that enables its collection, has the potential to strengthen that foundation. Overall, with the greatest goal of data to be harnessed for the protection and safety of law enforcement officers.

In this webinar, you will learn how license plate recognition (LPR) data that is captured by the community and civilian agencies can support public safety efforts in real-time. Experience live LPR demonstrations and training tips that can be implemented in your current operations. Our panel of industry practitioners will guide you through best practices and LPR use cases that can help you bolster your operations and enhance community engagement when fighting crime.

Key takeaways:
- Firsthand LPR technology best practices to implement with your operations
- Insights on how to engage your community with technology to enhance crime-fighting efforts
- Key considerations when implementing new LPR technologies into your current systems and

operations

Tuesday, June 16, 2020
11:00 am ET | 8:00 am PT











Kyle Hoertsch
Motorola Solutions Associates
Sgt Sacramento County Sheriff's Office (Ret.)
Speaker Bio

James M. Wolfinbarger
Motorola Solutions
Col. Colorado State Patrol (Ret.)
FBINA #225
NEI #33
Speaker Bio

Scott Whittemore
Wellesley Police Department
Deputy Police Chief
FBINA #265
Speaker Bio

John Kennedy
FBI National Academy
Director of Education and Training

Learn More

This Training Webinar was brought to you through collaboration between two leading organizations dedicated to Law Enforcement and the Communities they serve.





FBI National Academy Associates, Inc., FBI Academy, Quantico, VA 22135

SafeUnsubscribe™ lauren.mora@motorolasolutions.com
Forward email | Update Profile | About our service provider
Sent by do-not-reply@fbinaa.org in collaboration with

Constant Contact



Try email marketing for free today!

--

Kevin Coughlin
Senior Account Manager, WatchGuard - New England

m: 603-305-6524
Kevin.Coughlin@MotorolaSolutions.com

Your privacy is important to us. That is why we have taken appropriate measures to ensure the data you provide to us is kept secure. To learn more about how we process your personal information, how we comply with applicable data protection laws, and care for the security and privacy of your personal data, please review our Privacy Policy. If you have any questions related to data protection and compliance with applicable laws, please contact us at our Security Operations Center at 1-800-674-4357.

Subject: ALRP
Date: Monday, December 21, 2020 11:59:39 AM

Currently the Truck team has a quote for replacing there current LPR system with new Neology cameras. The grant can also support Gov cloud hosting for the data, but not all the data. A decision is requested on how/if to move forward on this project.

Now that the
Neology Recommendations

Short term:

For Fixed

- Disable all cameras in BOSS 3.6 On-Prem (EOPSS)
- Turn on system (allowing access to users)
- Patch each 492 & 525 Camera, configure new watermark and then enable the camera to send to backend system. (need confirmation that new "NTP Flag" metadata will work with 3.6, also if data without NTP lock is being sent)

For Mobiles

- write a new purge script to delete all Mobile data.
- Remove all of these mobiles from hotlists (except NCIC, RMV, Warrants etc.), ensuring no hits are generated.
- Inventory all SX4 &SX4e systems (2017-Present) to identify which systems can be upgraded
- Older systems will need to be decommissioned or configured not to send data to BOSS 3.6 and data would need to be purged.
- The SX4 &SX4e systems (2017-Present) will need to be Patched in order for reads to be sent to the back end. (still reviewing process, might be able to VNC remote)

In Parallel

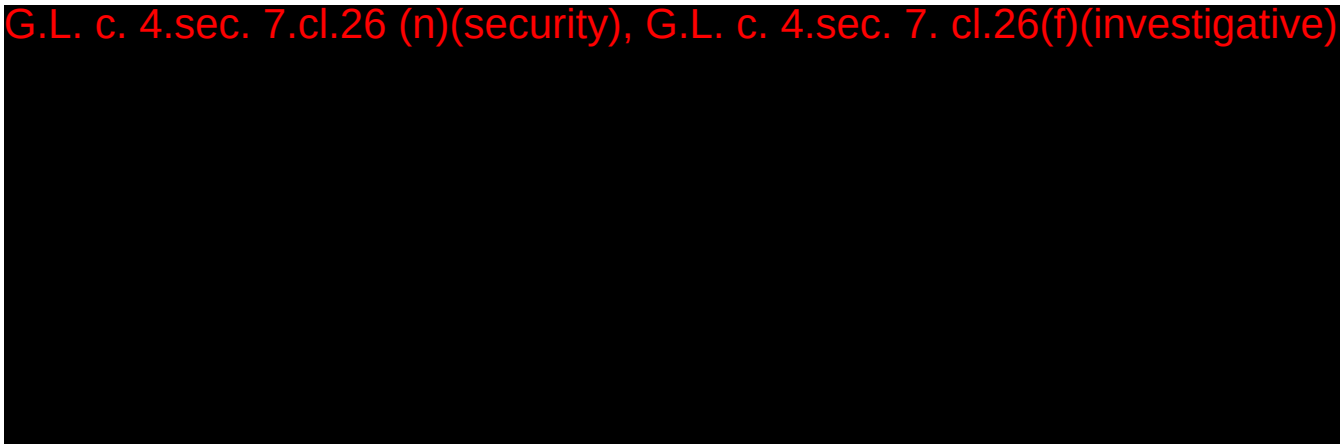
Establish a new MSP ALPR System
Create data sharing agreements, Include data standards and audit requirements for all submitting Agencies
Complete cloud agreement with Neology (DCJIS)
Move forward with Truck Team purchase, rolling in Gov. Cloud BOSS 4.0 (New MSP System) subscription
Fund remaining cameras and migrate cameras to cloud system over time
Then preserve or decommission EOPSS BOSS 3.6

Brian Egnitz
Commonwealth Fusion Center

Massachusetts State Police
Phone: 978-451-3710 (Maynard) 508-988-7302 (GHQ)
Email: Brian.Egnitz@massmail.state.ma.us
Monday - Friday, 8 to 4

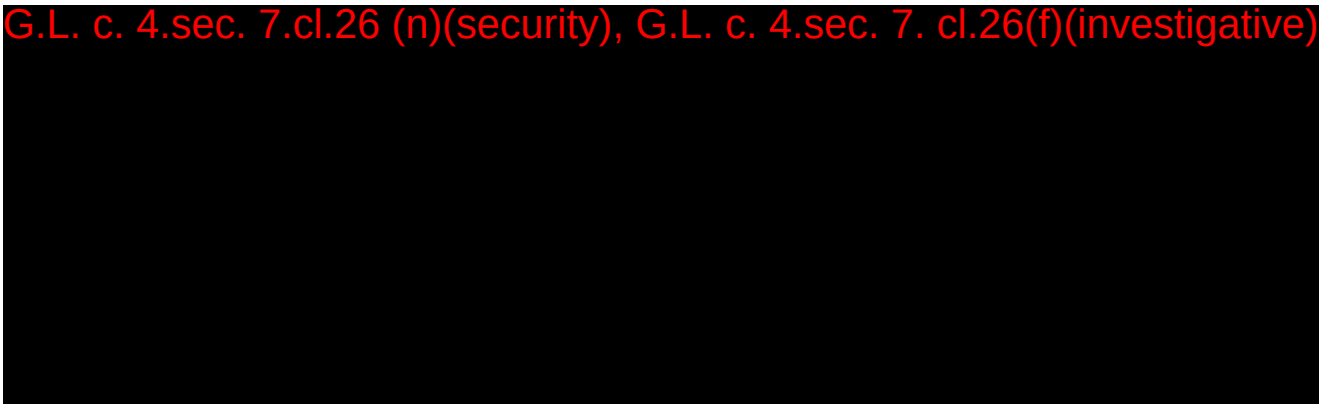
CONFIDENTIALITY NOTICE: *The information contained in this email and any attachment is privileged and confidential law enforcement information. If you have received this email in error, please call 978-451-3700 immediately. Thank you.*

From: BossAlerts@state.ma.us
To: ALPR Alerts (POL)
Subject: G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative
Date: Tuesday, February 11, 2020 12:24:30 PM



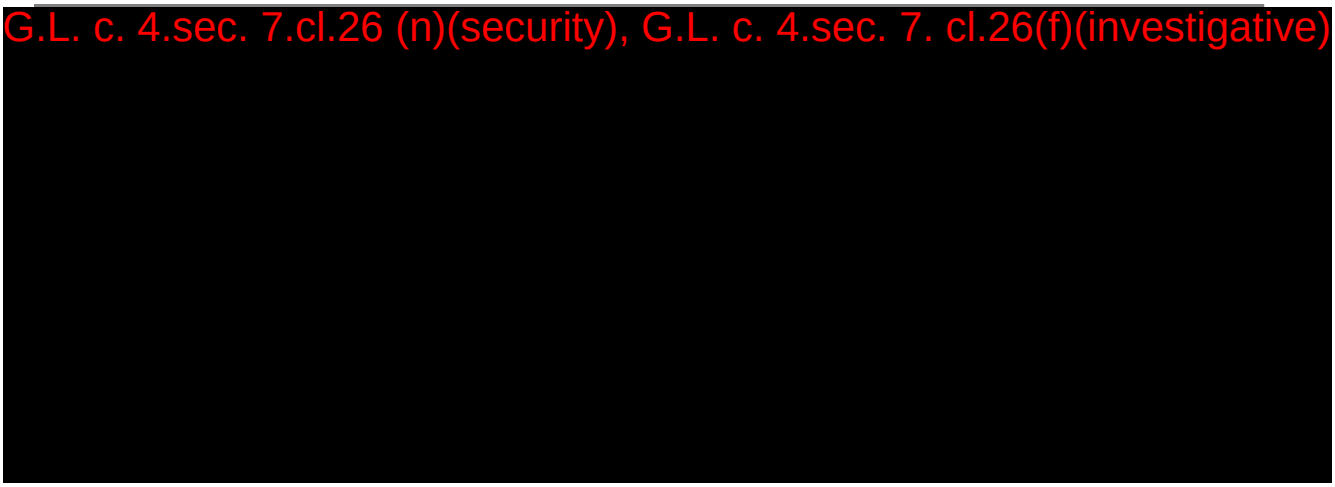
From: BossAlerts@state.ma.us
To: ALPR Alerts (POL)
Subject: BOSS License Plate#: [redacted]
Date: Tuesday, February 11, 2020 2:18:11 PM

Hit on LPR Hotlist: [redacted]
License Plate# [redacted]
Date Time of [redacted]

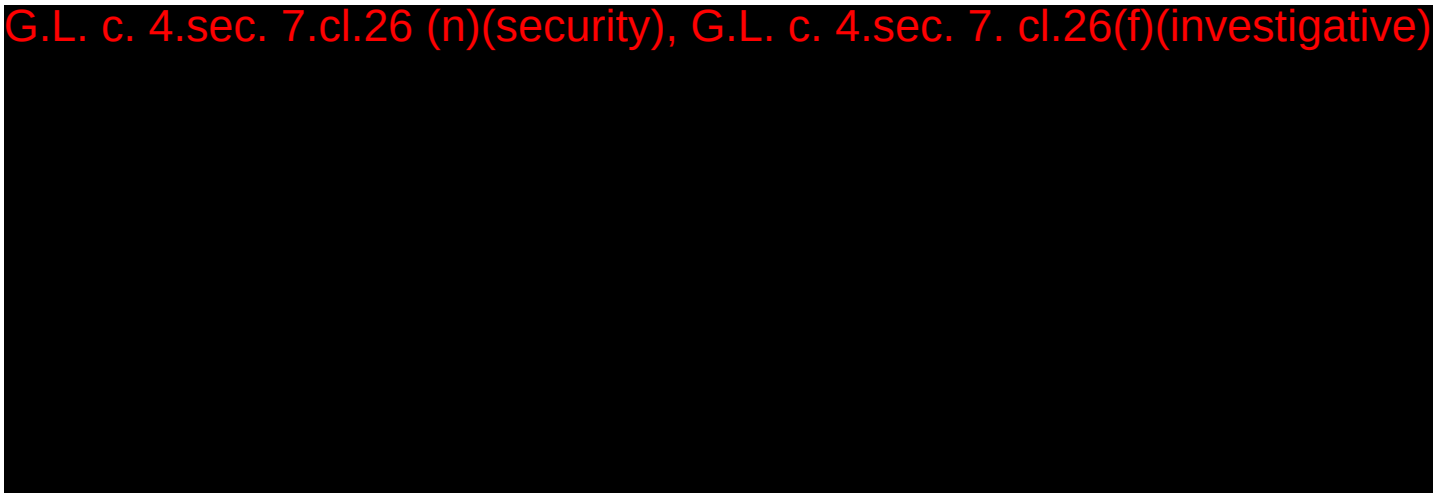


Defendant failed to appear
License Plate#: 8EP232

From: BossAlerts@state.ma.us
To: ALPR Alerts (POL)
Subject: BOSS License Plate#: [redacted]
Date: Tuesday, February 11, 2020 2:18:08 PM



From: BossAlerts@state.ma.us
To: ALPR Alerts (POL)
Subject: BOSS License Plate#: G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26
Date: Tuesday, January 7, 2020 3:42:13 PM



From: BossAlerts@state.ma.us
To: ALPR Alerts (POL)
Subject: BOSS License Plate#: G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)
Date: Friday, October 23, 2020 12:07:52 PM



From: Grant, Marguerite (DA)
To: [redacted]
Cc: [redacted]
Subject: Case Update - ending 4 c 194 with ALPRs at Bourne/Sagamore Bridges and 4 search
Date: Friday, April 17, 2020 5:33:47 PM



Chiefs

Commonwealth v. McCarthy (SJC 12750) ← click on that link to see the case
In this case the SJC ruled that police tracking D's car using 4 automatic license plate readers (ALPRs) at both ends of the Bourne and Sagamore Bridges was too limited to amount to a constitutional "search." The SJC declined to say exactly how detailed digital surveillance would have to be to constitute a search leaving that issue for future cases.

State Po lice maintain ALPRs including ones at both ends of the Bourne and Sagamore Bridges. (p.3) The ALPRs photograph vehicles' license plates; that data along with the date and time of the sighting is retained by EOPPS for a year. (p.3-4) Authorized users including police may put a license plate number on a "hot list " and receive an alert if that plate is sighted; reasons to put someone on the "hot list" include not only criminal investigations but also Amber alerts missing persons and BOLO alerts. (p. 3 25 n.13)

Through surveillance controlled buys and information from 4 Cis Barnstable police suspected that the co-D was selling heroin out of his house in Barnstable. (p.4) Police saw a black Hyundai driven by D visit there briefly so they suspected that D was the co-D's supplier. Police put the Hyundai's license plate number on the State Police ALPR "hot list " so that they'd be notified whenever the Hyundai crossed one of the bridges. (p.5) After getting an alert that the Hyundai had crossed onto the Cape police followed both the Hyundai and the co-D to the buy location on a quiet residential street where D and co-D met for about 30 seconds but police could not see a physical exchange. (p.5) From the ALPR data police generated a spreadsheet showing that in mid-winter the Hyundai had crossed the bridges dozens of times sometimes more than once a day adding to police suspicion that D was the heroin supplier. (p.5-6) When police got a second alert that the Hyundai had crossed onto the Cape they again followed D and co-D to the buy location and saw a 30-second meeting but could not see any exchange. This time police stopped both cars handcuffed both co-D and D and read them Miranda. (In co-D police found heroin; on D police found 2 cell phones and cash. (p.6-7) At the station police repeatedly told D he was "not under arrest " and D made statements.

D moved to suppress the ALPR data his statements and evidence obtained from the stop. A Superior Court judge found that the moment of arrest was when D and co-D were handcuffed at the scene of the traffic stop but denied the motion to suppress. (p.33) The SJC upheld the denial.

ALPRs and expectation of privacy in digital surveillance At some length the SJC discussed the constitutional issues raised by digital surveillance. (p.7-24) Police conduct amounts to a search if: (1) it intrudes on a D's expectation of privacy and (2) society is willing to recognize the expectation of privacy as reasonable. Here the SJC ruled D did have an expectation of privacy because D and co-D chose a buy location in a quiet residential area. (p.8 n.5) As to what expectation of privacy society recognizes as reasonable with regard to digital surveillance the SJC was guided by historical understandings of what was an unreasonable search and seizure when the U.S. and Mass. Constitutions were adopted in the late 1700s in reaction to redicasts' rummaging without restraint through colonists' homes. (p.8-10) New technologies like ALPRs raise difficult legal issues because they are easier and less expensive for police than traditional surveillance can be done secretly and permit police to search back in time for a vehicle's movements even before police suspicion arose. (p.12-14) Society does not recognize as reasonable an expectation of privacy in what someone "knowingly exposes" to public view like a license plate – which by statute must be "displayed conspicuously." (p.15-16 & n.8) In older cases involving less advanced technology courts have held that a D did not have an expectation of privacy in contents of a phone conversation in a phone booth or a radio beeper" tracking a single journey. (p.14-17) But technology like ALPRs GPS and CSLI are different because they may give police a **mosaic** of information where each piece may be public but when viewed together they create a picture that implicates someone's privacy interests like their political religious or sexual associations. (p.17-21) The SJC was concerned that with enough ALPRs police could track someone's location everywhere which would be "creepy." (p.21) Exigent circumstances would likely justify using an ALPR in a situation involving an Amber alert or missing person. (p.25 n.13) The D urged the SJC to consider not just these four ALPRs on the Bourne and Sagamore Bridges but the hundreds of ALPRs across Massachusetts; the SJC declined to do so because that evidence is not in the record of this case. (p.24) The **limited number of cameras** here and their placements on the bridges was not enough to give D an expectation of privacy that society would recognize as reasonable. (p.28) The SJC declined to say how much digital surveillance would give such an expectation and admitted that its unwillingness to do so **"may bring some interim confusion"** until further cases develop the law on this issue. (p.28 n.15) Chief Justice Gants wrote a separate concurrence suggesting that one thing the SJC could do is to require police who want to search a vast amount of digital data to apply for a court order supported by an affidavit showing reasonable suspicion to do so. (concurrence p.1) This would be like a SW but with a lower standard than PC.

Written policy The SJC rejected D's argument that Barnstable PD should have had a written policy about ALPRs and the MSP policy on which Barnstable relied was not specific enough. (p.30) Written policies are required to justify certain exceptions to the SW requirement (like inventory searches and sobriety checkpoints) – they do not apply to the threshold question whether a search occurred in the first place. (p.31)

Miranda issues At the station police repeatedly told D that D was "not under arrest." But the motion judge found that the moment of arrest was when police handcuffed D at the traffic stop. (p.33) D argued that his statements should be suppressed because police telling him he was not under arrest amounted to "deceit or trickery" to get D to confess. The motion judge and the SJC rejected that argument saying that even if telling D he was not under arrest amounted to deceit or trickery it was just one factor to be used in determining voluntariness.

Bottom line: Police use of ALPRs at limited locations is not a constitutional search – but we don't know how many locations it'd have to be to amount to one. Using an ALPR in **exigent circumstances** like an Amber Alert is likely OK. Local police don't need a written policy to use ALPRs maintained by MSP. After a D has been handcuffed police should not tell D that D is "not under arrest" – police will likely be accused later of deceit and trickery.

A thought: There are news stories online that cell phones may be used to do contact tracing for people exposed to COVID-19. If lots of people willingly agree to let their cell phone data be used to track their whereabouts would that ever change courts' view of what society recognizes as a reasonable expectation of privacy? At some point if members of the pub ic come to expect that they're being tracked should police be allowed to use that evidence too? Or at the very least should there be a jury instruction explaining that police have less access to the data than other entities (like software companies or public health agencies)?

As always email me with any questions. Wash your hands!

Marguerite

Marguerite T. Grant
Grizzell Counsel – Director of Training
Office of Norfolk District Attorney Michael W. Morrissey
45 Shawmut Road
Canton, MA 02021
781-830-4159

From: Rudnick, James (NSC)
To: Public, Media (NSC)
Subject: Memo re: Dy SJC ruling D v Pitt with ALPRs on Bourne/Sagamore Bridges not a search
Date: Wednesday, July 15, 2020 8:24:07 AM

April 2020



Chiefs
Commonwealth v. McCarthy (SJC 12750) ← click on that link to see the case
In this case the SJC ruled that police tracking D's car using 4 automatic license plate readers (ALPRs) at both ends of the Bourne and Sagamore Bridges was too limited to amount to a constitutional "search." The SJC declined to say exactly how detailed digital surveillance would have to be to constitute a search leaving that issue for future cases.

State Po ice maintain ALPRs including ones at both ends of the Bourne and Sagamore Bridges. (p.3) The ALPRs photograph vehicles' license plates; that data along with the date and time of the sighting is retained by EOPPS for a year. (p.3-4) Authorized users including police may put a license plate number on a "hot list " and receive an alert if that plate is sighted; reasons to put someone on the "hot list" include not only criminal investigations but also Amber alerts missing persons and BOLO alerts. (p. 3 25 n.13)

Through surveillance controlled buys and information from 4 Cis Barnstable police suspected that the co-D was selling heroin out of his house in Barnstable. (p.4) Police saw a black Hyundai driven by D visit there briefly so they suspected that D was the co-D's supplier. Police put the Hyundai's license plate number on the State Police ALPR "hot list " so that they'd be notified whenever the Hyundai crossed one of the bridges. (p.5) After getting an alert that the Hyundai had crossed onto the Cape police followed both the Hyundai and the co-D to the buy location on a quiet residential street where D and co-D met for about 30 seconds but police could not see a physical exchange. (p.5) From the ALPR data police generated a spreadsheet showing that in mid-winter the Hyundai had crossed the bridges dozens of times sometimes more than once a day adding to police suspicion that D was the heroin supplier. (p.5-6) When police got a second alert that the Hyundai had crossed onto the Cape they again followed D and co-D to the buy location and saw a 30-second meeting but could not see any exchange. This time police stopped both cars handcuffed both co-D and D and read them Miranda. On co-D police found heroin; on D police found 2 cell phones and cash. (p.6-7) At the station police repeatedly told D he was "not under arrest " and D made statements.

D moved to suppress the ALPR data his statements and evidence obtained from the stop. A Superior Court judge found that the moment of arrest was when D and co-D were handcuffed at the scene of the traffic stop but denied the motion to suppress. (p.33) The SJC upheld the denial.

ALPRs and expectation of privacy in digital surveillance: At some length the SJC discussed the constitutional issues raised by digital surveillance. (p.7-29) Police conduct amounts to a search if: (1) it intrudes on a D's expectation of privacy and (2) society is willing to recognize the expectation of privacy as reasonable. Here the SJC ruled D did have an expectation of privacy because D and co-D chose a buy location in a quiet residential area. (p.8 n.5) As to what expectation of privacy society recognizes as reasonable with regard to digital surveillance the SJC was guided by historical understandings of what was an unreasonable search and seizure when the U.S. and Mass. Constitutions were adopted in the late 1700s in reaction to redcoats' rummaging without restraint through colonists' homes. (p.8-10) New technologies like ALPRs raise difficult legal issues because they are easier and less expensive for police than traditional surveillance can be done secretly and permit police to search back in time for a vehicle's movements even before police suspicion arose. (p.12-14) Society does not recognize as reasonable an expectation of privacy in what someone "knowingly exposes" to public view like a license plate – which by statute must be "displayed conspicuously." (p.15-16 & n.8) In older cases involving less advanced technology courts have held that a D did not have an expectation of privacy in contents of a phone conversation in a phone booth or a radio beeper" tracking a single journey. (p14-17) But technology like ALPRs GPS and CSLI are different because they may give police a **mosaic** of information where each piece may be public but when viewed together they create a picture that implicates someone's privacy interests like their political religious or sexual associations. (p.17-21) The SJC was concerned that with enough ALPRs police could track someone's location everywhere which would be "creepy." (p.25) Exigent circumstances would likely justify using an ALPR in a situation involving an Amber alert or missing person. (p.25 n.13) The D urged the SJC to consider not just these four ALPRs on the Bourne and Sagamore Bridges but the hundreds of ALPRs across Massachusetts; the SJC declined to do so because that evidence is not in the record of this case. (p.26) The **limited number of cameras** here and their placements on the bridges was not enough to give D an expectation of privacy that society would recognize as reasonable. (p.28) The SJC declined to say how much digital surveillance would give such an expectation and admitted that its unwillingness to do so "**may bring some interim confusion**" until further cases develop the law on this issue. (p.28 n.15) Chief Justice Gants wrote a separate concurrence suggesting that one thing the SJC could do is to require police who want to search a vast amount of digital data to apply for a court order supported by an affidavit showing reasonable suspicion to do so. (concurrence p.3) This would be like a SW but with a lower standard than PC.

Written policy: The SJC rejected D's argument that Barnstable PD should have had a written policy about ALPRs and the MSP policy on which Barnstable relied was not specific enough. (p.30) Written policies are required to justify certain exceptions to the SW requirement (like inventory searches and sobriety checkpoints) – they do not apply to the threshold question whether a search occurred in the first place. (p.31)

Miranda issue: At the station police repeatedly told D that D was "not under arrest." But the motion judge found that the moment of arrest was when police handcuffed D at the traffic stop. (p.33) D argued that his statements should be suppressed because police telling him he was not under arrest amounted to "deceit or trickery" to get D to confess. The motion judge and the SJC rejected that argument saying that even if telling D he was not under arrest amounted to deceit or trickery it was just one factor to be used in determining voluntariness.

Bottom line: Police use of ALPRs at limited locations is not a constitutional search – but we don't know how many locations it'd have to be to amount to one. Using an ALPR in **exigent circumstances** like an Amber Alert is likely OK. Local police don't need a written policy to use ALPRs maintained by MSP. After a D has been handcuffed police should not tell D that D is "not under arrest" – police will likely be accused later of deceit and trickery.

A thought: There are news stories online that cell phones may be used to do contact tracing for people exposed to COVID-19. If lots of people willingly agree to let their cell phone data be used to track their whereabouts would that ever change courts' view of what society recognizes as a reasonable expectation of privacy? At some point if members of the pub ic come to expect that they're being tracked should police be allowed to use that evidence too? Or at the very least should there be a jury instruction explaining that police have less access to the data than other entities (like software companies or public health agencies)?

As always email me with any questions. Wash your hands!

Marguerite

Marguerite T. Grassa
General Counsel + Director of Training
Office of Norfolk District Attorney Michael W. Morrissey
45 Shawmut Road
Canton, MA 02021
781-830-4819

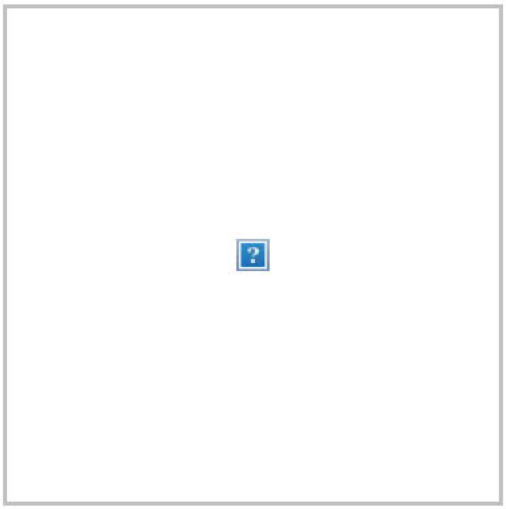
From: Traffic Technology Today
To: Griffin, Daniel (POL)
Subject: Covid-19: London to rapidly expand space for cycling and walking, post-lockdown
Date: Thursday, May 7, 2020 6:57:10 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

View this email online

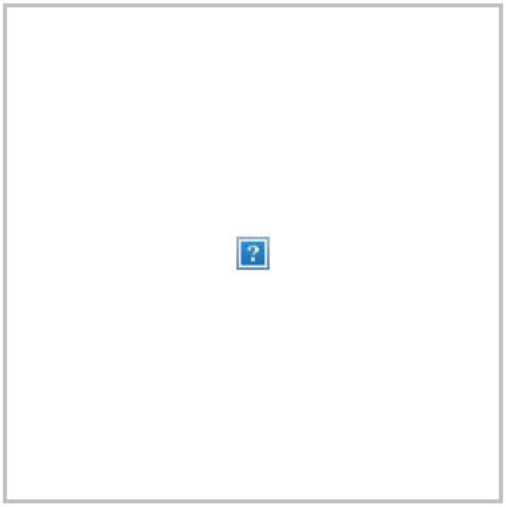
TOP NEWS THIS WEEK

Covid-19: London to rapidly expand space for cycling and walking, post-lockdown



Transport for London (TfL) and London Mayor Sadiq Kahn are preparing to rapidly expand physical infrastructure dedicated to cycling and walking in the capital, to relieve pressure on other transport modes and help enable social distancing, post-Covid-19 lockdown **more...**

World's most powerful city mayors join to pledge "no return to business as usual" post Covid-19

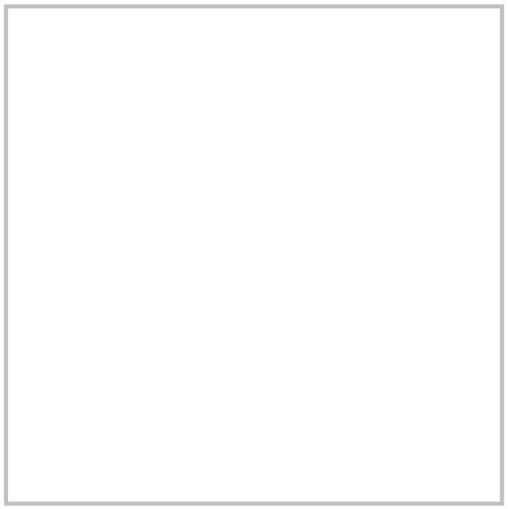


As the world begins to look to defining the 'new normal' post-coronavirus lockdowns, mayors from around the world – part of the C40 climate leadership group – have joined together to seize the opportunity to make the recovery one that is defined by sustainability and low emissions **more...**

PODCAST LAUNCH EPISODE!

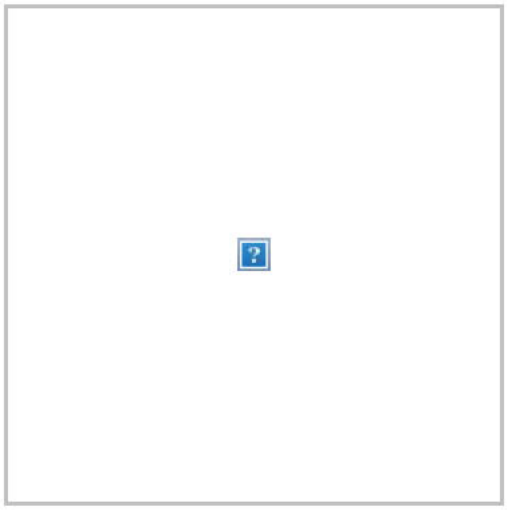
Adapting to the Covid-19 world: Interview with JJ Eden

FIRST EVER TRAFFIC TECHNOLOGY INTERNATIONAL PODCAST! Covid-19 has taken the world by surprise, endangering millions, affecting billions and changing the workplace for everyone. We speak to JJ Eden, executive director of North Carolina Turnpike, tolling giant and co-founder of the E-Z Pass network, to gauge how traffic is being affected by the pandemic. Plus news and conversation



with TTi editors Tom Stone and Saul Wordsworth **more...**

Podcast preview: video clip



Check out this quick video clip from the podcast interview, which captures JJ Eden and Tom Stone chatting using the video conferencing software we have all become so accustomed to in the past few weeks **more...**

More Covid-19 News…

- VIDEO: ITS leaders discuss post-Covid transport world
- MaaS tech firm launches transit occupancy feature to assist social distancing
- Covid-19: New data analysis techniques show 88% reduction in traffic in Melbourne

Bookmark our Covid-19 news hub, to stay up-to-date, every day

MORE NEWS…

- UK's biggest road project opens to traffic eight months early
- UK's Transport for West Midlands commissions new data sharing platform
- 5G NetMobil project delivers V2X standardisation recommendations
- Q-Free teams up with Raytheon to improve ALPR and tolling for MassDOT
- Ubicquia acquires AI platform to strengthen its smart city, traffic optimisation services

NEW: DOWNLOAD FULL MAGAZINE PDF HERE

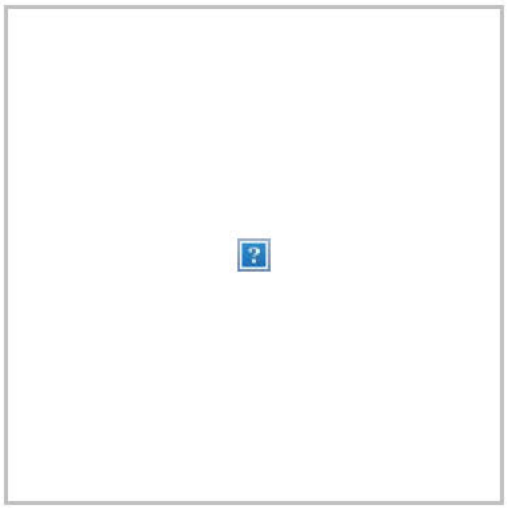




<< LOW EMISSION ZONES

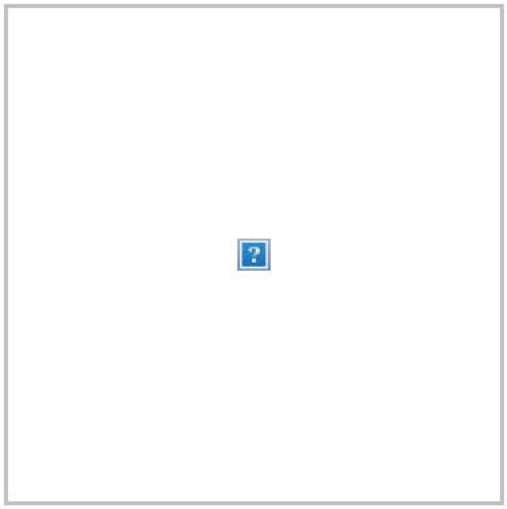
JUST BE CAZ

How the city of Birmingham's emissions-based private-car restrictions (the first in the UK outside London) will be enforced



<< WORKZONES
SMART WORKZONES AHEAD

Workzones are notoriously dangerous for those driving or working in them, but research into connected and automated technologies is helping to rectify this situation



<< COVID-19
GREG WINFREE

The Mode Warrior begins the debate on ways transportation in our interconnected world should change in order to better protect public health, in light of the coronavirus pandemic

CLICK HERE TO RECEIVE YOUR FREE COPY

If you wish to unsubscribe from Traffic Technology International News emails, please click here.
To understand how we process, use & safeguard your data, please read our Privacy Policy. If you would like to update your marketing contact preferences, then please click here.

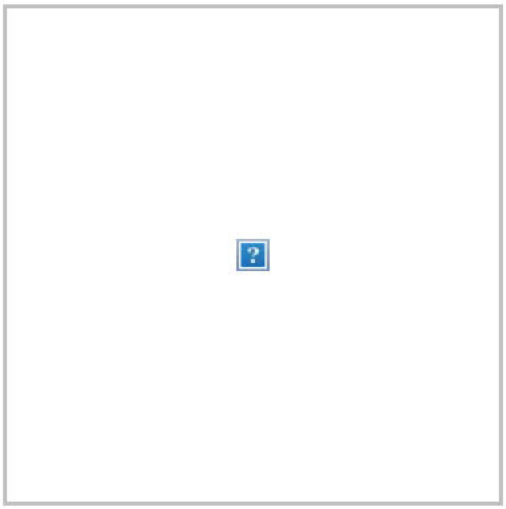
From: Traffic Technology Today
To: zzDowd, Timothy (POL)
Subject: Covid-19: London to rapidly expand space for cycling and walking, post-lockdown
Date: Thursday, May 7, 2020 6:58:49 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

View this email online

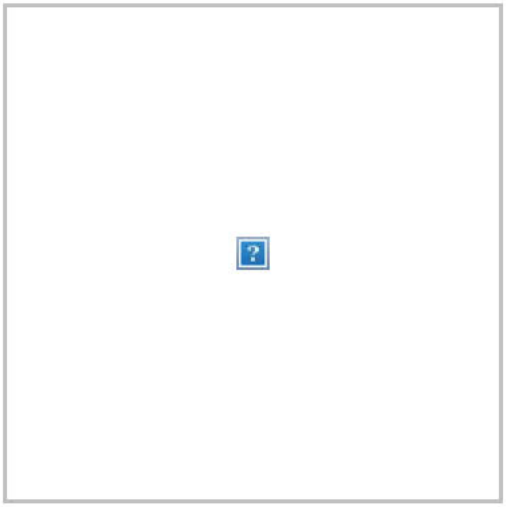
TOP NEWS THIS WEEK

Covid-19: London to rapidly expand space for cycling and walking, post-lockdown



Transport for London (TfL) and London Mayor Sadiq Kahn are preparing to rapidly expand physical infrastructure dedicated to cycling and walking in the capital, to relieve pressure on other transport modes and help enable social distancing, post-Covid-19 lockdown **more...**

World's most powerful city mayors join to pledge "no return to business as usual" post Covid-19

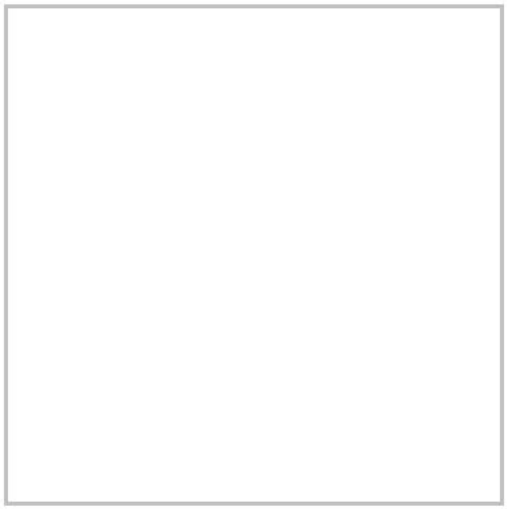


As the world begins to look to defining the 'new normal' post-coronavirus lockdowns, mayors from around the world – part of the C40 climate leadership group – have joined together to seize the opportunity to make the recovery one that is defined by sustainability and low emissions **more...**

PODCAST LAUNCH EPISODE!

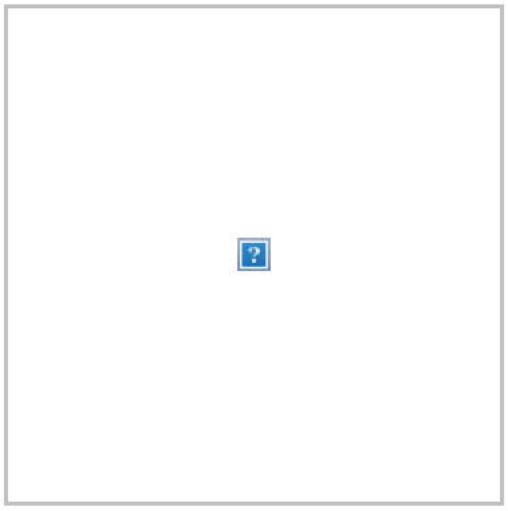
Adapting to the Covid-19 world: Interview with JJ Eden

FIRST EVER TRAFFIC TECHNOLOGY INTERNATIONAL PODCAST! Covid-19 has taken the world by surprise, endangering millions, affecting billions and changing the workplace for everyone. We speak to JJ Eden, executive director of North Carolina Turnpike, tolling giant and co-founder of the E-Z Pass network, to gauge how traffic is being affected by the pandemic. Plus news and conversation



with TTi editors Tom Stone and Saul Wordsworth more...

Podcast preview: video clip



Check out this quick video clip from the podcast interview, which captures JJ Eden and Tom Stone chatting using the video conferencing software we have all become so accustomed to in the past few weeks more...

More Covid-19 News…

- **VIDEO: ITS leaders discuss post-Covid transport world**
- **MaaS tech firm launches transit occupancy feature to assist social distancing**
- **Covid-19: New data analysis techniques show 88% reduction in traffic in Melbourne**

Bookmark our Covid-19 news hub, to stay up-to-date, every day

MORE NEWS…

- UK's biggest road project opens to traffic eight months early
- UK's Transport for West Midlands commissions new data sharing platform
- 5G NetMobil project delivers V2X standardisation recommendations
- Q-Free teams up with Raytheon to improve ALPR and tolling for MassDOT
- Ubicquia acquires AI platform to strengthen its smart city, traffic optimisation services

NEW: DOWNLOAD FULL MAGAZINE PDF HERE

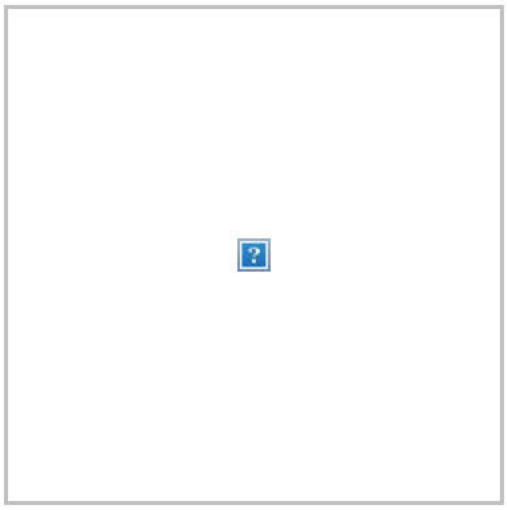




<< LOW EMISSION ZONES

JUST BE CAZ

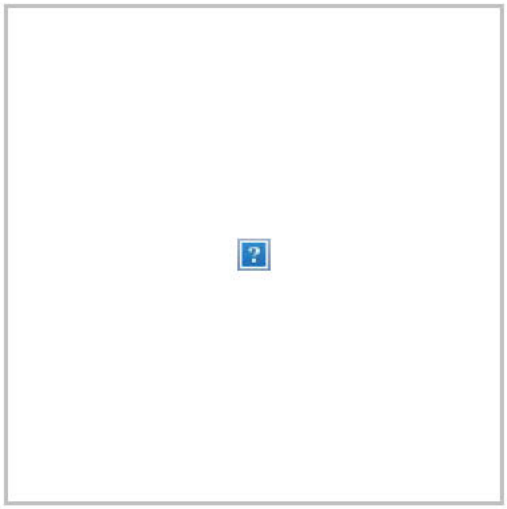
How the city of Birmingham's emissions-based private-car restrictions (the first in the UK outside London) will be enforced



<< WORKZONES

SMART WORKZONES AHEAD

Workzones are notoriously dangerous for those driving or working in them, but research into connected and automated technologies is helping to rectify this situation



<< COVID-19

GREG WINFREE

The Mode Warrior begins the debate on ways transportation in our interconnected world should change in order to better protect public health, in light of the coronavirus pandemic

CLICK HERE TO RECEIVE YOUR FREE COPY

If you wish to unsubscribe from Traffic Technology International News emails, please click here.

To understand how we process, use & safeguard your data, please read our Privacy Policy. If you would like to update your marketing contact preferences, then please click here.

From: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: DHS: Agents targeting "violent criminals"; Gag order lifted in Floyd case
Date: Wednesday, July 22, 2020 2:09:12 PM

July 22, 2020 | View as webpage

TOP STORIES

Federal officials say agents in Portland are legally targeting 'violent criminals'

"We are not patrolling the streets of Portland, as has been falsely reported multiple times in the last few days," Chad Wolf, the acting secretary of DHS, said

Chicago mayor expects influx of federal agents but warns 'we do not welcome dictatorship'

Police chiefs criticize Mass. lawmakers on rushing reform bills

Video: Calif. congresswoman monitors LEOs conducting traffic stop

Starbucks worker charged after 'bragging' about spitting in cop's coffee, police chief says

Minnesota judge lifts gag order in George Floyd case

FEATURED CONTENT

Lessons from the Norway

terror attack

By Mike Wood

It was estimated that 1 in 4 Norwegians knew someone who had been directly affected by the deadliest attack in Norway since World War II



The AAR: An effective assessment tool for police

By International Public Safety Association

The After-Action Review is an extremely effective method of analyzing what occurred and how to improve performance in the future

Do You Think Your Agency Is Too Small for ALPR?



Read how Leonardo's license plate readers bring efficiency and cost savings to daily policework and investigations at agencies small to large.

Download the e-book now

How to Speed up Use-Of-Force Investigations



Show transparency and accountability using purpose-built software to document and investigate.

Learn more

OTHER HIGHLIGHTS



Building trust one conversation at a time

By Ed Wojcicki

Discussions between the Illinois NAACP and Illinois police chiefs identified common ground between local LE and the

communities they serve



4 ways officers can improve neighborhood relationships

By Booker Hodges

If you know more criminals on your beat than citizens you protect, that's a problem – here are four ways to remedy that



SPONSORED CONTENT



When this officer went down, his body camera system sent help

One officer's story of distress and assistance illustrates how a bodycam can do more than record video – it can be a lifesaver.



FEATURED JOB



Recruit Police Officer/Lateral Police Officer Job

Top Pay: $105,248 annual.

FEATURED EDUCATION



Study Criminal Justice @ Boston University

Gain skills and expertise in Crime Analysis, Strategic Management, and Cybercrime through BU MET's part-time, 100% online grad programs in Criminal Justice.



Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: FBI National Academy Associates, Inc.
To: McCarthy, Steven (POL)
Subject: FBINAA Training Bulletin
Date: Tuesday, June 16, 2020 10:47:20 AM

VISIT ALL TRAINING & WEBINARS

FBINAA APB Leadership Podcast Series
COMING SOON!

Plan on joining us monthly for the launch of the **FBINAA APB Leadership Podcast Series**. This Series will engage law enforcement and public safety executives in discussions on timely and current topics affecting first responders around the world. These leaders will share with you their leadership and managerial philosophies and successes and obstacles they have encountered in their careers.

The podcasts **are free audio programs distributed to FBI National Academy Associates' members, their staffs, and other law enforcement executives that** provide our communities, states, countries, and profession with the highest degree of law enforcement professionalism and expertise.

NEW RELEASES:
1st Wednesday/Month

A new APB Leadership Podcast will be available the first Wednesday of each Month.

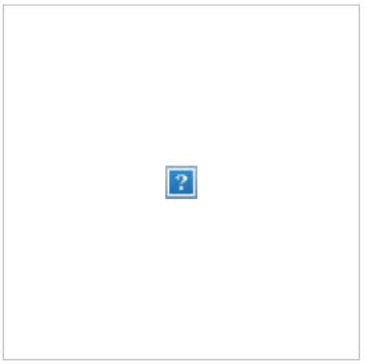
TRAINING WEBINAR SERIES

Engage the Community by Leveraging License Plate Recognition Technology

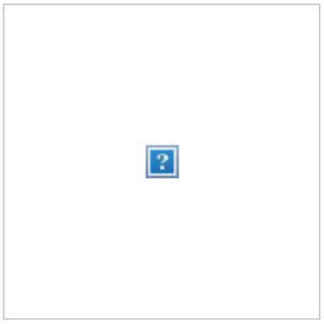
In this webinar, you will learn how license plate recognition (LPR) data that is captured by the community and civilian agencies can support public safety efforts in real-time. Experience live LPR demonstrations and training tips that can be implemented in your current operations. Our panel of industry practitioners will guide you through best practices and LPR use cases that can help you bolster your operations and enhance community engagement when fighting crime.

Key takeaways:

- Firsthand LPR technology best practices to implement within your operations
- Insights on how to engage your community with technology to enhance crime-fighting efforts
- Key considerations when implementing new LPR technologies into your current systems and operations



Tuesday, June 16, 2020
11:00 am ET | 8:00 am PT



TRAINING WEBINAR SERIES

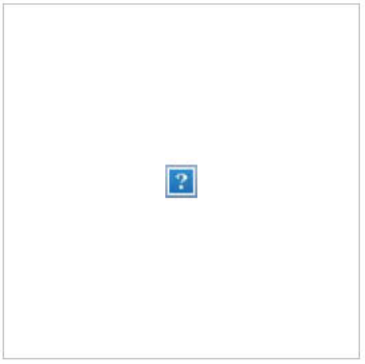
Advanced Investigative Call Data Records (CDR) Cleansing & Analysis

JOIN US and Discover How to Optimize Call Data Records (CDR) Cleansing and Analysis Which Typically Results in Solving Cases Faster and Saving Analysts 97% of Time Spent on a Case.

Chorus is the leading provider of data cleansing and analysis software in the UK and is used by 80% of regional police forces, all Counter Terror Units and the Home Office. Chorus is now making its software available for North American law enforcement.

Chorus is exceptional at:

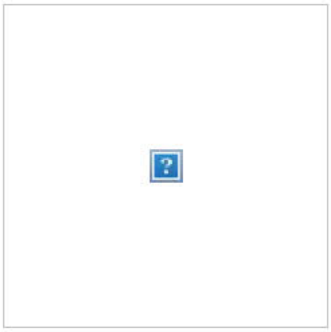
- **Rules-based data cleansing.** Taking communications data from providers such as T-Mobile, AT&T, Sprint and Verizon in the USA as well as Bell, Telus and Rogers Communications in Canada, removing the noise and normalizing it ready for analysis.
- **Connecting data.** Combining disparate data such



Thursday, June 25, 2020
11:00 am ET | 8:00 am PT

as CDR, ALPR, RF surveys and device downloads and overlaying it with communications data to spot crucial connections using maps and charts.
- **Evidence quality reporting**. Maintaining data integrity so reports and maps can be used in court as evidence.
- **Integration with IBM® i2 products.**



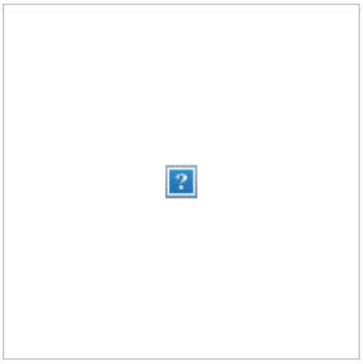


HIDS VIRTUAL CONFERENCE

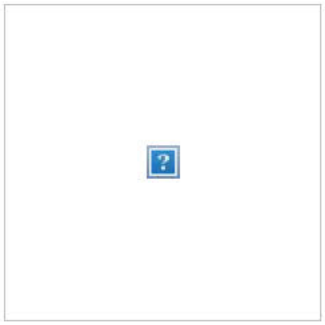
6th Annual Human Identification Solutions (HIDS) Conference

HIDS provides a unique platform for forensic scientists, practitioners, and criminal investigators from around the world to discuss the latest developments and trends in forensic DNA analysis, as well as the importance of effective partnerships between investigators and forensic scientists in solving crimes faster.

HIDS sessions across all regions will feature over 40 of the most prominent speakers in the industry including forensic scientists, criminal investigators, and legal experts to discuss their findings and best practices.



June 24-25, 2020



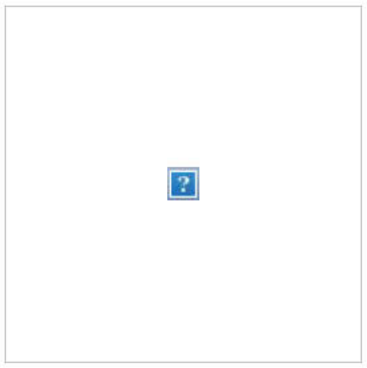
SCHOOL SHOOTING PREVENTION LEADERSHIP FORUM

Phoenix, AZ

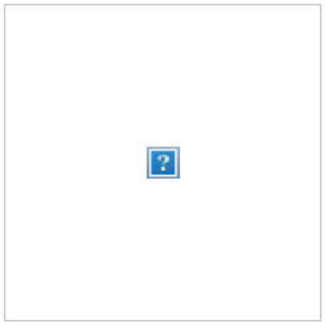
Each day law enforcement and school districts across the United States are responsible for protecting our almost 133,000 schools and 63 million students, faculty, and staff. The **FBI National Academy Associates** and the **School Safety Advocacy Council** have partnered and announced a series of 2-day Leadership Forums for law enforcement executives and school administrators throughout the country. The Forums will provide attendees with the knowledge, skills, and resources needed to improve the overall security of their community's schools while developing coordinated plans for a crisis response.

Program Overview:

- Review of school security trends & threat concerns
- Lessons learned: A review of past incidents
- The dynamics of active assailant situation
- Multi-agency response: Coordinating law enforcement, fire, EMS, and schools
- Understanding and conducting a school security survey & assessment
- Building capacity; Conducting Drills and Exercises



October 7-8, 2020
Phoenix, AZ



Who Should Attend

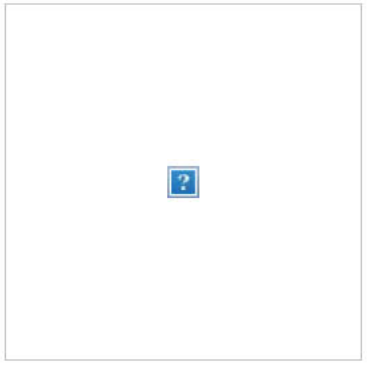
Law Enforcement Commanders
School Administrators
School Resource Officers
Fire/EMS Officials
School Security Directors

SCHOOL SHOOTING PREVENTION LEADERSHIP FORUM
Detroit, MI

Each day law enforcement and school districts across the United States are responsible for protecting our almost 133,000 schools and 63 million students, faculty, and staff. The **FBI National Academy Associates** and the **School Safety Advocacy Council** have partnered and announced a series of 2-day Leadership Forums for law enforcement executives and school administrators throughout the country. The Forums will provide attendees with the knowledge, skills, and resources needed to improve the overall security of their community's schools while developing coordinated plans for a crisis response.

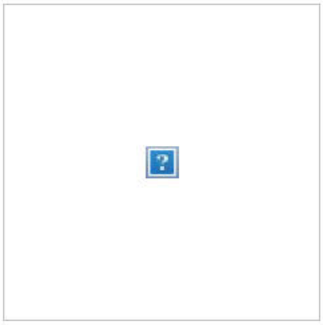
Program Overview:

- Review of school security trends & threat concerns
- Lessons learned: A review of past incidents
- The dynamics of active assailant situation
- Multi-agency response: Coordinating law enforcement, fire, EMS, and schools
- Understanding and conducting a school security survey &



October 27-28, 2020
Detroit, MI

assessment
- Building capacity; Conducting Drills and Exercises



For additional information:
Contact John Kennedy
at jkennedy@fbinaa.org.

For hotel/agenda/logistics:
Contact Laura Masterton
at lmasterton@fbinaa.org.

For Sponsorship Opportunities:
Contact Greg Guiton
at gguiton@fbinaa.org

CO-HOST A WEBINAR WITH THE FBINAA

Sponsorships Are Available!

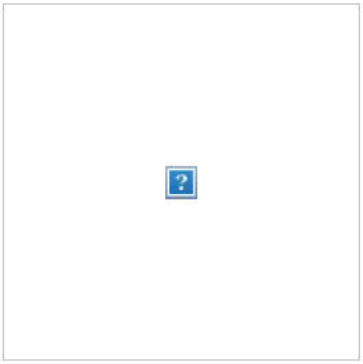
Share Your Thought Leadership and Professional Expertise by Being a Part of the 2020 FBINAA Leadership Webinar Series

These 60-90 minute webinars focus on cutting-edge law enforcement topics and trends and are delivered by law enforcement and public safety experts. Sponsorship provides your organization the opportunity to discuss your products and services to a focused audience, as well as, contributing to the knowledge base of the law enforcement profession. Your Marketing messages will be seen by hundreds of law enforcement professionals with interest in your products/services.

Sponsorships are available! Selected companies will pay a $4,000 sponsorship fee which allows them the use of their company logo and product/service information in the introduction to the educational session. Those selected will also be provided a list of webinar dates throughout 2020 from which they can choose on a first-come, first-serve basis.

These webinars are free to FBINAA members and non-members who can listen in live or get access to the recorded version after the event.

Please contact John Kennedy, Director of Education & Training, for further information at jkennedy@fbinaa.org or call (630) 464-7637.



Did You Know....

FBINAA members control assets and services well in excess of $100 Billion dollars each year, representing significant purchasing power and influence.

COLLABORATIVE REFORM INITIATIVE TECHNICAL ASSISTANCE CENTER: CRI-TAC

As part of our roles and responsibilities as a partner in the COPS Collaborative Reform Initiative Technical Assistance Center (CRI-TAC) Project, each partner has been asked to compile a list of Subject Matter Experts (SMEs) in the CRI-TAC priority areas. The selection of the SMEs will be related to each partner's membership and constituent base (can be both sworn and non-sworn) and will be included in the CRI-TA Resource Center. The CRI-TA Resource Center will be designed to support law enforcement agencies and provides free, customized technical assistance solutions designed to meet the unique needs of state, local, tribal, and campus communities throughout the United States.

CLICK HERE for additional information.

Questions & Information:
For questions and information regarding training programs, registrations, agendas and hotel accommodations, please contact Laura Masterton at lmasterton@fbinaa.org or (540) 810-2725.

Please contact John Kennedy with questions on Training and Webinars at jkennedy@fbinaa.org or (630) 464-7637.

Visit our website

The Mission of the FBINAA is "Impacting communities by providing and promoting law enforcement leadership through training and networking." We are committed to providing cutting-edge education and training to our members around the globe. Our goal is to increase the number of education and training opportunities for our members. Interested in co-hosting a Webinar with the FBINAA? Please contact John Kennedy, Director, Education & Training, at jkennedy@fbinaa.org.

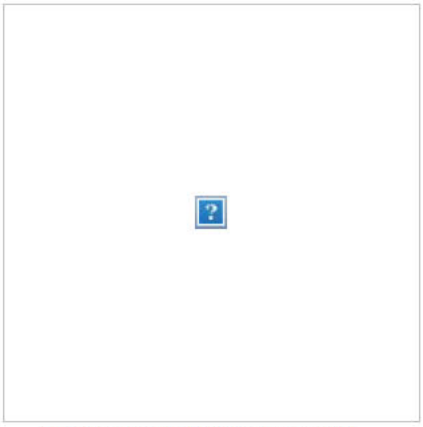
STAY CONNECTED

FBI National Academy Associates, Inc. | FBI Academy, Quantico, VA 22135

Unsubscribe steven.mccarthy@pol.state.ma.us

Update Profile | About Constant Contact

Sent by do-not-reply@fbinaa.org in collaboration with



Try email marketing for free today!

From: FBI National Academy Associates, Inc.
To: Wilcox, Christopher (POL)
Subject: FBINAA Training Bulletin
Date: Tuesday, June 16, 2020 10:47:18 AM

VISIT ALL TRAINING & WEBINARS

FBINAA APB Leadership Podcast Series
COMING SOON!

Plan on joining us monthly for the launch of the **FBINAA APB Leadership Podcast Series**. This Series will engage law enforcement and public safety executives in discussions on timely and current topics affecting first responders around the world. These leaders will share with you their leadership and managerial philosophies and successes and obstacles they have encountered in their careers.

The podcasts **are free audio programs distributed to FBI National Academy Associates' members, their staffs, and other law enforcement executives that** provide our communities, states, countries, and profession with the highest degree of law enforcement professionalism and expertise.

NEW RELEASES:
1st Wednesday/Month

A new APB Leadership Podcast will be available the first Wednesday of each Month.

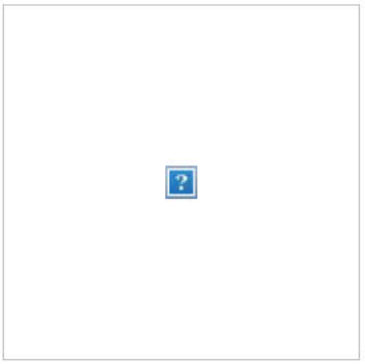
TRAINING WEBINAR SERIES

Engage the Community by Leveraging License Plate Recognition Technology

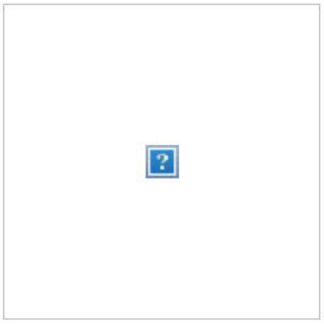
In this webinar, you will learn how license plate recognition (LPR) data that is captured by the community and civilian agencies can support public safety efforts in real-time. Experience live LPR demonstrations and training tips that can be implemented in your current operations. Our panel of industry practitioners will guide you through best practices and LPR use cases that can help you bolster your operations and enhance community engagement when fighting crime.

Key takeaways:

- Firsthand LPR technology best practices to implement within your operations
- Insights on how to engage your community with technology to enhance crime-fighting efforts
- Key considerations when implementing new LPR technologies into your current systems and operations



Tuesday, June 16, 2020
11:00 am ET | 8:00 am PT



TRAINING WEBINAR SERIES

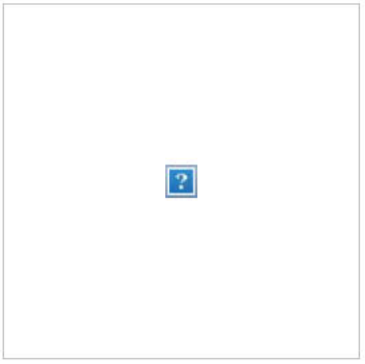
Advanced Investigative Call Data Records (CDR) Cleansing & Analysis

JOIN US and Discover How to Optimize Call Data Records (CDR) Cleansing and Analysis Which Typically Results in Solving Cases Faster and Saving Analysts 97% of Time Spent on a Case.

Chorus is the leading provider of data cleansing and analysis software in the UK and is used by 80% of regional police forces, all Counter Terror Units and the Home Office. Chorus is now making its software available for North American law enforcement.

Chorus is exceptional at:

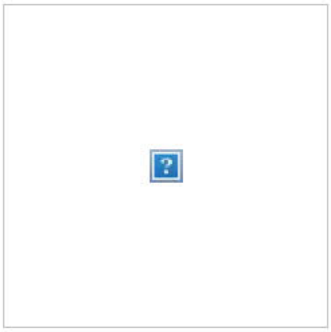
- **Rules-based data cleansing.** Taking communications data from providers such as T-Mobile, AT&T, Sprint and Verizon in the USA as well as Bell, Telus and Rogers Communications in Canada, removing the noise and normalizing it ready for analysis.
- **Connecting data.** Combining disparate data such



Thursday, June 25, 2020
11:00 am ET | 8:00 am PT

as CDR, ALPR, RF surveys and device downloads and overlaying it with communications data to spot crucial connections using maps and charts.
- **Evidence quality reporting**. Maintaining data integrity so reports and maps can be used in court as evidence.
- **Integration with IBM® i2 products.**



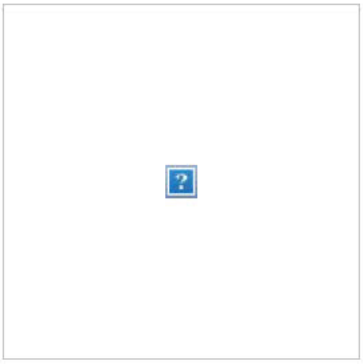


HIDS VIRTUAL CONFERENCE

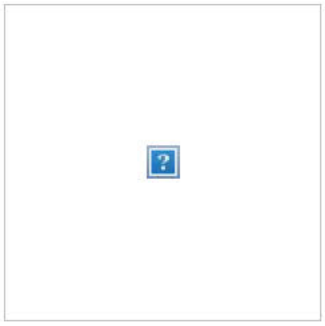
6th Annual Human Identification Solutions (HIDS) Conference

HIDS provides a unique platform for forensic scientists, practitioners, and criminal investigators from around the world to discuss the latest developments and trends in forensic DNA analysis, as well as the importance of effective partnerships between investigators and forensic scientists in solving crimes faster.

HIDS sessions across all regions will feature over 40 of the most prominent speakers in the industry including forensic scientists, criminal investigators, and legal experts to discuss their findings and best practices.



June 24-25, 2020



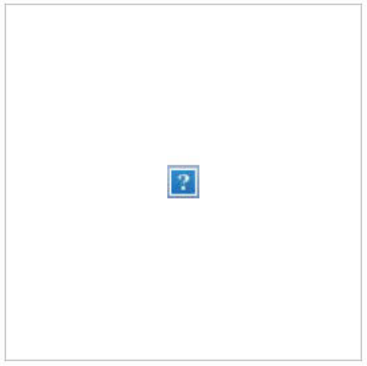
SCHOOL SHOOTING PREVENTION LEADERSHIP FORUM

Phoenix, AZ

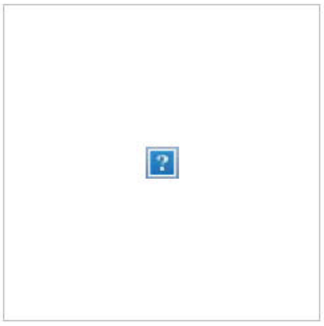
Each day law enforcement and school districts across the United States are responsible for protecting our almost 133,000 schools and 63 million students, faculty, and staff. The **FBI National Academy Associates** and the **School Safety Advocacy Council** have partnered and announced a series of 2-day Leadership Forums for law enforcement executives and school administrators throughout the country. The Forums will provide attendees with the knowledge, skills, and resources needed to improve the overall security of their community's schools while developing coordinated plans for a crisis response.

Program Overview:

- Review of school security trends & threat concerns
- Lessons learned: A review of past incidents
- The dynamics of active assailant situation
- Multi-agency response: Coordinating law enforcement, fire, EMS, and schools
- Understanding and conducting a school security survey & assessment
- Building capacity; Conducting Drills and Exercises



October 7-8, 2020
Phoenix, AZ



Who Should Attend

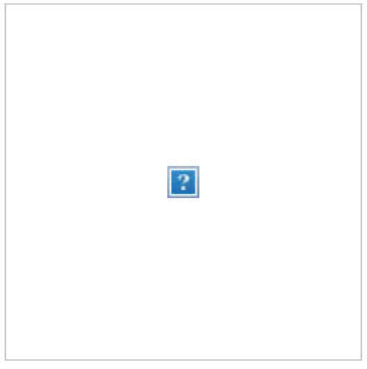
Law Enforcement Commanders
School Administrators
School Resource Officers
Fire/EMS Officials
School Security Directors

SCHOOL SHOOTING PREVENTION LEADERSHIP FORUM
Detroit, MI

Each day law enforcement and school districts across the United States are responsible for protecting our almost 133,000 schools and 63 million students, faculty, and staff. The **FBI National Academy Associates** and the **School Safety Advocacy Council** have partnered and announced a series of 2-day Leadership Forums for law enforcement executives and school administrators throughout the country. The Forums will provide attendees with the knowledge, skills, and resources needed to improve the overall security of their community's schools while developing coordinated plans for a crisis response.

Program Overview:

- Review of school security trends & threat concerns
- Lessons learned: A review of past incidents
- The dynamics of active assailant situation
- Multi-agency response: Coordinating law enforcement, fire, EMS, and schools
- Understanding and conducting a school security survey &



October 27-28, 2020
Detroit, MI

assessment
- Building capacity; Conducting Drills and Exercises

For additional information:
Contact John Kennedy
at jkennedy@fbinaa.org.

For hotel/agenda/logistics:
Contact Laura Masterton
at lmasterton@fbinaa.org.

For Sponsorship Opportunities:
Contact Greg Guiton
at gguiton@fbinaa.org

CO-HOST A WEBINAR WITH THE FBINAA
Sponsorships Are Available!

Share Your Thought Leadership and Professional Expertise by Being a Part of the 2020 FBINAA Leadership Webinar Series

These 60-90 minute webinars focus on cutting-edge law enforcement topics and trends and are delivered by law enforcement and public safety experts. Sponsorship provides your organization the opportunity to discuss your products and services to a focused audience, as well as, contributing to the knowledge base of the law enforcement profession. Your Marketing messages will be seen by hundreds of law enforcement professionals with interest in your products/services.

Sponsorships are available! Selected companies will pay a $4,000 sponsorship fee which allows them the use of their company logo and product/service information in the introduction to the educational session. Those selected will also be provided a list of webinar dates throughout 2020 from which they can choose on a first-come, first-serve basis.

These webinars are free to FBINAA members and non-members who can listen in live or get access to the recorded version after the event.

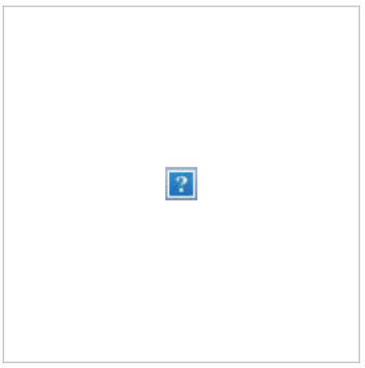
Please contact John Kennedy, Director of Education & Training, for further information at jkennedy@fbinaa.org or call (630) 464-7637.

Did You Know....

FBINAA members control assets and services well in excess of $100 Billion dollars each year, representing significant purchasing power and influence.

COLLABORATIVE REFORM INITIATIVE TECHNICAL ASSISTANCE CENTER: CRI-TAC

As part of our roles and responsibilities as a partner in the COPS Collaborative Reform Initiative Technical Assistance Center (CRI-TAC) Project, each partner has been asked to compile a list of Subject Matter Experts (SMEs) in the CRI-TAC priority areas. The selection of the SMEs will be related to each partner's membership and constituent base (can be both sworn and non-sworn) and will be included in the CRI-TA Resource Center. The CRI-TA Resource Center will be designed to support law enforcement agencies and provides free, customized technical assistance solutions designed to meet the unique needs of state, local, tribal, and campus communities throughout the United States.



CLICK HERE for additional information.

Questions & Information:
For questions and information regarding training programs, registrations, agendas and hotel accommodations, please contact Laura Masterton at lmasterton@fbinaa.org or (540) 810-2725.

Please contact John Kennedy with questions on Training and Webinars at jkennedy@fbinaa.org or (630) 464-7637.

Visit our website

The Mission of the FBINAA is "Impacting communities by providing and promoting law enforcement leadership through training and networking." We are committed to providing cutting-edge education and training to our members around the globe. Our goal is to increase the number of education and training opportunities for our members. Interested in co-hosting a Webinar with the FBINAA? Please contact John Kennedy, Director, Education & Training, at jkennedy@fbinaa.org.

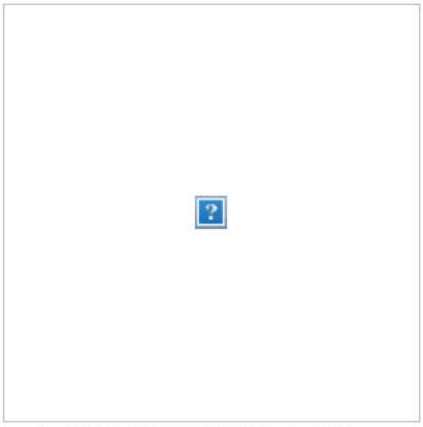
STAY CONNECTED

FBI National Academy Associates, Inc. | FBI Academy, Quantico, VA 22135

Unsubscribe christopher.wilcox@state.ma.us

Update Profile | About Constant Contact

Sent by do-not-reply@fbinaa.org in collaboration with



Try email marketing for free today!

From: FBI National Academy Associates, Inc.
To: D"Amore, Paul (POL)
Subject: FBINAA Training Bulletin
Date: Tuesday, June 16, 2020 10:47:18 AM

VISIT ALL TRAINING & WEBINARS

FBINAA APB Leadership Podcast Series
COMING SOON!

Plan on joining us monthly for the launch of the **FBINAA APB Leadership Podcast Series**. This Series will engage law enforcement and public safety executives in discussions on timely and current topics affecting first responders around the world. These leaders will share with you their leadership and managerial philosophies and successes and obstacles they have encountered in their careers.

The podcasts **are free audio programs distributed to FBI National Academy Associates' members, their staffs, and other law enforcement executives that** provide our communities, states, countries, and profession with the highest degree of law enforcement professionalism and expertise.

NEW RELEASES:
1st Wednesday/Month

A new APB Leadership Podcast will be available the first Wednesday of each Month.

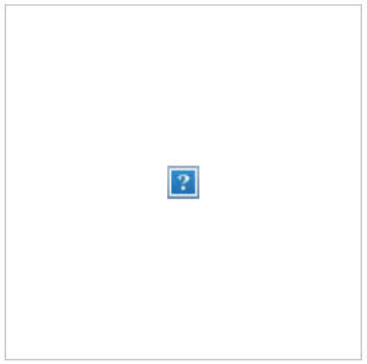
TRAINING WEBINAR SERIES

Engage the Community by Leveraging License Plate Recognition Technology

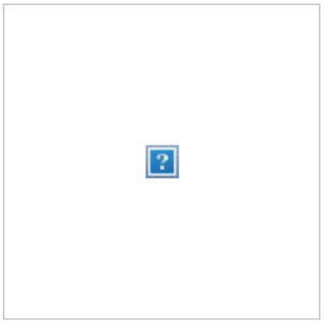
In this webinar, you will learn how license plate recognition (LPR) data that is captured by the community and civilian agencies can support public safety efforts in real-time. Experience live LPR demonstrations and training tips that can be implemented in your current operations. Our panel of industry practitioners will guide you through best practices and LPR use cases that can help you bolster your operations and enhance community engagement when fighting crime.

Key takeaways:

- Firsthand LPR technology best practices to implement within your operations
- Insights on how to engage your community with technology to enhance crime-fighting efforts
- Key considerations when implementing new LPR technologies into your current systems and operations



Tuesday, June 16, 2020
11:00 am ET | 8:00 am PT



TRAINING WEBINAR SERIES

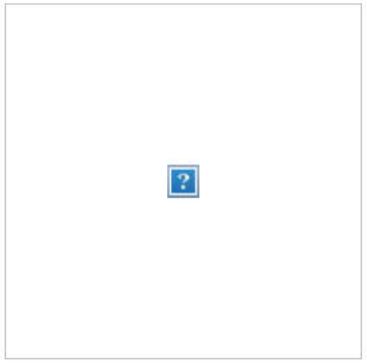
Advanced Investigative Call Data Records (CDR) Cleansing & Analysis

JOIN US and Discover How to Optimize Call Data Records (CDR) Cleansing and Analysis Which Typically Results in Solving Cases Faster and Saving Analysts 97% of Time Spent on a Case.

Chorus is the leading provider of data cleansing and analysis software in the UK and is used by 80% of regional police forces, all Counter Terror Units and the Home Office. Chorus is now making its software available for North American law enforcement.

Chorus is exceptional at:

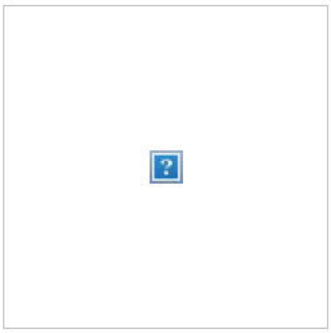
- **Rules-based data cleansing.** Taking communications data from providers such as T-Mobile, AT&T, Sprint and Verizon in the USA as well as Bell, Telus and Rogers Communications in Canada, removing the noise and normalizing it ready for analysis.
- **Connecting data.** Combining disparate data such



Thursday, June 25, 2020
11:00 am ET | 8:00 am PT

as CDR, ALPR, RF surveys and device downloads and overlaying it with communications data to spot crucial connections using maps and charts.
- **Evidence quality reporting**. Maintaining data integrity so reports and maps can be used in court as evidence.
- **Integration with IBM® i2 products.**



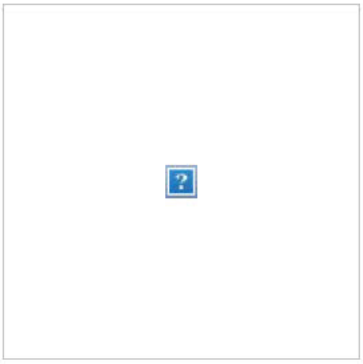


HIDS VIRTUAL CONFERENCE

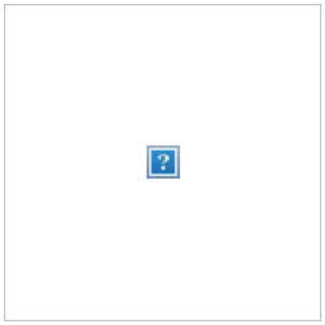
6th Annual Human Identification Solutions (HIDS) Conference

HIDS provides a unique platform for forensic scientists, practitioners, and criminal investigators from around the world to discuss the latest developments and trends in forensic DNA analysis, as well as the importance of effective partnerships between investigators and forensic scientists in solving crimes faster.

HIDS sessions across all regions will feature over 40 of the most prominent speakers in the industry including forensic scientists, criminal investigators, and legal experts to discuss their findings and best practices.



June 24-25, 2020



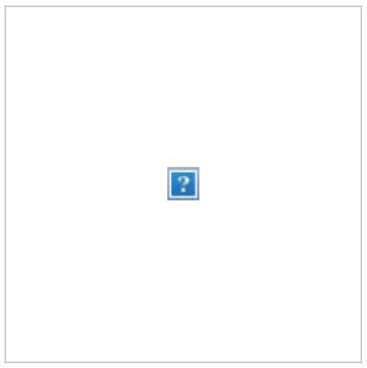
SCHOOL SHOOTING PREVENTION LEADERSHIP FORUM

Phoenix, AZ

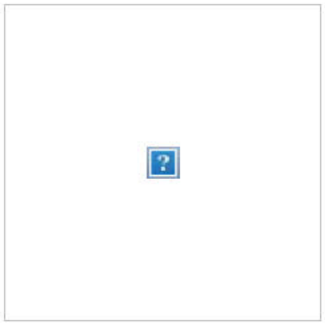
Each day law enforcement and school districts across the United States are responsible for protecting our almost 133,000 schools and 63 million students, faculty, and staff. The **FBI National Academy Associates** and the **School Safety Advocacy Council** have partnered and announced a series of 2-day Leadership Forums for law enforcement executives and school administrators throughout the country. The Forums will provide attendees with the knowledge, skills, and resources needed to improve the overall security of their community's schools while developing coordinated plans for a crisis response.

Program Overview:

- Review of school security trends & threat concerns
- Lessons learned: A review of past incidents
- The dynamics of active assailant situation
- Multi-agency response: Coordinating law enforcement, fire, EMS, and schools
- Understanding and conducting a school security survey & assessment
- Building capacity; Conducting Drills and Exercises



October 7-8, 2020
Phoenix, AZ



Who Should Attend

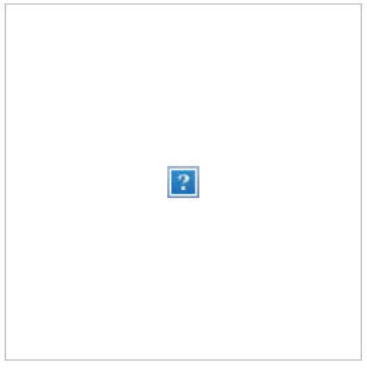
Law Enforcement Commanders
School Administrators
School Resource Officers
Fire/EMS Officials
School Security Directors

SCHOOL SHOOTING PREVENTION LEADERSHIP FORUM
Detroit, MI

Each day law enforcement and school districts across the United States are responsible for protecting our almost 133,000 schools and 63 million students, faculty, and staff. The **FBI National Academy Associates** and the **School Safety Advocacy Council** have partnered and announced a series of 2-day Leadership Forums for law enforcement executives and school administrators throughout the country. The Forums will provide attendees with the knowledge, skills, and resources needed to improve the overall security of their community's schools while developing coordinated plans for a crisis response.

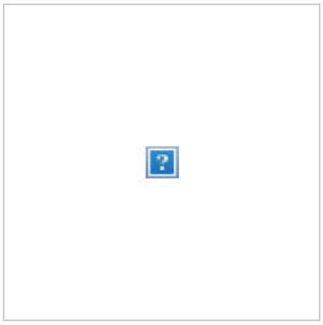
Program Overview:

- Review of school security trends & threat concerns
- Lessons learned: A review of past incidents
- The dynamics of active assailant situation
- Multi-agency response: Coordinating law enforcement, fire, EMS, and schools
- Understanding and conducting a school security survey &



October 27-28, 2020
Detroit, MI

assessment
- Building capacity; Conducting Drills and Exercises



For additional information:
Contact John Kennedy
at jkennedy@fbinaa.org.

For hotel/agenda/logistics:
Contact Laura Masterton
at lmasterton@fbinaa.org.

For Sponsorship Opportunities:
Contact Greg Guiton
at gguiton@fbinaa.org

CO-HOST A WEBINAR WITH THE FBINAA
Sponsorships Are Available!

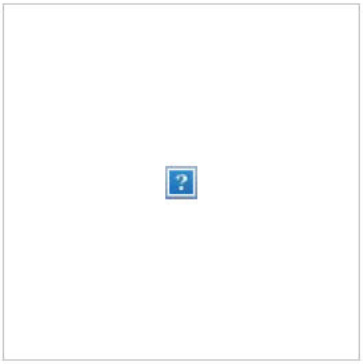
Share Your Thought Leadership and Professional Expertise by Being a Part of the 2020 FBINAA Leadership Webinar Series

These 60-90 minute webinars focus on cutting-edge law enforcement topics and trends and are delivered by law enforcement and public safety experts. Sponsorship provides your organization the opportunity to discuss your products and services to a focused audience, as well as, contributing to the knowledge base of the law enforcement profession. Your Marketing messages will be seen by hundreds of law enforcement professionals with interest in your products/services.

Sponsorships are available! Selected companies will pay a $4,000 sponsorship fee which allows them the use of their company logo and product/service information in the introduction to the educational session. Those selected will also be provided a list of webinar dates throughout 2020 from which they can choose on a first-come, first-serve basis.

These webinars are free to FBINAA members and non-members who can listen in live or get access to the recorded version after the event.

Please contact John Kennedy, Director of Education & Training, for further information at jkennedy@fbinaa.org or call (630) 464-7637.



Did You Know....

FBINAA members control assets and services well in excess of $100 Billion dollars each year, representing significant purchasing power and influence.

COLLABORATIVE REFORM INITIATIVE TECHNICAL ASSISTANCE CENTER: CRI-TAC

As part of our roles and responsibilities as a partner in the COPS Collaborative Reform Initiative Technical Assistance Center (CRI-TAC) Project, each partner has been asked to compile a list of Subject Matter Experts (SMEs) in the CRI-TAC priority areas. The selection of the SMEs will be related to each partner's membership and constituent base (can be both sworn and non-sworn) and will be included in the CRI-TA Resource Center. The CRI-TA Resource Center will be designed to support law enforcement agencies and provides free, customized technical assistance solutions designed to meet the unique needs of state, local, tribal, and campus communities throughout the United States.

CLICK HERE for additional information.

Questions & Information:
For questions and information regarding training programs, registrations, agendas and hotel accommodations, please contact Laura Masterton at lmasterton@fbinaa.org or (540) 810-2725.

Please contact John Kennedy with questions on Training and Webinars at jkennedy@fbinaa.org or (630) 464-7637.

Visit our website

The Mission of the FBINAA is "Impacting communities by providing and promoting law enforcement leadership through training and networking." We are committed to providing cutting-edge education and training to our members around the globe. Our goal is to increase the number of education and training opportunities for our members. Interested in co-hosting a Webinar with the FBINAA? Please contact John Kennedy, Director, Education & Training, at jkennedy@fbinaa.org.

STAY CONNECTED

FBI National Academy Associates, Inc. | FBI Academy, Quantico, VA 22135

Unsubscribe paul.d'amore@massmail.state.ma.us

Update Profile | About Constant Contact

Sent by do-not-reply@fbinaa.org in collaboration with

Try email marketing for free today!

From: FBI National Academy Associates, Inc.
To: Upton, Paul (POL)
Subject: FBINAA Training Bulletin
Date: Tuesday, June 16, 2020 10:47:17 AM

VISIT ALL TRAINING & WEBINARS



FBINAA APB Leadership Podcast Series
COMING SOON!

Plan on joining us monthly for the launch of the **FBINAA APB Leadership Podcast Series**. This Series will engage law enforcement and public safety executives in discussions on timely and current topics affecting first responders around the world. These leaders will share with you their leadership and managerial philosophies and successes and obstacles they have encountered in their careers.

The podcasts **are free audio programs distributed to FBI National Academy Associates' members, their staffs, and other law enforcement executives that** provide our communities, states, countries, and profession with the highest degree of law enforcement professionalism and expertise.

NEW RELEASES:
1st Wednesday/Month

A new APB Leadership Podcast will be available the first Wednesday of each Month.

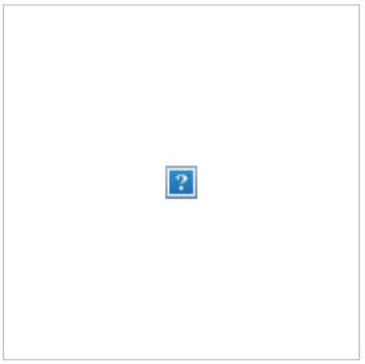
TRAINING WEBINAR SERIES

Engage the Community by Leveraging License Plate Recognition Technology

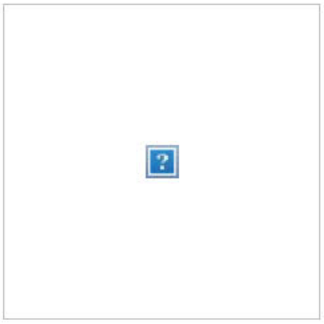
In this webinar, you will learn how license plate recognition (LPR) data that is captured by the community and civilian agencies can support public safety efforts in real-time. Experience live LPR demonstrations and training tips that can be implemented in your current operations. Our panel of industry practitioners will guide you through best practices and LPR use cases that can help you bolster your operations and enhance community engagement when fighting crime.

Key takeaways:

- Firsthand LPR technology best practices to implement within your operations
- Insights on how to engage your community with technology to enhance crime-fighting efforts
- Key considerations when implementing new LPR technologies into your current systems and operations



Tuesday, June 16, 2020
11:00 am ET | 8:00 am PT



TRAINING WEBINAR SERIES

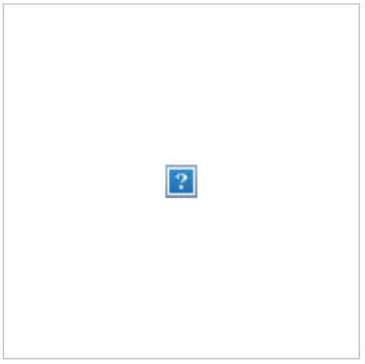
Advanced Investigative Call Data Records (CDR) Cleansing & Analysis

JOIN US and Discover How to Optimize Call Data Records (CDR) Cleansing and Analysis Which Typically Results in Solving Cases Faster and Saving Analysts 97% of Time Spent on a Case.

Chorus is the leading provider of data cleansing and analysis software in the UK and is used by 80% of regional police forces, all Counter Terror Units and the Home Office. Chorus is now making its software available for North American law enforcement.

Chorus is exceptional at:

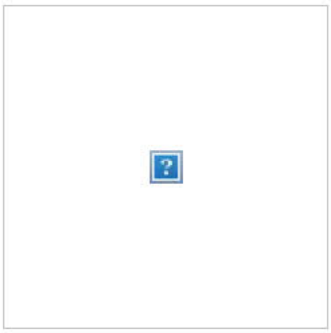
- **Rules-based data cleansing.** Taking communications data from providers such as T-Mobile, AT&T, Sprint and Verizon in the USA as well as Bell, Telus and Rogers Communications in Canada, removing the noise and normalizing it ready for analysis.
- **Connecting data.** Combining disparate data such



Thursday, June 25, 2020
11:00 am ET | 8:00 am PT

as CDR, ALPR, RF surveys and device downloads and overlaying it with communications data to spot crucial connections using maps and charts.
- **Evidence quality reporting**. Maintaining data integrity so reports and maps can be used in court as evidence.
- **Integration with IBM® i2 products.**



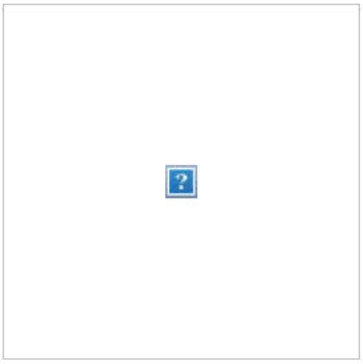


HIDS VIRTUAL CONFERENCE

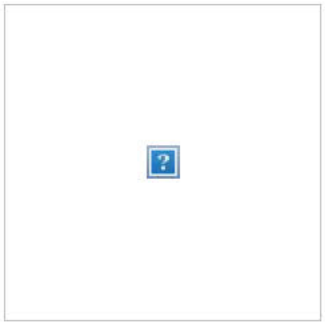
6th Annual Human Identification Solutions (HIDS) Conference

HIDS provides a unique platform for forensic scientists, practitioners, and criminal investigators from around the world to discuss the latest developments and trends in forensic DNA analysis, as well as the importance of effective partnerships between investigators and forensic scientists in solving crimes faster.

HIDS sessions across all regions will feature over 40 of the most prominent speakers in the industry including forensic scientists, criminal investigators, and legal experts to discuss their findings and best practices.



June 24-25, 2020



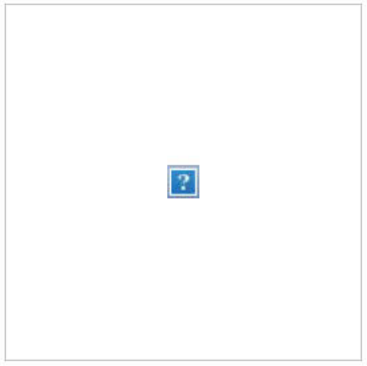
SCHOOL SHOOTING PREVENTION LEADERSHIP FORUM

Phoenix, AZ

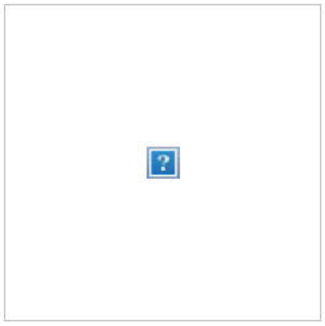
Each day law enforcement and school districts across the United States are responsible for protecting our almost 133,000 schools and 63 million students, faculty, and staff. The **FBI National Academy Associates** and the **School Safety Advocacy Council** have partnered and announced a series of 2-day Leadership Forums for law enforcement executives and school administrators throughout the country. The Forums will provide attendees with the knowledge, skills, and resources needed to improve the overall security of their community's schools while developing coordinated plans for a crisis response.

Program Overview:

- Review of school security trends & threat concerns
- Lessons learned: A review of past incidents
- The dynamics of active assailant situation
- Multi-agency response: Coordinating law enforcement, fire, EMS, and schools
- Understanding and conducting a school security survey & assessment
- Building capacity; Conducting Drills and Exercises



October 7-8, 2020
Phoenix, AZ



Who Should Attend

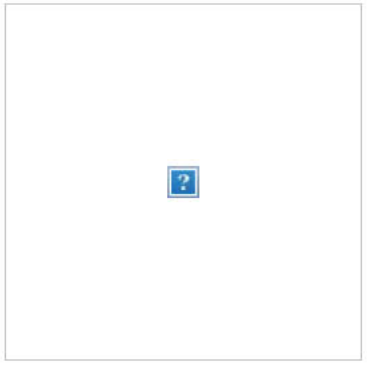
Law Enforcement Commanders
School Administrators
School Resource Officers
Fire/EMS Officials
School Security Directors

SCHOOL SHOOTING PREVENTION LEADERSHIP FORUM
Detroit, MI

Each day law enforcement and school districts across the United States are responsible for protecting our almost 133,000 schools and 63 million students, faculty, and staff. The **FBI National Academy Associates** and the **School Safety Advocacy Council** have partnered and announced a series of 2-day Leadership Forums for law enforcement executives and school administrators throughout the country. The Forums will provide attendees with the knowledge, skills, and resources needed to improve the overall security of their community's schools while developing coordinated plans for a crisis response.

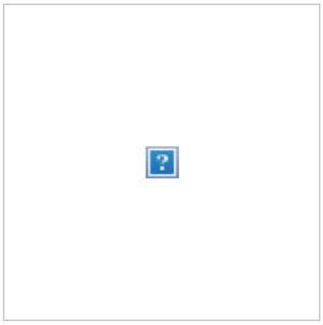
Program Overview:

- Review of school security trends & threat concerns
- Lessons learned: A review of past incidents
- The dynamics of active assailant situation
- Multi-agency response: Coordinating law enforcement, fire, EMS, and schools
- Understanding and conducting a school security survey &



October 27-28, 2020
Detroit, MI

assessment
- Building capacity; Conducting Drills and Exercises



For additional information:
Contact John Kennedy
at jkennedy@fbinaa.org.

For hotel/agenda/logistics:
Contact Laura Masterton
at lmasterton@fbinaa.org.

For Sponsorship Opportunities:
Contact Greg Guiton
at gguiton@fbinaa.org

CO-HOST A WEBINAR WITH THE FBINAA

Sponsorships Are Available!

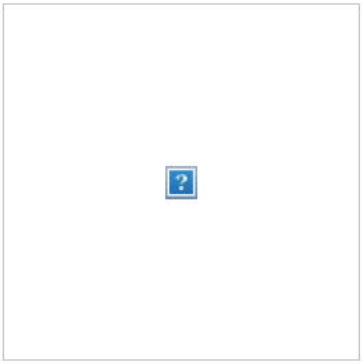
Share Your Thought Leadership and Professional Expertise by Being a Part of the 2020 FBINAA Leadership Webinar Series

These 60-90 minute webinars focus on cutting-edge law enforcement topics and trends and are delivered by law enforcement and public safety experts. Sponsorship provides your organization the opportunity to discuss your products and services to a focused audience, as well as, contributing to the knowledge base of the law enforcement profession. Your Marketing messages will be seen by hundreds of law enforcement professionals with interest in your products/services.

Sponsorships are available! Selected companies will pay a $4,000 sponsorship fee which allows them the use of their company logo and product/service information in the introduction to the educational session. Those selected will also be provided a list of webinar dates throughout 2020 from which they can choose on a first-come, first-serve basis.

These webinars are free to FBINAA members and non-members who can listen in live or get access to the recorded version after the event.

Please contact John Kennedy, Director of Education & Training, for further information at jkennedy@fbinaa.org or call (630) 464-7637.



Did You Know....

FBINAA members control assets and services well in excess of $100 Billion dollars each year, representing significant purchasing power and influence.

COLLABORATIVE REFORM INITIATIVE TECHNICAL ASSISTANCE CENTER: CRI-TAC

As part of our roles and responsibilities as a partner in the COPS Collaborative Reform Initiative Technical Assistance Center (CRI-TAC) Project, each partner has been asked to compile a list of Subject Matter Experts (SMEs) in the CRI-TAC priority areas. The selection of the SMEs will be related to each partner's membership and constituent base (can be both sworn and non-sworn) and will be included in the CRI-TA Resource Center. The CRI-TA Resource Center will be designed to support law enforcement agencies and provides free, customized technical assistance solutions designed to meet the unique needs of state, local, tribal, and campus communities throughout the United States.

CLICK HERE for additional information.

Questions & Information:
For questions and information regarding training programs, registrations, agendas and hotel accommodations, please contact Laura Masterton at lmasterton@fbinaa.org or (540) 810-2725.

Please contact John Kennedy with questions on Training and Webinars at jkennedy@fbinaa.org or (630) 464-7637.

Visit our website

The Mission of the FBINAA is "Impacting communities by providing and promoting law enforcement leadership through training and networking." We are committed to providing cutting-edge education and training to our members around the globe. Our goal is to increase the number of education and training opportunities for our members. Interested in co-hosting a Webinar with the FBINAA? Please contact John Kennedy, Director, Education & Training, at jkennedy@fbinaa.org.

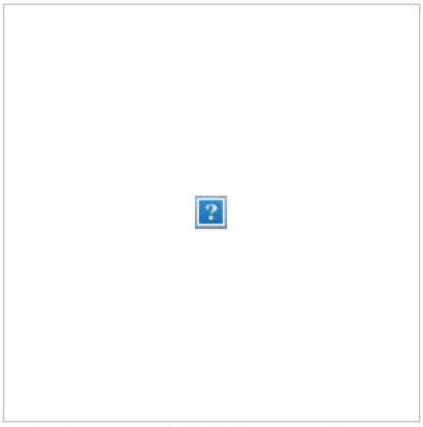
STAY CONNECTED

FBI National Academy Associates, Inc. | FBI Academy, Quantico, VA 22135

Unsubscribe paul.upton@pol.state.ma.us

Update Profile | About Constant Contact

Sent by do-not-reply@fbinaa.org in collaboration with



Try email marketing for free today!

From: FBI National Academy Associates, Inc.
To: Upton, Paul (POL)
Subject: FBINAA Training Bulletin
Date: Tuesday, June 16, 2020 10:47:12 AM

VISIT ALL TRAINING & WEBINARS



FBINAA APB Leadership Podcast Series
COMING SOON!

Plan on joining us monthly for the launch of the **FBINAA APB Leadership Podcast Series**. This Series will engage law enforcement and public safety executives in discussions on timely and current topics affecting first responders around the world. These leaders will share with you their leadership and managerial philosophies and successes and obstacles they have encountered in their careers.

The podcasts **are free audio programs distributed to FBI National Academy Associates' members, their staffs, and other law enforcement executives that** provide our communities, states, countries, and profession with the highest degree of law enforcement professionalism and expertise.

NEW RELEASES:
1st Wednesday/Month

A new APB Leadership Podcast will be available the first Wednesday of each Month.

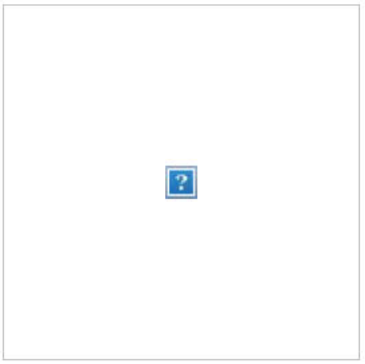
TRAINING WEBINAR SERIES

Engage the Community by Leveraging License Plate Recognition Technology

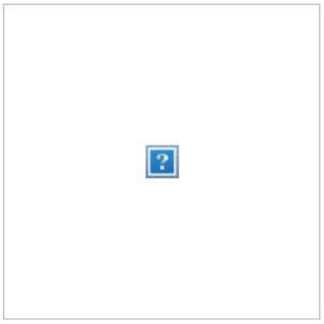
In this webinar, you will learn how license plate recognition (LPR) data that is captured by the community and civilian agencies can support public safety efforts in real-time. Experience live LPR demonstrations and training tips that can be implemented in your current operations. Our panel of industry practitioners will guide you through best practices and LPR use cases that can help you bolster your operations and enhance community engagement when fighting crime.

Key takeaways:

- Firsthand LPR technology best practices to implement within your operations
- Insights on how to engage your community with technology to enhance crime-fighting efforts
- Key considerations when implementing new LPR technologies into your current systems and operations



Tuesday, June 16, 2020
11:00 am ET | 8:00 am PT



TRAINING WEBINAR SERIES

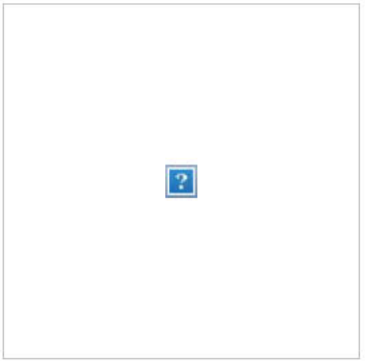
Advanced Investigative Call Data Records (CDR) Cleansing & Analysis

JOIN US and Discover How to Optimize Call Data Records (CDR) Cleansing and Analysis Which Typically Results in Solving Cases Faster and Saving Analysts 97% of Time Spent on a Case.

Chorus is the leading provider of data cleansing and analysis software in the UK and is used by 80% of regional police forces, all Counter Terror Units and the Home Office. Chorus is now making its software available for North American law enforcement.

Chorus is exceptional at:

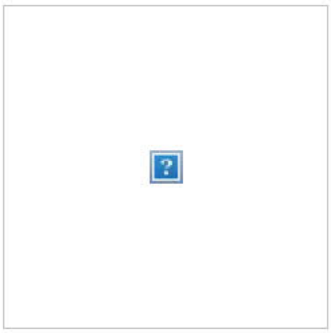
- **Rules-based data cleansing.** Taking communications data from providers such as T-Mobile, AT&T, Sprint and Verizon in the USA as well as Bell, Telus and Rogers Communications in Canada, removing the noise and normalizing it ready for analysis.
- **Connecting data.** Combining disparate data such



Thursday, June 25, 2020
11:00 am ET | 8:00 am PT

as CDR, ALPR, RF surveys and device downloads and overlaying it with communications data to spot crucial connections using maps and charts.
- **Evidence quality reporting**. Maintaining data integrity so reports and maps can be used in court as evidence.
- **Integration with IBM® i2 products.**



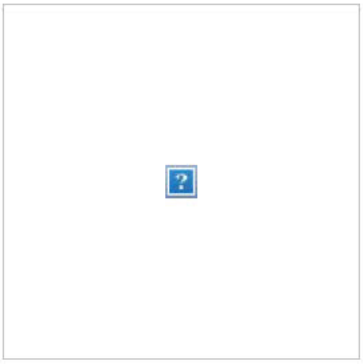


HIDS VIRTUAL CONFERENCE

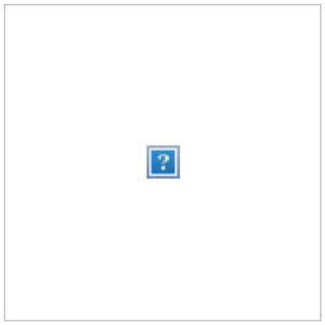
6th Annual Human Identification Solutions (HIDS) Conference

HIDS provides a unique platform for forensic scientists, practitioners, and criminal investigators from around the world to discuss the latest developments and trends in forensic DNA analysis, as well as the importance of effective partnerships between investigators and forensic scientists in solving crimes faster.

HIDS sessions across all regions will feature over 40 of the most prominent speakers in the industry including forensic scientists, criminal investigators, and legal experts to discuss their findings and best practices.



June 24-25, 2020



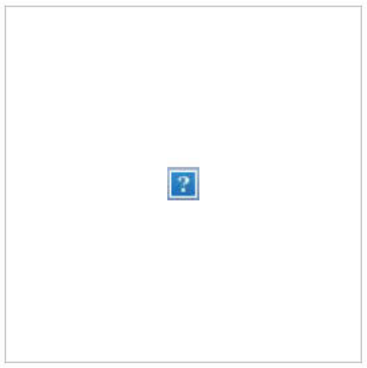
SCHOOL SHOOTING PREVENTION LEADERSHIP FORUM

Phoenix, AZ

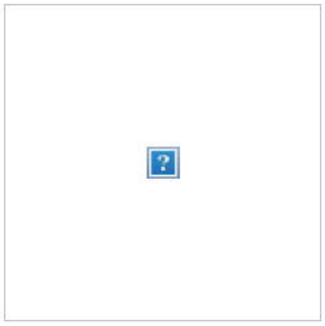
Each day law enforcement and school districts across the United States are responsible for protecting our almost 133,000 schools and 63 million students, faculty, and staff. The **FBI National Academy Associates** and the **School Safety Advocacy Council** have partnered and announced a series of 2-day Leadership Forums for law enforcement executives and school administrators throughout the country. The Forums will provide attendees with the knowledge, skills, and resources needed to improve the overall security of their community's schools while developing coordinated plans for a crisis response.

Program Overview:

- Review of school security trends & threat concerns
- Lessons learned: A review of past incidents
- The dynamics of active assailant situation
- Multi-agency response: Coordinating law enforcement, fire, EMS, and schools
- Understanding and conducting a school security survey & assessment
- Building capacity; Conducting Drills and Exercises



October 7-8, 2020
Phoenix, AZ



Who Should Attend

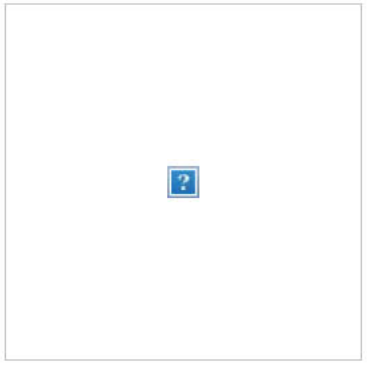
Law Enforcement Commanders
School Administrators
School Resource Officers
Fire/EMS Officials
School Security Directors

SCHOOL SHOOTING PREVENTION LEADERSHIP FORUM
Detroit, MI

Each day law enforcement and school districts across the United States are responsible for protecting our almost 133,000 schools and 63 million students, faculty, and staff. The **FBI National Academy Associates** and the **School Safety Advocacy Council** have partnered and announced a series of 2-day Leadership Forums for law enforcement executives and school administrators throughout the country. The Forums will provide attendees with the knowledge, skills, and resources needed to improve the overall security of their community's schools while developing coordinated plans for a crisis response.

Program Overview:

- Review of school security trends & threat concerns
- Lessons learned: A review of past incidents
- The dynamics of active assailant situation
- Multi-agency response: Coordinating law enforcement, fire, EMS, and schools
- Understanding and conducting a school security survey &



October 27-28, 2020
Detroit, MI

assessment
- Building capacity; Conducting Drills and Exercises

For additional information:
Contact John Kennedy
at jkennedy@fbinaa.org.

For hotel/agenda/logistics:
Contact Laura Masterton
at lmasterton@fbinaa.org.

For Sponsorship Opportunities:
Contact Greg Guiton
at gguiton@fbinaa.org

CO-HOST A WEBINAR WITH THE FBINAA
Sponsorships Are Available!

Share Your Thought Leadership and Professional Expertise by Being a Part of the 2020 FBINAA Leadership Webinar Series

These 60-90 minute webinars focus on cutting-edge law enforcement topics and trends and are delivered by law enforcement and public safety experts. Sponsorship provides your organization the opportunity to discuss your products and services to a focused audience, as well as, contributing to the knowledge base of the law enforcement profession. Your Marketing messages will be seen by hundreds of law enforcement professionals with interest in your products/services.

Sponsorships are available! Selected companies will pay a $4,000 sponsorship fee which allows them the use of their company logo and product/service information in the introduction to the educational session. Those selected will also be provided a list of webinar dates throughout 2020 from which they can choose on a first-come, first-serve basis.

These webinars are free to FBINAA members and non-members who can listen in live or get access to the recorded version after the event.

Please contact John Kennedy, Director of Education & Training, for further information at jkennedy@fbinaa.org or call (630) 464-7637.

Did You Know....

FBINAA members control assets and services well in excess of $100 Billion dollars each year, representing significant purchasing power and influence.

COLLABORATIVE REFORM INITIATIVE TECHNICAL ASSISTANCE CENTER: CRI-TAC

As part of our roles and responsibilities as a partner in the COPS Collaborative Reform Initiative Technical Assistance Center (CRI-TAC) Project, each partner has been asked to compile a list of Subject Matter Experts (SMEs) in the CRI-TAC priority areas. The selection of the SMEs will be related to each partner's membership and constituent base (can be both sworn and non-sworn) and will be included in the CRI-TA Resource Center. The CRI-TA Resource Center will be designed to support law enforcement agencies and provides free, customized technical assistance solutions designed to meet the unique needs of state, local, tribal, and campus communities throughout the United States.

CLICK HERE for additional information.

Questions & Information:
For questions and information regarding training programs, registrations, agendas and hotel accommodations, please contact Laura Masterton at lmasterton@fbinaa.org or (540) 810-2725.

Please contact John Kennedy with questions on Training and Webinars at jkennedy@fbinaa.org or (630) 464-7637.

Visit our website

The Mission of the FBINAA is "Impacting communities by providing and promoting law enforcement leadership through training and networking." We are committed to providing cutting-edge education and training to our members around the globe. Our goal is to increase the number of education and training opportunities for our members. Interested in co-hosting a Webinar with the FBINAA? Please contact John Kennedy, Director, Education & Training, at jkennedy@fbinaa.org.

STAY CONNECTED

FBI National Academy Associates, Inc. | FBI Academy, Quantico, VA 22135

Unsubscribe paul.upton@massmail.state.ma.us

Update Profile | About Constant Contact

Sent by do-not-reply@fbinaa.org in collaboration with

Try email marketing for free today!

From: FBI National Academy Associates, Inc.
To: Wilcox, Christopher (POL)
Subject: FBINAA Training Bulletin
Date: Tuesday, June 16, 2020 10:47:23 AM

VISIT ALL TRAINING & WEBINARS

FBINAA APB Leadership Podcast Series
COMING SOON!

Plan on joining us monthly for the launch of the **FBINAA APB Leadership Podcast Series**. This Series will engage law enforcement and public safety executives in discussions on timely and current topics affecting first responders around the world. These leaders will share with you their leadership and managerial philosophies and successes and obstacles they have encountered in their careers.

The podcasts **are free audio programs distributed to FBI National Academy Associates' members, their staffs, and other law enforcement executives that** provide our communities, states, countries, and profession with the highest degree of law enforcement professionalism and expertise.

NEW RELEASES:
1st Wednesday/Month

A new APB Leadership Podcast will be available the first Wednesday of each Month.

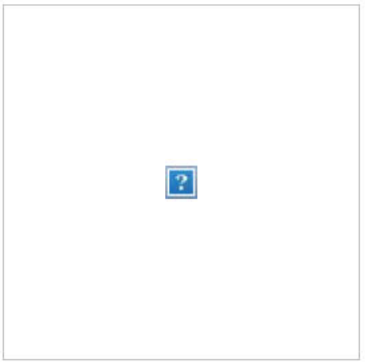
TRAINING WEBINAR SERIES

Engage the Community by Leveraging License Plate Recognition Technology

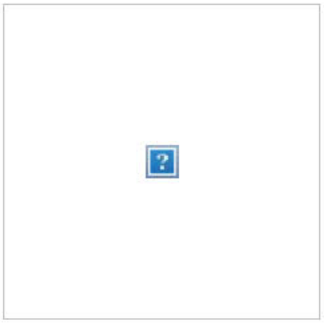
In this webinar, you will learn how license plate recognition (LPR) data that is captured by the community and civilian agencies can support public safety efforts in real-time. Experience live LPR demonstrations and training tips that can be implemented in your current operations. Our panel of industry practitioners will guide you through best practices and LPR use cases that can help you bolster your operations and enhance community engagement when fighting crime.

Key takeaways:

- Firsthand LPR technology best practices to implement within your operations
- Insights on how to engage your community with technology to enhance crime-fighting efforts
- Key considerations when implementing new LPR technologies into your current systems and operations



Tuesday, June 16, 2020
11:00 am ET | 8:00 am PT



TRAINING WEBINAR SERIES

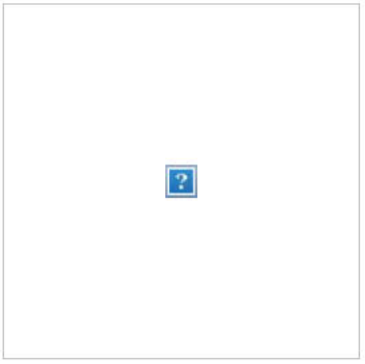
Advanced Investigative Call Data Records (CDR) Cleansing & Analysis

JOIN US and Discover How to Optimize Call Data Records (CDR) Cleansing and Analysis Which Typically Results in Solving Cases Faster and Saving Analysts 97% of Time Spent on a Case.

Chorus is the leading provider of data cleansing and analysis software in the UK and is used by 80% of regional police forces, all Counter Terror Units and the Home Office. Chorus is now making its software available for North American law enforcement.

Chorus is exceptional at:

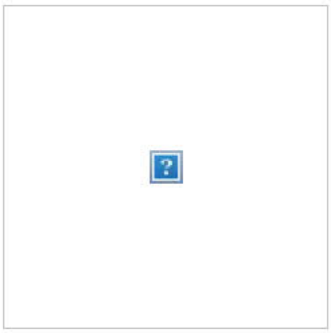
- **Rules-based data cleansing.** Taking communications data from providers such as T-Mobile, AT&T, Sprint and Verizon in the USA as well as Bell, Telus and Rogers Communications in Canada, removing the noise and normalizing it ready for analysis.
- **Connecting data.** Combining disparate data such



Thursday, June 25, 2020
11:00 am ET | 8:00 am PT

as CDR, ALPR, RF surveys and device downloads and overlaying it with communications data to spot crucial connections using maps and charts.
- **Evidence quality reporting**. Maintaining data integrity so reports and maps can be used in court as evidence.
- **Integration with IBM® i2 products.**



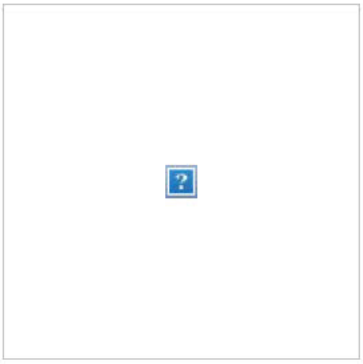


HIDS VIRTUAL CONFERENCE

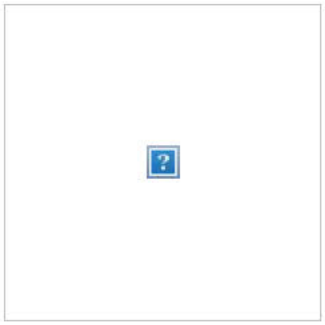
6th Annual Human Identification Solutions (HIDS) Conference

HIDS provides a unique platform for forensic scientists, practitioners, and criminal investigators from around the world to discuss the latest developments and trends in forensic DNA analysis, as well as the importance of effective partnerships between investigators and forensic scientists in solving crimes faster.

HIDS sessions across all regions will feature over 40 of the most prominent speakers in the industry including forensic scientists, criminal investigators, and legal experts to discuss their findings and best practices.



June 24-25, 2020



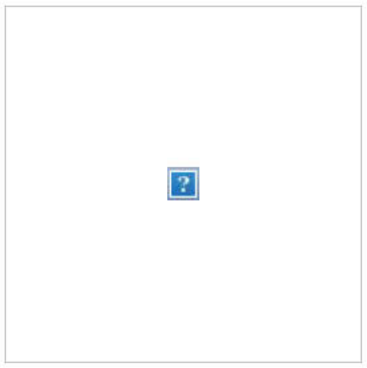
SCHOOL SHOOTING PREVENTION LEADERSHIP FORUM

Phoenix, AZ

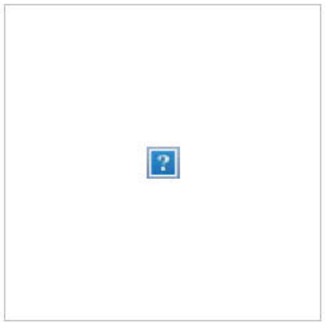
Each day law enforcement and school districts across the United States are responsible for protecting our almost 133,000 schools and 63 million students, faculty, and staff. The **FBI National Academy Associates** and the **School Safety Advocacy Council** have partnered and announced a series of 2-day Leadership Forums for law enforcement executives and school administrators throughout the country. The Forums will provide attendees with the knowledge, skills, and resources needed to improve the overall security of their community's schools while developing coordinated plans for a crisis response.

Program Overview:

- Review of school security trends & threat concerns
- Lessons learned: A review of past incidents
- The dynamics of active assailant situation
- Multi-agency response: Coordinating law enforcement, fire, EMS, and schools
- Understanding and conducting a school security survey & assessment
- Building capacity; Conducting Drills and Exercises



October 7-8, 2020
Phoenix, AZ



Who Should Attend

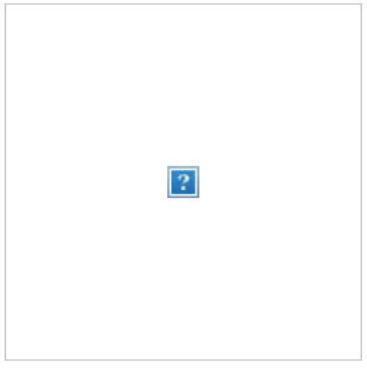
Law Enforcement Commanders
School Administrators
School Resource Officers
Fire/EMS Officials
School Security Directors

SCHOOL SHOOTING PREVENTION LEADERSHIP FORUM
Detroit, MI

Each day law enforcement and school districts across the United States are responsible for protecting our almost 133,000 schools and 63 million students, faculty, and staff. The **FBI National Academy Associates** and the **School Safety Advocacy Council** have partnered and announced a series of 2-day Leadership Forums for law enforcement executives and school administrators throughout the country. The Forums will provide attendees with the knowledge, skills, and resources needed to improve the overall security of their community's schools while developing coordinated plans for a crisis response.

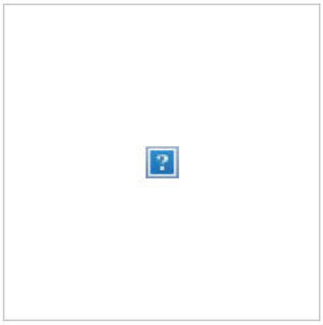
Program Overview:

- Review of school security trends & threat concerns
- Lessons learned: A review of past incidents
- The dynamics of active assailant situation
- Multi-agency response: Coordinating law enforcement, fire, EMS, and schools
- Understanding and conducting a school security survey &



October 27-28, 2020
Detroit, MI

assessment
- Building capacity; Conducting Drills and Exercises



For additional information:
Contact John Kennedy
at jkennedy@fbinaa.org.

For hotel/agenda/logistics:
Contact Laura Masterton
at lmasterton@fbinaa.org.

For Sponsorship Opportunities:
Contact Greg Guiton
at gguiton@fbinaa.org

CO-HOST A WEBINAR WITH THE FBINAA
Sponsorships Are Available!

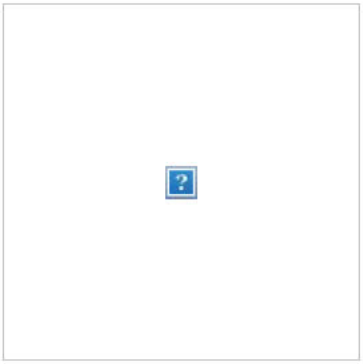
Share Your Thought Leadership and Professional Expertise by Being a Part of the 2020 FBINAA Leadership Webinar Series

These 60-90 minute webinars focus on cutting-edge law enforcement topics and trends and are delivered by law enforcement and public safety experts. Sponsorship provides your organization the opportunity to discuss your products and services to a focused audience, as well as, contributing to the knowledge base of the law enforcement profession. Your Marketing messages will be seen by hundreds of law enforcement professionals with interest in your products/services.

Sponsorships are available! Selected companies will pay a $4,000 sponsorship fee which allows them the use of their company logo and product/service information in the introduction to the educational session. Those selected will also be provided a list of webinar dates throughout 2020 from which they can choose on a first-come, first-serve basis.

These webinars are free to FBINAA members and non-members who can listen in live or get access to the recorded version after the event.

Please contact John Kennedy, Director of Education & Training, for further information at jkennedy@fbinaa.org or call (630) 464-7637.

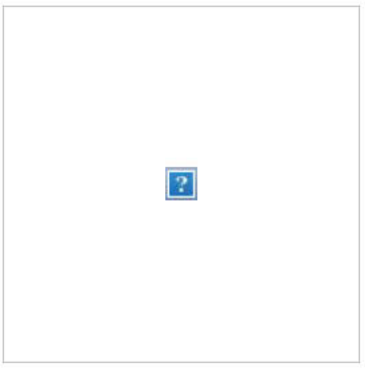


Did You Know....

FBINAA members control assets and services well in excess of $100 Billion dollars each year, representing significant purchasing power and influence.

COLLABORATIVE REFORM INITIATIVE TECHNICAL ASSISTANCE CENTER: CRI-TAC

As part of our roles and responsibilities as a partner in the COPS Collaborative Reform Initiative Technical Assistance Center (CRI-TAC) Project, each partner has been asked to compile a list of Subject Matter Experts (SMEs) in the CRI-TAC priority areas. The selection of the SMEs will be related to each partner's membership and constituent base (can be both sworn and non-sworn) and will be included in the CRI-TA Resource Center. The CRI-TA Resource Center will be designed to support law enforcement agencies and provides free, customized technical assistance solutions designed to meet the unique needs of state, local, tribal, and campus communities throughout the United States.



CLICK HERE for additional information.

Questions & Information:
For questions and information regarding training programs, registrations, agendas and hotel accommodations, please contact Laura Masterton at lmasterton@fbinaa.org or (540) 810-2725.

Please contact John Kennedy with questions on Training and Webinars at jkennedy@fbinaa.org or (630) 464-7637.

Visit our website

The Mission of the FBINAA is "Impacting communities by providing and promoting law enforcement leadership through training and networking." We are committed to providing cutting-edge education and training to our members around the globe. Our goal is to increase the number of education and training opportunities for our members. Interested in co-hosting a Webinar with the FBINAA? Please contact John Kennedy, Director, Education & Training, at jkennedy@fbinaa.org.

STAY CONNECTED

FBI National Academy Associates, Inc. | FBI Academy, Quantico, VA 22135

Unsubscribe christopher.wilcox@massmail.state.ma.us

Update Profile | About Constant Contact

Sent by do-not-reply@fbinaa.org in collaboration with

Try email marketing for free today!

From: Police Chief Magazine
To: Pinkham, John (POL)
Subject: February 2020: Investigations
Date: Wednesday, February 5, 2020 3:41:05 PM

View Online

The Police Chief Update

POLICE CHIEF MAGAZINE / ARCHIVES / THE IACP / CAREERS / ADVERTISE WITH US

February Issue

FEBRUARY 2020 ISSUE

February 2020 – Investigations

Investigative practices vary depending on the city, state, or country in which a crime occurred, but some practices and techniques apply across the field. From organized crime to homicide to critical incidents, crimes of all types can only be solved by investigators armed with knowledge, experience, and access to the best practices and tools available.

READ CURRENT ISSUE

FEATURES

Death Investigations

Cooperation between medical examiners and law enforcement—both in the lab and in the field—is crucial to the investigations of traumatic, suspicious, or unexpected deaths.

Rapport is the Truth Serum Interviewers Have Been Seeking

While many interrogation models recognize the importance of rapport, a whole new approach is needed to pivot away from accusation and toward information as the interviewer's goal in order to solve crimes and remove dangerous offenders from communities.

Intelligence-Led Policing on a Shoestring Budget

Data mapping is the first layer of intelligence gathering and analysis, and a step that can be accomplished by any agency, regardless of budget constraints, with readily available no-cost software.

ADVERTISEMENT
Utility

COLUMNS

President's Message

Policing in an Age of Digital Evidence and DNA

Available in five languages!

Chief's Counsel

A Rodriguez Ripple

Focus on Officer Wellness

Rhabdomyolysis—More Than Dehydration

Products and Services

Access the latest tools in this month's *Police Chief* magazine

VIEW ALL CONTENT

Utility

SPONSORED CONTENT

More Than Just a Body Camera

BodyWorn by Utility, Inc. provides an Intelligent Ecosystem of Technology with automated recording, alerting, and uploading. From body cameras to in-car video systems, interview rooms to evidence management, ALPR, and gunshot detection, Utility is leading the industry in cutting-edge technology that makes a difference in modern law enforcement. Learn More.

JOB POSTINGS

Discover Policing Career Center is the official job board of the IACP and a police recruitment resource. Visit discoverpolicing.org for more information.

Police Chief

City of East Wenatchee, Washington

Police Senior Media Relations Specialist

Town of Castle Rock, Colorado

Police Chief

City of Sebastopol, California

SPOTLIGHT

Police Chief's new Spotlight showcases innovative ideas and projects from agencies worldwide. Does you agency have an initiative you'd like to see featured? Email the editor at editor@theiacp.org to learn more!

Spotlight

VIEW ALL JOBS

VISIT SPOTLIGHT

Connect with IACP

International Association of Chiefs of Police
44 Canal Center Plaza, Suite 200, Alexandria, VA 22314
1.800.THE IACP | www.theIACP.org

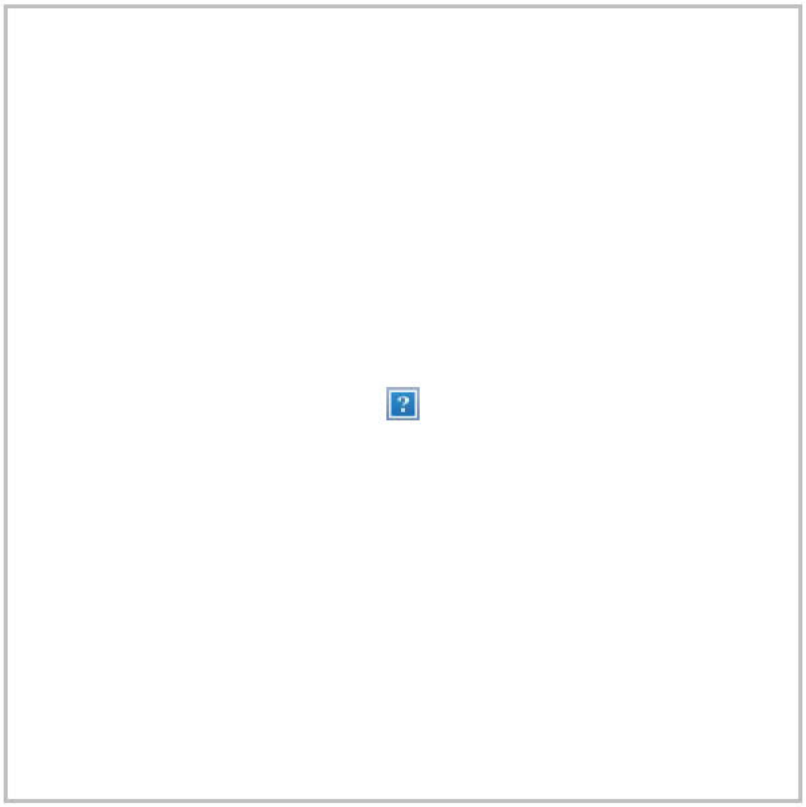
From: Evidence Technology Magazine
To: Hughes, David (POL)
Subject: Fingerprint Test Detects Cocaine
Date: Thursday, February 20, 2020 10:02:11 AM

Here's your February issue of ETM's Crime Scene News

View this email in your browser



Evidence Technology Magazine • Crime Scene News • February 2020



Sponsored

Forensic Healthcare

Webinar: Providing Forensic Healthcare to Native Communities

February 18, 2020 — A webinar on February 27, 2020 presented by the NIJ's Forensic Technology Center of Excellence aims to heighten awareness among forensic examiners of the importance of providing culturally appropriate and trauma-informed services to the American Indian / Alaska Native (AI/AN) community. The webinar will discuss jurisdictional factors affecting examinations, pertinent laws to consider, and health care services that may be available to AI/AN populations.

>Read More

Support

Foundation Supports Families of First Responders Who Paid the Ultimate Price

February 12, 2020 — The Front Line Foundation announced recently they have started 2020 by paying death benefits to six families of first responders who died while serving others.

>Read More



NEW ISSUE! Read the January-February Issue of ETM

Crime Prevention

Fewer Liquor Stores May Lead to Less Homicide

February 13, 2020 — Reducing the number of businesses in Baltimore that sell alcohol in residential areas may lower the homicide rate, according to new research in the Journal of Studies on Alcohol and Drugs.

>Read More

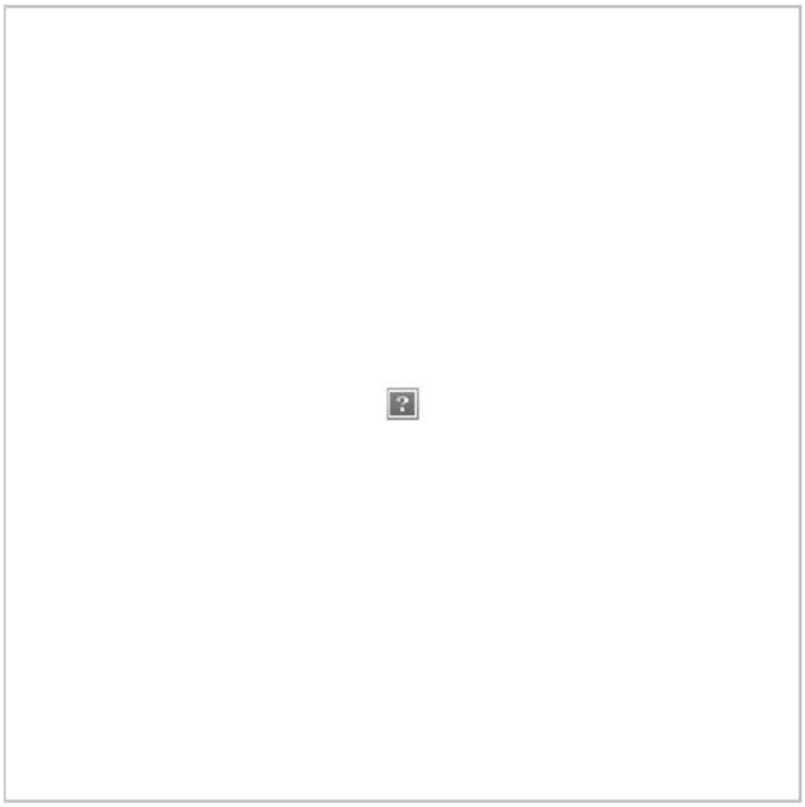
Drug Screening

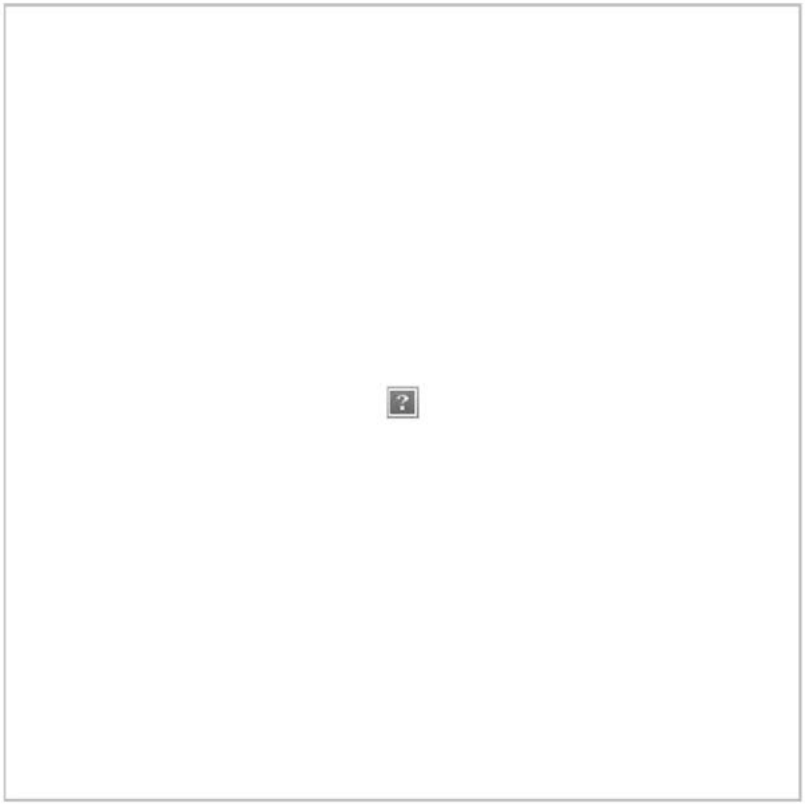
Experimental Fingerprint Test Detects Traces of Cocaine on Skin

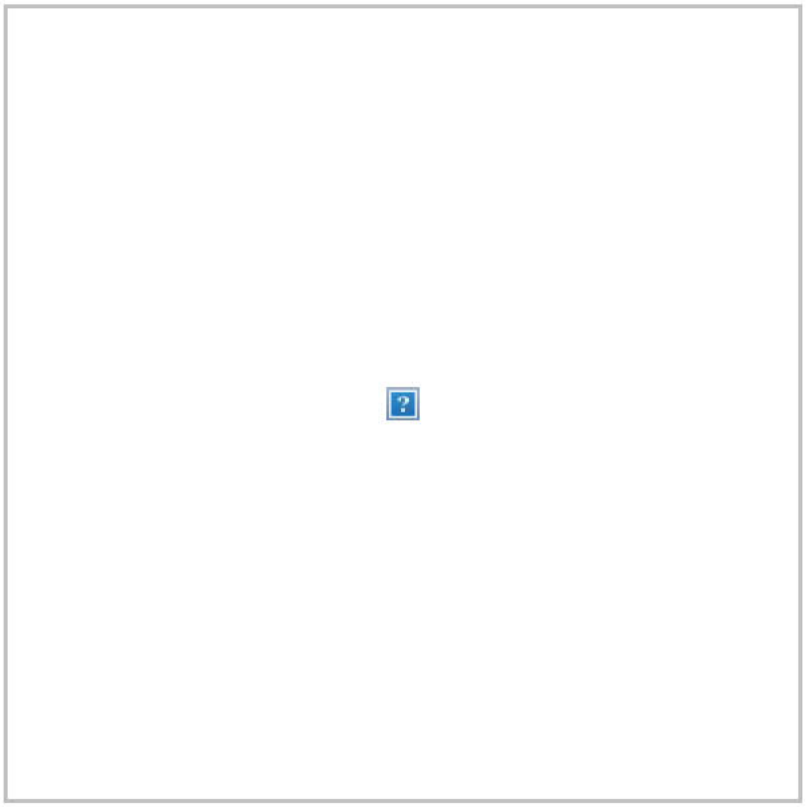
February 4, 2020 — An experimental fingerprint detection approach can identify traces of cocaine on human skin, even after someone has washed their hands — and the test is also smart enough to tell whether an individual has actually consumed the class A drug, or simply handled it.

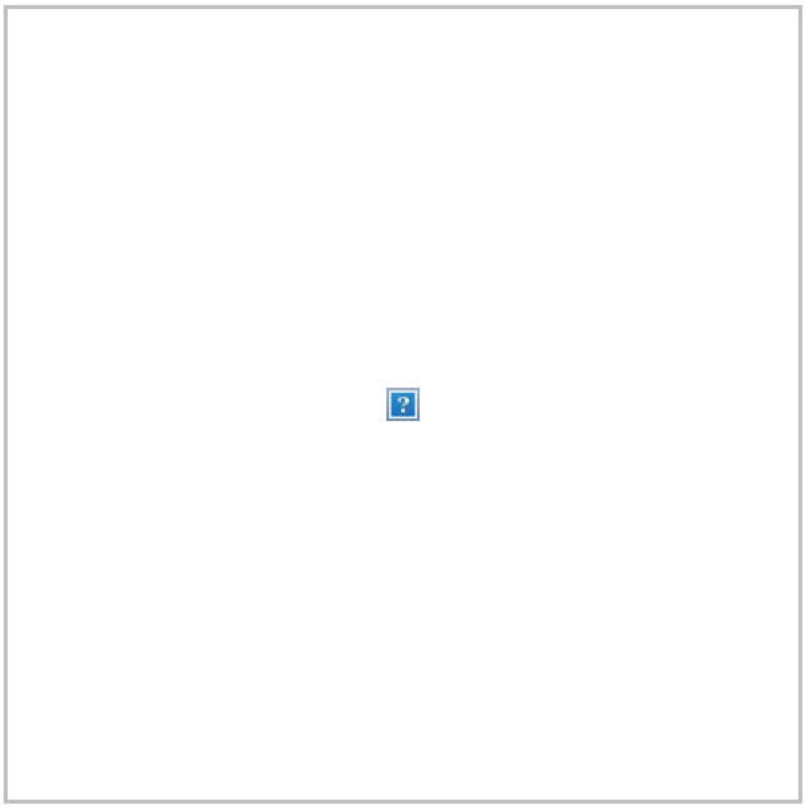
>Read More

Upcoming Conferences









Vendor News

Cloud Explorer Extracts Google Fit Data

February 18, 2020 — ElcomSoft Co. Ltd. recently announced Elcomsoft Cloud Explorer 2.30, which adds support for health and activity information collected by the Android Google Fit app and synchronized to the user's Google Account. >Read More

Motorola Solutions Adds New Analytics to In-Car Video System

February 13, 2020 — Motorola Solutions recently announced the availability of new video security and analytics capabilities for law enforcement. Automated license plate recognition (ALPR) is now part of the WatchGuard 4RE® in-car video system. >Read More

New Touch Screen Repeating Pipette with Advanced Features

February 13, 2020 — The BRAND® HandyStep® touch S repeating pipette has advanced pipetting features for versatility. In addition to standard pipetting, dispensing, auto dispensing and a proprietary "learn" function, advanced modes include sequential dispensing of different volumes, multi-aspiration of different volumes and a titration mode. >Read More

Companies Partner to Deliver Hybrid Video Management Solution

February 11, 2020 — Arcules, a company focusing on integrated video and access control cloud services, recently announced the commercial availability of the Arcules-XProtect Hybrid™ VMS Solution in North America and Europe. >Read More

Subscribe to ETM Today!

New Desktop 3D Scanner for Tiny Objects

February 11, 2020 — Exact Metrology recently announced the availability of the new Artec Micro 3D scanner. The Artec Micro, an automated, metrology-grade desktop 3D scanner is Artec 3D's most accurate 3D scanner to date, and is used for scanning tiny mechanical parts, such as engine valves or connectors, for inspection and reverse engineering, as well as other small objects for industries such as heritage preservation, dentistry, and medical. >Read More

Open Source Web Intelligence Company Opens Office in U.S.

January 22, 2020 — Cobwebs Technologies — the specialized open-source web intelligence company that supports national security agencies, law enforcement agencies, and corporate security departments in rapidly identifying and locating malicious threat actors on the open, deep, and dark webs — is entering the American market with an office in New York City. With little more than a click, Cobwebs makes it highly difficult for terrorists, active shooters, hackers, and other criminal entities to hide, plan, communicate, or ply their nefarious trade in any part of the online world. >Read More

Nearly Half of First Responders Under-Equipped to Handle Extended

Power Outage, Report Finds

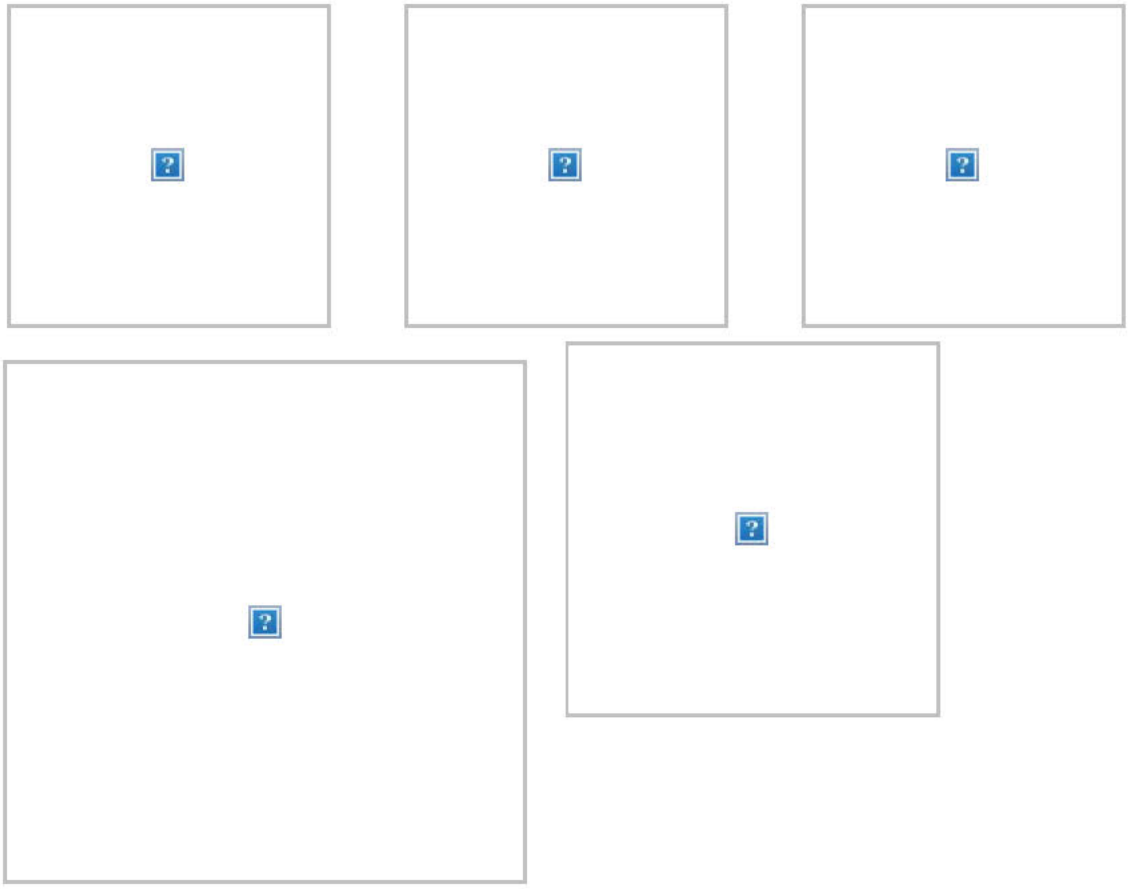
January 23, 2020 — IWCE, an event for the critical communications industry, surveyed more than 597 first responders and public safety professionals to benchmark the current technologies they are using and to understand current technological challenges within the industry. >Read More

Environmentally Friendly Alternative to Canned Air

January 21, 2020 — Canless Air System is a highly effective and environmentally friendly alternative to traditional canned air cleaning products. The line of Hurricane dusters is nontoxic, rechargeable, and provides more power than any canned air competitor. >Read More

---

There's more in the ETM Digital Edition:



Website LinkedIn Twitter Facebook Subscribe

Copyright © 2020 Wordsmith Publishing, All rights reserved.
You are receiving this eNewsletter because you subscribed to Evidence Technology Magazine. You can change your communication preferences at any time by following the links below. Thank you for your readership!

Our mailing address is:
Wordsmith Publishing
PO Box 555

Kearney, MO 64060

Add us to your address book

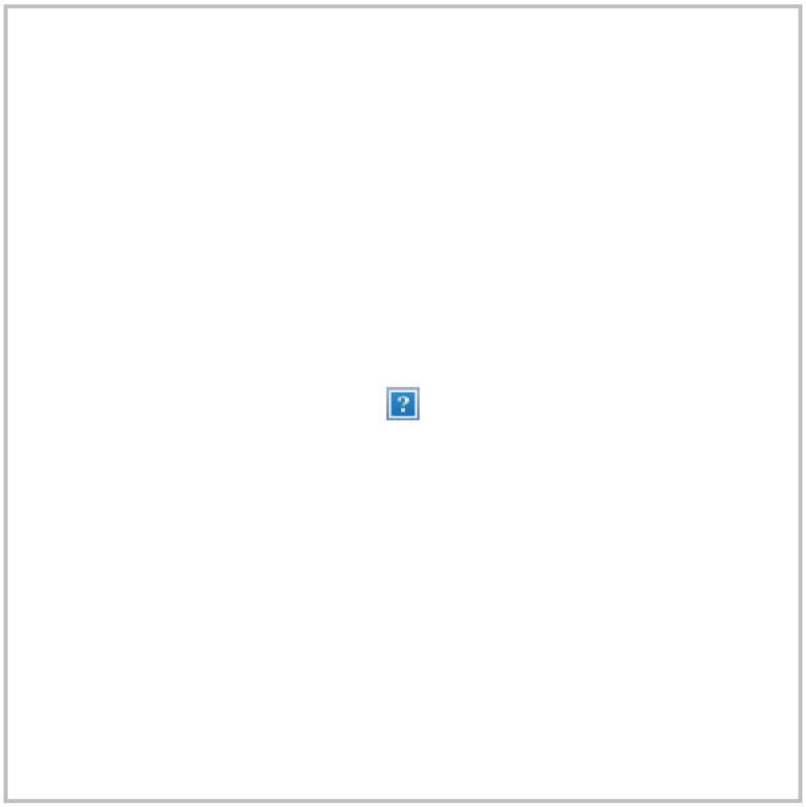
unsubscribe from this list update subscription preferences

From: Evidence Technology Magazine
To: Saucier, Beth (POL)
Subject: Fingerprint Test Detects Cocaine
Date: Thursday, February 20, 2020 10:01:39 AM

Here's your February issue of ETM's Crime Scene News

View this email in your browser





Sponsored

Forensic Healthcare

Webinar: Providing Forensic Healthcare to Native Communities

February 18, 2020 — A webinar on February 27, 2020 presented by the NIJ's Forensic Technology Center of Excellence aims to heighten awareness among forensic examiners of the importance of providing culturally appropriate and trauma-informed services to the American Indian / Alaska Native (AI/AN) community. The webinar will discuss jurisdictional factors affecting examinations, pertinent laws to consider, and health care services that may be available to AI/AN populations.

>Read More

Support

Foundation Supports Families of First Responders Who Paid the Ultimate Price

February 12, 2020 — The Front Line Foundation announced recently they have started 2020 by paying death benefits to six families of first responders who died while serving others.

>Read More



NEW ISSUE! Read the January-February Issue of ETM

Crime Prevention

Fewer Liquor Stores May Lead to Less Homicide

February 13, 2020 — Reducing the number of businesses in Baltimore that sell alcohol in residential areas may lower the homicide rate, according to new research in the Journal of Studies on Alcohol and Drugs.

>Read More

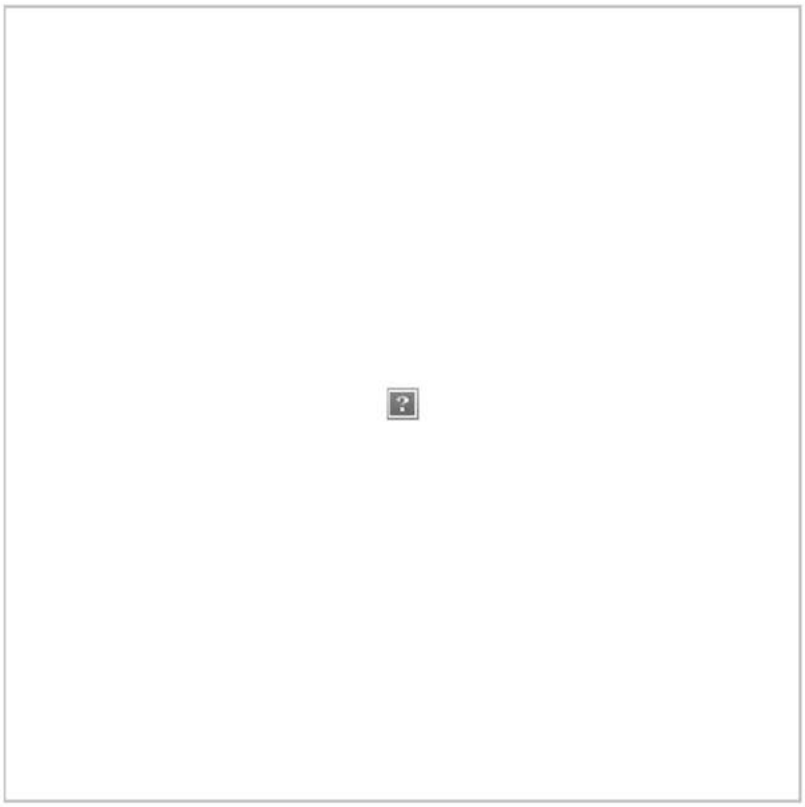
Drug Screening

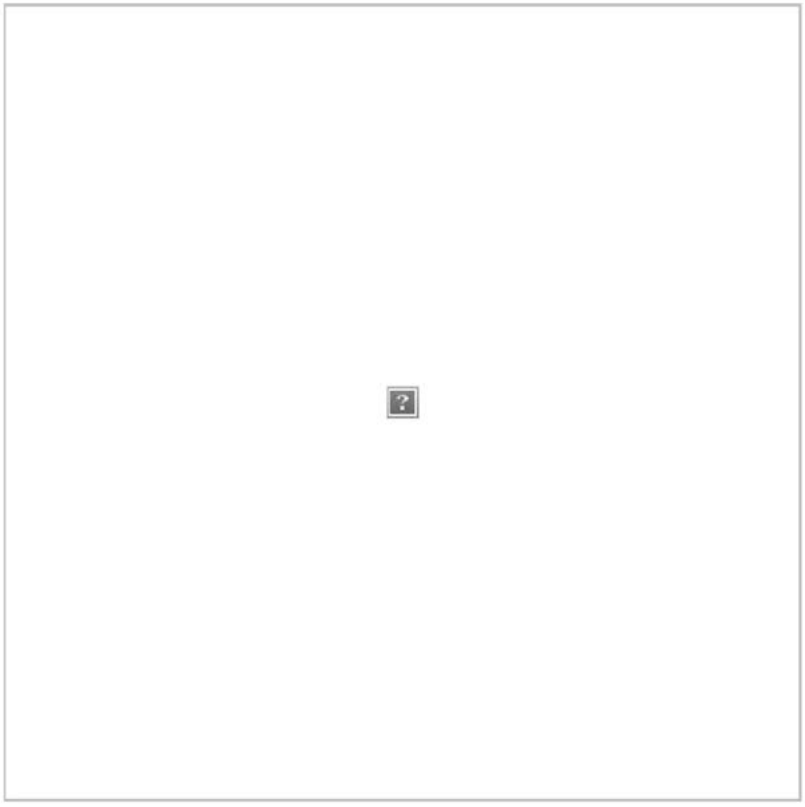
Experimental Fingerprint Test Detects Traces of Cocaine on Skin

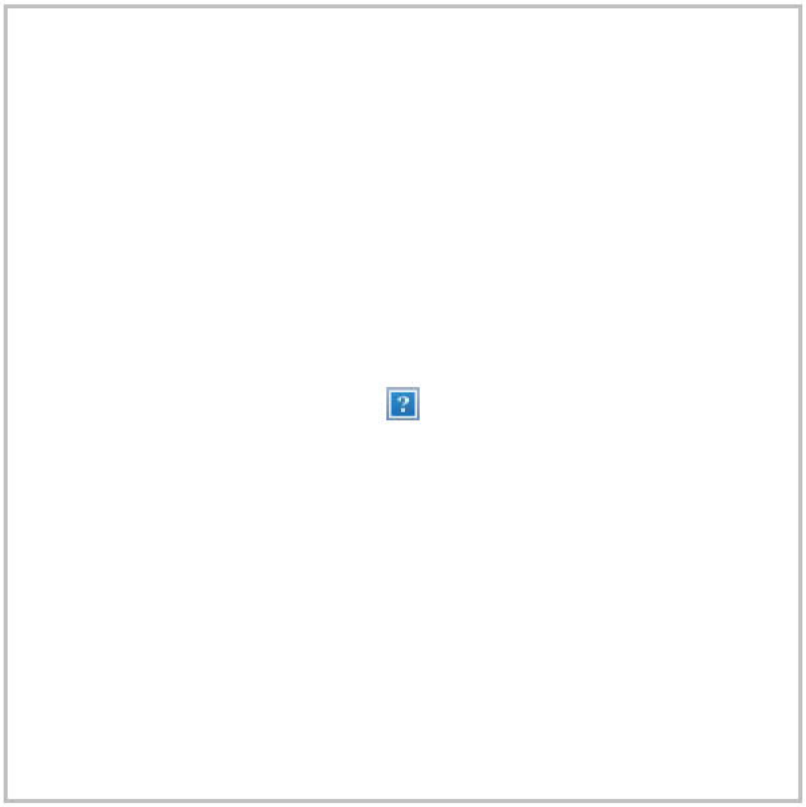
February 4, 2020 — An experimental fingerprint detection approach can identify traces of cocaine on human skin, even after someone has washed their hands — and the test is also smart enough to tell whether an individual has actually consumed the class A drug, or simply handled it.

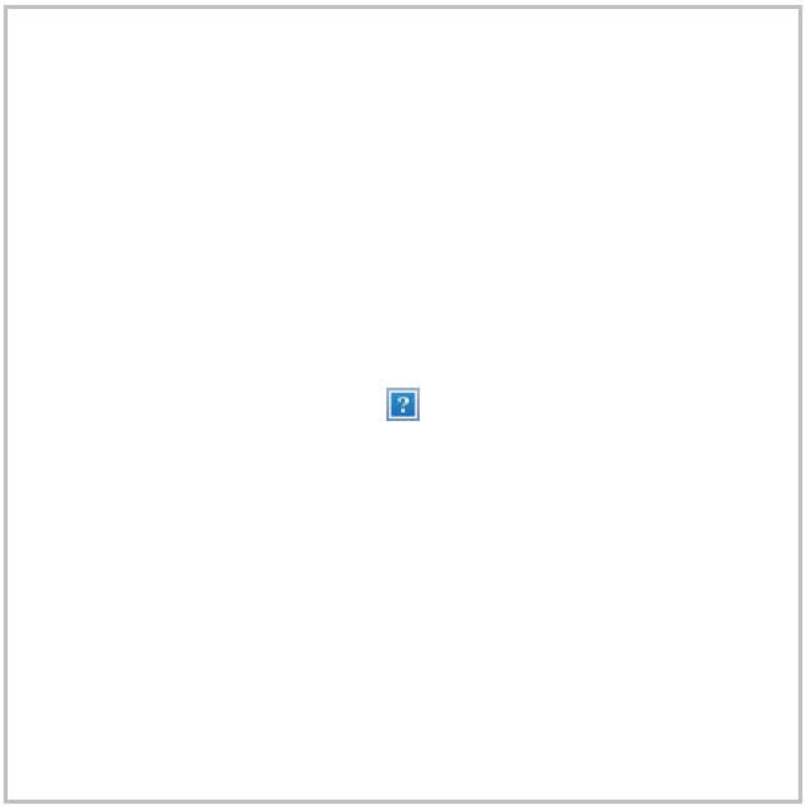
>Read More

Upcoming Conferences









Cloud Explorer Extracts Google Fit Data

February 18, 2020 — ElcomSoft Co. Ltd. recently announced Elcomsoft Cloud Explorer 2.30, which adds support for health and activity information collected by the Android Google Fit app and synchronized to the user's Google Account. >Read More

Motorola Solutions Adds New Analytics to In-Car Video System

February 13, 2020 — Motorola Solutions recently announced the availability of new video security and analytics capabilities for law enforcement. Automated license plate recognition (ALPR) is now part of the WatchGuard 4RE® in-car video system. >Read More

New Touch Screen Repeating Pipette with Advanced Features

February 13, 2020 — The BRAND® HandyStep® touch S repeating pipette has advanced pipetting features for versatility. In addition to standard pipetting, dispensing, auto dispensing and a proprietary "learn" function, advanced modes include sequential dispensing of different volumes, multi-aspiration of different volumes and a titration mode. >Read More

Companies Partner to Deliver Hybrid Video Management Solution

February 11, 2020 — Arcules, a company focusing on integrated video and access control cloud services, recently announced the commercial availability of the Arcules-XProtect Hybrid™ VMS Solution in North America and Europe. >Read More

Subscribe to ETM Today!

New Desktop 3D Scanner for Tiny Objects

February 11, 2020 — Exact Metrology recently announced the availability of the new Artec Micro 3D scanner. The Artec Micro, an automated, metrology-grade desktop 3D scanner is Artec 3D's most accurate 3D scanner to date, and is used for scanning tiny mechanical parts, such as engine valves or connectors, for inspection and reverse engineering, as well as other small objects for industries such as heritage preservation, dentistry, and medical. >Read More

Open Source Web Intelligence Company Opens Office in U.S.

January 22, 2020 — Cobwebs Technologies — the specialized open-source web intelligence company that supports national security agencies, law enforcement agencies, and corporate security departments in rapidly identifying and locating malicious threat actors on the open, deep, and dark webs — is entering the American market with an office in New York City. With little more than a click, Cobwebs makes it highly difficult for terrorists, active shooters, hackers, and other criminal entities to hide, plan, communicate, or ply their nefarious trade in any part of the online world. >Read More

Nearly Half of First Responders Under-Equipped to Handle Extended

Power Outage, Report Finds

January 23, 2020 — IWCE, an event for the critical communications industry, surveyed more than 597 first responders and public safety professionals to benchmark the current technologies they are using and to understand current technological challenges within the industry. >Read More

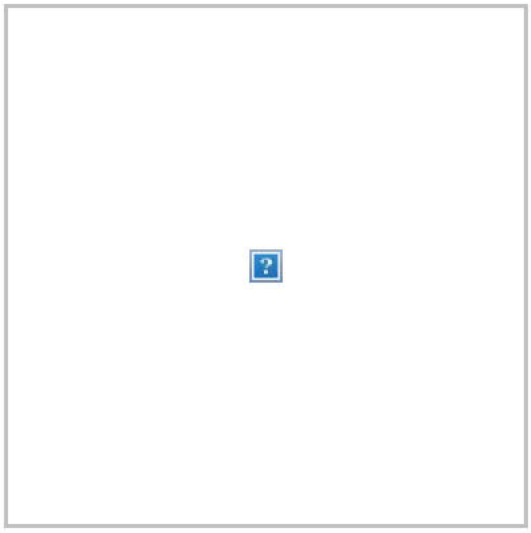
Environmentally Friendly Alternative to Canned Air

January 21, 2020 — Canless Air System is a highly effective and environmentally friendly alternative to traditional canned air cleaning products. The line of Hurricane dusters is nontoxic, rechargeable, and provides more power than any canned air competitor. >Read More

---

There's more in the ETM Digital Edition:




Website LinkedIn Twitter Facebook Subscribe

Copyright © 2020 Wordsmith Publishing, All rights reserved.
You are receiving this eNewsletter because you subscribed to Evidence Technology Magazine. You can change your communication preferences at any time by following the links below. Thank you for your readership!

Our mailing address is:
Wordsmith Publishing
PO Box 555

Kearney, MO 64060

Add us to your address book

unsubscribe from this list update subscription preferences

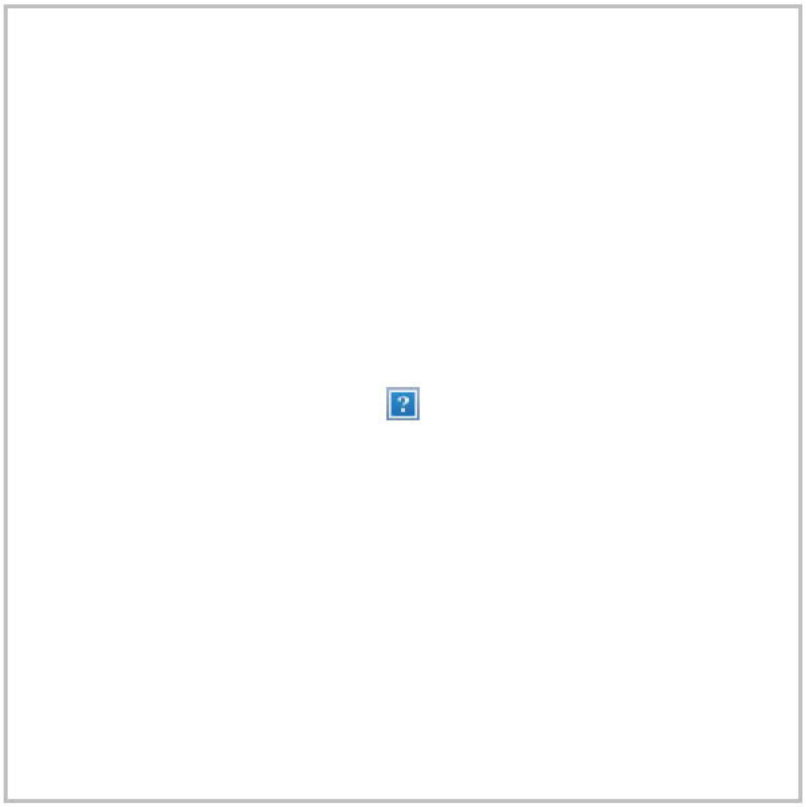
From: Evidence Technology Magazine
To: Girouard, Todd (POL)
Subject: Fingerprint Test Detects Cocaine
Date: Thursday, February 20, 2020 10:02:24 AM

Here's your February issue of ETM's Crime Scene News

View this email in your browser



Evidence Technology Magazine • Crime Scene News • February 2020



Sponsored

Forensic Healthcare

Webinar: Providing Forensic Healthcare to Native Communities

February 18, 2020 — A webinar on February 27, 2020 presented by the NIJ's Forensic Technology Center of Excellence aims to heighten awareness among forensic examiners of the importance of providing culturally appropriate and trauma-informed services to the American Indian / Alaska Native (AI/AN) community. The webinar will discuss jurisdictional factors affecting examinations, pertinent laws to consider, and health care services that may be available to AI/AN populations.

>Read More

Support

Foundation Supports Families of First Responders Who Paid the Ultimate Price

February 12, 2020 — The Front Line Foundation announced recently they have started 2020 by paying death benefits to six families of first responders who died while serving others.

>Read More



NEW ISSUE! Read the January-February Issue of ETM

Crime Prevention

Fewer Liquor Stores May Lead to Less Homicide

February 13, 2020 — Reducing the number of businesses in Baltimore that sell alcohol in residential areas may lower the homicide rate, according to new research in the Journal of Studies on Alcohol and Drugs.

>Read More

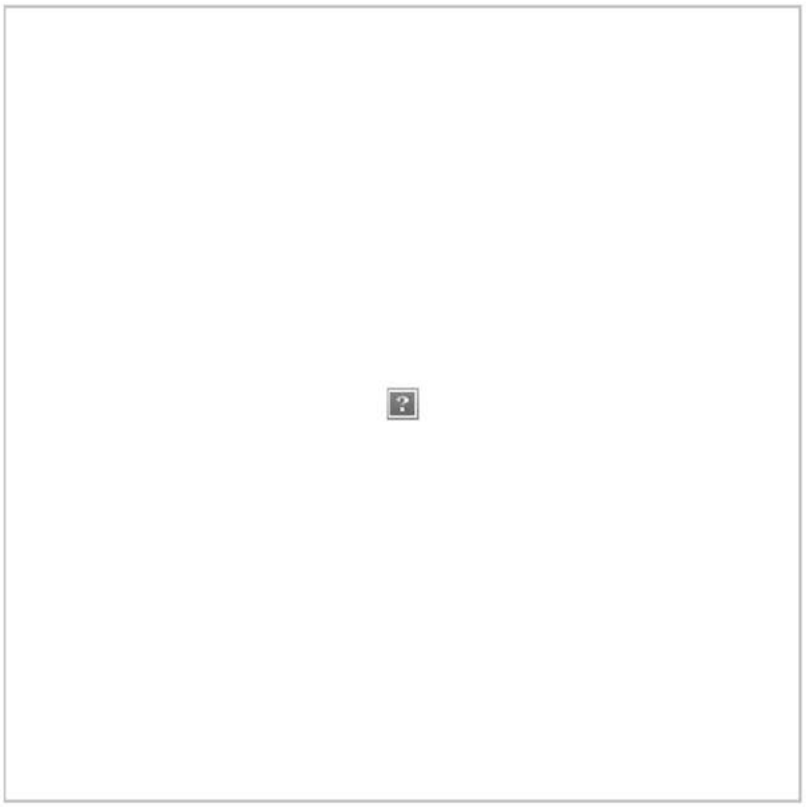
Drug Screening

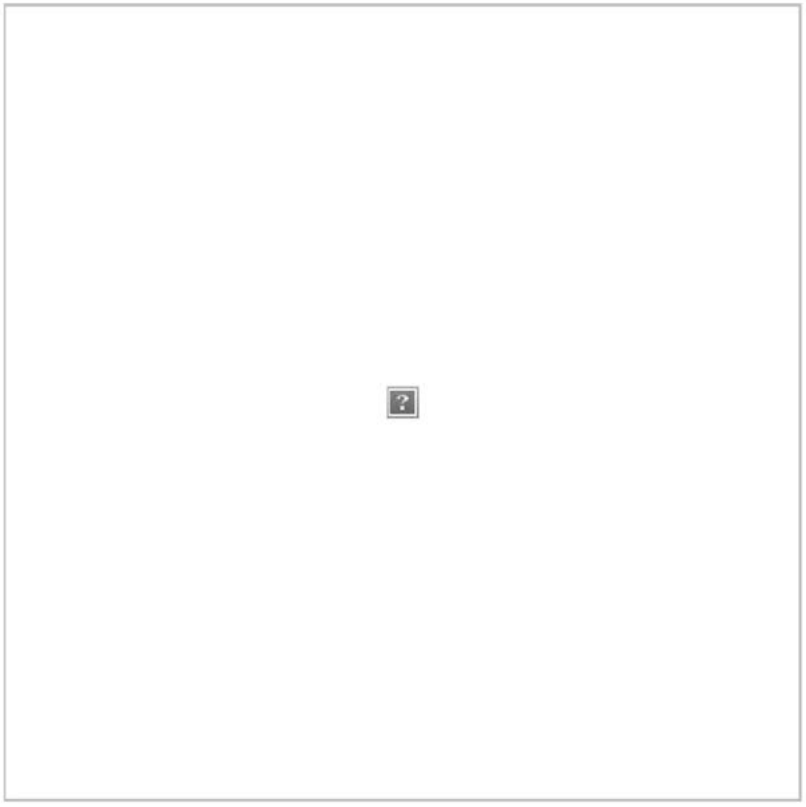
Experimental Fingerprint Test Detects Traces of Cocaine on Skin

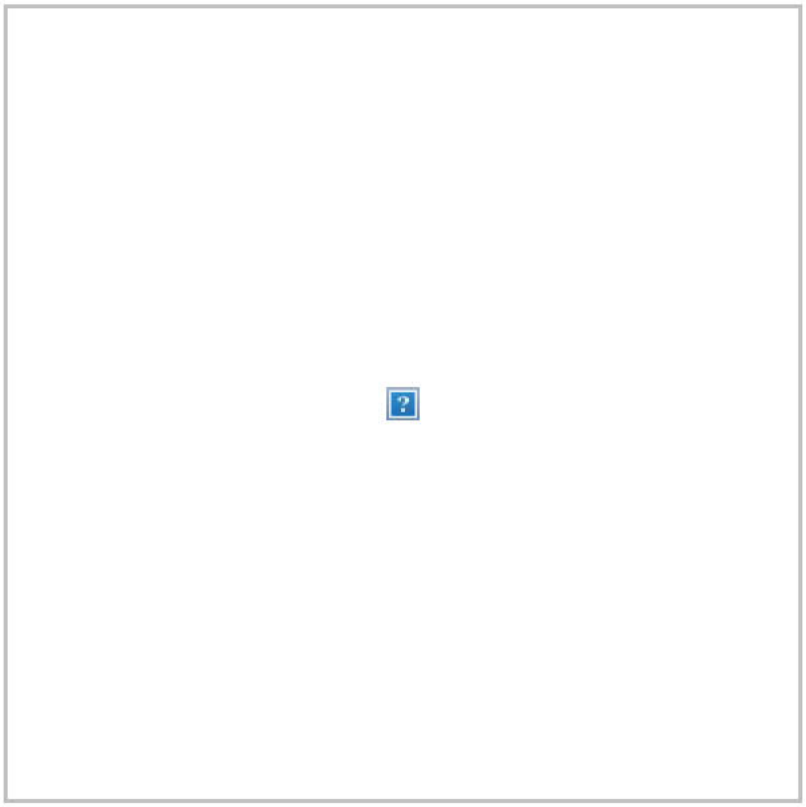
February 4, 2020 — An experimental fingerprint detection approach can identify traces of cocaine on human skin, even after someone has washed their hands — and the test is also smart enough to tell whether an individual has actually consumed the class A drug, or simply handled it.

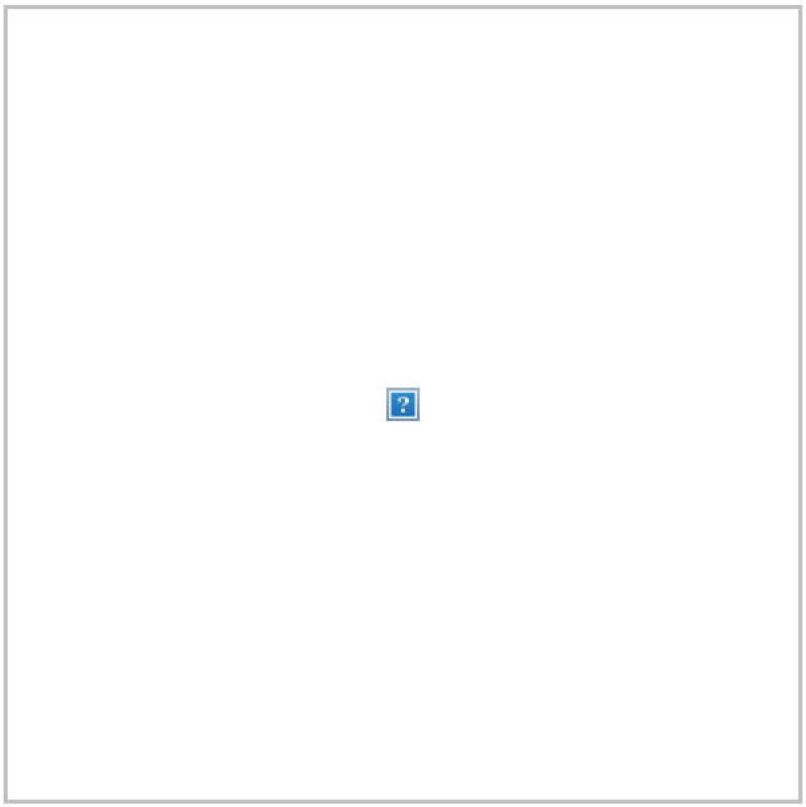
>Read More

Upcoming Conferences









Cloud Explorer Extracts Google Fit Data

February 18, 2020 — ElcomSoft Co. Ltd. recently announced Elcomsoft Cloud Explorer 2.30, which adds support for health and activity information collected by the Android Google Fit app and synchronized to the user's Google Account. >Read More

Motorola Solutions Adds New Analytics to In-Car Video System

February 13, 2020 — Motorola Solutions recently announced the availability of new video security and analytics capabilities for law enforcement. Automated license plate recognition (ALPR) is now part of the WatchGuard 4RE® in-car video system. >Read More

New Touch Screen Repeating Pipette with Advanced Features

February 13, 2020 — The BRAND® HandyStep® touch S repeating pipette has advanced pipetting features for versatility. In addition to standard pipetting, dispensing, auto dispensing and a proprietary "learn" function, advanced modes include sequential dispensing of different volumes, multi-aspiration of different volumes and a titration mode. >Read More

Companies Partner to Deliver Hybrid Video Management Solution

February 11, 2020 — Arcules, a company focusing on integrated video and access control cloud services, recently announced the commercial availability of the Arcules-XProtect Hybrid™ VMS Solution in North America and Europe. >Read More

Subscribe to ETM Today!

New Desktop 3D Scanner for Tiny Objects

February 11, 2020 — Exact Metrology recently announced the availability of the new Artec Micro 3D scanner. The Artec Micro, an automated, metrology-grade desktop 3D scanner is Artec 3D's most accurate 3D scanner to date, and is used for scanning tiny mechanical parts, such as engine valves or connectors, for inspection and reverse engineering, as well as other small objects for industries such as heritage preservation, dentistry, and medical. >Read More

Open Source Web Intelligence Company Opens Office in U.S.

January 22, 2020 — Cobwebs Technologies — the specialized open-source web intelligence company that supports national security agencies, law enforcement agencies, and corporate security departments in rapidly identifying and locating malicious threat actors on the open, deep, and dark webs — is entering the American market with an office in New York City. With little more than a click, Cobwebs makes it highly difficult for terrorists, active shooters, hackers, and other criminal entities to hide, plan, communicate, or ply their nefarious trade in any part of the online world. >Read More

Nearly Half of First Responders Under-Equipped to Handle Extended

Power Outage, Report Finds

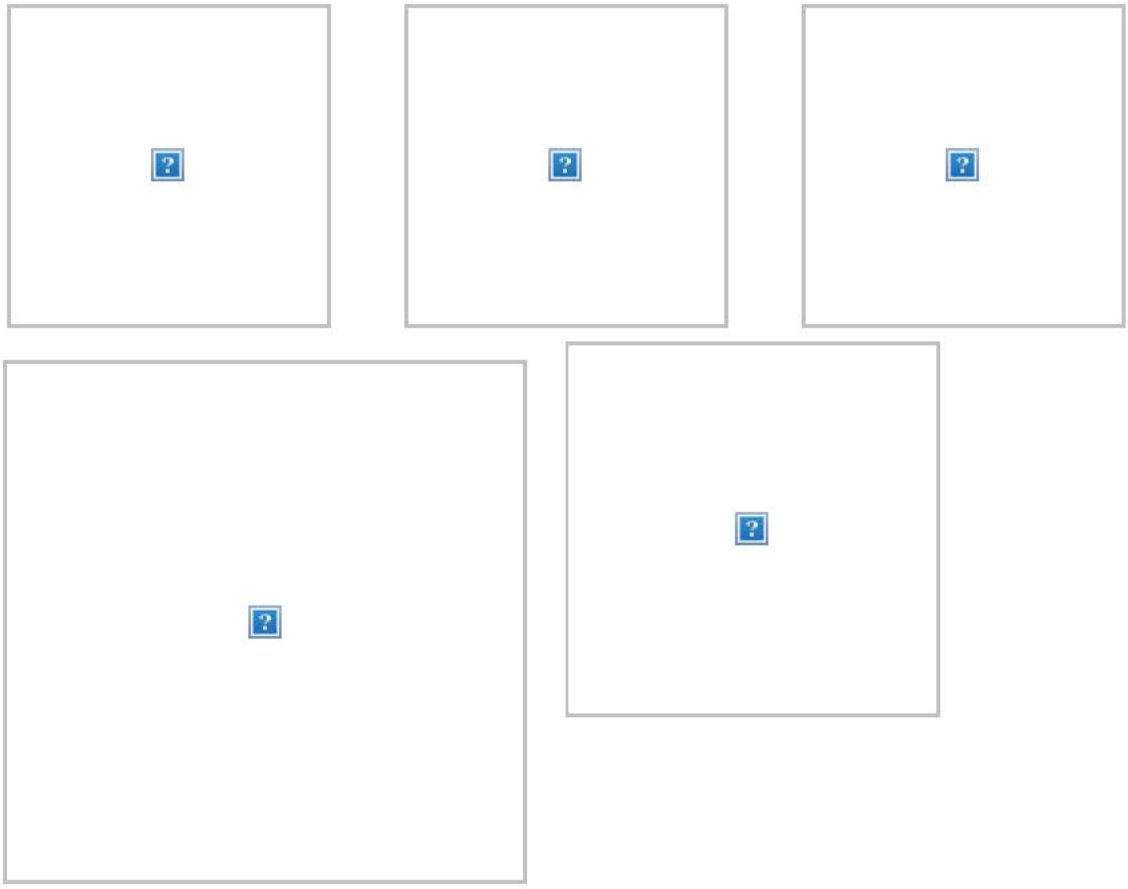
January 23, 2020 — IWCE, an event for the critical communications industry, surveyed more than 597 first responders and public safety professionals to benchmark the current technologies they are using and to understand current technological challenges within the industry. >Read More

Environmentally Friendly Alternative to Canned Air

January 21, 2020 — Canless Air System is a highly effective and environmentally friendly alternative to traditional canned air cleaning products. The line of Hurricane dusters is nontoxic, rechargeable, and provides more power than any canned air competitor. >Read More

---

There's more in the ETM Digital Edition:



Website LinkedIn Twitter Facebook Subscribe

Copyright © 2020 Wordsmith Publishing, All rights reserved.
You are receiving this eNewsletter because you subscribed to Evidence Technology Magazine. You can change your communication preferences at any time by following the links below. Thank you for your readership!

Our mailing address is:
Wordsmith Publishing
PO Box 555

Kearney, MO 64060

Add us to your address book

unsubscribe from this list update subscription preferences

From: Babbin, Timothy (AGO) <Timothy.G.Babbin@mass.gov>
Sent: Tuesday, August 18, 2020 10:03 AM
To: Gallagher, David (POL) <david.gallagher3@MassMail.State.MA.US>
Subject: RE: ALPR Accounts

Major-

Thank you for the prompt assistance with the ALPR.

Could you advise me who would handle password resets?

I had the ALPR when I was down at Plainville but have not had access since.

What (I thought) was my then password no longer works.

Thanks,

Tim

From: Gallagher, David (POL) <david.gallagher3@MassMail.State.MA.US>
Sent: Monday, August 17, 2020 7:44 PM
To: Babbin, Timothy (AGO) <Timothy.G.Babbin@mass.gov>
Subject: ALPR Accounts

DLT Babbin,

Sgt. Tirella reached out and requested I set up ALPR accounts for the following:

DLT Timothy Babbin #2120 *****
Lt. Michael Ahern #2486
Lt. Walter Foley #3110
Lt. Steven Connolly #2719 *****
Lt. Joseph Ross #2264
Lt. Michelle Sutherland #2466
Sgt. Michael Leo #2887
Sgt. Maura McCarthy #2759
Sgt. Patrick Johnson #3128
Sgt. Matthew Hannigan #3281
Sgt. Thomas Mahon #3146
Tpr. John MacDonald #3143
Tpr. Loming Chan #0741 *****
Tpr. Robert Noonan #3327
Tpr. Jose Cuevas #3237
Tpr. Carly Rose #3347
Tpr. Robert Soldani #3879
Tpr. Daniel Nunes #3674 *****
Tpr. Erin McLaughlin #3655
Tpr. Kevin Flynn #3791
Tpr. Christopher Andrade #3738 *****
Tpr. Martin Concannon #3409
Tpr. Shawn Murphy #3481
Tpr. Joshua Rucho #3704
Tpr. Nicholas Pellegrino #3684
Tpr. Shawn LeBlanc #3015
Tpr. Steven Grasso #3803
Tpr. Julio Barbosa #4074

***** Indicates that there is already account created.

I will send a separate email with user guide / link to download software.

Logon will be mspXXXX (users 4 digit ID#)

Initial password will be Lastname#XXXX! ex: Flynn#3791! McLaughlin#3655!

They can change it after initial login.

If you can designate a single POC to address any issues, that would be greatly appreciated.

Lt's and Sgt's have advanced access. Tprs. have basic access.

Please let me know if you need any further assistance.

Respectfully,

David M. Gallagher
Major, Massachusetts State Police
Special Operations
508-820-2162
David.Gallagher3@MassMail.state.ma.us

From: Kayla, Brian (POL)
To: Hurley, Dennis (POL)
Subject: FW: Comm v. McCarthy - locating D's MV with ALPRs on Bourne/Sagamore Bridges not a `search`
Date: Tuesday, April 14, 2020 1:45:00 PM

From: mdoc@listserv.rias.net [mailto:mdoc@listserv.rias.net]
Sent: Tuesday, April 14, 2020 1:29 PM
To: mdoc@listserv.rias.net
Subject: Fw: Comm v. McCarthy - locating D's MV with ALPRs on Bourne/Sagamore Bridges not a "search"

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

All

I hope this message finds you all safe and healthy. I am forwarding ADA Marguerite Grant's breakdown of the McCarthy case on ALPRs issued last week. Congratulations to ADA Elizabeth Sweeney on the result.

-CK

Christopher W. Kelly Director
Digital Evidence Laboratory
Commonwealth of Massachusetts
Office of the Attorney General
One Ashburton Place
Boston, MA 02108
617.963.2146 (office)
617.963.2620 (lab main)
christopher.kelly@mass.gov

From: Grant Marguerite (NFK) <Marguerite.Grant@MassMail.State.MA.US>
Sent: Friday April 17 2020 5:33 PM
To: 'jbukunt@worc-ma.gov' <jbukunt@worc-ma.gov>; 'mdubois@braintreema.gov' <mdubois@braintreema.gov>; 'mmorgan@brooklinema.gov' <mmorgan@brooklinema.gov>; Berkowitz Kenneth <kberkowitz@town.canton.ma.us>; 'mdeluca@cohassetpolice.com' <mdeluca@cohassetpo ice.com>; Lennon Gregory <glennon@cohassetpolice.com>; Quigley William <wquigley@cohassetpolice.com>; d'Entremont Michael <mdentremont@police.dedham-ma.gov>; McGowan Peter <pamcgowan@dovermapd.com>; Grace Michael <mgrace@foxboroughpolice.com>; Thomas I. Lynch (tlynch@franklinpo ice.com)" <tlynch@franklinpolice.com>; 'jmi@franklinpolice.com' <jmi@franklinpolice.com>; 'wsmith@holbrookpolice.com' <wsmith@holbrookpolice.com>; 'mguerrette@medfield.net' <mguerrette@medfield.net>; 'amtingley@medwaypolice.com' <amtingley@medwaypolice.com>; 'csoffayer@mis.la.net>; 'jking@mpdmilton.org' <jking@mpdm lton.org>; 'jschiller@mwdhamma.gov' <jschiller@mwdhamma.gov>; 'cstone@norfolk.ma.us' <cstone@norfolk.ma.us>; Brooks William G. III <adcnsubs@norwoodma.gov>; 'pkelly@norwoodma.gov' <pkelly@norwoodma.gov>; 'James Alfred (jalfred@police.plainville.ma.us)' <jalfred@police.plainville.ma.us>; Keenan Paul <pkeenan@quincyma.gov>; 'ell lampard@randolphmapolice.com' <ellampard@randolphmapolice.com>; 'jford@townofnharon.org' <jford@townofnharon.org>; 'dmcnamara@stoughton-ma.gov' <dmcnamara@stoughton-ma.gov>; 'jcarmichael@walpolepd.com' <jcarmichael@walpolepd.com>; golecki <jgolecki@wellesleyma.gov>; julva@wentwoodpd.org' <julva@wentwoodpd.org>; Grimes Richard C. <rgrimes@weymouth.ma.us>; 'chief@police.wrentham.ma.us' <chief@police.wrentham.ma.us>; Baker Chris (ELA) <chris.baker@mass.gov>; 'powerma2@wit.edu' <powerma2@wit.edu>; 'jconnolly2@suffolk.edu' <jconnolly2@suffolk.edu>; zzMullaney Stephen (POL) <zzStephen.zzMullaney@pol.state.ma.us>; 'Matthew Reardon (mreardon@medwaypo ice.com)' <mreardon@medwaypolice.com>; 'akingsbury@medwaypolice.com' <akingsbury@medwaypolice.com>; Hannon John <jhannon@foxboroughpolice.com>; Brewer Don <dbrewer@townofnharon.org>; Guerriero Michael (POL) <michael.guerriero@pol.state.ma.us>; 'Adams Jerry (pd104) (jadams@police.nantucket-ma.gov)' <jadams@police.nantucket-ma.gov>; Donoghue William (NOR) <WI liam.J.Donoghue@MassMail.State.MA.US>; Hunte Alan (MED) <Alan.Hunte@MassMail.State.MA.US>; Fontes Steven M. (NSC) <steven.m.fontes@MassMail.State.MA.US>; Robert Connor (connor@fbc.edu)' <connorr@fbc.edu>; Staryanki Christopher <cstaryinski@gardner-ma.gov>; Solimini Ronald (POL) <ronald.solimini@pol.state.ma.us>; 'wward@mpdmilton.org' <award@mpdmilton.org>; 'slydon@braintreema.gov' <slydon@braintreema.gov>; Goulding Michael J. <Goulding.M@westonmass.org>; Kennedy Kevin <kkennedy@lincolntown.org>; zzClte David (POL) <zzDavid.zzClte@pol.state.ma.us>; 'David Flaherty (flaherdb@bc.edu)' <flaherdb@bc.edu>; Moriarty Dan <daniel.moriarty.2@bc.edu>; 'LSullibar@gmail.com' <LSullibar@gmail.com>; Antosiw Romere (POL) <romere.antosiw@pol.state.ma.us>; Rudolph James (POL) <James.Rudolph@pol.state.ma.us>; 'mcollins@mpdmilton.org' <mcollins@mpdmilton.org>; Bulman Paul (NOR) <Paul.Bulman@MassMail.State.MA.US>; Pantazakos Keith (NFK) <keith.pantazakos@MassMail.State.MA.US>; Farioli Mark (NFK) <Mark.R.Farioli@MassMail.State.MA.US>; Sullivan Brian (POL) <Brian.Sullivan@pol.state.ma.us>; Lynch Dennis (NFK) <Dennis.M.Lynch@MassMail.State.MA.US>; Powers Meaghan (NFK) <megan.powers@MassMail.State.MA.US>; Dicicco David M (POL) <David.M.Dicicco@pol.state.ma.us>; Bukhenik Yuriy (POL) <yuriy.bukhenik@pol.state.ma.us>; Dunne Matthew (POL) <MAtthew.Dunne@pol.state.ma.us>; Nichol Kevin (POL) <kevin.nichol@pol.state.ma.us>; 'Matthew Murphy (mmurphy@brocktonpo ice.com)' <mmurphy@brocktonpolice.com>; 'ebell@brocktonpolice.com' <ebell@brocktonpolice.com>; 'arelly@hullpolice.org' <arelly@hullpolice.org>; Donovan Gerald (POL) <gerald.donovan@pol.state.ma.us>; 'sbrady@marshfield.org' <sbrady@marshfield.org>; 'matthieu.leitch@jeff.gov' <matthieu.leitch@jeff.gov>; 'jmclaughlin@wellesleyma.gov' <jmclaughlin@wellesleyma.gov>; 'juan.seoane@pd.boston.gov' <juan.seoane@pd.boston.gov>; Dziadosz Peter <detective@gnantpolice.org>; Pack Noah (POL) <noah.pack@pol.state.ma.us>; O Brien Sean (NOR) <Sean.P.OBrien@MassMail.State.MA.US>; Delaney Mark (NOR) <mark.delaney1@MassMail.State.MA.US>; John Perchard <jperchard@weymouth.ma.us>; O'Neill Russ <roneill@brooklinema.gov>; 'Shannon Ducharme' <educharme@chicopeepolice.com>; 'Det. Lt. Melissa Greener' <melissagreener@randolphmapolice.com>; Bishop Kevin <kbishop@townofnharon.org>; 'jpenders@townofnharon.org' <jpenders@townofnharon.org>
Cc: Morrissey Michael (NFK) <Michael.W.Morrissey@MassMa l.State.MA.US>; Doherty Denise (NFK) <Denise.M.Doherty@MassMail.State.MA.US>; Fanning John (NFK) <John.m.fanning@MassMail.State.MA.US>; Keefe Edward (NFK) <Edward.T.Keefe@MassMa l.State.MA.US>; Mattallano Gerard (NFK) <Gerard.Mattallano@MassMail.State.MA.US>; 'Justin Fitzsimmons (justin@nsarch.org)' <justin@search.org>; Quirk Sean (POL) <sean.quirk@pol.state.ma.us>; Tully Brian (NFK) <Brian.F.Tully@MassMail.State.MA.US>; NFK-DL-ADA-Superior-ct <NFK-DL-ADA-Superior-ct@MassMail.State.MA.US>; NFK-DL-ADA-District-ct <NFK-DL-ADA-District-ct@MassMail.State.MA.US>; NFK-DL-ADA- Appeals <NFK-DL-ADA-Appeals2@MassMail.State.MA.US>; Kelly Christopher (AGO) <christopher.kelly@mass.gov>
Subject: Comm v. McCarthy - locating D's MV with ALPRs on Bourne/Sagamore Bridges not a "search"



Chiefs
Commonwealth v. McCarthy (SJC 12750) ← click on that link to see the case
In this case the SJC ruled that police tracking D's car using 4 automatic license plate readers (ALPRs) at both ends of the Bourne and Sagamore Bridges was too limited to amount to a constitutional "search." The SJC declined to say exactly how detailed digital surveillance would have to be to constitute a search leaving that issue for future cases.

State Po ice maintain ALPRs including ones at both ends of the Bourne and Sagamore Bridges. (p.3) The ALPRs photograph vehicles' license plates; that data along with the date and time of the sighting is retained by EOPPS for a year. (p.3-4) Authorized users including police may put a license plate number on a "hot list " and receive an alert if that plate is sighted; reasons to put someone on the "hot list" include not only criminal investigations but also Amber alerts missing persons and BOLO alerts. (p. 3 25 n.13)

Through surveillance controlled buys and information from 4 Cs Barnstable police suspected that the co-D was selling heroin out of his house in Barnstable. (p.4) Police saw a black Hyundai driven by D visit there briefly so they suspected that D was the co-D's supplier. Police put the Hyundai's license plate number on the State Police ALPR "hot list " so that they'd be notified whenever the Hyundai crossed one of the bridges. (p.5) After getting an alert that the Hyundai had crossed onto the Cape police followed both the Hyundai and the co-D to the buy location on a quiet residential street where D and co-D met for about 30 seconds but police could not see a physical exchange. (p.5) From the ALPR data police generated a spreadsheet showing that in mid-winter the Hyundai had crossed the bridges dozens of times sometimes more than once a day adding to police suspicion that D was the heroin supplier. (p.5-6) When police got a second alert that the Hyundai had crossed onto the Cape they again followed D and co-D to the buy location and saw a 30-second meeting but could not see any exchange. This time police stopped both cars handcuffed both co-D and D and read them Miranda. On co-D police found heroin; on D police found 2 cell phones and cash. (p.6-7) At the station police repeatedly told D he was "not under arrest " and D made statements.

D moved to suppress the ALPR data his statements and evidence obtained from the stop. A Superior Court judge found that the moment of arrest was when D and co-D were handcuffed at the scene of the traffic stop but denied the motion to suppress. (p.33) The SJC upheld the denial.

ALPRs and expectation of privacy in digital surveillance: At some length the SJC discussed the constitutional issues raised by digital surveillance. (p.7-24) Police conduct amounts to a search if: (1) it intrudes on a D's expectation of privacy and (2) society is willing to recognize the expectation of privacy as reasonable. Here the SJC ruled D did have an expectation of privacy because D and co-D chose a buy location in a quiet residential area. (p.8 n.5) As to what expectation of privacy society recognizes as reasonable with regard to digital surveillance the SJC was guided by historical understandings of what was an unreasonable search and seizure when the U.S. and Mass. Constitutions were adopted in the late 1700s in reaction to redicasts' rummaging without restraint through colonists' homes. (p.8-10) New technologies like ALPRs raise difficult legal issues because they are easier and less expensive for police than traditional surveillance can be done secretly and permit police to search back in time for a vehicle's movements even before police suspicion arose. (p.12-14) Society does not recognize as reasonable an expectation of privacy in what someone "knowingly exposes" to public view like a license plate – which by statute must be "displayed conspicuously." (p.15-16 & n.8) In older cases involving less advanced technology courts have held that a D did not have an expectation of privacy in contents of a phone conversation in a phone booth or a radio beeper" tracking a single journey. (p.14-17) But technology like ALPRs GPS and CSLI are different because they may give police a **mosaic** of information where each piece may not be public but when viewed together they create a picture that implicates someone's privacy interests like their political religious or sexual associations. (p.17-21) The SJC was concerned that with enough ALPRs police could track someone's location everywhere which would be "creepy." (p.21) Exigent circumstances would likely justify using an ALPR in a situation involving an Amber alert or missing person. (p.21 n.13) The D urged the SJC to consider not just these four ALPRs on the Bourne and Sagamore Bridges but the hundreds of ALPRs across Massachusetts; the SJC declined to do so because that evidence is not in the record of this case. (p.24) The **limited number of cameras** here and their placements on the bridges was not enough to give D an expectation of privacy that society would recognize as reasonable. (p.28) The SJC declined to say how much digital surveillance would give such an expectation and admitted that its unwillingness to do so **"may bring some interim confusion"** until further cases develop the law on this issue. (p.28 n.15) Chief Justice Gants wrote a separate concurrence suggesting that one thing the SJC could do is to require police who want to search a vast amount of digital data to apply for a court order supported by an affidavit showing reasonable suspicion to do so. (concurrence p.1) This would be like a Stlr but with a lower standard than PC.

Written policy: The SJC rejected D's argument that Barnstable PD should have had a written policy about ALPRs and the MSP policy on which Barnstable relied was not specific enough. (p.30) Written policies are required to justify certain exceptions to the SW requirement (like inventory searches and sobriety checkpoints) – they do not apply to the threshold question whether a search occurred in the first place. (p.31)

Minority opinion: At the station police repeatedly told D that D was "not under arrest." But the motion judge found that the moment of arrest was when police handcuffed D at the traffic stop. (p.33) D argued that his statements should be suppressed because police telling him he was not under arrest amounted to "deceit or trickery" to get D to confess. The motion judge and the SJC rejected that argument saying that even if telling D he was not under arrest amounted to deceit or trickery it was just one factor to be used in determining voluntariness.

Bottom line: Police use of ALPRs at limited locations is not a constitutional search – but we don't know how many locations it'd have to be to amount to one. Using an ALPR in **exigent circumstances** like an Amber Alert is likely OK. Local police don't need a written policy to use ALPRs maintained by MSP. After a D has been handcuffed police should not tell D that D is "not under arrest" – police will likely be accused later of deceit and trickery.

A thought: There are news stories online that cell phones may be used to do contact tracing for people exposed to COVID-19. If lots of people willingly agree to let their cell phone data be used to track their whereabouts would that ever change courts' view of what society recognizes as a reasonable expectation of privacy? At some point if members of the pub ic come to expect that they're being tracked should police be allowed to use that evidence too? Or at the very least should there be a jury instruction explaining that police have less access to the data than other entities (like software companies or public health agencies)?

As always email me with any questions. Wash your hands!

Marguerite

Marguerite T. Grant
Grand Counsel – Director of Training
Office of Norfolk District Attorney Michael W. Morrissey
45 Shawmut Road
Canton, MA 02021
781-830-4820

This message is sent to you because you are subscribed to
the mailing list mdoc@listserv.rias.net.
To unsubscribe, E-mail to: mdoc-off@listserv.rias.net

Confidentiality Notice This e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure, forwarding or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply e-mail and destroy all copies of the original message.

Any information that is disseminated via listserv.rias.net is considered property of the issuing agency.

From: Anthony Holloway
To: Antonio G. Gilliam; Colleen J. Dunphy; David J. Gerardo; Frank J. Williams; Jacquelyn J. Yeager; Jerry M. Hensley; Joseph J. Dente; Laura A. Roe; Mary A. Watkins; Matthew Mckinney; Matthew T. Furse; Michael J. Kovacsev; Michael L. McDonald; Nathaly M Patterson; Pamela West; Patrice N. Hubbard; Phillip J. Beahn; Richard Ferner; Robert E. Mailhiot; Shannon Halstead; Suzanne M. Strocsher; Sylvia K. Kapous; Tim T. Brockman; Yolanda F. Fernandez
Cc: Upton, Paul (POL)
Subject: FW: IACP"s The Lead: Survey Finds Most Police Departments In US Have Issued Guidance To Officers During COVID-19 Pandemic.
Date: Friday, April 17, 2020 8:17:10 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

From: The IACP <TheLead@iacp.bulletinmedia.com>
Sent: Friday, April 17, 2020 8:05 AM
To: Anthony Holloway <anthony.holloway@stpete.org>
Subject: IACP's The Lead: Survey Finds Most Police Departments In US Have Issued Guidance To Officers During COVID-19 Pandemic.

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

If you are unable to see the message or images below, click here to view

Please add us to your address book

Please add us to your address book

Greetings Anthony Holloway

Friday, April 17, 2020

POLICING & POLICY

Advertisement

Survey Finds Most Police Departments In US Have Issued Guidance To Officers During COVID-19 Pandemic

ABC News (4/16) reports, "A recent survey done by the International Association of Chiefs of Police and George Mason University shows that 91% of the responding departments have offered guidance to officers over COVID-19 concerns. The survey, obtained by ABC News, shows that most police departments were prepared for COVID-19 and more than 1,000 departments around the country were ready to instruct their men and women on calls of service," but "the departments could be doing more to obtain personal protective equipment for officers. Just 15% of agency respondents rated their ability to provide PPE as 'excellent.' Steve Casstevens, the president of the IACP and chief of the Buffalo Grove Police Department, told ABC News that some agencies didn't realize the long-term effects of the virus. 'I don't think a lot of them expected it to go on this long,' he said. 'As this got worse and worse, policies changed.' Now it is standard procedure for all officers to wear masks, Casstevens noted."

Police Departments Finding Help In Unexpected Places Amid Coronavirus Outbreak

NBC News (4/16) reports that coronavirus infection "has already spread to officers in several small departments in several states, including Florida, Washington and Pennsylvania, where the interim police chief of a 20-member force died of COVID-19-related complications on Monday. The coronavirus has taken a toll on several segments of society, but small police departments are especially vulnerable – officers are embedded in the close-knit communities they're struggling to protect while also trying to protect themselves." NBC News adds, "Many departments are planning layers of fail-safes in the event of mass contagion within their force. Help is coming from several places, some as unexpected as dentists' offices. Deficiencies in resources to handle the pandemic have created significant pangs within small departments that frequently find themselves at the back of the line for supplies."

US Cities See Spike In Speeders During Pandemic

The New York Times (4/16, Hu) reports, "Drivers have roared through deserted New York City streets as if they were taking a lap at Le Mans. They have openly drag raced on major commuting arteries, including Sixth Avenue and the West Side Highway in Manhattan. And they have racked up thousands of speeding tickets across the city — and in some cases, they have left behind wrecked cars and lives." The Times adds, "As traffic has disappeared from New York's streets during the coronavirus pandemic, some drivers have responded by revving their engines and taking off. The open streets have also brought out motorcycle gangs and daredevils on dirt bikes and all-terrain vehicles doing wheelies and stunts in traffic lanes, residents said. 'Now that the streets are empty, the Fast & Furious wannabes really think they're living in a video game,' tweeted City Councilman Justin Brannan, a Democrat who represents southwest Brooklyn, adding that the sounds of racing cars and motorcycles on the Belt Parkway in Bay Ridge 'have become a scary lullaby.'"

The Atlanta Journal-Constitution (4/16, Dixon) reports, "Sandy Springs isn't the only city seeing an increase in motorists driving like they are competing in the NASCAR Cup Series on roadways clear of traffic due to the coronavirus pandemic. Smyrna police report quite a few drivers with lead feet are disregarding posted speed limit signs and putting the pedal to the metal." According to the AJC, "Within the last week, officers with the department's Selected Traffic Enforcement Program have written an estimated 50 to 100 tickets along the East-West Connector, said spokesman Sgt. Louis Defense. 'We were noticing that the speeds throughout the city were steadily increasing, so we had to go back to doing some enforcement.'"

Massachusetts Court OKs Limited Use Of License Plate Readers By State Police

The Boston Globe (4/16, Ellement) reports that "the state's high court ruled Thursday that automatic license plate readers used by the State Police do not violate 21st-century privacy protections – under limited circumstances." According to the Globe, "In its unanimous ruling, the Supreme Judicial Court cautioned that it might elevate privacy issues in future cases if State Police and other law enforcement agencies start tapping information in the secretive data base, known by the acronym of ALPR, without proper justification." The court "noted that both the federal and state constitutions have strong protections against unlawful search and seizures by law enforcement built into them by founders who had personal experience with the 'abuses of arbitrary power under British rule.' 'The framers had first-hand experience with abuses of arbitrary power under British rule...The surveillance implications of new technologies must be scrutinized carefully, lest scientific advances give police surveillance powers akin to these general warrants,' Justice Frank M. Gaziano wrote."

Police In US Using Drones To Promote Social Distancing

Fox News (4/16, Sherman) reports from Daytona Beach, Florida, "Kim Andrade was just walking along Daytona beach when a drone came buzzing by. It caught her attention, and she even went ahead and snapped a few photos. What she did not expect to learn, however, is that the drone has a voice. 'This is the Volusia Sheriff's office, please adhere to social distancing guidelines,' said a voice piping out of the unit's onboard speaker." The Volusia County Sheriff's Office "told Fox News that it currently has 18 drones at its disposal. Because of the coronavirus outbreak, officials are increasingly turning to them. 'Unfortunately in law enforcement, we can't practice social distancing,' Volusia County Sheriff Mike Chitwood told Fox News." Chitwood "explains that by using the drones, they can encourage social distancing using the drone's speakers and can break up large gatherings of people without running the risk of getting a deputy infected."

The IACP, with support from the National Highway Traffic Safety Administration (NHTSA), launched the new Traffic Safety Resource Guide (TSRG) designed to help law enforcement officers address the elements of traffic safety from education to enforcement as well as share research and promising practices to support leaders in responding to traffic safety issues encountered in their community. To learn more, access the TSRG here: https://bit.ly/2seLUTg.

Connect with the IACP online: **IACP Event Calendar:**

CRIME & DRUGS

Italian Mafia Seeks To Profit From Coronavirus Pandemic

Reuters (4/16, Amante) reports, "Italy's mafia clans are taking advantage of the coronavirus pandemic to buy favour with poor families facing financial ruin, prosecutors and officials say, and are offering loans and food in what is seen as an age-old

recruitment tactic." Reuters adds, "After decades of campaigning to curb the influence of the mafia in its traditional strongholds of southern Italy, officials and charitable groups say the pandemic has created new opportunities for organised crime to regain people's loyalties. 'We know that "families of friends", all of them loan sharks, are making themselves available to give money to the people in difficulty,' said Amedeo Scaramella, using a euphemism by which clans of the Camorra criminal syndicate are known." Scaramella "heads the San Giuseppe Moscato Foundation, a Catholic group in Naples that fights loan sharking, in part by guaranteeing bank loans to people normally considered credit risks. He told Reuters the sharks start by offering loans at rates that compete with banks and later entrap borrowers by driving them up to 300%."

Police Warn Of Coronavirus Text Scam Containing Fake Alert Of Potential Infection

Newsweek (4/16) reports, "Police in Maine have warned about a text message phishing scam currently in circulation that uses the ongoing novel coronavirus outbreak as a convincing lure." Newsweek adds, "The fraudulent message is spreading a suspicious link with a warning telling recipients they may have contracted COVID-19, the infectious respiratory disease currently spreading across the U.S. In response, law enforcement urged all local citizens to avoid clicking unsolicited URLs. The phishing text message reads: 'Someone who came into contact with you tested positive or has shown symptoms for COVID-19 and recommends you self-isolate/get tested.'" According to Newsweek, "The destination of the link was not clear, but experts have previously warned scammers will be exploiting fears of the virus to steal personal data and financial details."

Pandemic Disrupting Supply Of Illegal Drugs In US

The Wall Street Journal (4/16, Kamp, Subscription Publication) reports the pandemic has appeared to disrupt the supply of illegal drugs, according to Acting DEA Administrator Uttam Dhillon. However, treatment advocates say the supply shortage can pose a risk for opioid users, who could fatally overdose after a period of withdrawal during which their tolerance declines.

Inmates Escape Wisconsin Jail

The Green Bay (WI) Press-Gazette (4/16) reports James Robert Newman and Thomas E. Deering escaped from Columbia Correctional Institution on Thursday. The jail confirmed the escape and said that the inmates "climbed over the prison fence, went to a hotel and took a cab out of the area."

Five Pennsylvania Men Arrested In Connection To Triple Murder In Virginia

WTVR-TV Richmond, VA (4/16) reports James Christopher Myers, Durward Anthony Allen, Jamal Kelvin Bailey, Hugh Cameron Green, and Montel Jaleek Wilson "have been charged with first-degree murder in the slayings of a teenager and two adults found dead inside a Spotsylvania home last May." Spotsylvania County Sheriff Roger L. Harris said, "I'm very grateful for the tireless efforts our Detectives were faced with along with the collaborative multi-agency assistance to bring these suspects to justice. My continued prayers for peace and comfort to the Ozuna and Coleman families."

UK Man Jailed For Claiming He Had Coronavirus, Spitting At Police Officer

The Independent (UK) (4/16) reports, "A man has been jailed for three months for spitting at a police officer after claiming he had coronavirus." Nicholas Hazell, 36, "from Epsom in Surrey, assaulted the officer at a hospital. He had been taken there after falsely claiming to have swallowed some drugs. Surrey Police said Hazell had been arrested on 7 April in connection with an ongoing investigation. Following his arrest he told officers he was infected with coronavirus and urinated in the back of the police van. After being further arrested for criminal damage, he claimed to have swallowed drugs and was taken to hospital. He spat at an officer while waiting to be seen by medics and was later charged with assaulting an emergency worker."

TECHNOLOGY

Interpol: Hospitals Targeted With Array Of Ransomware

The Wall Street Journal (4/16, Stupp, Subscription Publication) reports that Interpol has warned that hackers have used a number of variations of ransomware to launch cyberattacks on hospitals and healthcare facilities in multiple countries, adding to the concerns of medical providers during the coronavirus pandemic.

GLOBAL SECURITY

Military Task Force Prepares to Secure Washington, DC Area

Newsweek (4/16) reports federal officials in the nation's capital "expect a New York-like epidemic in the District, Maryland and Virginia, one that could potentially cripple the government." A little-known military task force "charged with evacuating Washington has already been activated, a task force charged with the most sensitive government mission of 'securing' Washington in the face of attackers, foreign and domestic." Activated on March 16, Joint Task Force National Capital Region

(JTF-NCR) "is chartered to 'defend' Washington on land, in the air, and even on its waterfronts." JTF-NCR is not "only real and operating, reporting directly to the Secretary of Defense for some of its mission, but some of its units are already on 24/7 alert, specially sequestered on military bases and kept out of coronavirus support duties to ensure their readiness." JTF-NCR is charged "with facilitating continuity of government, particularly moving civil and military leaders to secret locations were the order given to evacuate the city."

US Issues Warning Ahead Of 25th Anniversary Of Oklahoma City Bombing

ABC News (4/16) reports, "Marking 25 years since the deadliest domestic terrorist attack on U.S. soil, federal authorities on Thursday warned law enforcement agencies across the country that the threat from violent white supremacists and anti-government extremists remains 'persistent and evolving.' 'The prevalence of lethal [domestic terrorist] attacks in the 25 years following the bombing of the Alfred P. Murrah Federal Building in Oklahoma City highlights the continued threat they pose,' the FBI, Department of Homeland Security and National Counterterrorism said in a joint intelligence bulletin issued nationwide." The bulletin "noted that the April 19, 1995, bombing by anti-government extremist Timothy McVeigh killed 168 people and injured several hundreds more, making 1995 the nation's deadliest year for domestic terrorist attacks."

The AP (4/16, Murphy) reports from Oklahoma City, "In the 25 years since a truck bomb ripped through a federal building in downtown Oklahoma City and killed 168 people, the United States has suffered through foreign wars, a rise in mass shootings and a much deadlier act of terror, the Sept. 11 attacks," but "the April 19, 1995, assault on a sleepy city in the nation's heartland shocked many Americans out of their sense of security and awakened them to their own vulnerability. Terror wasn't just a foreign problem, it was here. Events since have only contributed to a shared anxiety." The AP adds, "Ordinarily, survivors and victims' families would gather Sunday at the memorial where the Alfred P. Murrah Building once stood to pay tribute to the lives that were lost and tragically altered, as they have every year since the bombing," but "the 25th anniversary ceremony was canceled due to the coronavirus restrictions, denying the public the chance to collectively grieve a past tragedy because a current one is unfolding."

Three Reputed White Supremacists Denied Bond Amid Coronavirus Concerns

The AP (4/16) reports from Rome, Georgia, "Three Georgia men accused of belonging to a white supremacist group and of plotting to kill a couple were denied bond Thursday after requesting a hearing because of coronavirus concerns, authorities said." Floyd County Superior Court Chief Judge Bryant Durham "rejected bond requests for 25-year-old Michael Helterbrand of Dalton; 19-year-old Jacob Kaderli of Dacula; and 21-year-old Luke Lane of Silver Creek, news outlets reported. The three men face charges of conspiring to kill members of a militant anti-fascist group and participation in a criminal gang." Floyd County police "said the men belong to 'the Base,' a group described by the FBI as a collective of hardcore neo-Nazis, operating as a paramilitary organization that is hostile to minority communities."

The Atlanta Journal-Constitution (4/16, Redmon, Joyner) reports, "Three North Georgia men accused of belonging to a white supremacist group and of plotting the murder of a Bartow County couple were denied bond Thursday after citing concerns about the coronavirus pandemic. Floyd County Superior Court Chief Judge Bryant Durham rejected their requests after a hearing in which the defendants were patched in by video from the county jail. The men – Michael Helterbrand, 25, of Dalton; Jacob Kaderli, 19, of Dacula; and Luke Lane, 21, of Silver Creek – have each been charged with participating in a criminal gang and conspiracy to commit murder. Floyd County Police allege they are members of 'the Base,' described as a violent organization that is seeking to 'establish a white ethno-state.' A different judge denied them bond in February."

Federal Prosecutors Appeal Release Of Massachusetts Nursing Home Arson Suspect

The Springfield (MA) Republican (4/16, Barry) reports, "Hours after his arrest Wednesday in connection with the attempted firebombing of a Jewish assisted living facility, John Rathbun was back home at his mother's house in East Longmeadow, released by a federal magistrate judge." Prosecutors "are appealing that decision to U.S. District Judge Mark G. Mastroianni, arguing the magistrate's decision appeared to be based heavily on the COVID-19 pandemic, as opposed to established bail standards." The Republican adds, "There has been an earnest movement in this state and across the country to reduce incarceration rates in order to stem the spread of the coronavirus in prisons and county jails. FBI agents raided Rathbun's Lori Lane home Wednesday morning, looking for evidence from the April 2 attempted firebombing of Ruth's House, a Jewish-sponsored assisted living facility in Longmeadow, according to court records. The alleged attempt occurred six days before the start of Passover."

The Washington Post (4/16, Zauzmer) reports, "A Massachusetts man is accused of planting a homemade bomb at a Jewish assisted-living home, in an act that federal prosecutors say appears to have been motivated by online forums that encouraged violence against Jews." The Post adds, "The bomb did not go off and no one was injured. Authorities arrested John Michael Rathbun, 36, on Wednesday, two weeks after police found the incendiary device at the entrance to Ruth's House, the assisted-living facility in Longmeadow, Mass." Federal prosecutors in Massachusetts "connected Rathbun's alleged actions to a white supremacist group that they did not name, but said the FBI's Western Massachusetts Joint Terrorism Task Force has been

tracking it since March. The members of this group, prosecutors said, have discussed carrying out mass killings using explosive devices to target racial and religious minorities, including people worshiping at synagogues and mosques."

THURSDAY'S LEAD STORIES

- **Crime In UK Falls Sharply Amid Coronavirus Lockdown**
- **European Police Foil Coronavirus Scam After Germany Is Duped Out Of 10,000 Mask**
- **Providers Reportedly Face Uptick In Cyberattacks Amid Coronavirus Pandemic**
- **FBI: Government's Response To Coronavirus Spurred Would-Be Missouri Bomber**
- **Bennington, Vermont Police Review Report To Be Presented Monday**

Subscriber Tools

- Change Email Address
- Send Feedback
- Unsubscribe
- Email Help
- Archives

The Lead is a daily news briefing selected from thousands of sources by the editors of Bulletin Media. Neither Bulletin Media nor the International Association of Chiefs of Police is liable for the use of or reliance on any information contained in this briefing. The presence of articles and/or advertising does not endorse, nor imply endorsement of, any products or services by the IACP.

This complimentary copy of *The Lead* was sent to anthony.holloway@stpete.org as a member benefit. To see how we protect our data, or for any questions on data access, view Bulletin Media's privacy policy.

For information about other member benefits, please contact the IACP at membership@theiacp.org or 1.800.THE IACP.

International Association of Chiefs of Police | 44 Canal Center Plaza Suite 200 | Alexandria, VA 22314

Copyright © 2020 by Bulletin Media | 11190 Sunrise Valley Drive Suite 20 | Reston, VA 20191

From: Plante, Michelle (POL)
To: OToole, Kevin (POL)
Subject: FW: job description for grant
Date: Wednesday, November 18, 2020 11:48:00 AM

DRAFT DRAFT DRAFT

From: Plante, Michelle (POL)
Sent: Wednesday, November 18, 2020 11:05 AM
To: Scott, Michael (POL) <Michael.Scott@pol.state.ma.us>
Subject: job description for grant

Condensed job description you requested for the Heroin/Meth grant:
Intelligence Analyst II

Establish criminal profiles on drug trafficking organization members via sophisticated searches into several law enforcement databases, open source and social media databases and through use of investigative software including, but not limited to: TLO, CLEAR, ISO, Facial Recognition, ALPR, CJISWeb, InmateWeb, MIDNet and OSINT. Run historical ALPR queries and create "hot lists" in the ALPR system in order to track particular drug trafficking organization vehicles in real time and determine narcotics trafficking patterns. Determine the structure and operation of criminal groups on a tactical level and identify criminal associations and relationships by performing various kinds of analyses to support investigative work and produce intelligence products such as link analyses, telephone toll analyses, timeline analyses, and any analyses through which data are integrated to determine the existence of networks and patterns.

Justification for Cellebrite renewal:

Cellebrite is the leader in forensic cell phone extractions and as a trained and certified examiner, it is incumbent upon the CINRET West unit to utilize an in-house analyst to perform cell phone extractions in a time-efficient manner to gain access to valuable intelligence related to narcotics investigations. It is imperative that the license be renewed as the program is updated multiples times a month to keep up to date with the ever-changing software and applications used on mobile devices. If the license is not renewed, we will not be able to update the software with critical updates. This can either lead to not being able to extract complete data from a device, or not being able to extract from a device at all.

Justification for computer:

I was hired by MSP in May 2020 to perform specific duties providing intelligence and investigative field support to the CINRET West Unit. The unit did not have a computer for me to perform my duties and six months later still has not received approval for a computer for me to perform my duties despite being awarded a multi-million dollar grant. Detective Lieutenant Loiselle let me use his old Panasonic CF-54 that was issued to him when he was in IA. This was intended to be a

temporary solution. The laptop is sufficient for basic duties using the internet, but is not sufficient for running I2 Analyst Notebook, RAMS, BOSS LPRs, and the internet at the same time. Since there were multiple previous users on this laptop, it was given to me with half of the available space.

Michelle Plante, Intelligence Analyst II
Massachusetts State Police
Commonwealth Interstate Narcotics Reduction Enforcement Team
CINRET - Western Region
53 Elliot Street
Springfield, Massachusetts 01105
Cell: [redacted]
michelle.plante@pol.state.ma.us

From: Egnitz, Brian (POL)
To: Range, Scott (POL)
Subject: FW: MassPort LPR Cameras
Date: Thursday, May 7, 2020 5:11:00 PM

-----Original Message-----
From: Egnitz, Brian (POL)
Sent: Wednesday, May 6, 2020 6:57 PM
To: Warmington, Scott (POL); Quinn, Dermot (POL)
Cc: Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Mason, Christopher (POL); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL)
Subject: RE: MassPort LPR Cameras

Hi Sirs,

We have begun cutting over the MassPort LPR Cameras into the EOPSS BOSS LPR Server. Today, [redacted] at Airport Road arrivals were migrated and are now writing data to Chelsea. I will continue to cut the remaining cameras over in the next few days and weeks. I will advise when the project is complete.

- Brian

-----Original Message-----
From: Warmington, Scott (POL)
Sent: Tuesday, March 10, 2020 11:36 AM
To: Quinn, Dermot (POL)
Cc: Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Mason, Christopher (POL); Egnitz, Brian (POL); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL)
Subject: Re: MassPort LPR Cameras

What is the cost?

Sent from my iPhone

> On Mar 10, 2020, at 11:28 AM, Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us> wrote:
>
> Michelle and Kyra,
>
> This purchase request is for equipment to allow Mass Port Sierra Wireless modems to communicate directly with the existing ALPR Boss server in Chelsea. This is the fastest way to bring the Massport LPR cameras on line. EOTSS and EOPSS are OK with this solution as is Major Deb Ryan, the CO at Troop F.
>
> As you can see from the thread, this has been going on for some time. I think we can close it out with this small purchase.
>
> This does not resolve the replacement of the existing ALPR equipment that we discussed at Command Staff yesterday. That is a different issue.
>
> Thanks
>
>
> Lieutenant Colonel Dermot J. Quinn #1765
> Division Commander
> Division of Homeland Security & Preparedness

> Massachusetts State Police
>
>
>
>
>
> -----Original Message-----
> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> Sent: Tuesday, March 10, 2020 10:52 AM
> To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
> Subject: FW: MassPort LPR Cameras
>
> Hi LTC.,
>
> Can we order this equipment for the MassPort project?
>
> Thanks, Brian
>
> -----Original Message-----
> From: Slater, James (CHS)
> Sent: Tuesday, March 10, 2020 10:26 AM
> To: Egnitz, Brian (POL)
> Subject: RE: MassPort LPR Cameras
>
> Hi, Brian!
>
> This needs to go through MSP fiscal. They need to enter the purchase in OPAS.
>
> Jim
>
> -----Original Message-----
> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> Sent: Tuesday, March 10, 2020 08:06
> To: Slater, James (CHS) <james.slater@mass.gov>
> Subject: RE: MassPort LPR Cameras
>
> Is this something you can order or does it need to go through MSP?
>
> -----Original Message-----
> From: Slater, James (CHS)
> Sent: Monday, March 9, 2020 10:36 AM
> To: Egnitz, Brian (POL)
> Subject: RE: MassPort LPR Cameras
>
> Thanks, Brian...I will check with TSS.
>
> Jim
>
> -----Original Message-----
> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> Sent: Monday, March 9, 2020 10:29
> To: Slater, James (CHS) <james.slater@mass.gov>
> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
> Subject: RE: MassPort LPR Cameras
>
> Thanks Jim,
>

> I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need [redacted] I have reached out to BCM for a quote.
>
> I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.
>
> I plan to cut one sector ([redacted]) over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?
>
> -Brian
>
> -----Original Message-----
> From: Slater, James (CHS)
> Sent: Friday, March 6, 2020 1:43 PM
> To: Egnitz, Brian (POL)
> Cc: Quinn, Dermot (POL)
> Subject: RE: MassPort LPR Cameras
>
> Hi, Brian!
>
> I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.
>
> So, assuming you move forward with this, who would actually make this happen?
>
> Thanks.
>
> Jim
>
> -----Original Message-----
> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> Sent: Wednesday, March 4, 2020 17:53
> To: Slater, James (CHS) <james.slater@mass.gov>
> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
> Subject: Re: MassPort LPR Cameras
>
> Hi Jim,
>
> Regarding the Massport cameras; in the early days of AVL we [redacted] modem's in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don't we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn't have to do any firewall work either because they have [redacted] and communicate like all of the MDT's . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.
>
> We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.
>
> Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.
>
>> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>>
>> Thank you sir

>>
>> Major Charles W. Atchison III
>> Troop F Commander
>> Massachusetts State Police
>> Director of Aviation Security
>> 2 Service Road
>> East Boston, Ma 02128
>> Office: 617-568-7555
>> Cell: 50[redacted]
>>
>>
>> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>>
>> All,
>> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>>
>> Thanks
>>
>> CW
>>
>> From: Quinn, Dermot (POL)
>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
>> Sent: Monday, February 10, 2020 10:31 AM
>> To: Egnitz, Brian (POL)
>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
>> Slater, James (CHS)
>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
>> Robert (EOTSS)
>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
>> Warmington, Scott (POL)
>> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
>> .us>>; Peek, Brian T. (EOTSS)
>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>> Timothy (EPS)
>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
>> Michalski, Maria (EPS)
>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
>> Christopher (POL)
>> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
>> Hughes, Sean M. (EOTSS)
>> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
>> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
>> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
>> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
>> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
>> Atchison, Charles (POL)
>> <catchison@massport.com<mailto:catchison@massport.com>>
>> Subject: RE: MassPort LPR Cameras
>>
>> Good Morning,
>>
>> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License

Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>>
>> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>>
>> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>>
>> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>>
>> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>>
>> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>>
>> I can’t overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security’s technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>>
>> Respectfully,
>>
>>
>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
>> of Homeland Security & Preparedness Massachusetts State Police
>> <image006.png>
>>
>>
>>
>>
>> From: Egnitz, Brian (POL)
>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
>> Sent: Friday, January 17, 2020 1:10 PM
>> To: Slater, James (CHS)
>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
>> Cc: Quinn, Dermot (POL)
>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
>> Guerriero, Robert (EOTSS)
>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
>> Brian T. (EOTSS)

>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>> Timothy (EPS)
>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
>> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
>> Maria (EPS)
>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi Jim,
>>
>> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>>
>> -Brian
>>
>>
>> From: Egnitz, Brian (POL)
>> Sent: Monday, January 6, 2020 1:33 PM
>> To: Slater, James (CHS)
>> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
>> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
>> Crary
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi Jim,
>>
>> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>>
>> Thanks Brian
>>
>>
>> From: John Tedona [mailto:jtedona@neology.net]
>> Sent: Monday, December 9, 2019 4:55 PM
>> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>> Timothy (EPS); Slater, James (CHS)
>> Subject: RE: MassPort LPR Cameras
>>
>> Alex,
>>
>> I can be available most anytime tomorrow for a call.
>>
>>
>> Regards,
>>
>> John Tedona
>> PIPS TECHNOLOGY - A Neology Business
>> Sales Manager
>> 12760 Danielson Ct. Suite A
>> Poway, CA 92064
>> Phone: 201-841-6237

>> Email: jtedona@neology.net<mailto:jtedona@neology.net>
>> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
>> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
>> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
>> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
>> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ
>> U2sB_fmM6g&e=>
>>
>>
>> From: Chute, Alexander
>> <AChute@massport.com<mailto:AChute@massport.com>>
>> Sent: Monday, December 9, 2019 4:38 PM
>> To: Egnitz, Brian (POL)
>> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
>> <pcrary@neology.net<mailto:pcrary@neology.net>>
>> Cc: Guerriero, Robert (MASSIT)
>> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
>> Peek, Brian T. (EOTSS)
>> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
>> Timothy (EPS)
>> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
>> Slater III, James F (CHS)
>> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
>> Subject: RE: MassPort LPR Cameras
>>
>> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>>
>> Hello All,
>>
>> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>>
>> Respectfully,
>>
>> ~Alex
>>
>>
>> <image007.png>
>>
>> Alexander B. Chute
>> Program Manager, Public Safety Systems Massachusetts Port Authority
>> Cell: [redacted]
>> Office: 617.568.5942
>> achute@massport.com<mailto:achute@massport.com>
>>
>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>
>>

>>
>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>> Sent: Monday, November 18, 2019 3:26 PM
>> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
>> pcrary@neology.net<mailto:pcrary@neology.net>
>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi John, Peter
>>
>> Any issues with moving Massports cameras to the Chelsea DB?
>>
>> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>>
>> The current app server
>> <image008.png>
>>
>> Current DB server
>>
>> <image009.png>
>> <image010.png>
>>
>> Our current reads by month for G.L. c. 4G.L. c. 4,sec. 7,cl.26 (n)(security)
>>
>> Year
>>
>> Month
>>
>> Day
>>
>> Month Name
>>
>> Reads Count
>>
>> 2019
>>
>> 11
>>
>> 1
>>
>> November
>>
>> 495,113
>>
>> 2019
>>
>> 11
>>
>> 2
>>
>> November
>>
>> 472,907
>>
>> 2019
>>

>> 11
>>
>> 3
>>
>> November
>>
>> 384,409
>>
>> 2019
>>
>> 11
>>
>> 4
>>
>> November
>>
>> 411,440
>>
>> 2019
>>
>> 11
>>
>> 5
>>
>> November
>>
>> 434,085
>>
>> 2019
>>
>> 11
>>
>> 6
>>
>> November
>>
>> 495,537
>>
>> 2019
>>
>> 11
>>
>> 7
>>
>> November
>>
>> 444,123
>>
>> 2019
>>
>> 11
>>
>> 8
>>
>> November
>>
>> 542,492

>>
>> 2019
>>
>> 11
>>
>> 9
>>
>> November
>>
>> 443,463
>>
>> 2019
>>
>> 11
>>
>> 10
>>
>> November
>>
>> 389,514
>>
>> 2019
>>
>> 11
>>
>> 11
>>
>> November
>>
>> 362,548
>>
>> 2019
>>
>> 11
>>
>> 12
>>
>> November
>>
>> 236,539
>>
>>
>>
>>
>>
>> From: Chute, Alexander [mailto:AChute@massport.com]
>> Sent: Wednesday, November 13, 2019 2:49 PM
>> To: Egnitz, Brian (POL)
>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>> Timothy (EPS)
>> Subject: RE: MassPort LPR Cameras
>>
>> These stats are from [redacted] we have in the system for this month:
>>
>> <image011.png>
>>
>> ~Alex

>>
>>
>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>> Sent: Tuesday, November 12, 2019 5:28 PM
>> To: Chute, Alexander
>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>> Timothy (EPS)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi Alex,
>>
>> Can you please provide the updated reads per day? Previously you were interested in [redacted] approximately 75,000 reads per day.
>>
>> Here is the [redacted] confi I mentioned.
>>
>> Set host to boss [redacted]
>> Set image [redacted]
>> Set number of [redacted]
>> Set Ping [redacted]
>> Set udp ping [redacted]
>> Set ping [redacted]
>> Set security [redacted]
>>
>> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
>> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>>
>> -Brian
>>
>>
>>
>> From: Chute, Alexander [mailto:AChute@massport.com]
>> Sent: Tuesday, November 12, 2019 2:08 PM
>> To: Egnitz, Brian (POL)
>> Subject: MassPort LPR Cameras
>>
>> Brian,
>>
>> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we [redacted], with [redacted] to come online within the next two months. I anticipate this number growing to [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.
>>
>> Respectfully,
>>
>> ~Alex
>>
>> <image007.png>
>>
>> Alexander B. Chute

>> Program Manager, Public Safety Systems Massachusetts Port Authority
>> Cell: [redacted]
>> Office: 617.568.5942
>> achute@massport.com<mailto:achute@massport.com>
>>
>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>
> <SierraQuoteForMassPort.pdf>

From: Small, Michelle (POL)
To: Silva, Kyra (POL); Sullivan, Margaret (POL)
Subject: FW: MassPort LPR Cameras
Date: Thursday, April 16, 2020 2:19:55 PM

Here you go...

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Tuesday, March 10, 2020 11:37 AM
To: Warmington, Scott (POL) <Scott.Warmington@pol.state.ma.us>; Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Cc: Small, Michelle (POL) <Michelle.E.Small@pol.state.ma.us>; Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>; Slater, James (CHS) <james.slater@mass.gov>; Mason, Christopher (POL) <Chris.Mason@pol.state.ma.us>; Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>; Shaw, Harold <HShaw@massport.com>; Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>; Ball, Richard (POL) <Richard.Ball@pol.state.ma.us>
Subject: RE: MassPort LPR Cameras

$273.60

-----Original Message-----
From: Warmington, Scott (POL)
Sent: Tuesday, March 10, 2020 11:36 AM
To: Quinn, Dermot (POL)
Cc: Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Mason, Christopher (POL); Egnitz, Brian (POL); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL)
Subject: Re: MassPort LPR Cameras

What is the cost?

Sent from my iPhone

> On Mar 10, 2020, at 11:28 AM, Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us> wrote:
>
> Michelle and Kyra,
>
> This purchase request is for equipment to allow Mass Port Sierra Wireless modems to communicate directly with the existing ALPR Boss server in Chelsea. This is the fastest way to bring the Massport LPR cameras on line. EOTSS and EOPSS are OK with this solution as is Major Deb Ryan, the CO at Troop F.
>
> As you can see from the thread, this has been going on for some time. I think we can close it out with this small purchase.
>
> This does not resolve the replacement of the existing ALPR equipment that we discussed at Command Staff yesterday. That is a different issue.
>
> Thanks
>
>
> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
> of Homeland Security & Preparedness Massachusetts State Police
>
>
>

>
>
> -----Original Message-----
> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> Sent: Tuesday, March 10, 2020 10:52 AM
> To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
> Subject: FW: MassPort LPR Cameras
>
> Hi LTC.,
>
> Can we order this equipment for the MassPort project?
>
> Thanks, Brian
>
> -----Original Message-----
> From: Slater, James (CHS)
> Sent: Tuesday, March 10, 2020 10:26 AM
> To: Egnitz, Brian (POL)
> Subject: RE: MassPort LPR Cameras
>
> Hi, Brian!
>
> This needs to go through MSP fiscal. They need to enter the purchase in OPAS.
>
> Jim
>
> -----Original Message-----
> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> Sent: Tuesday, March 10, 2020 08:06
> To: Slater, James (CHS) <james.slater@mass.gov>
> Subject: RE: MassPort LPR Cameras
>
> Is this something you can order or does it need to go through MSP?
>
> -----Original Message-----
> From: Slater, James (CHS)
> Sent: Monday, March 9, 2020 10:36 AM
> To: Egnitz, Brian (POL)
> Subject: RE: MassPort LPR Cameras
>
> Thanks, Brian...I will check with TSS.
>
> Jim
>
> -----Original Message-----
> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> Sent: Monday, March 9, 2020 10:29
> To: Slater, James (CHS) <james.slater@mass.gov>
> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
> Subject: RE: MassPort LPR Cameras
>
> Thanks Jim,
>
> I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need [redacted] wireless AC adapters and [redacted] I have reached out to BCM for a quote.
>

> I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.
>
> I plan to cut one sector ([redacted]) over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?
>
> -Brian
>
> -----Original Message-----
> From: Slater, James (CHS)
> Sent: Friday, March 6, 2020 1:43 PM
> To: Egnitz, Brian (POL)
> Cc: Quinn, Dermot (POL)
> Subject: RE: MassPort LPR Cameras
>
> Hi, Brian!
>
> I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.
>
> So, assuming you move forward with this, who would actually make this happen?
>
> Thanks.
>
> Jim
>
> -----Original Message-----
> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> Sent: Wednesday, March 4, 2020 17:53
> To: Slater, James (CHS) <james.slater@mass.gov>
> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
> Subject: Re: MassPort LPR Cameras
>
> Hi Jim,
>
> Regarding the Massport cameras; in the early days of AVL we installed [redacted] modem's in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don't we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn't have to do any firewall work either because they [redacted] and communicate like all of the MDT's . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.
>
> We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.
>
> Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.
>
>> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>>
>> Thank you sir
>>
>> Major Charles W. Atchison III
>> Troop F Commander
>> Massachusetts State Police

>> Director of Aviation Security
>> 2 Service Road
>> East Boston, Ma 02128
>> Office: 617-568-7555
>> Cell: [redacted]
>>
>>
>> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>>
>> All,
>> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>>
>> Thanks
>>
>> CW
>>
>> From: Quinn, Dermot (POL)
>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
>> Sent: Monday, February 10, 2020 10:31 AM
>> To: Egnitz, Brian (POL)
>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
>> Slater, James (CHS)
>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
>> Robert (EOTSS)
>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
>> Warmington, Scott (POL)
>> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
>> .us>>; Peek, Brian T. (EOTSS)
>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>> Timothy (EPS)
>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
>> Michalski, Maria (EPS)
>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
>> Christopher (POL)
>> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
>> Hughes, Sean M. (EOTSS)
>> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
>> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
>> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
>> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
>> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
>> Atchison, Charles (POL)
>> <catchison@massport.com<mailto:catchison@massport.com>>
>> Subject: RE: MassPort LPR Cameras
>>
>> Good Morning,
>>
>> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.

>>
>> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>>
>> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>>
>> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>>
>> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>>
>> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>>
>> I can’t overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security’s technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>>
>> Respectfully,
>>
>>
>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
>> of Homeland Security & Preparedness Massachusetts State Police
>> <image006.png>
>>
>>
>>
>>
>> From: Egnitz, Brian (POL)
>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
>> Sent: Friday, January 17, 2020 1:10 PM
>> To: Slater, James (CHS)
>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
>> Cc: Quinn, Dermot (POL)
>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
>> Guerriero, Robert (EOTSS)
>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
>> Brian T. (EOTSS)
>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>> Timothy (EPS)
>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,

>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
>> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
>> Maria (EPS)
>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi Jim,
>>
>> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>>
>> -Brian
>>
>>
>> From: Egnitz, Brian (POL)
>> Sent: Monday, January 6, 2020 1:33 PM
>> To: Slater, James (CHS)
>> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
>> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
>> Crary
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi Jim,
>>
>> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>>
>> Thanks Brian
>>
>>
>> From: John Tedona [mailto:jtedona@neology.net]
>> Sent: Monday, December 9, 2019 4:55 PM
>> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>> Timothy (EPS); Slater, James (CHS)
>> Subject: RE: MassPort LPR Cameras
>>
>> Alex,
>>
>> I can be available most anytime tomorrow for a call.
>>
>>
>> Regards,
>>
>> John Tedona
>> PIPS TECHNOLOGY - A Neology Business
>> Sales Manager
>> 12760 Danielson Ct. Suite A
>> Poway, CA 92064
>> Phone: 201-841-6237
>> Email: jtedona@neology.net<mailto:jtedona@neology.net>
>> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
>> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http

>> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
>> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
>> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ
>> U2sB_fmM6g&e=>
>>
>>
>> From: Chute, Alexander
>> <AChute@massport.com<mailto:AChute@massport.com>>
>> Sent: Monday, December 9, 2019 4:38 PM
>> To: Egnitz, Brian (POL)
>> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
>> <pcrary@neology.net<mailto:pcrary@neology.net>>
>> Cc: Guerriero, Robert (MASSIT)
>> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
>> Peek, Brian T. (EOTSS)
>> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
>> Timothy (EPS)
>> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
>> Slater III, James F (CHS)
>> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
>> Subject: RE: MassPort LPR Cameras
>>
>> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>>
>> Hello All,
>>
>> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>>
>> Respectfully,
>>
>> ~Alex
>>
>>
>> <image007.png>
>>
>> Alexander B. Chute
>> Program Manager, Public Safety Systems Massachusetts Port Authority
>> Cell: [redacted]
>> Office: 617.568.5942
>> achute@massport.com<mailto:achute@massport.com>
>>
>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>
>>
>>
>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>> Sent: Monday, November 18, 2019 3:26 PM
>> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);

>> pcrary@neology.net<mailto:pcrary@neology.net>
>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi John, Peter
>>
>> Any issues with moving Massports cameras to the Chelsea DB?
>>
>> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>>
>> The current app server
>> <image008.png>
>>
>> Current DB server
>>
>> <image009.png>
>> <image010.png>
>>
>> Our current reads by month for about [redacted]
>>
>> Year
>>
>> Month
>>
>> Day
>>
>> Month Name
>>
>> Reads Count
>>
>> 2019
>>
>> 11
>>
>> 1
>>
>> November
>>
>> 495,113
>>
>> 2019
>>
>> 11
>>
>> 2
>>
>> November
>>
>> 472,907
>>
>> 2019
>>
>> 11
>>
>> 3
>>

>> November
>>
>> 384,409
>>
>> 2019
>>
>> 11
>>
>> 4
>>
>> November
>>
>> 411,440
>>
>> 2019
>>
>> 11
>>
>> 5
>>
>> November
>>
>> 434,085
>>
>> 2019
>>
>> 11
>>
>> 6
>>
>> November
>>
>> 495,537
>>
>> 2019
>>
>> 11
>>
>> 7
>>
>> November
>>
>> 444,123
>>
>> 2019
>>
>> 11
>>
>> 8
>>
>> November
>>
>> 542,492
>>
>> 2019
>>
>> 11

>>
>> 9
>>
>> November
>>
>> 443,463
>>
>> 2019
>>
>> 11
>>
>> 10
>>
>> November
>>
>> 389,514
>>
>> 2019
>>
>> 11
>>
>> 11
>>
>> November
>>
>> 362,548
>>
>> 2019
>>
>> 11
>>
>> 12
>>
>> November
>>
>> 236,539
>>
>>
>>
>>
>>
>> From: Chute, Alexander [mailto:AChute@massport.com]
>> Sent: Wednesday, November 13, 2019 2:49 PM
>> To: Egnitz, Brian (POL)
>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>> Timothy (EPS)
>> Subject: RE: MassPort LPR Cameras
>>
>> These stats are from the [redacted] we have in the system for this month:
>>
>> <image011.png>
>>
>> ~Alex
>>
>>
>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>> Sent: Tuesday, November 12, 2019 5:28 PM

>> To: Chute, Alexander
>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>> Timothy (EPS)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi Alex,
>>
>> Can you please provide the updated reads per day? Previously you were interested in sharing [redacted] at approximately 75,000 reads per day.
>>
>> Here is [redacted] I mentioned.
>>
>> Set host to [redacted]
>> Set image [redacted]
>> Set numbe [redacted]
>> Set Ping [redacted]
>> Set udp pi [redacted]
>> Set ping [redacted]
>> Set securit [redacted]
>>
>> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
>> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>>
>> -Brian
>>
>>
>>
>> From: Chute, Alexander [mailto:AChute@massport.com]
>> Sent: Tuesday, November 12, 2019 2:08 PM
>> To: Egnitz, Brian (POL)
>> Subject: MassPort LPR Cameras
>>
>> Brian,
>>
>> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have [redacted], with another [redacted] to come online within the next two months. I anticipate this number growing to approximately [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.
>>
>> Respectfully,
>>
>> ~Alex
>>
>> <image007.png>
>>
>> Alexander B. Chute
>> Program Manager, Public Safety Systems Massachusetts Port Authority
>> Cell: [redacted]
>> Office: 617.568.5942
>> achute@massport.com<mailto:achute@massport.com>

>>
>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>
> <SierraQuoteForMassPort.pdf>

From: Chavis, Michael J.
To: Alves, Joe
Cc: O'Leary, John F; Egnitz, Brian (POL)
Subject: FW: MassPort LPR Cameras
Date: Thursday, July 16, 2020 12:48:40 PM

Joe,

Thank you for getting back to me about the LPR work mentioned in the email thread below. I've been told that the remaining 2 locations are in areas that require Detail Support due to the length of time required to perform the work and the fact that partial lane closures are necessary.

Any information you could provide would be helpful so that we could figure out logistics (exact locations, how the detail areas will be set up and billing. As you can see, they would like to complete this work sometime in the next month.

I look forward to hearing from you.

Sgt Michael J. Chavis #0751
Paid Detail Office Supervisor
Mass. State Police – Logan International Airport
2 Service Road
East Boston, MA 02128
(617)568-7324

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Wednesday, July 15, 2020 11:28 AM
To: Chavis, Michael J.
Cc: Ryan, Deborah (POL); Alves, Joe; Gilmore, Joey; Crouse, David (POL); Doherty, Gregory (POL)
Subject: RE: MassPort LPR Cameras

Hi Sgt.,

Thanks for taking my call, as follow up:

- There are 2 sites remaining for cutover.
- I've included the MassPort IT contacts who can tell you specifically where the sites are located.
- I estimate the job to take between 2-6 hours per site.
- I'd like to do one site per day
- Afterhours would be preferred when traffic is lower and there are less eyeballs.
- Tuesday or Thursday eves are open for me now for the next 4 weeks
- A member of the Technical Services Unit will be onsite with me during the cutover in case we have a problem with one of the cameras (you do not need to include them in the detail, they will use TSU OT budget)

-Brian

From: Ryan, Deborah (POL)
Sent: Wednesday, July 15, 2020 11:01 AM
To: Egnitz, Brian (POL)

Subject: Re: MassPort LPR Cameras

Ok, you can work with Sgt. Mike Chavis directly to coordinate details. mchavis@massport.com 617-[redacted]

Best,

Major Ryan

THIS EMAIL MAY CONTAIN INFORMATION FOR OFFICIAL USE ONLY AND LAW ENFORCEMENT SENSITIVE INFORMATION. This E-mail (including attachments) is covered by the Electronic Communications Privacy Act, 18 USC 2510-2521, is confidential and may be legally privileged. If you are not the intended recipient, you are hereby notified that any retention, dissemination, distribution, or copying of this communication is strictly prohibited and may be unlawful. Please reply to the sender that you have received the message in error and then delete the message and any attachments.

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Tuesday, July 14, 2020 8:59 AM
To: Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>
Subject: Re: MassPort LPR Cameras

Yes, it hasn't been scheduled

On Jul 14, 2020, at 7:52 AM, Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us> wrote:

> Hi Brian,
>
> Where was it left off? Utilizing details for the road closure?
>
> THIS EMAIL MAY CONTAIN INFORMATION FOR OFFICIAL USE ONLY AND LAW ENFORCEMENT SENSITIVE INFORMATION. This E-mail (including attachments) is covered by the Electronic Communications Privacy Act, 18 USC 2510-2521, is confidential and may be legally privileged. If you are not the intended recipient, you are hereby notified that any retention, dissemination, distribution, or copying of this communication is strictly prohibited and may be unlawful. Please reply to the sender that you have received the message in error and then delete the message and any attachments.
>
> ---
>
> **From:** Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Sent:** Tuesday, July 14, 2020 7:29 AM
> **To:** Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>
> **Subject:** Re: MassPort LPR Cameras

Hi Maj.,

Are you aware of any movement on this? I'd like to finish the cutover of the remaining cameras.

Thanks, Brian

On May 21, 2020, at 10:57 AM, Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us> wrote:

> Hi Brian,
>
> Could you give me a call at your convenience regarding the rest of the LPR cutovers.
>
> Thank you,
>
> Major Ryan
> 781-281-5177
>
> THIS EMAIL MAY CONTAIN INFORMATION FOR OFFICIAL USE ONLY AND LAW ENFORCEMENT SENSITIVE INFORMATION. This E-mail (including attachments) is covered by the Electronic Communications Privacy Act, 18 USC 2510-2521, is confidential and may be legally privileged. If you are not the intended recipient, you are hereby notified that any retention, dissemination, distribution, or copying of this communication is strictly prohibited and may be unlawful. Please reply to the sender that you have received the message in error and then delete the message and any attachments.

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Monday, May 18, 2020 4:58 PM
To: Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>
Cc: Crouse, David (POL) <david.crouse@pol.state.ma.us>
Subject: RE: MassPort LPR Cameras

Hi Major,

I have finished cutting over the LPR cameras that were accessible off the road. [redacted] cameras ([redacted] G.L. c. 4.sec. 7.cl.26 (n)(security) and needs inspection). [redacted] G.L. c. 4.sec. 7.cl.26 (n)(security) need lane closures. [redacted] G.L. c. 4.sec. 7.cl.26 (n)(security) [redacted] and [redacted] G.L. c. 4.sec. 7.cl.26 (n)(security) I estimate needing 2-5 hours per site. Lt. Crouse has offered to assist in lane closures using unmarked vehicles, how would you like to proceeded in completing the cut over of the remaining sites.

Thanks, Brian

From: Ryan, Deborah (POL)
Sent: Wednesday, May 6, 2020 9:46 PM
To: Mason, Christopher (POL); Egnitz, Brian (POL)
Cc: Warmington, Scott (POL); Quinn, Dermot (POL); Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Warren, Rosemary (POL); Shaw, Harold; Ball, Richard (POL)
Subject: Re: MassPort LPR Cameras

Thank you Brian.

Major Deborah A. Ryan
Massachusetts State Police
Troop F Commander
485 Maple St

From: Mason, Christopher (POL) <Chris.Mason@pol.state.ma.us>
Sent: Wednesday, May 6, 2020 7:00 PM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Cc: Warmington, Scott (POL) <Scott.Warmington@pol.state.ma.us>; Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Small, Michelle (POL) <Michelle.E.Small@pol.state.ma.us>; Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>; Slater, James (CHS) <james.slater@mass.gov>; Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>; Shaw, Harold <HShaw@massport.com>; Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>; Ball, Richard (POL) <Richard.Ball@pol.state.ma.us>
Subject: Re: MassPort LPR Cameras

Thank you Brian. Great work grabbing this data.

Colonel Christopher Mason
Superintendent
Massachusetts State Police

> On May 6, 2020, at 6:57 PM, Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us> wrote:
>
> Hi Sirs,
>
> We have begun cutting over the MassPort LPR Cameras into the EOPSS BOSS LPR Server. Today, [redacted] at Airport Road arrivals were migrated and are now writing data to Chelsea. I will continue to cut the remaining cameras over in the next few days and weeks. I will advise when the project is complete.
>
> - Brian

>
> -----Original Message-----
> From: Warmington, Scott (POL)
> Sent: Tuesday, March 10, 2020 11:36 AM
> To: Quinn, Dermot (POL)
> Cc: Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Mason, Christopher (POL); Egnitz, Brian (POL); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL)
> Subject: Re: MassPort LPR Cameras
>
> What is the cost?
>
> Sent from my iPhone
>
>> On Mar 10, 2020, at 11:28 AM, Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us> wrote:
>>
>> Michelle and Kyra,
>>
>> This purchase request is for equipment to allow Mass Port Sierra Wireless modems to communicate directly with the existing ALPR Boss server in Chelsea. This is the fastest way to bring the Massport LPR cameras on line. EOTSS and EOPSS are OK with this solution as is Major Deb Ryan, the CO at Troop F.
>>
>> As you can see from the thread, this has been going on for some time. I think we can close it out with this small purchase.
>>
>> This does not resolve the replacement of the existing ALPR equipment that we discussed at Command Staff yesterday. That is a different issue.
>>
>> Thanks
>>
>>
>> Lieutenant Colonel Dermot J. Quinn #1765
>> Division Commander
>> Division of Homeland Security & Preparedness
>> Massachusetts State Police
>>
>>
>>
>>
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 10:52 AM
>> To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: FW: MassPort LPR Cameras
>>
>> Hi LTC.,
>>
>> Can we order this equipment for the MassPort project?
>>
>> Thanks, Brian
>>
>> -----Original Message-----
>> From: Slater, James (CHS)

>> Sent: Tuesday, March 10, 2020 10:26 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> This needs to go through MSP fiscal. They need to enter the purchase in OPAS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 08:06
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Subject: RE: MassPort LPR Cameras
>>
>> Is this something you can order or does it need to go through MSP?
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Monday, March 9, 2020 10:36 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks, Brian...I will check with TSS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Monday, March 9, 2020 10:29
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks Jim,
>>
>> I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need [redacted] AC adapters [redacted] I have reached out to BCM for a quote.
>>
>> I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.
>>
>> I plan to cut one sector ([redacted]) over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?
>>
>> -Brian
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Friday, March 6, 2020 1:43 PM

>> To: Egnitz, Brian (POL)
>> Cc: Quinn, Dermot (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.
>>
>> So, assuming you move forward with this, who would actually make this happen?
>>
>> Thanks.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Wednesday, March 4, 2020 17:53
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: Re: MassPort LPR Cameras
>>
>> Hi Jim,
>>
>> Regarding the Massport cameras; in the early days of AVL we installed [redacted] modem‘s in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don’t we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn’t have to do any firewall work either because they have a 166. and communicate like all of the MDT‘s . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.
>>
>> We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.
>>
>> Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.
>>
>>>> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>>>
>>> Thank you sir
>>>
>>> Major Charles W. Atchison III
>>> Troop F Commander
>>> Massachusetts State Police
>>> Director of Aviation Security
>>> 2 Service Road
>>> East Boston, Ma 02128

>>> Office: 617-568-7555
>>> Cell: 508[redacted]
>>>
>>>
>>>> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>>>
>>> All,
>>> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>>>
>>> Thanks
>>>
>>> CW
>>>
>>> From: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
>>> Sent: Monday, February 10, 2020 10:31 AM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
>>> Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
>>> Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
>>> Warmington, Scott (POL)
>>>
<Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
>>> .us>>; Peek, Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
>>> Michalski, Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>;
Mason,
>>> Christopher (POL)
>>> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
>>> Hughes, Sean M. (EOTSS)
>>> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis
(EOTSS)
>>> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
>>> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard
(POL)
>>> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
>>> Atchison, Charles (POL)
>>> <catchison@massport.com<mailto:catchison@massport.com>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Good Morning,
>>>
>>> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been

on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>>>
>>> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>>>
>>> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>>>
>>> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>>>
>>> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>>>
>>> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>>>
>>> I can’t overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security’s technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>>>
>>> Respectfully,
>>>
>>>
>>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
>>> of Homeland Security & Preparedness Massachusetts State Police
>>> <image006.png>
>>>
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL)

>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
>>> Sent: Friday, January 17, 2020 1:10 PM
>>> To: Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
>>> Cc: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
>>> Guerriero, Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
Peek,
>>> Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
Peter
>>> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
>>> Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>
>>> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>>>
>>> -Brian
>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> Sent: Monday, January 6, 2020 1:33 PM
>>> To: Slater, James (CHS)
>>> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
>>> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
>>> Crary
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>
>>> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>>>
>>> Thanks Brian
>>>
>>>
>>> From: John Tedona [mailto:jtedona@neology.net]
>>> Sent: Monday, December 9, 2019 4:55 PM
>>> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Slater, James (CHS)
>>> Subject: RE: MassPort LPR Cameras

>>>
>>> Alex,
>>>
>>> I can be available most anytime tomorrow for a call.
>>>
>>>
>>> Regards,
>>>
>>> John Tedona
>>> PIPS TECHNOLOGY - A Neology Business
>>> Sales Manager
>>> 12760 Danielson Ct. Suite A
>>> Poway, CA 92064
>>> Phone: 201-841-6237
>>> Email: jtedona@neology.net<mailto:jtedona@neology.net>
>>> PIPS Support:
support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-
7577, Option 1 for sales, Option 2 for Support
>>> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
>>>
-3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
>>>
EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
>>>
baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-
lyPhyJ
>>> U2sB_fmM6g&e=>
>>>
>>>
>>> From: Chute, Alexander
>>> <AChute@massport.com<mailto:AChute@massport.com>>
>>> Sent: Monday, December 9, 2019 4:38 PM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>
>>> Cc: Guerriero, Robert (MASSIT)
>>> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
>>> Peek, Brian T. (EOTSS)
>>> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
>>> Slater III, James F (CHS)
>>> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> CAUTION: This email originated from outside of the organization. Do not
click links or open attachments unless you recognize the sender and know the
content is safe.
>>>
>>> Hello All,
>>>
>>> I just wanted to follow up with this request to see what the next steps for
this project are. I believe that we can make the connections to the EOPSS
network, but will want to work within your desired IP scheme and ensure that
there aren't any concerns around the network routing, security, etc. Let me
know if we can have a quick call to discuss the details.

>>>
>>> Respectfully,
>>>
>>> ~Alex
>>>
>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Monday, November 18, 2019 3:26 PM
>>> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
>>> pcrary@neology.net<mailto:pcrary@neology.net>
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi John, Peter
>>>
>>> Any issues with moving Massports cameras to the Chelsea DB?
>>>
>>> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>>>
>>> The current app server
>>> <image008.png>
>>>
>>> Current DB server
>>>
>>> <image009.png>
>>> <image010.png>
>>>
>>> Our current reads by month for about [redacted]
>>>
>>> Year
>>>
>>> Month
>>>
>>> Day
>>>
>>> Month Name

>>>
>>> Reads Count
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 1
>>>
>>> November
>>>
>>> 495,113
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 2
>>>
>>> November
>>>
>>> 472,907
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 3
>>>
>>> November
>>>
>>> 384,409
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 4
>>>
>>> November
>>>
>>> 411,440
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 5
>>>
>>> November
>>>
>>> 434,085
>>>
>>> 2019
>>>
>>> 11
>>>

>>> 6
>>>
>>> November
>>>
>>> 495,537
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 7
>>>
>>> November
>>>
>>> 444,123
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 8
>>>
>>> November
>>>
>>> 542,492
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 9
>>>
>>> November
>>>
>>> 443,463
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 10
>>>
>>> November
>>>
>>> 389,514
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 11
>>>
>>> November
>>>
>>> 362,548
>>>
>>> 2019

>>>
>>> 11
>>>
>>> 12
>>>
>>> November
>>>
>>> 236,539
>>>
>>>
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Wednesday, November 13, 2019 2:49 PM
>>> To: Egnitz, Brian (POL)
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> These stats are from the [redacted] we have in the system for this month:
>>>
>>> <image011.png>
>>>
>>> ~Alex
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Tuesday, November 12, 2019 5:28 PM
>>> To: Chute, Alexander
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Alex,
>>>
>>> Can you please provide the updated reads per day? Previously you were interested in sharing [redacted] at approximately 75,000 reads per day.
>>>
>>> Here is the [redacted] confi I mentioned.
>>>
>>> Set host to bo [redacted]
>>> Set image [redacted]
>>> Set number o [redacted]
>>> Set Ping [redacted]
>>> Set udp ping [redacted]
>>> Set ping [redacted]
>>> Set security [redacted]
>>>
>>> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
>>> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>>>
>>> -Brian
>>>

>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Tuesday, November 12, 2019 2:08 PM
>>> To: Egnitz, Brian (POL)
>>> Subject: MassPort LPR Cameras
>>>
>>> Brian,
>>>
>>> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to approximately [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.
>>>
>>> Respectfully,
>>>
>>> ~Alex
>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>> <SierraQuoteForMassPort.pdf>

From: Egnitz, Brian (POL)
To: Crouse, David (POL)
Subject: FW: MSP LPR
Date: Thursday, May 21, 2020 2:34:00 PM

FYI

-----Original Message-----
From: Egnitz, Brian (POL)
Sent: Thursday, May 21, 2020 2:34 PM
To: 'Alves, Joe'
Subject: RE: MSP LPR

Can we schedule last two cut overs for 5/28 & 5/29. In speaking with Maj. Ryan, a coordinated road closure via the detail office is warranted.

Thanks, Brian

-----Original Message-----
From: Alves, Joe [mailto:JAlves@massport.com]
Sent: Wednesday, May 13, 2020 6:44 AM
To: Egnitz, Brian (POL)
Subject: Re: MSP LPR

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Ok.

Sent from my iPhone

> On May 13, 2020, at 6:22 AM, Egnitz, Brian (POL) <brian.egnitz@state.ma.us> wrote:
>
> I have a meeting today at 12:00 that I need to go to, but will try and come in after. -Brian
>
>> On May 8, 2020, at 8:26 AM, Alves, Joe <JAlves@massport.com> wrote:
>>
>>
>> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>>
>>
>> Ok.
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
>> Sent: Friday, May 08, 2020 8:26 AM
>> To: Alves, Joe <JAlves@massport.com>
>> Subject: RE: MSP LPR
>>
>> Thanks should be in for 10 ish. I'll give you a call when I'm a few out.
>>
>> Tks, Brian
>>
>> -----Original Message-----
>> From: Alves, Joe [mailto:JAlves@massport.com]
>> Sent: Thursday, May 7, 2020 9:01 PM
>> To: Egnitz, Brian (POL)
>> Subject: Re: MSP LPR
>>
>>
>> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>>
>>
>> Yes. I'll be around. I can get you in just let me know the time.
>>
>>
>>
>> Sent from my iPhone
>>
>>
>>
>> On May 7, 2020, at 7:49 PM, Egnitz, Brian (POL) <brian.egnitz@state.ma.us> wrote:
>>
>>
>>
>>
>>
>> Are you available tomorrow?
>>
>>
>>
>> On May 4, 2020, at 9:41 AM, Gilmore, Joey <JGilmore@massport.com> wrote:
>>
>>
>>
>>
>>
>> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>>
>>
>>
>>
>>
>> Joe,
>>
>> Later today Brian will send over the actual IMEI numbers that they are using for this project. Once received, can you please confirm if they are unlimited data plans?
>>
>>
>>
>> Brian,
>>
>> Joe Alves is in onsite Wednesday and Friday. He said the[redacted] is accessible without road closure and would make a good first install. Can you please reach out to him to arrange a time for Wednesday? Joe's cell number is [redacted]
>>
>>
>>
>>
>>
>> Thank you,
>>
>> Joey Gilmore
>>
>> Manager - IT Security Systems
>>

>> Information Technology
>>
>> Massachusetts Port Authority
>>
>> One Harborside Drive, Suite 200S
>>
>> East Boston, MA 02128-2909
>>
>> Tel: 617-568-5915
>>
>> Cell: 617[redacted]
>>
>>
>>
>>
>>
>>
>>
>>
>>
>> From: Egnitz, Brian (POL) <brian.egnitz@state ma.us>
>>
>> Sent: Thursday, April 23, 2020 10:30 AM
>>
>> To: Gilmore, Joey <JGilmore@massport.com>; Alves, Joe <JAlves@massport.com>; Sillsby, Blane <BSillsby@massport.com>; Quinn, Michael <MQuinn@massport.com>
>>
>> Cc: Haverty, Robert <RHaverty@massport.com>; Harney, Michael <MHarney@massport.com>
>>
>> Subject: RE: MSP LPR
>>
>>
>>
>>
>>
>> -----Original Appointment-----
>>
>> From: Gilmore, Joey [mailto:JGilmore@massport.com]
>>
>> Sent: Wednesday, April 22, 2020 11:35 AM
>>
>> To: Gilmore, Joey; Alves, Joe; Sillsby, Blane; Quinn, Michael; Egnitz, Brian (POL)
>>
>> Cc: Haverty, Robert; Harney, Michael
>>
>> Subject: MSP LPR
>>
>> When: Thursday, April 23, 2020 10:00 AM-11:00 AM (UTC-05:00) Eastern Time (US & Canada).
>>
>> Where: https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_join_500426357&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=3ivMD3mXVSpxMv-g-ajiMkf38VVpxAIvxzFU7zoD-C0&s=ZHyfYIPsksOBeyci6ra3KwL4O4SCPoA_7WEhraXS96Y&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_join_500426357&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FNEWIHnzbfZimE&r=v1eRT_PuOlmt3sh7Lyk24rX9MBSQCKldPuclQWjOSPk&m=PXOFyIolm_rZpuk6yADM63jFy9ok8VUjYC-nn_w6rMY&s=1D-DGoR18hVhptpvf47Fn_SFGKSpwE2u7SIK57_YdrA&e=>
>>
>>
>>
>>
>>
>> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>>
>>
>>
>>
>>
>>
>>
>>
>> Hi Guys,
>>
>>
>>
>>
>>
>>
>>
>>
>> This meeting is to discuss the method of bringing Logan LPR cameras to the EOPSS network.
>>
>>
>>
>>
>>
>>
>>
>>
>> This is the last status update from Chute before he left:
>>
>>
>>
>> "Currently MassPort has[redacted] After several iterations of the system architecture, it has been decided that the path of least resistance is to employ commercial carrier service on the MSP MPLS to the CJIS Datacenter in Chelsea. MSP is working to procure the necessary power adapter and antenna equipment while also identifying accounts and equipment that can be re-purposed for this project. If/when it is feasible for this system to be networked through terrestrial means, MassPort has the switch infrastructure in place to make a direct connection to the EOPSS network at[redacted] I hope this gives a brief overview of where we are at, and please do not hesitate to reach out to me via my personal contact information if any questions come up."
>>
>>
>>
>>
>>
>>
>>
>>
>> MPA - MSP
>>
>> Thu, Apr 23, 2020 10:00 AM - 11:30 AM (EDT)
>>
>>
>>
>> Please join my meeting from your computer, tablet or smartphone.
>>
>> https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_join_500426357&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=3ivMD3mXVSpxMv-g-ajiMkf38VVpxAIvxzFU7zoD-C0&s=ZHyfYIPsksOBeyci6ra3KwL4O4SCPoA_7WEhraXS96Y&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_join_500426357&d=DwMF-g&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=YrOyBDqzLm4zddutRwcvrC8An9e-bx9zIO8EMq0-X7Q&s=bt8qRm7QQabR-s9uIfBIIjV-_W5RvGI9slrF4D65fw4&e=>
>>
>>
>>
>> This meeting is locked with a password.[redacted]
>>
>>
>>

>> You can also dial in using your phone.
>>
>> United States: +1 (571) 317-3122<tel:+15713173122,,500426357>
>>
>>
>>
>> Access Code: 500-426-357
>>
>>
>>
>> New to GoToMeeting? Get the app now and be ready when your first meeting starts:
>>
>> https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_install_500426357&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=3ivMD3mXVSpxMv-g-ajiMkf38VVpxAIvxzFU7zoD-C0&s=sPSeiG_aGKwV8Di-BEroqcIxtAzk0va1AAxVy6gZ3Tg&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_install_500426357&d=DwMF-g&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=YrOyBDqzLm4zddutRwcvrC8An9e-bx9zIO8EMq0-X7Q&s=73yCNI9YJUXzkHRvG6ehrB7JBvLK4l12EYJ4ThBmY-M&e=>
>>
>>
>>
>>
>>
>>
>>
>> Thank you,
>>
>>
>>
>> Joey Gilmore
>>
>>
>>
>> Manager - IT Security Systems
>>
>> Information Technology
>>
>> Massachusetts Port Authority
>>
>> One Harborside Drive, Suite 200S
>>
>> East Boston, MA 02128-2909
>>
>> Tel: 617-568-5915
>>
>> Cell: 617[redacted]
>>
>>
>>
>>
>>
>>
>>
>>
>>
>>
>>
>>
>>
>>

From: Bryant, Michael
To: Griffin, Daniel (POL)
Cc: Griffin, Daniel (POL)
Subject: FW: RE: ALPR Login
Date: Wednesday, February 12, 2020 4:03:57 PM

Lt I am just following up on my e-mail (see below) to see if you have had any time to look at my account.

Thank you,

Mike

From: Bryant, Michael
Sent: Wednesday, January 29, 2020 2:17 PM
To: 'daniel.griffin2@state.ma.us' <daniel.griffin2@state.ma.us>
Subject: RE: ALPR Login

Daniel, Det. Lundegren gave me the info to setup my account, I got as far as the Login screen but the password was rejected 3 times and it looks like it kicked me out?
I used 3282$Ypd & $Ypd3282 but neither worked.

Any help would be great.

Thank you

Mike

Lieutenant Michael A. Bryant
Yarmouth Police Department
One Brad Erickson Way
West Yarmouth Ma 02673
508-775-0445 Ext. 2122
Fax 508-775-0409

LAW ENFORCEMENT USE ONLY The document accompanying this email contains information from the Yarmouth Police Department that maybe CONFIDENTIAL and / or PRIVILEGED. The information is intended to be for the use of the individual or entity named on the email. If you are not the intended recipient, be aware that any misuse of this information is strictly PROHIBITED.

From: MACrimeNet (POL)
To: nevjc@aol.com
Subject: FW: Workflow
Date: Thursday, October 1, 2020 8:15:00 AM

From: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Sent: Thursday, September 24, 2020 1:58 PM
To: MACrimeNet (POL) <MACrimeNet@pol.state.ma.us>
Subject: RE: Workflow

I think if you could take some of your work for that day from start to finish and walk us through it, that would be very helpful. I also have a list of things you do when we had to write it for the 960's. They want to know about all processes and duties so if there is something you don't do on a regular basis that's important, you may want to note it so that we cover it.

This is what I have below. I think its more the processes vs the what.

Chris Neville

- Intake, review, editing and redistribution of incoming email and outgoing intelligence to aid local investigators in identifying suspects and patterns of criminal activity to upwards of 2,000 individual recipients 365 days a year.
- Annual selective distribution by county, of approximately 4,000 emails to the email network which includes representatives of almost every State, Local and Federal Agency in Eastern and Central MA, neighboring states, Bank Industry Security Professionals and Retail Asset Protection Professionals.
- Participation in area detective's meetings to share intelligence regarding crimes and arrests of regional significance.
- Comprehensive review and re-distribution in excel spreadsheet format of Pawnshop Information provided by more than a dozen local agencies including highlighting of persons of interest.
- Statewide liaison to NABI (National Association of Bunco Investigators).
- Review and redistribution of Intelligence published by NESPIN and NEORCA.
- Complete responsibility for the addition, subtraction and update of email addresses stored in the 'listserv manager".
- Maintenance, upkeep and distribution of a home-grown Area Wide Detectives Contact List with email and telephone contact information from 1,800 sources.
- Routine access to CJIS systems to perform RMV, CJIS and NCIC related inquiries from law enforcement.

- Routine access to Coplink and other data sources (TLO) to assist local detectives in providing photographs, known associates, associated vehicles and prior incidents while assisting in investigations pertaining to email traffic.

- Routine access and review of ALPR's to provide investigative assistance and documentation to local Law Enforcement, specifically in connection with Organized Crime organizations based out of State but operating in MA and the surrounding New England States.

- Daily review of Area Crime Bulletins from municipal agencies including the BRIC, Cambridge, Everett, Lynn, and others as they are distributed. (Many of whom re-post information previously distributed on Macrimenet).

- Guest presenter to new area detectives providing an overview of what services the CFC provides for local law enforcement.

- Participation in area intelligence sharing meetings specifically directed to targeted crimes such as ATM B&E's, Robberies, Regional Check Frauds or outbreaks of commercial or residential B&Es.

- Daily review of national Crimedex Alerts to ascertain links to other incidents occurring across the country. (ie: Panera Bread Thefts, Felony Lane Gang, and Transient Scams).

From: MACrimeNet (POL)
Sent: Thursday, September 24, 2020 1:54 PM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Subject: RE: Workflow

Thank you.

Do you want me to prepare something in advance of the things that most people might not know that I do, or we just want to pick at it as we go?

Chris

-----Original Appointment-----
From: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Sent: Thursday, September 24, 2020 1:24 PM
To: Smith, Eleanor (POL); MACrimeNet (POL)
Subject: Workflow
When: Thursday, October 1, 2020 10:00 AM-12:00 PM (UTC-05:00) Eastern Time (US & Canada).
Where: gotomeeting

MA Crimenet

Thu, Oct 1, 2020 10:00 AM - 12:30 PM (EDT)

Please join my meeting from your computer, tablet or smartphone.
https://global.gotomeeting.com/join/756196341

You can also dial in using your phone.
United States: +1 (408) 650-3123

Access Code: 756-196-341

New to GoToMeeting? Get the app now and be ready when your first meeting starts:
https://global.gotomeeting.com/install/756196341

From: michael.guerriero@sjc.state.ma.us
To: Keith Halliday; Tully
Subject: Comm v. McCarthy - re:d rig D v PR with ALPRs on Bourne/Sagamore Bridges not a search
Date: Friday, April 17, 2020 3:43:00 PM

Sent from my iPhone

Begin forwarded message

From: "Grant, Marguerite (NFK)" <Marguerite.Grant@MassMail.State.MA.US>
Date: April 17, 2020 at 5 53 47 PM EDT
To: "jbakan@avon-ma.gov" <jbakan@avon-ma.gov>, "mbabois@braintreema.gov" <mbabois@braintreema.gov>, "mmorgan@brookline.gov" <mmorgan@brookline.gov>, "Berkowitz, Kenneth" <kberkowitz@town.canton.ma.us>, "mdeluca@cohassetpolice.com" <mdeluca@cohassetpolice.com>, "Lennon, Gregory" <glennon@cohassetpolice.com>, "Quigley, William" <wquigley@cohassetpolice.com>, "d'Entremont, Michael" <mdentremont@police.dedham-ma.gov>, "McGowan, Peter" <pmcgowan@dovermapl.com>, "Graci, Michael" <mgraci@foxboroughpolice.com>, "Thomas J. Lynch (tlynch@franklinpolice.com)" <tlynch@franklinpolice.com>, "jmelli@frankinpolice.com" <jmelli@frankinpolice.com>, "wsmith@hellbrookpolice.com" <wsmith@hellbrookpolice.com>, "bguerette@medfield.net" <bguerette@medfield.net>, "amingley@medwaypolice.com" <amingley@medwaypolice.com>, "asoffryer@millis.net" <asoffryer@millis.net>, "asoffryer@millis.net" <asoffryer@millis.net>, "jking@mpdmilton.org" <jking@mpdmilton.org>, "jschlittler@needhamma.gov" <jschlittler@needhamma.gov>, "cstone@norfolk.ma.us" <cstone@norfolk.ma.us>, "Brooks, William G. III" <wbrooks@norwoodma.gov>, "pkelly@norwoodma.gov" <pkelly@norwoodma.gov>, "James Alfred (jalfred@police.plainville.ma.us)" <jalfred@police.plainville.ma.us>, "Keenan, Paul" <pkeenan@quincyma.gov>, "williampace@randolphmapolice.com" <williampace@randolphmapolice.com>, "jfenli@townofsharon.org" <jfenli@townofsharon.org>, "dmcnamara@stoughton-ma.gov" <dmcnamara@stoughton-ma.gov>, "jcarmichael@walpolepd.com" <jcarmichael@walpolepd.com>, jpilecki <jpilecki@wellesleyma.gov>, "jultza@westwoodpd.org" <jultza@westwoodpd.org>, "Grimes, Richard C." <rgrimes@weymouth.ma.us>, "cherli@police.wrentham.ma.us" <cherli@police.wrentham.ma.us>, "Baker, Chris (EEAT)" <chris.baker@mass.gov>, "pewoven2@wtd.edu" <pewoven2@wtd.edu>, "jconnolly2@suffolk.edu" <jconnolly2@suffolk.edu>, "zrMullaney, Stephen (POL)" <zrStephen.zrMullaney@pol.state.ma.us>, "Matthew Reardon (mreardon@medwaypolice.com)" <mreardon@medwaypolice.com>, "wkingsbury@medwaypolice.com" <wkingsbury@medwaypolice.com>, "Hanson, John" <jhanson@foxboroughpolice.com>, "Brewer, Dan" <dbrewer@townofsharon.org>, "Guerriero, Michael (POL)" <michael.guerriero@pol.state.ma.us>, "Adams, Jerry (pd334) (jadams@police.nantucket-ma.gov)" <jadams@police.nantucket-ma.gov>, "Donoghue, William (NORF)" <William.J.Donoghue@MassMail.State.MA.US>, "Hunte, Alan (MED)" <Alan.Hunte@MassMail.State.MA.US>, "Fenton, Stewart M. (MCC)" <stewart.m.fenton@MassMail.State.MA.US>, "Robert Connor (connor@bc.edu)" <connor@bc.edu>, "Sherrywah, Christopher" <cmurywah@gmber-ma.gov>, "Solimini, Ronald (POL)" <ronald.solimini@pol.state.ma.us>, "wwest@mpdmilton.org" <wwest@mpdmilton.org>, "dyken@braintreema.gov" <dyken@braintreema.gov>, "Goulding, Michael J." <Goulding.Mj@woostonmass.org>, "Kennedy, Kevin" <kkennedy@lincolntown.org>, "orOtte, David (POL)" <orDavid.orOtte@pol.state.ma.us>, "David Flaherty (flaherdb@bc.edu)" <flaherdb@bc.edu>, "Moriarty, Dan" <daniel.moriarty.2@bc.edu>, "LSullBar@gmail.com" <LSullBar@gmail.com>, "Antoine, Romere (POL)" <romere.antoine@pol.state.ma.us>, "Rudolph, James (POL)" <James.Rudolph@pol.state.ma.us>, "mcollins@mpdmilton.org" <mcollins@mpdmilton.org>, "Bulman, Paul (NORF)" <Paul.Bulman@MassMail.State.MA.US>, "Pannuzlos, Keith (NPL)" <keith.pannuzlos@MassMail.State.MA.US>, "Farioli, Mark (NPL)" <Mark.R.Farioli@MassMail.State.MA.US>, "Sullivan, Brian (POL)" <Brian.Sullivan@pol.state.ma.us>, "Lynch, Dennis (NFK)" <Dennis.M.Lynch@MassMail.State.MA.US>, "Powers, Meaghan (NFK)" <meagan.powers@MassMail.State.MA.US>, "Dicicco, David M (POL)" <David.M.Dicicco@pol.state.ma.us>, "Budzenki, Yuriy (POL)" <yuriy.budzenki@pol.state.ma.us>, "Danse, Matthew (POL)" <Matthew.Danse@pol.state.ma.us>, "Nichol, Kevin (POL)" <kevin.nichol@pol.state.ma.us>, "Matthew Murphy (mmurphy@brocktonpolice.com)" <mmurphy@brocktonpolice.com>, "cbell@brocktonpolice.com" <cbell@brocktonpolice.com>, "cbell@brocktonpolice.com", "arailly@bellpolice.org" <arailly@bellpolice.org>, "Sean Walsh (swalsh@pol.state.ma.us)" <swalsh@pol.state.ma.us>, "Sean Walsh (swalsh@pol.state.ma.us)" <swalsh@pol.state.ma.us>, "O'Brien, Sean (NORF)" <Sean.P.O'Brien@MassMail.State.MA.US>, "Delaney, Mark (NORF)" <mark.delaney1@MassMail.State.MA.US>, John Purchard <jpurchard@weymouth.ma.us>, "O'Neill, Russ" <oneill@brooklinema.gov>, Shannon Ducharme <sducharme@chelseapolice.com>, "Det. Lt. Melissa Greene" <mellaspgreene@randolphmapolice.com>, "Bishop, Kevin" <kbishop@townofsharon.org>, "gmarkos@townofsharon.org" <gmarkos@townofsharon.org>
Cc: "Morrissey, Michael (NFK)" <Michael.W.Morrissey@MassMail.State.MA.US>, "Doherty, Denise (NFK)" <Denise.M.Doherty@MassMail.State.MA.US>, "Fanning, John (NFK)" <john.m.fanning@MassMail.State.MA.US>, "Keefe, Edward (NFK)" <Edward.T.Keefe@MassMail.State.MA.US>, "Mattaliano, Gerard (NFK)" <Gerard.Mattaliano@MassMail.State.MA.US>, "Justin Fitzsimmons (justin@search.org)" <justin@search.org>, "Quirk, Sean (POL)" <sean.quirk@pol.state.ma.us>, "Tully, Brian (NFK)" <Brian.P.Tully@MassMail.State.MA.US>, NFK-DL-ADA-Superior-ci <NFK-DL-ADA-Superior-ci@MassMail.State.MA.US>, NFK-DL-ADA-District-ct <NFK-DL-ADA-District-ct@MassMail.State.MA.US>, NFK-DL-ADA--Appeals <NFK-DL-ADA-Appeals2@MassMail.State.MA.US>, "Kelly, Christopher (AGO)" <christopher.kelly@mass.gov>
Subject: Comm v. McCarthy - locating D's MV with ALPRs on Bourne/Sagamore Bridges not a search



Chiefs:
Commonwealth v. McCarthy (SJC-12750)← click on that link to see the case
In this case the SJC ruled that police tracking D's car using 4 automatic license plate readers (ALPRs) at both ends of the Bourne and Sagamore Bridges was too limited to amount to a constitutional "search." The SJC declined to say exactly how detailed digital surveillance would have to be to constitute a search leaving that issue for future cases.

State Police maintain ALPRs including ones at both ends of the Bourne and Sagamore Bridges. (p.3) The ALPRs photograph vehicles' license plates; that data along with the date and time of the sighting is retained by EOPS for a year. (p.3-4) Authorized users including police may put a license plate number on a "hot list " and receive an alert if that plate is sighted; reasons to put someone on the "hot list" include not only criminal investigations but also Amber alerts missing persons and BOLO alerts. (p. 3 25 n.13)

Through surveillance controlled buys and information from 4 Cis Barnstable police suspected that the co-D was se ling heroin out of his house in Barnstable. (p.4) Police saw a black Hyundai driven by D visit there briefly so they suspected that D was the co-D's supplier. Police put the Hyundai's license plate number on the State Police ALPR "hot list " so that they'd be notified whenever the Hyundai crossed one of the bridges. (p.5) After getting an alert that the Hyundai had crossed onto the Cape police followed both the Hyundai and the co-D to the buy location on a quiet residential street where D and co-D met for about 30 seconds but police could not see a physical exchange. (p.5) From the ALPR data police generated a spreadsheet showing that in mid-winter the Hyundai had crossed the bridges dozens of times sometimes more than once a day adding to police suspicion that D was the heroin supplier. (p.5-6) When police got a second alert that the Hyundai had crossed onto the Cape they again followed D and co-D to the buy location and saw a 60-second meeting but could not see any exchange. This time police stopped both cars handcuffed both co-D and D and read them Miranda. On co-D police found heroin; on D police found 2 cell phones and cash. (p.6-7) At the station police repeatedly told D he was "not under arrest " and D made statements.

D moved to suppress the ALPR data his statements and evidence obtained from the stop. A Superior Court judge found that the moment of arrest was when D and co-D were handcuffed at the scene of the traffic stop but denied the motion to suppress. (p.33) The SJC upheld the denial.

ALPRs and expectation of privacy in digital surveillance At some length the SJC discussed the constitutional issues raised by digital surveillance. (p.7-29) Police conduct amounts to a search if: (1) it intrudes on a D's expectation of privacy and (2) society is willing to recognize the expectation of privacy as reasonable. Here the SJC ruled D did have an expectation of privacy because D and co-D chose a buy location in a quiet residential area. (p.8 n.5) As to what expectation of privacy society recognizes as reasonable with regard to digital surveillance the SJC was guided by historical understandings of what was an unreasonable search and seizure when the U.S. and Mass. Constitutions were adopted in the late 1700s in reaction to redcoats' rummaging without restraint through colonists' homes. (p.8-10) New technologies like ALPRs raise difficult legal issues because they are easier and less expensive for police than traditional surveillance can be done secretly and permit police to search back in time for a vehicle's movements even before po ice suspicion arose. (p.11-14) Society does not recognize as reasonable an expectation of privacy in what someone knowingly exposes" to public view like a license plate – which by statute must be "displayed conspicuously." (p.15-16 & n.8) In older cases involving less advanced technology courts have held that a D did not have an expectation of privacy in contents of a phone conversation in a phone booth or a radio beeper" tracking a single journey. (p.14-17) But technology like ALPRs GPS and CSLI are different because they may give police a **mosaic** of information where each piece may be public but when viewed together they create a picture that implicates someone's privacy interests like their political re gious or sexual associations. (p.17-21) The SJC was concerned that with enough ALPRs police could track someone's location everywhere which would be "creepy." (p.25) Exigent circumstances would likely justify using an ALPR in a situation involving an Amber alert or missing person. (p.25 n.13) The D urged the SJC to consider not just these four ALPRs on the Bourne and Sagamore Bridges but the hundreds of ALPRs across Massachusetts; the SJC declined to do so because that evidence is not in the record of this case. (p.26) The **limited number of cameras** here and their placements on the bridges was not enough to give D an expectation of privacy that society would recognize as reasonable. (p.26) The SJC declined to say how much digital surveillance would give such an expectation and admitted that its unwillingness to do so "**may bring some interim confusion**" until further cases develop the law on this issue. (p.28 n.15) Chief Justice Gants wrote a separate concurrence suggesting that one thing the SJC could do is to require police who want to search a vast amount of digital data to apply for a court order supported by an affidavit showing reasonable suspicion to do so. (concurrence p.3) This would be like a SW but with a lower standard than PC.

Written policy The SJC rejected D's argument that Barnstable PD should have had a written policy about ALPRs and the MSP policy on which Barnstable relied was not specific enough. (p.30) Written policies are required to justify certain exceptions to the SW requirement (like inventory searches and sobriety checkpoints) – they do not apply to the threshold question whether a search occurred in the first place. (p.31)

Miranda issues At the station police repeatedly told D that D was "not under arrest." But the motion judge found that the moment of arrest was when police handcuffed D at the traffic stop. (p.33) D argued that his statements should be suppressed because police tel ing him he was not under arrest amounted to "deceit or trickery" to get D to confess. The motion judge and the SJC rejected that argument saying that even if telling D he was not under arrest amounted to deceit or trickery it was just one factor to be used in determining voluntariness.

Bottom line: Police use of ALPRs at limited locations is not a constitutional search – but we don't know how many locations it'd have to be to amount to one. Using an ALPR in **exigent circumstances** like an Amber Alert is likely OK. Local police don't need a written policy to use ALPRs maintained by MSP. After a D has been handcuffed police should not tell D that D is "not under arrest" – po ice will likely be accused later of deceit and trickery.

A thought: There are news stories online that cell phones may be used to do contact tracing for people exposed to COVID-19. If lots of people willingly agree to let their cell phone data be used to track their whereabouts would that ever change courts' view of what society recognizes as a reasonable expectation of privacy? At some point if members of the public come to expect that they're being tracked should police be allowed to use that evidence too? Or at the very least should there be a jury instruction explaining that police have less access to the data than other entities (like software companies or public health agencies)?

As always email me with any questions. Wash your hands!

Marguerite

Marguerite T. Grant
General Counsel – Director of Training
Office of Norfolk District Attorney Michael W. Morrissey
45 Shawmut Road
Canton, MA 02021
781-830-4829

From: [C-mccarthy, Michael \(DAO\)](mailto:Michael.C-mccarthy@MassMail.State.MA.US)
To: [Nesbitt, Mary \(DA\)](mailto:Mary.Nesbitt@MassMail.State.MA.US)
Subject: Fwd: Comm v. McCarthy - seal ing D v PR with ALPRs on Bourne/Sagamore Bridges not a search
Date: Friday, April 17, 2020 3:43:00 PM

Sent from my iPhone

Begin forwarded message

From: "Grant, Marguerite (NFK)" <Marguerite.Grant@MassMail.State.MA.US>
Date: April 17, 2020 at 5 53 47 PM EDT
To: "jbakant@avon-ma.gov" <jbakant@avon-ma.gov>, "mbabois@braintreema.gov" <mbabois@braintreema.gov>, "mmorgan@brookline.gov" <mmorgan@brookline.gov>, "Berkowitz, Kenneth" <kberkowitz@town.canton.ma.us>, "mdeluca@cohassetpolice.com" <mdeluca@cohassetpolice.com>, "Lennon, Gregory" <glennon@cohassetpolice.com>, "Quigley, William" <wquigley@cohassetpolice.com>, "d'Entremont, Michael" <mdentremont@police.dedham-ma.gov>, "McGowan, Peter" <pmcgowan@dovermapl.com>, "Graci, Michael" <mgraci@foxboroughpolice.com>, "Thomas J. Lynch (tlynch@franklinpolice.com)" <tlynch@franklinpolice.com>, "jmelli@franklinpolice.com" <jmelli@franklinpolice.com>, "wsmith@hellbrookpolice.com" <wsmith@hellbrookpolice.com>, "bguerette@medfield.net" <bguerette@medfield.net>, "amingley@medwaypolice.com" <amingley@medwaypolice.com>, "amingley@medwaypolice.com" <amingley@medwaypolice.com>, "cseffryer@millis.net" <cseffryer@millis.net>, "cseffryer@millis.net" <cseffryer@millis.net>, "jking@mpdmilton.org" <jking@mpdmilton.org>, "jschlittler@needhamma.gov" <jschlittler@needhamma.gov>, "cstone@norfolk.ma.us" <cstone@norfolk.ma.us>, "Brooks, William G. III" <wbrooks@northreadingma.gov>, "pkelly@northreadingma.gov" <pkelly@northreadingma.gov>, "James Alfred (jalfred@police.plainville.ma.us)" <jalfred@police.plainville.ma.us>, "Keenan, Paul" <pkeenan@quincyma.gov>, "williampace@randolphmapolice.com" <williampace@randolphmapolice.com>, "jlimb@townofsharon.org" <jlimb@townofsharon.org>, "dmcnamara@stoughton-ma.gov" <dmcnamara@stoughton-ma.gov>, "jcarmichael@walpolepd.com" <jcarmichael@walpolepd.com>, jplucks <jplucks@wellesleyma.gov>, "julia@westwoodpd.org" <julia@westwoodpd.org>, "Grimes, Richard C." <rgrimes@weymouth.ma.us>, "cherf@police.wrentham.ma.us" <cherf@police.wrentham.ma.us>, "Baker, Chris (EEAT)" <chris.baker@mass.gov>, "pewoven2@wtd.edu" <pewoven2@wtd.edu>, "jconnolly2@suffolk.edu" <jconnolly2@suffolk.edu>, "zzMullaney, Stephen (POL)" <zzStephen.zzMullaney@pol.state.ma.us>, "Matthew Reardon (mreardon@medwaypolice.com)" <mreardon@medwaypolice.com>, "wkingsbury@medwaypolice.com" <wkingsbury@medwaypolice.com>, "Hanson, John" <jhanson@foxboroughpolice.com>, "Brewer, Dan" <dbrewer@townofduxbury.org>, "Guerriero, Michael (POL)" <michael.guerriero@pol.state.ma.us>, "Adams, Jerry (pd334) (jadams@police.nantucket-ma.gov)" <jadams@police.nantucket-ma.gov>, "Donoghue, William (NORF)" <William.J.Donoghue@MassMail.State.MA.US>, "Hunte, Alan (MED)" <Alan.Hunte@MassMail.State.MA.US>, "Fenton, Stewart M. (MCC)" <stewart.m.fenton@MassMail.State.MA.US>, "Robert Connor (connor@bc.edu)" <connor@bc.edu>, "Sherrywah, Christopher" <connorpaul@gunther-ma.gov>, "Solimini, Ronald (POL)" <ronald.solimini@pol.state.ma.us>, "wwest@mpdmilton.org" <wwest@mpdmilton.org>, "sbyden@braintreema.gov" <sbyden@braintreema.gov>, "Goulding, Michael J." <Goulding.M@swansonmass.org>, "Kennedy, Kevin" <kkennedy@lincolntown.org>, "orOtte, David (POL)" <orDavid.orOtte@pol.state.ma.us>, "David Flaherty (flaherdb@bc.edu)" <flaherdb@bc.edu>, "Moriarty, Dan" <daniel.moriarty.2@bc.edu>, "LSullBar@gmail.com" <LSullBar@gmail.com>, "Antoine, Romeo (POL)" <romeo.antoine@pol.state.ma.us>, "Rudolph, James (POL)" <James.Rudolph@pol.state.ma.us>, "mcollins@mpdmilton.org" <mcollins@mpdmilton.org>, "Bulman, Paul (NORF)" <Paul.Bulman@MassMail.State.MA.US>, "Pannuzlos, Keith (NPL)" <keith.pannuzlos@MassMail.State.MA.US>, "Farioli, Mark (NPL)" <Mark.R.Farioli@MassMail.State.MA.US>, "Sullivan, Brian (POL)" <Brian.Sullivan@pol.state.ma.us>, "Lynch, Dennis (NFK)" <Dennis.M.Lynch@MassMail.State.MA.US>, "Powers, Meaghan (NFK)" <meagan.powers@MassMail.State.MA.US>, "Dicicco, David M (POL)" <David.M.Dicicco@pol.state.ma.us>, "Budzenski, Yuriy (POL)" <yuriy.budzenski@pol.state.ma.us>, "Danne, Matthew (POL)" <Matthew.Danne@pol.state.ma.us>, "Nichol, Kevin (POL)" <kevin.nichol@pol.state.ma.us>, "Matthew Murphy (mmurphy@brocktonpolice.com)" <mmurphy@brocktonpolice.com>, "cbell@brocktonpolice.com" <cbell@brocktonpolice.com>, "cbell@brocktonpolice.com", "ameilly@bullpolice.org" <ameilly@bullpolice.org>, "Sean Walsh (swalsh@pol.state.ma.us)" <swalsh@pol.state.ma.us>, "Sean Walsh (swalsh@pol.state.ma.us)" <swalsh@pol.state.ma.us>, "O'Brien, Sean (NORF)" <Sean.P.O'Brien@MassMail.State.MA.US>, "Delaney, Mark (NORF)" <mark.delaney1@MassMail.State.MA.US>, John Purchard <jpurchard@weymouth.ma.us>, "O'Neill, Russ" <oneill@brooklinema.gov>, Shannon Ducharme <sducharme@chicopeepolice.com>, "Det. Lt. Melissa Greene" <melissagreene@randolphmapolice.com>, "Bishop, Kevin" <kbishop@townofduxbury.org>, "gmarkey@townofduxbury.org" <gmarkey@townofduxbury.org>
Cc: "Morrissey, Michael (NFK)" <Michael.W.Morrissey@MassMail.State.MA.US>, "Doherty, Denise (NFK)" <Denise.M.Doherty@MassMail.State.MA.US>, "Fanning, John (NFK)" <john.m.fanning@MassMail.State.MA.US>, "Keefe, Edward (NFK)" <Edward.T.Keefe@MassMail.State.MA.US>, "Mattaliano, Gerard (NFK)" <Gerard.Mattaliano@MassMail.State.MA.US>, "Justin Fitzsimmons (justin@search.org)" <justin@search.org>, "Quirk, Sean (POL)" <sean.quirk@pol.state.ma.us>, "Tully, Brian (NFK)" <Brian.P.Tully@MassMail.State.MA.US>, NFK-DL-ADA-Superior-ci <NFK-DL-ADA-Superior-ci@MassMail.State.MA.US>, NFK-DL-ADA-District-ct <NFK-DL-ADA-District-ct@MassMail.State.MA.US>, NFK-DL-ADA--Appeals <NFK-DL-ADA-Appeals2@MassMail.State.MA.US>, "Kelly, Christopher (AGO)" <christopher.kelly@mass.gov>
Subject: Comm v. McCarthy - locating D's MV with ALPRs on Bourne/Sagamore Bridges not a search



Chiefs:
Commonwealth v. McCarthy (SJC-12750)← click on that link to see the case
In this case the SJC ruled that police tracking D's car using 4 automatic license plate readers (ALPRs) at both ends of the Bourne and Sagamore Bridges was too limited to amount to a constitutional "search." The SJC declined to say exactly how detailed digital surveillance would have to be to constitute a search leaving that issue for future cases.

State Police maintain ALPRs including ones at both ends of the Bourne and Sagamore Bridges. (p.3) The ALPRs photograph vehicles' license plates; that data along with the date and time of the sighting is retained by EOPS for a year. (p.3-4) Authorized users including police may put a license plate number on a "hot list " and receive an alert if that plate is sighted; reasons to put someone on the "hot list" include not only criminal investigations but also Amber alerts missing persons and BOLO alerts. (p. 3 25 n.13)

Through surveillance controlled buys and information from 4 Cis Barnstable police suspected that the co-D was se ling heroin out of his house in Barnstable. (p.4) Police saw a black Hyundai driven by D visit there briefly so they suspected that D was the co-D's supplier. Police put the Hyundai's license plate number on the State Police ALPR "hot list " so that they'd be notified whenever the Hyundai crossed one of the bridges. (p.5) After getting an alert that the Hyundai had crossed onto the Cape police followed both the Hyundai and the co-D to the buy location on a quiet residential street where D and co-D met for about 30 seconds but police could not see a physical exchange. (p.5) From the ALPR data police generated a spreadsheet showing that in mid-winter the Hyundai had crossed the bridges dozens of times sometimes more than once a day adding to police suspicion that D was the heroin supplier. (p.5-6) When police got a second alert that the Hyundai had crossed onto the Cape they again followed D and co-D to the buy location and saw a 60-second meeting but could not see any exchange. This time police stopped both cars handcuffed both co-D and D and read them Miranda. On co-D police found heroin; on D police found 2 cell phones and cash. (p.6-7) At the station police repeatedly told D he was "not under arrest " and D made statements.

D moved to suppress the ALPR data his statements and evidence obtained from the stop. A Superior Court judge found that the moment of arrest was when D and co-D were handcuffed at the scene of the traffic stop but denied the motion to suppress. (p.33) The SJC upheld the denial.

ALPRs and expectation of privacy in digital surveillance At some length the SJC discussed the constitutional issues raised by digital surveillance. (p.7-29) Police conduct amounts to a search if: (1) it intrudes on a D's expectation of privacy and (2) society is willing to recognize the expectation of privacy as reasonable. Here the SJC ruled D did have an expectation of privacy because D and co-D chose a buy location in a quiet residential area. (p.8 n.5) As to what expectation of privacy society recognizes as reasonable with regard to digital surveillance the SJC was guided by historical understandings of what was an unreasonable search and seizure when the U.S. and Mass. Constitutions were adopted in the late 1700s in reaction to redcoats' rummaging without restraint through colonists' homes. (p.8-10) New technologies like ALPRs raise difficult legal issues because they are easier and less expensive for police than traditional surveillance can be done secretly and permit police to search back in time for a vehicle's movements even before po lice suspicion arose. (p.12-14) Society does not recognize as reasonable an expectation of privacy in what someone knowingly exposes" to public view like a license plate – which by statute must be "displayed conspicuously." (p.15-16 & n.8) In older cases involving less advanced technology courts have held that a D did not have an expectation of privacy in contents of a phone conversation in a phone booth or a radio beeper" tracking a single journey. (p.14-17) But technology like ALPRs GPS and CSLI are different because they may give police a **mosaic** of information where each piece may be public but when viewed together they create a picture that implicates someone's privacy interests like their political re ligious or sexual associations. (p.17-21) The SJC was concerned that with enough ALPRs police could track someone's location everywhere which would be "creepy." (p.25) Exigent circumstances would likely justify using an ALPR in a situation involving an Amber alert or missing person. (p.25 n.13) The D urged the SJC to consider not just these four ALPRs on the Bourne and Sagamore Bridges but the hundreds of ALPRs across Massachusetts; the SJC declined to do so because that evidence is not in the record of this case. (p.26) The **limited number of cameras** here and their placements on the bridges was not enough to give D an expectation of privacy that society would recognize as reasonable. (p.26) The SJC declined to say how much digital surveillance would give such an expectation and admitted that its unwillingness to do so "**may bring some interim confusion**" until further cases develop the law on this issue. (p.28 n.15) Chief Justice Gants wrote a separate concurrence suggesting that one thing the SJC could do is to require police who want to search a vast amount of digital data to apply for a court order supported by an affidavit showing reasonable suspicion to do so. (concurrence p.3) This would be like a SW but with a lower standard than PC.

Written policy The SJC rejected D's argument that Barnstable PD should have had a written policy about ALPRs and the MSP policy on which Barnstable relied was not specific enough. (p.30) Written policies are required to justify certain exceptions to the SW requirement (like inventory searches and sobriety checkpoints) – they do not apply to the threshold question whether a search occurred in the first place. (p.31)

Miranda issues At the station police repeatedly told D that D was "not under arrest." But the motion judge found that the moment of arrest was when police handcuffed D at the traffic stop. (p.33) D argued that his statements should be suppressed because police tel ling him he was not under arrest amounted to "deceit or trickery" to get D to confess. The motion judge and the SJC rejected that argument saying that even if telling D he was not under arrest amounted to deceit or trickery it was just one factor to be used in determining voluntariness.

Bottom line: Police use of ALPRs at limited locations is not a constitutional search – but we don't know how many locations it'd have to be to amount to one. Using an ALPR in **exigent circumstances** like an Amber Alert is likely OK. Local police don't need a written policy to use ALPRs maintained by MSP. After a D has been handcuffed police should not tell D that D is "not under arrest" – po ice will likely be accused later of deceit and trickery.

A thought: There are news stories online that cell phones may be used to do contact tracing for people exposed to COVID-19. If lots of people willingly agree to let their cell phone data be used to track their whereabouts would that ever change courts' view of what society recognizes as a reasonable expectation of privacy? At some point if members of the public come to expect that they're being tracked should police be allowed to use that evidence too? Or at the very least should there be a jury instruction explaining that police have less access to the data than other entities (like software companies or public health agencies)?

As always email me with any questions. Wash your hands!

Marguerite

Marguerite T. Grant
General Counsel – Director of Training
Office of Norfolk District Attorney Michael W. Morrissey
45 Shawmut Road
Canton, MA 02021
781-830-4829

From: Shaw, Harold
To: Quinn, Dermot (POL)
Subject: Fwd: MassPort LPR Cameras
Date: Tuesday, August 18, 2020 8:44:20 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Dermot,

Thanks for all of your work on this! A long time in coming but you made it happen. Hope you're well and let's catch up soon.

All my best,

Hank

Harold H. Shaw
Chief Security Officer
Massachusetts Port Authority
617-568-3173 (w)
347-582-9976 (c)

Begin forwarded message:

From: "Egnitz, Brian (POL)" <brian.egnitz@state.ma.us>
Date: August 18, 2020 at 7:09:00 PM EDT
To: "Warmington, Scott (POL)" <scott.warmington@state.ma.us>, "Quinn, Dermot (POL)" <dermot.quinn@state.ma.us>
Cc: "Small, Michelle E (POL)" <michelle.e.small@state.ma.us>, "Silva, Kyra (POL)" <kyra.silva2@state.ma.us>, "Slater III, James F (CHS)" <james.slater@state.ma.us>, "Mason, Chris (POL)" <chris.mason@state.ma.us>, "Warren, Rosemary (POL)" <rosemary.warren@state.ma.us>, "Shaw, Harold" <HShaw@massport.com>, "Ryan, Deborah (POL)" <deborah.ryan@state.ma.us>, Richard Ball <Richard.Ball@state.ma.us>, "Crouse, David (POL)" <david.crouse@state.ma.us>
Subject: Re: MassPort LPR Cameras

The Technical Service Unit and I have completed cutting over all of the Massport LPR cameras and they are reporting back to boss and Chelsea.

Brian

On May 6, 2020, at 6:57 PM, Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us> wrote:

Hi Sirs,

We have begun cutting over the MassPort LPR Cameras into the EOPSS BOSS LPR Server. [redacted] at Airport Road arrivals were migrated and are now writing data to Chelsea. I will continue to cut the remaining cameras over in the next few days and weeks. I will advise when the project is complete.

- Brian

-----Original Message-----

From: Warmington, Scott (POL)
Sent: Tuesday, March 10, 2020 11:36 AM
To: Quinn, Dermot (POL)
Cc: Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Mason, Christopher (POL); Egnitz, Brian (POL); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL)
Subject: Re: MassPort LPR Cameras

What is the cost?

Sent from my iPhone

On Mar 10, 2020, at 11:28 AM, Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us> wrote:
Michelle and Kyra,
This purchase request is for equipment to allow Mass Port Sierra Wireless modems to communicate directly with the existing ALPR Boss server in Chelsea. This is the fastest way to bring the Massport LPR cameras on line. EOTSS and EOPSS are OK with this solution as is Major Deb Ryan, the CO at Troop F.
As you can see from the thread, this has been going on for some time. I think we can close it out with this small purchase.
This does not resolve the replacement of the existing ALPR equipment that we discussed at Command Staff yesterday. That is a different issue.
Thanks
Lieutenant Colonel Dermot J. Quinn #1765
Division Commander
Division of Homeland Security & Preparedness
Massachusetts State Police
-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Tuesday, March 10, 2020 10:52 AM
To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: FW: MassPort LPR Cameras
Hi LTC.,
Can we order this equipment for the MassPort project?
Thanks, Brian
-----Original Message-----
From: Slater, James (CHS)
Sent: Tuesday, March 10, 2020 10:26 AM
To: Egnitz, Brian (POL)
Subject: RE: MassPort LPR Cameras
Hi, Brian!
This needs to go through MSP fiscal. They need to enter the purchase in OPAS.
Jim
-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Tuesday, March 10, 2020 08:06
To: Slater, James (CHS) <james.slater@mass.gov>
Subject: RE: MassPort LPR Cameras
Is this something you can order or does it need to go through MSP?
-----Original Message-----
From: Slater, James (CHS)
Sent: Monday, March 9, 2020 10:36 AM
To: Egnitz, Brian (POL)
Subject: RE: MassPort LPR Cameras
Thanks, Brian...I will check with TSS.
Jim
-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Monday, March 9, 2020 10:29

To: Slater, James (CHS) <james.slater@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: RE: MassPort LPR Cameras
Thanks Jim,
I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need [redacted] wireless AC adapters and [redacted] I have reached out to BCM for a quote.
I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.
I plan to cut one sector ([redacted]) over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?
-Brian
-----Original Message-----
From: Slater, James (CHS)
Sent: Friday, March 6, 2020 1:43 PM
To: Egnitz, Brian (POL)
Cc: Quinn, Dermot (POL)
Subject: RE: MassPort LPR Cameras
Hi, Brian!
I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.
So, assuming you move forward with this, who would actually make this happen?
Thanks.
Jim
-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Wednesday, March 4, 2020 17:53
To: Slater, James (CHS) <james.slater@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Subject: Re: MassPort LPR Cameras
Hi Jim,
Regarding the Massport cameras; in the early days of AVL we installed [redacted] modem's in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don't we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn't have to do any firewall work either because they have a [redacted] communicate like all of the MDT's . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.
We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.
Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.
On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
Thank you sir
Major Charles W. Atchison III
Troop F Commander
Massachusetts State Police
Director of Aviation Security
2 Service Road
East Boston, Ma 02128
Office: 617-568-7555
Cell: [redacted]
11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
All,
Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan

further.
Thanks
CW
From: Quinn, Dermot (POL)
<dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
Sent: Monday, February 10, 2020 10:31 AM
To: Egnitz, Brian (POL)
<brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
Slater, James (CHS)
<james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
Robert (EOTSS)
<Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
Warmington, Scott (POL)
<Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
.us>>; Peek, Brian T. (EOTSS)
<Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
Timothy (EPS)
<timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
Michalski, Maria (EPS)
<maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
Christopher (POL)
<Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
Hughes, Sean M. (EOTSS)
<sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
<pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
<curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
<HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
<Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
Atchison, Charles (POL)
<catchison@massport.com<mailto:catchison@massport.com>>
Subject: RE: MassPort LPR Cameras
Good Morning,
I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.

To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
I can't overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security's technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
Respectfully,
Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
of Homeland Security & Preparedness Massachusetts State Police
<image006.png>
From: Egnitz, Brian (POL)
<brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
Sent: Friday, January 17, 2020 1:10 PM
To: Slater, James (CHS)
<james.slater@mass.gov<mailto:james.slater@mass.gov>>
Cc: Quinn, Dermot (POL)
<dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
Guerriero, Robert (EOTSS)
<Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
Brian T. (EOTSS)
<Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
Timothy (EPS)
<timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
Maria (EPS)
<maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
Subject: RE: MassPort LPR Cameras
Hi Jim,
BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
-Brian
From: Egnitz, Brian (POL)
Sent: Monday, January 6, 2020 1:33 PM
To: Slater, James (CHS)
Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
(EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
Crary
Subject: RE: MassPort LPR Cameras
Hi Jim,
We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
Thanks Brian
From: John Tedona [mailto:jtedona@neology.net]
Sent: Monday, December 9, 2019 4:55 PM
To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
Timothy (EPS); Slater, James (CHS)
Subject: RE: MassPort LPR Cameras
Alex,

I can be available most anytime tomorrow for a call.
Regards,
John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net<mailto:jtedona@neology.net>
PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http-3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FNEWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJbaP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJU2sB_fmM6g&e=>
From: Chute, Alexander
<AChute@massport.com<mailto:AChute@massport.com>>
Sent: Monday, December 9, 2019 4:38 PM
To: Egnitz, Brian (POL)
<brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary <pcrary@neology.net<mailto:pcrary@neology.net>>
Cc: Guerriero, Robert (MASSIT)
<robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>; Peek, Brian T. (EOTSS)
<brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell, Timothy (EPS)
<timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>; Slater III, James F (CHS)
<james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
Subject: RE: MassPort LPR Cameras
CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
Hello All,
I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
Respectfully,
~Alex
<image007.png>
Alexander B. Chute
Program Manager, Public Safety Systems Massachusetts Port Authority
Cell: [redacted]
Office: 617.568.5942
achute@massport.com<mailto:achute@massport.com>
WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Monday, November 18, 2019 3:26 PM
To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>); pcrary@neology.net<mailto:pcrary@neology.net>
Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,

Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
Subject: RE: MassPort LPR Cameras
Hi John, Peter
Any issues with moving Massports cameras to the Chelsea DB?
Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
The current app server
<image008.png>
Current DB server
<image009.png>
<image010.png>
Our current reads by month for about [redacted]
Year
Month
Day
Month Name
Reads Count
2019
11
1
November
495,113
2019
11
2
November
472,907
2019
11
3
November
384,409
2019
11
4
November
411,440
2019
11
5
November
434,085
2019
11
6
November
495,537
2019
11
7
November
444,123
2019
11
8
November
542,492
2019

11
9
November
443,463
2019
11
10
November
389,514
2019
11
11
November
362,548
2019
11
12
November
236,539

From: Chute, Alexander [mailto:AChute@massport.com]
Sent: Wednesday, November 13, 2019 2:49 PM
To: Egnitz, Brian (POL)
Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
Subject: RE: MassPort LPR Cameras

These stats are from the [redacted] we have in the system for this month:

<image011.png>

~Alex

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Tuesday, November 12, 2019 5:28 PM
To: Chute, Alexander
Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
Subject: RE: MassPort LPR Cameras

Hi Alex,

Can you please provide the updated reads per day? Previously you were interested in sharing [redacted] at approximately 75,000 reads per day.

Here is the [redacted] confi I mentioned.

Set host to boss [redacted]
Set image [redacted]
Set number of [redacted]
Set Ping [redacted]
Set udp ping [redacted]
Set ping [redacted]
Set security [redacted]

I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week. For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.

-Brian

From: Chute, Alexander [mailto:AChute@massport.com]
Sent: Tuesday, November 12, 2019 2:08 PM
To: Egnitz, Brian (POL)
Subject: MassPort LPR Cameras

Brian,

Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the [redacted] well as the [redacted] I would propose that we extend

this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to approximately [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.

Respectfully,

~Alex

<image007.png>

Alexander B. Chute
Program Manager, Public Safety Systems Massachusetts Port Authority
Cell: [redacted]
Office: 617.568.5942
achute@massport.com<mailto:achute@massport.com>

WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

<SierraQuoteForMassPort.pdf>

The information contained in this communication, including any attachments, is confidential and is intended only for the use of the recipient(s) named above. If the reader of this message is not an intended recipient, you are notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you receive this communication in error, please notify the sender immediately, and delete the communication, any attachments, and all copies.

From: steven.mccarthy@pol.state.ma.us
To: Quinn, Dermot (POL)
Subject: Fwd: Now Available! License Plate Recognition with WatchGuard In-Car System
Date: Tuesday, January 21, 2020 5:56:10 PM

Thought you might find this interesting Col.

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
480 Worcester Rd
Framingham, MA 01702

Begin forwarded message:

From: WatchGuard <products@watchguardvideo.com>
Date: January 21, 2020 at 5:40:03 PM EST
To: "McCarthy, Steven (POL)" <steven.mccarthy@pol.state.ma.us>
Subject: Now Available! License Plate Recognition with WatchGuard In-Car System
Reply-To: products@watchguardvideo.com

Not rendering correctly? View this email as a web page here.

Small on Grey.jpg

ALPR-in-car-1with WG Logos-blur-email-600

Now Available! License Plate Recognition with WatchGuard 4RE In-Car Video System

The WatchGuard 4RE Mobile ALPR Solution harnesses the power of the industry-leading WatchGuard 4RE in-car video system and high-definition cameras to detect and match vehicle license plates of interest stored in a database of over 20 billion detections.

Increase Officer Safety - Help distinguish between a routine traffic infraction stop and something potentially more serious.

Proactively Interrupt Crimes - Alert officers to vehicles of interest in real-time, potentially interrupting a string of crime.

Deliver Leads to Solve More Cases - Use historical data to determine a vehicle's proximity to crime scenes, providing leads crucial to an investigation.

Discover the WatchGuard 4RE Mobile ALPR Solution

WatchGuard Video

415 E Exchange Parkway
Allen, TX 75002
USA

You received this email because you are subscribed to Products from WatchGuard Video.

Update your email preferences to choose the types of emails you receive.

Unsubscribe from all future emails

From: McCarthy, Steven (POL)
To: Quinn, Dermot (POL)
Subject: Fwd: Now Available! License Plate Recognition with WatchGuard In-Car System
Date: Tuesday, January 21, 2020 5:56:14 PM

Thought you might find this interesting Col.

Detective Captain Steven McCarthy
Massachusetts State Police
Division of Homeland Security and Preparedness
480 Worcester Rd
Framingham, MA 01702

Begin forwarded message:

From: WatchGuard <products@watchguardvideo.com>
Date: January 21, 2020 at 5:40:03 PM EST
To: "McCarthy, Steven (POL)" <steven.mccarthy@pol.state.ma.us>
Subject: Now Available! License Plate Recognition with WatchGuard In-Car System
Reply-To: products@watchguardvideo.com

Not rendering correctly? View this email as a web page here.

Small on Grey.jpg

ALPR-in-car-1with WG Logos-blur-email-600

Now Available! License Plate Recognition with WatchGuard 4RE In-Car Video System

The WatchGuard 4RE Mobile ALPR Solution harnesses the power of the industry-leading WatchGuard 4RE in-car video system and high-definition cameras to detect and match vehicle license plates of interest stored in a database of over 20 billion detections.

Increase Officer Safety - Help distinguish between a routine traffic infraction stop and something potentially more serious.

Proactively Interrupt Crimes - Alert officers to vehicles of interest in real-time, potentially interrupting a string of crime.

Deliver Leads to Solve More Cases - Use historical data to determine a vehicle's proximity to crime scenes, providing leads crucial to an investigation.

Discover the WatchGuard 4RE Mobile ALPR Solution

WatchGuard Video

415 E Exchange Parkway
Allen, TX 75002
USA

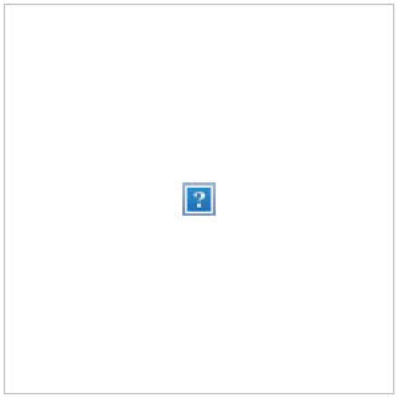
You received this email because you are subscribed to Products from WatchGuard Video.

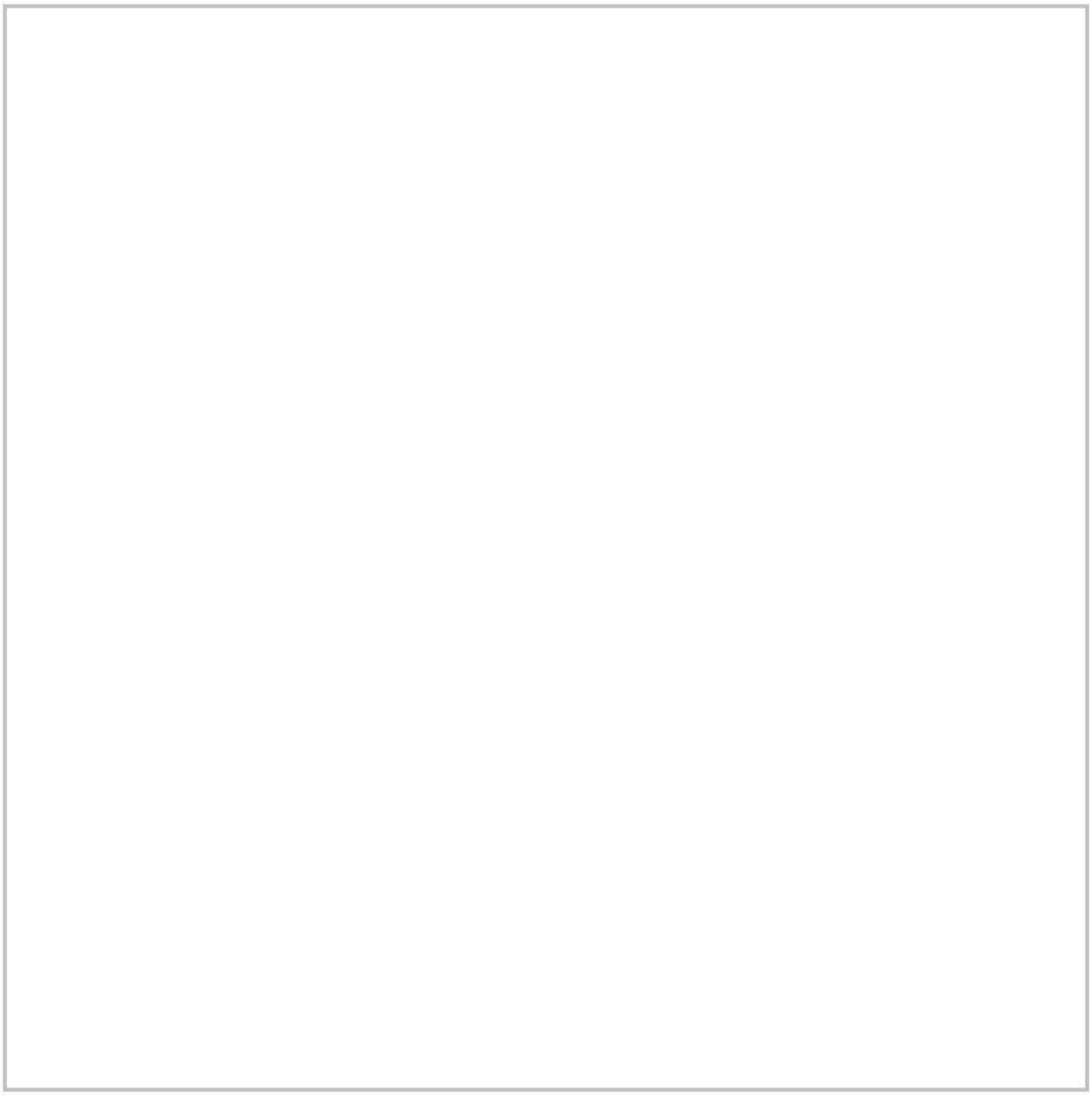
Update your email preferences to choose the types of emails you receive.

Unsubscribe from all future emails

From: Ness and Associates Law Enforcement Daily News
To: D"Amore, Paul (POL)
Subject: Good Morning! The Power of Information - Law Enforcement News of the Day: February 18, 2020
Date: Monday, February 17, 2020 11:30:27 PM

View this email in your browser



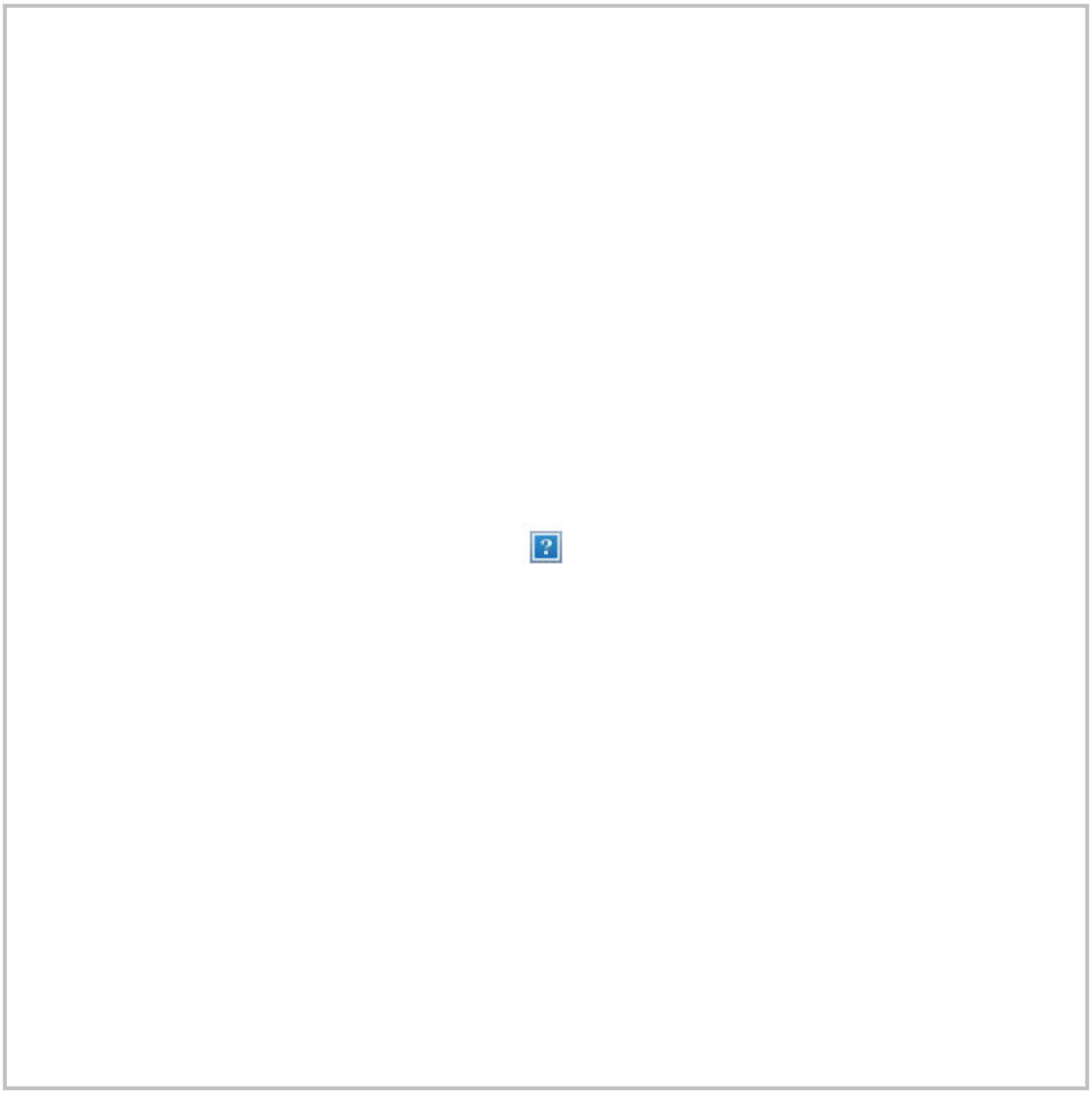


Your daily source for what's interesting and newsworthy around the country and the rest of the world

THOUGHT FOR THE DAY

"It's a new day!
Let go of old issues, relationships,
or apprehensions that are holding you back.
Decide to move forward
using the knowledge you've gained,
from your failures and triumphs,
while making room for new accomplishments.

Cleaning isn't just good for your house,
it's healthy for your mind.
Adopt the attitude that you can
and will achieve your dreams,
because it's true.
You have greatness within you!"
~ Les Brown



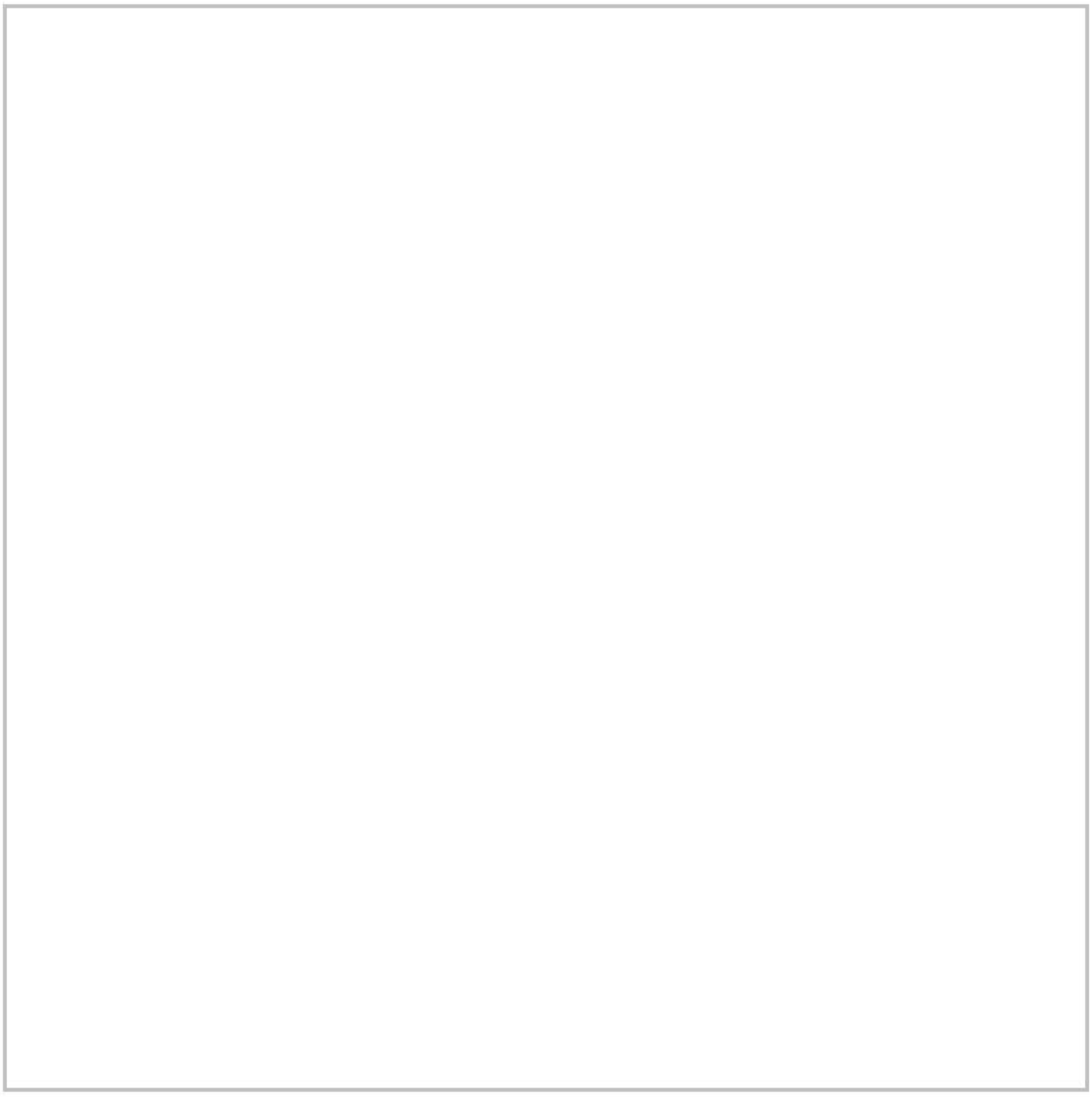
Can courts do more to force FOID card violators to give up their guns? Cook and DuPage counties considering how following Tribune report.

Cook County Sheriff Tom Dart is calling for changes in how the judicial system handles defendants with revoked gun licenses following a Tribune investigation into the ballooning backlog of people declared too dangerous to own firearms

and the state's failure to address it. The move comes after the Tribune highlighted the story of Christopher Miller, a Joliet man who fatally shot his 18-month-old son, Colton, with a gun he should have relinquished after having his firearm owner's identification card revoked more than a year earlier. According to a Tribune analysis, Miller was among the more than 70% of revoked FOID permit holders statewide who ignored police orders to account for their weapons.

During his 20 months on the revocation list, Miller appeared before judges in two separate counties on criminal charges and never once was asked if he complied. No one at the hearings — one in DuPage County and one in Cook County — ordered the Illinois National Guardsman to give up the multiple firearms he kept in violation of state law.

Read: https://www.chicagotribune.com/news/criminal-justice/ct-foid-revoke-illinois-gun-laws-courts-20200217-k3cjsh5xsfgfpeelzgc6yimkni-story.html

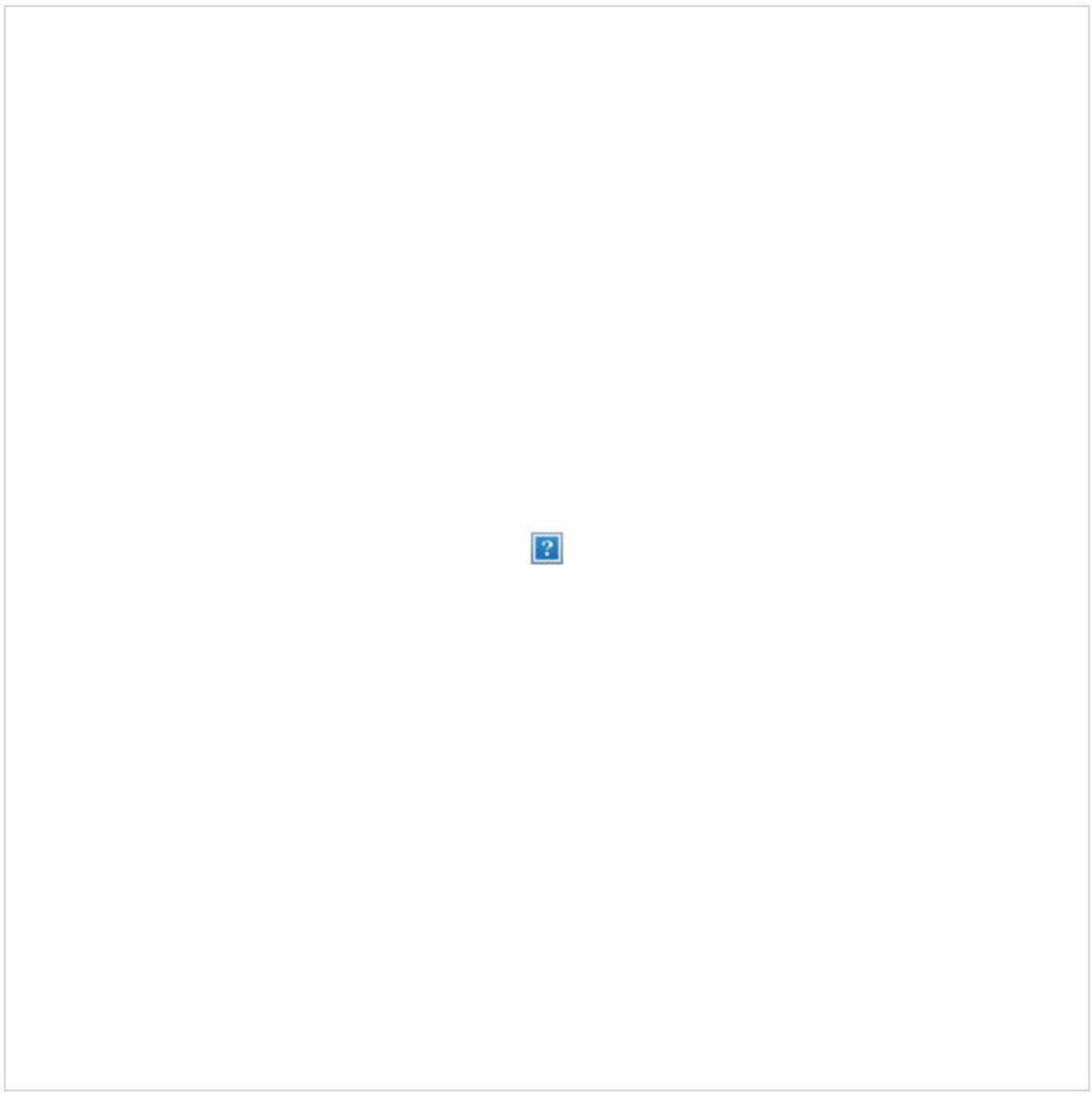


LAPD automatic license plate readers pose a massive privacy risk, audit says

The Los Angeles Police Department and three other California law enforcement agencies have not provided sufficient privacy protections for the hundreds of millions of images collected by automated license plate readers and shared with other jurisdictions, the state auditor said Thursday. Most of the images collected by the devices are unrelated to criminal cases. The audit found that 99.9% of the 320 million images the LAPD stored came from vehicles that were not on a list of those involved in criminal investigations when the image was made by the automated license plate readers, or ALPR. State Auditor Elaine Howle said in a letter to Gov. Gavin Newsom and the Legislature that changes were needed to better safeguard the privacy of license plate data collected by the Fresno Police Department, Marin County Sheriff's Office, Sacramento

County Sheriff's Office and LAPD."Local law enforcement agencies did not always follow practices that adequately consider the individual's privacy in handling and retaining the ALPR images and associated data," the audit said. "None of the agencies have an ALPR usage and privacy policy that implements all the legally mandated — since 2016 — requirements."

Read: https://www.latimes.com/california/story/2020-02-13/privacy-risks-automatic-license-plate-readers-lapd

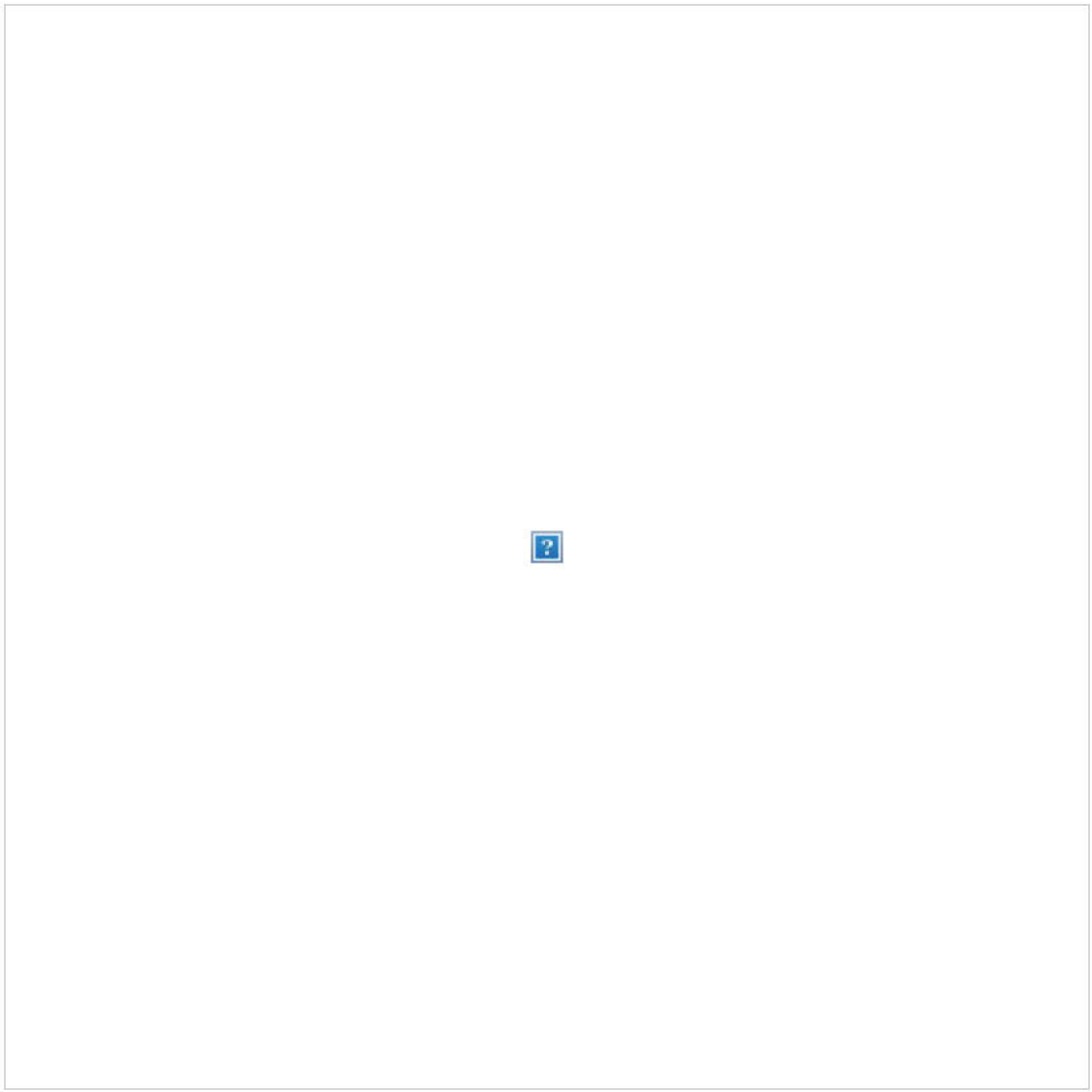


OUAGADOUGOU, Burkina Faso (AP) — Gunmen killed 24 civilians, including a church pastor, and kidnapped three others on Sunday in Burkina Faso, an official said. It was the latest attack against a religious leader in the increasingly unstable West African nation. The mayor of Boundore commune, Sihanri

Osangola Brigadie, said the attack occurred in the town of Pansi in Yagha province. The roughly 20 attackers separated men from women close to a Protestant church. At least 18 other people were injured. “It hurt me when I saw the people,” Brigadie said after visiting some of the victims in the hospital in Dori town, 180 kilometers (110 miles) from the attack. The gunmen looted oil and rice from shops and forced the three youth they kidnapped to help transport it on their motorbikes, he said.

Both Christians and Muslims were killed before the church was set on fire, said a government security official in Dori who spoke on condition of anonymity because they weren’t authorized to speak to the media.

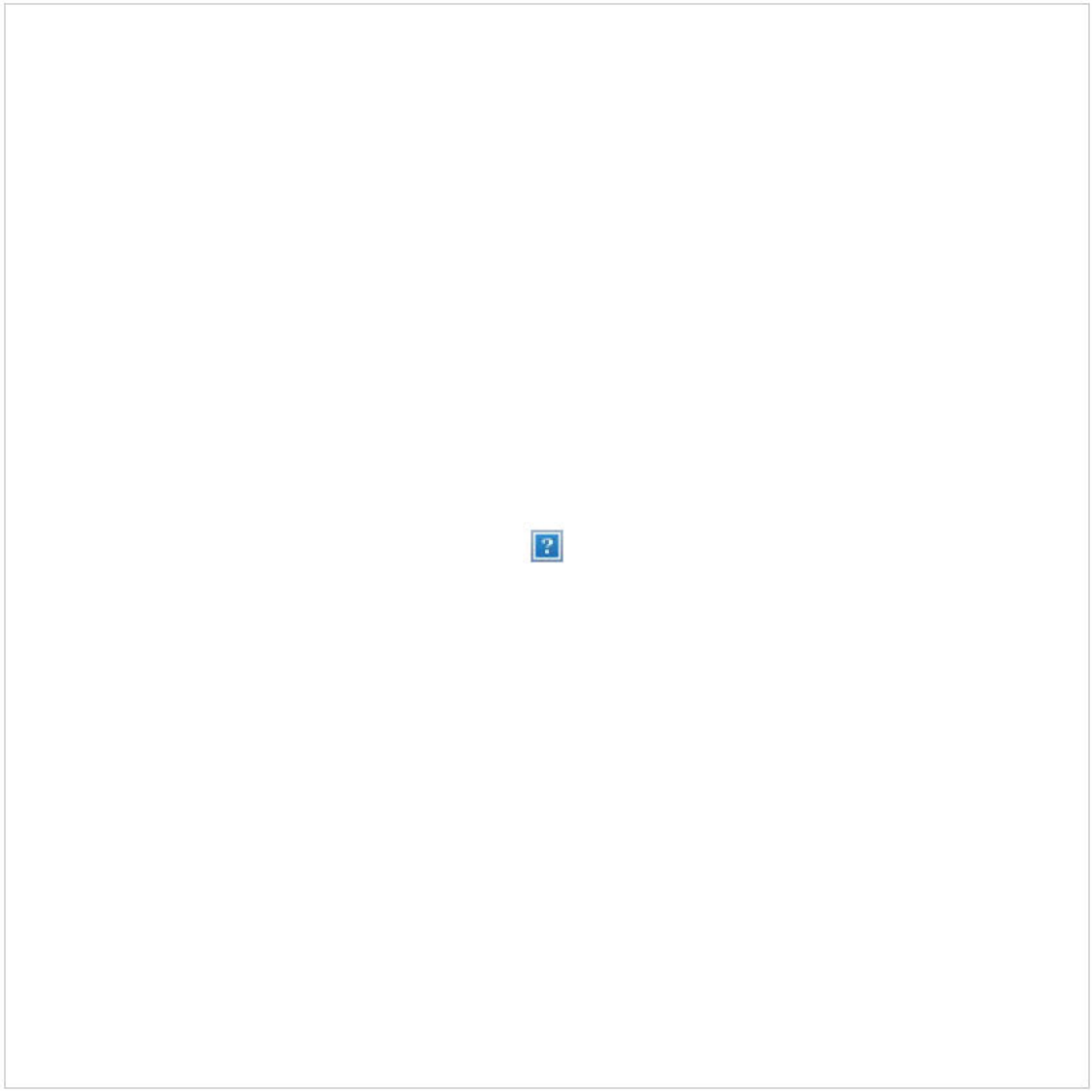
Read: https://apnews.com/83683091944c433d3731e94350bc56c1



HONOLULU (AP) — Police in Hawaii are investigating the theft of fruit valued

at about $1,000 including durian, which is known for its powerful odor. Two men entered a property in Hilo on the Big Island and removed 18 durian and other types of fruit on the night of Feb. 1, the Hawaii Police Department said. Authorities released a surveillance camera image of two suspects and asked the public for additional information that could lead to the capture of the fruit bandits. The tropical, spiky durian fruit resembles a small porcupine and typically weighs from 2 to 7 pounds (1 to 3 kilograms). Durian is known for a pale yellow flesh with a sweet taste but a smell that has been compared to moldy cheese, rotten onions, dead fish and far worse. Durian is popular across Southeast Asia but also is commonly banned from hotel rooms and public transportation there.

Read: https://apnews.com/7e0d6b4a52e6b48008e376e2e3a69ad0



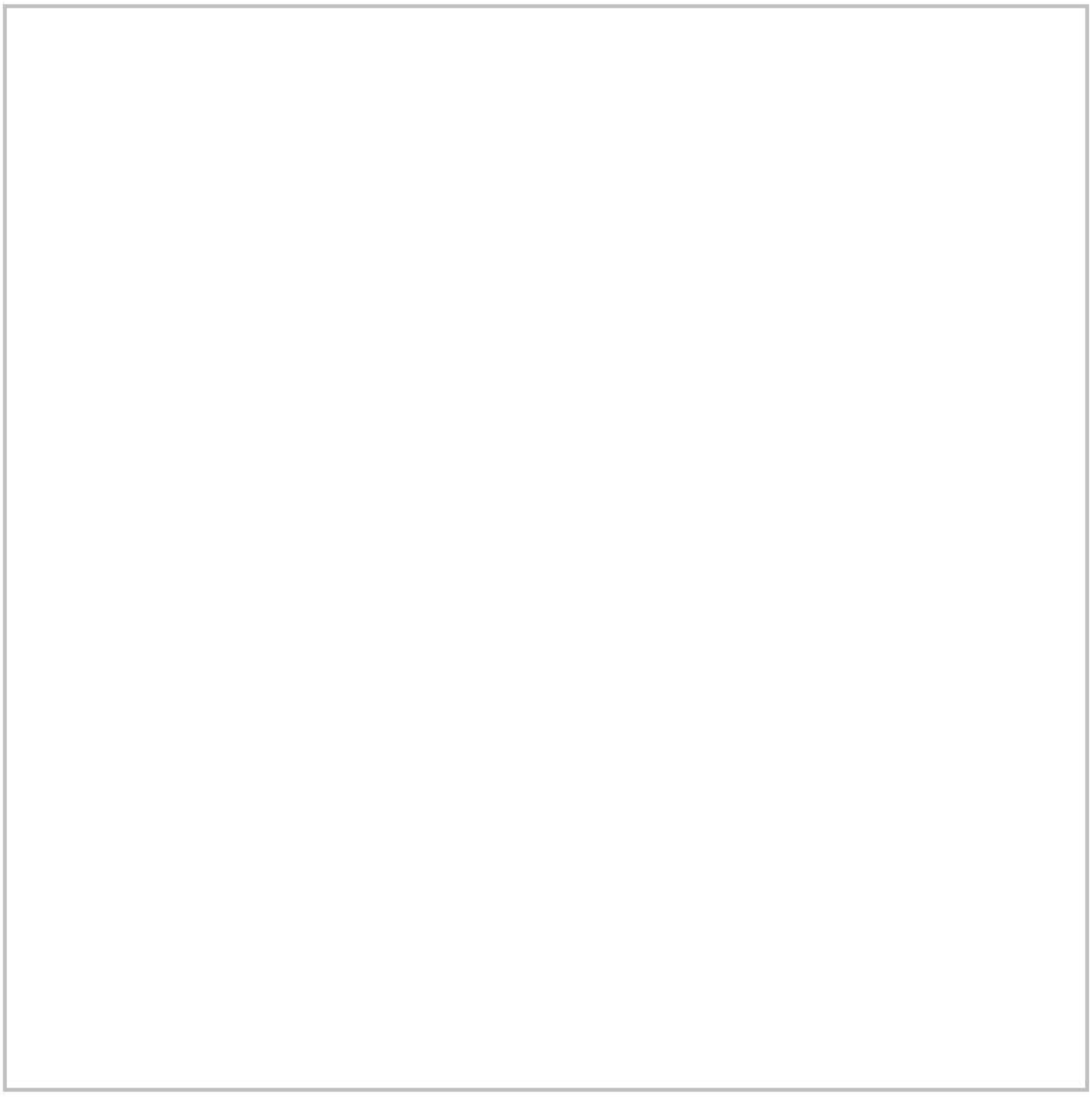
White Mountain Apache Police Officer David Kellywood shot, killed Monday morning

FORT APACHE INDIAN RESERVATION (3TV/CBS 5) -- A White Mountain Apache Police Department officer was killed early Monday morning. Releasing information on behalf of the White Mountain Apache Tribe and Governing Body, the Navajo County Sheriff's Office said the White Mountain Apache Police Department received a report of gunfire near the Hon-Dah Resort Casino shortly before 1 a.m. The first officer on the scene found the man described in that call.

[VIDEO: News conference on shooting death of Officer David Kellywood]

"The subject immediately engaged in a violent, physical altercation with the officer, during which, the officer was shot," NCSO said in news release. "A second responding officer arrived shortly after, and fearing for his life and the public's safety, shot the suspect."

Read: https://www.azfamily.com/news/white-mountain-apache-police-officer-david-kellywood-shot-killed-monday/article_d529bd7c-519d-11ea-9cf5-73e272ef61e0.html

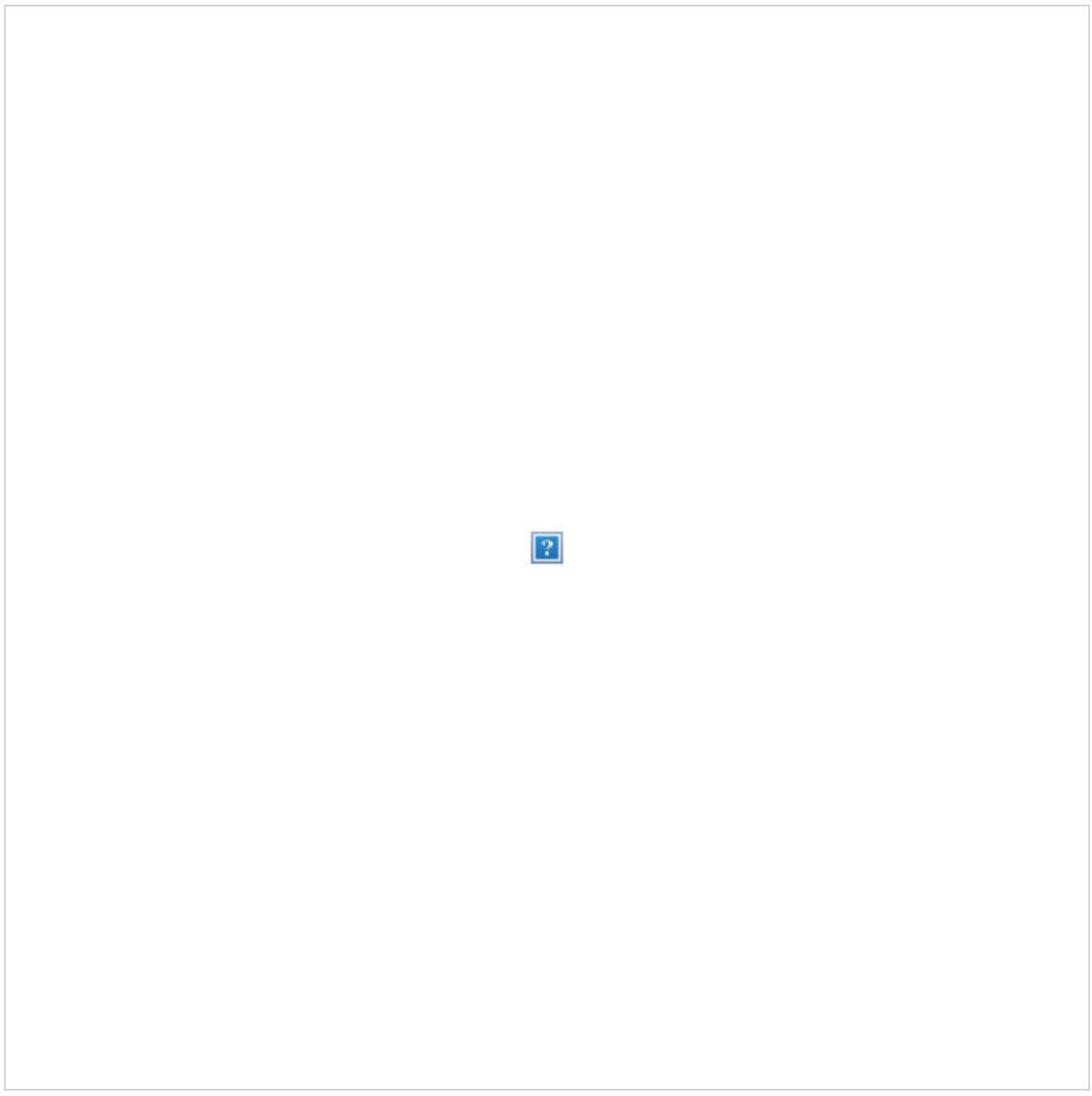


Georgia Sheriff's Deputy Hits Another Deputy on Head With Flashlight

RICHMOND COUNTY, Georgia -- Richmond County Sheriff Richard Roundtree says an altercation involving two deputies at the scene of a Friday shooting was a "heat of the moment" incident that is "embarrassing" to the department.
Deputy Brandon Keathley hit Deputy Nicholas Nunes on the head with a flashlight as they tried to attend to a shooting victim at a convenience store. Both were later disciplined. Nunes and Keathley got into the altercation after responding to Circle K in the 2800 block of Peach Orchard Road, where Deangelo Burns, 17, was taken after being shot on Abelia Drive.
At a news conference Tuesday, Roundtree said Keathley and a trainee were the first to arrive and found Burns inside a vehicle. He was removed and deputies began to administer aid. Nunes arrived shortly afterward and tried to take over the situation, Roundtree said. Keathley told Nunes to step back

because deputies already there were assessing the victim's injuries.

Read: https://www.officer.com/on-the-street/news/21125860/georgia-sheriffs-deputy-hits-another-deputy-on-head-with-flashlight

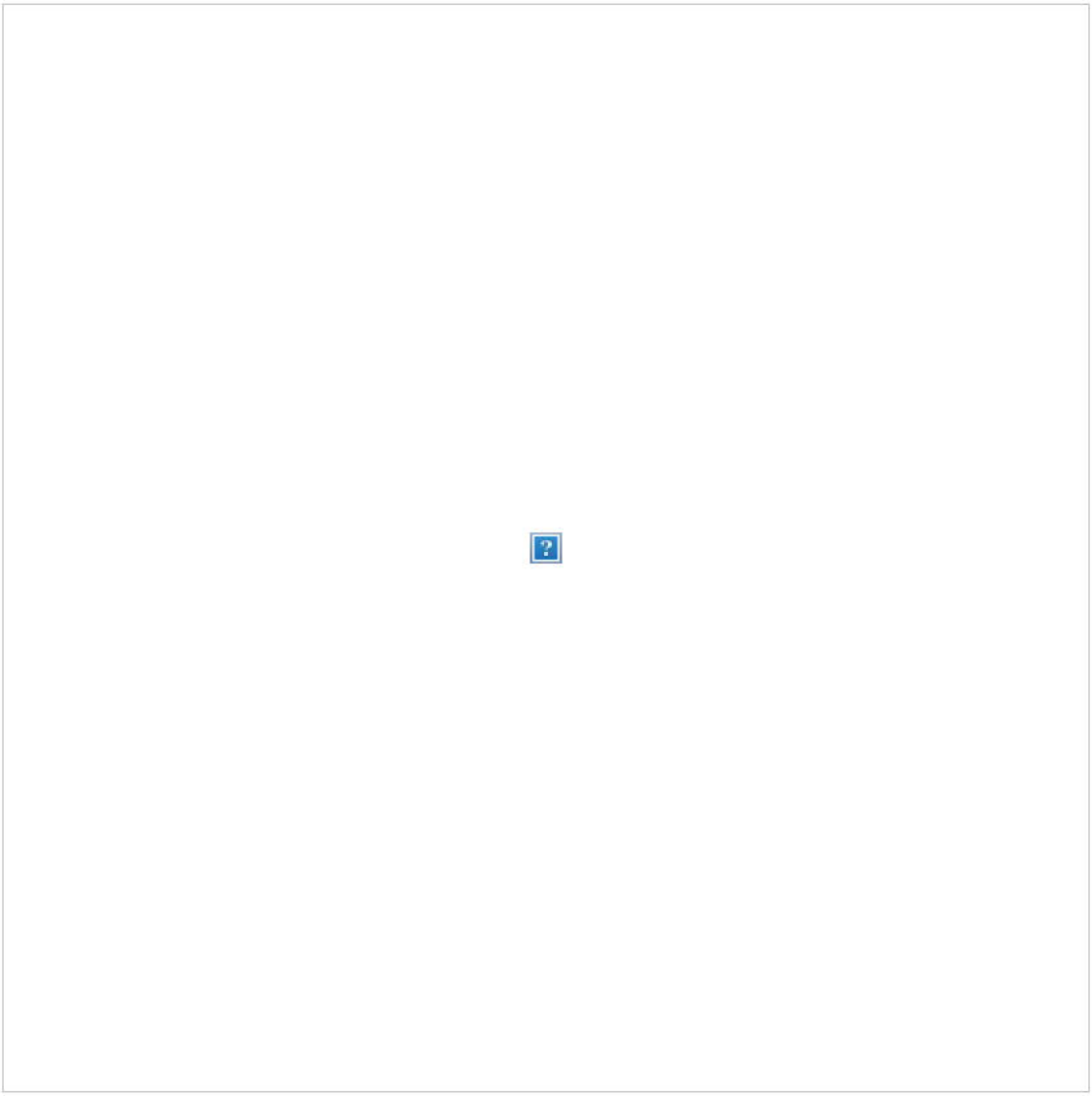


Suspended Ashland police chief files lawsuit against city, mayor

ASHLAND. Mo. (KMIZ) Ashland's suspended police chief filed a lawsuit against the City of Ashland and its mayor on Monday after city officials placed him on administrative leave. According to the lawsuit filed in Boone County court, Mayor Gene Rhorer removed Police Chief Lyn Woolford as city administrator and suspended him as chief after Woolford refused to remove Rhorer's girlfriend from Rhorer's home. Since there was no threat of violence Woolford refused to intervene, but sent officers to "keep the peace," the lawsuit

says. The petition states that since this incident Rhorer has taken "retaliatory action" by firing Woolford as city administrator and then by placing him on administrative leave.

Read: https://abc17news.com/news/ashland/2020/02/17/suspended-ashland-police-chief-files-lawsuit-against-city-mayor/

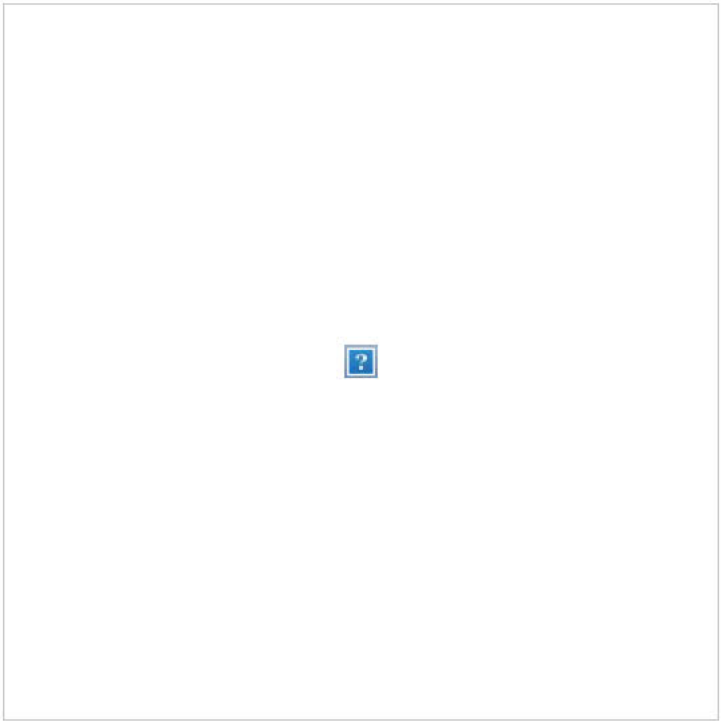


How suburban police departments are courting minority recruits

Ever since Pradeep Singh Deol was old enough to dress up for Halloween, his costume of choice was a police uniform. A Buffalo Grove High School alumnus, Deol now is one of just three Sikh law enforcement professionals in the suburbs. Unwittingly, his lifelong passion has made him the poster child for departments seeking to diversify their ranks. A few suburban police

departments are recruiting in earnest within the Sikh, Muslim, Hindu, and other minority communities to better mirror and serve the growing racial and ethnic diversity of the suburbs. Others are using a common recruitment tactic -- hitting up high school and college campuses. That was the kind of connection that lured Deol, 28, who now is a Prospect Heights police officer. He said his first impressions of law enforcement were drawn from engaging with his school's resource officer and from participation in Drug Abuse Resistance Education and another youth program offered by Wheeling Police Department.

Read: https://www.dailyherald.com/news/20200217/how-suburban-police-departments-are-courting-minority-recruits



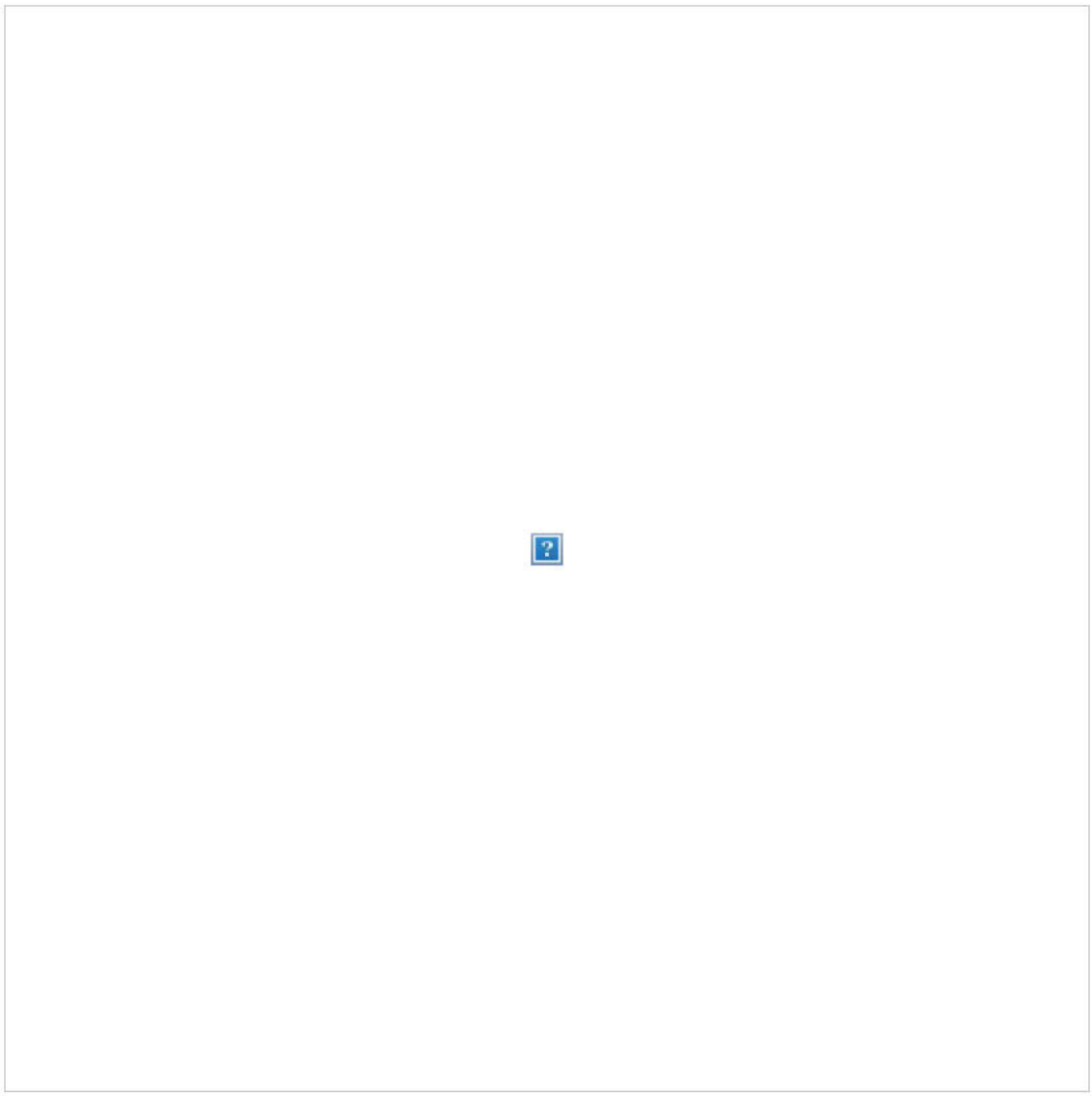
Las Vegas restaurants show officers support after bizarre incident

UPDATE 11 P.M. Two local establishments, Distill and Remedy's, are offering free meals to all officers in uniform from midnight to 8 a.m. through Feb. 21 at all of their locations in the Las Vegas valley after earlier reports had officers not being served at a competitor's bar and grill.

ORIGINAL STORY LAS VEGAS (KTNV) -- 13 Investigates has learned that two uniformed police officers with the Las Vegas Metropolitan Police Department were denied service Thursday night at The Lodge at Cactus near Cactus Avenue and Southern Highlands Parkway. A post about the incident has received a lot of attention on social media. The graveyard police officers

had gone into the restaurant for food and the bartender reportedly told them that the restaurant did not serve "you guys" anymore. The police union sent its membership a letter earlier today that called the incident disgusting and offensive.
13 Investigates was able to confirm that there was an incident and The Lodge has since apologized.

Read: https://www.ktnv.com/news/2-las-vegas-police-officers-denied-service-at-local-bar-and-restaurant



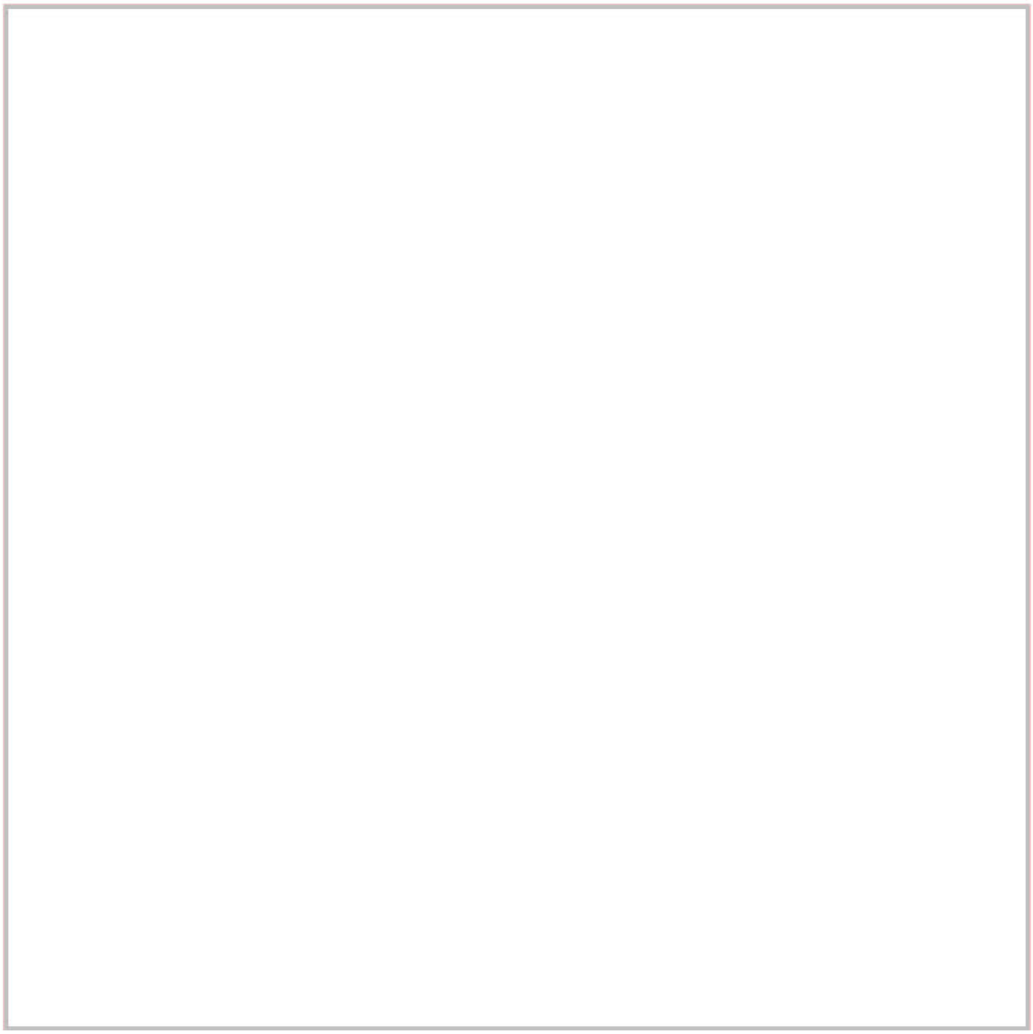
"TEDDY BEAR" POLICE OFFICER ADDS SAFETY AND POSTIVITY TO SOUTHERN ELEMENTARY

Chief Shannon Clem sees Officer Mark Branham, with utmost respect, as a

teddy bear.

Mayor Ron Stinson calls Branham “a home run.” Southern Elementary Principal Mark Hegyi sees Branham as another element of security in a place where no one should feel unsafe. Branham? Branham sees himself as a someone who is made for the job. Branham recently returned to the Falmouth Police Department after 17 years with the Alexandria Police where he spent four years as a school resource officer for Campbell County Middle School, Day Treatment, and Campbell Ridge Elementary, respectively. He is not unfamiliar with the area. He worked with the department for 11 months in the early 2000s, but this time, he has more experience under his belt, and a lot of experience is in the SRO position. Almost as soon as he walked into the job, he saw where he was most needed and where he would have the most impact: Southern Elementary.

Read: https://www.falmouthoutlook.com/school/teddy-bear-police-officer-adds-safety-and-postivity-southern-elementary



The Law Enforcement News of the Day is a compilation of daily news articles selected from thousands of sources by the editors of Ness & Associates. Ness & Associates are not liable for the use of or reliance on any information contained in these articles. The presence of advertising does not endorse, nor imply endorsement of, any products or services by Ness & Associates.

Copyright © 2020 Ness & Associates

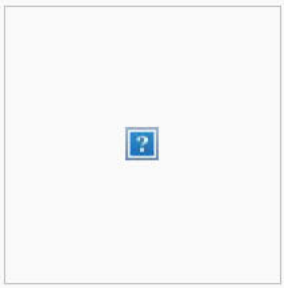
To Unsubscribe, email jness23@cox.net

Copyright © 2020 Ness Associates, All rights reserved.
You are receiving this email because you opted in via our website.

Our mailing address is:
Ness Associates
9241 E Grandview St
Mesa, AZ 85207-4318

Add us to your address book

Want to change how you receive these emails?
You can update your preferences or unsubscribe from this list.



From: Ness and Associates Law Enforcement Daily News
To: D"Amore, Paul (POL)
Subject: Good Morning! The Power of Information - Law Enforcement News of the Day: May 6, 2020
Date: Wednesday, May 6, 2020 7:00:29 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

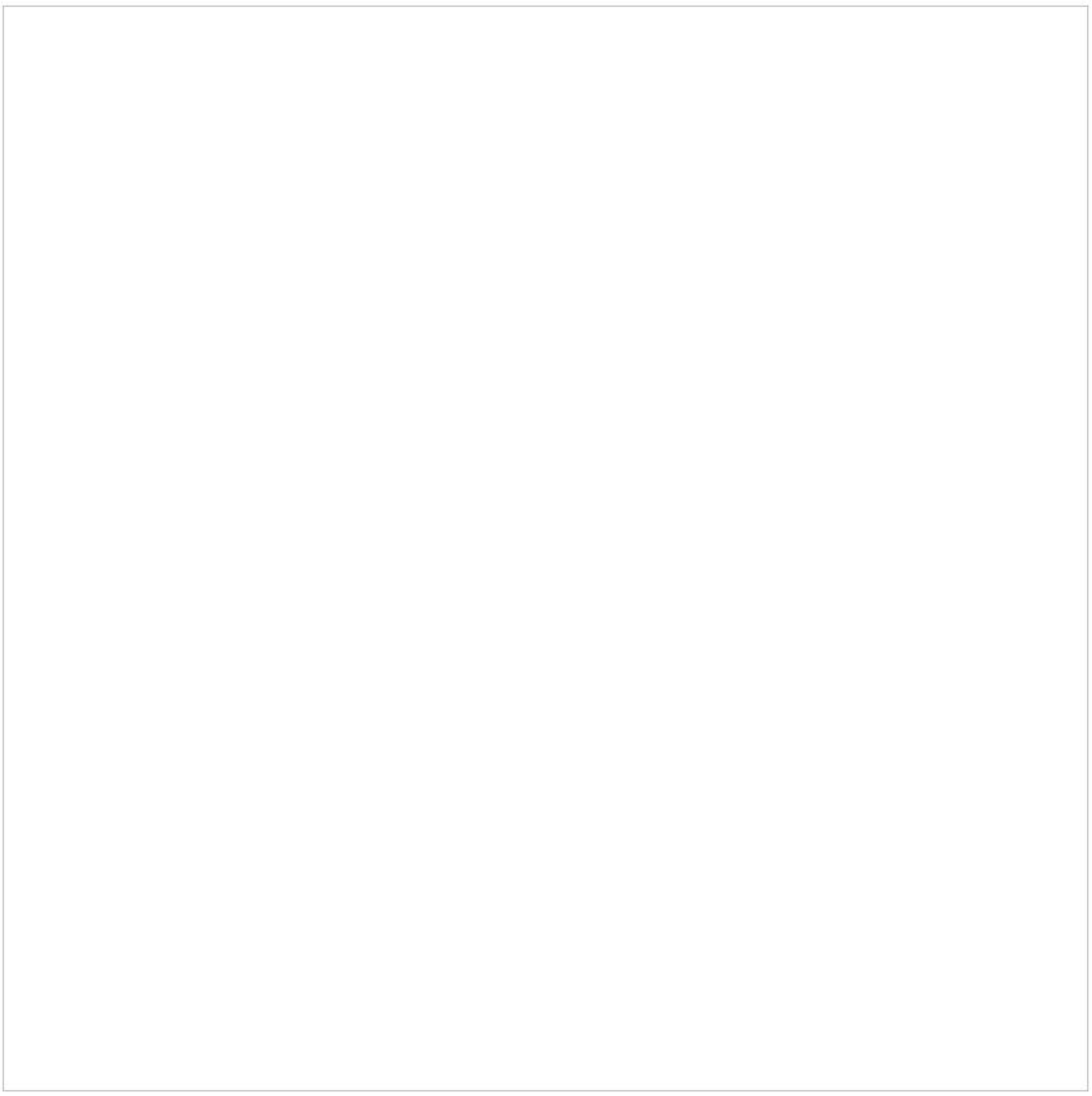
View this email in your browser

Your daily source for what's interesting and news worthy around the country and the rest of the world

Daily News & Updates for Wednesday May 6, 2020
There will no publication on Thursday, May 7 and Friday, May 8

THOUGHT FOR THE DAY

**“Fear does not stop death.
It stops life.
And worrying
does not take away tomorrow’s troubles.
It takes away today’s peace.”**



Michigan officials look at banning guns inside state capitol after armed 'reopen' protests

John Truscott (R), vice chairman of the Michigan State Capitol Commission, said the body, which is charged with managing and maintaining the state Capitol and surrounding grounds, is looking into a possible gun ban inside the building after protesters entered the state Capitol brandishing firearms last week.

Truscott told the Detroit Free Press on Tuesday that the commission is reviewing a century-old open carry law and seeking legal help to determine whether the body has the power to implement such a ban.

"We'll be getting a more comprehensive briefing at our meeting on Monday," he told the paper.

"One way to easily deal with this would be to pass a law," he also told the paper.

However, the commission — which consists of the secretary of the state

Senate, the clerk of the state House, two individuals appointed by the secretary and clerk, and two individuals appointed by the governor — is not able to pass such legislation.

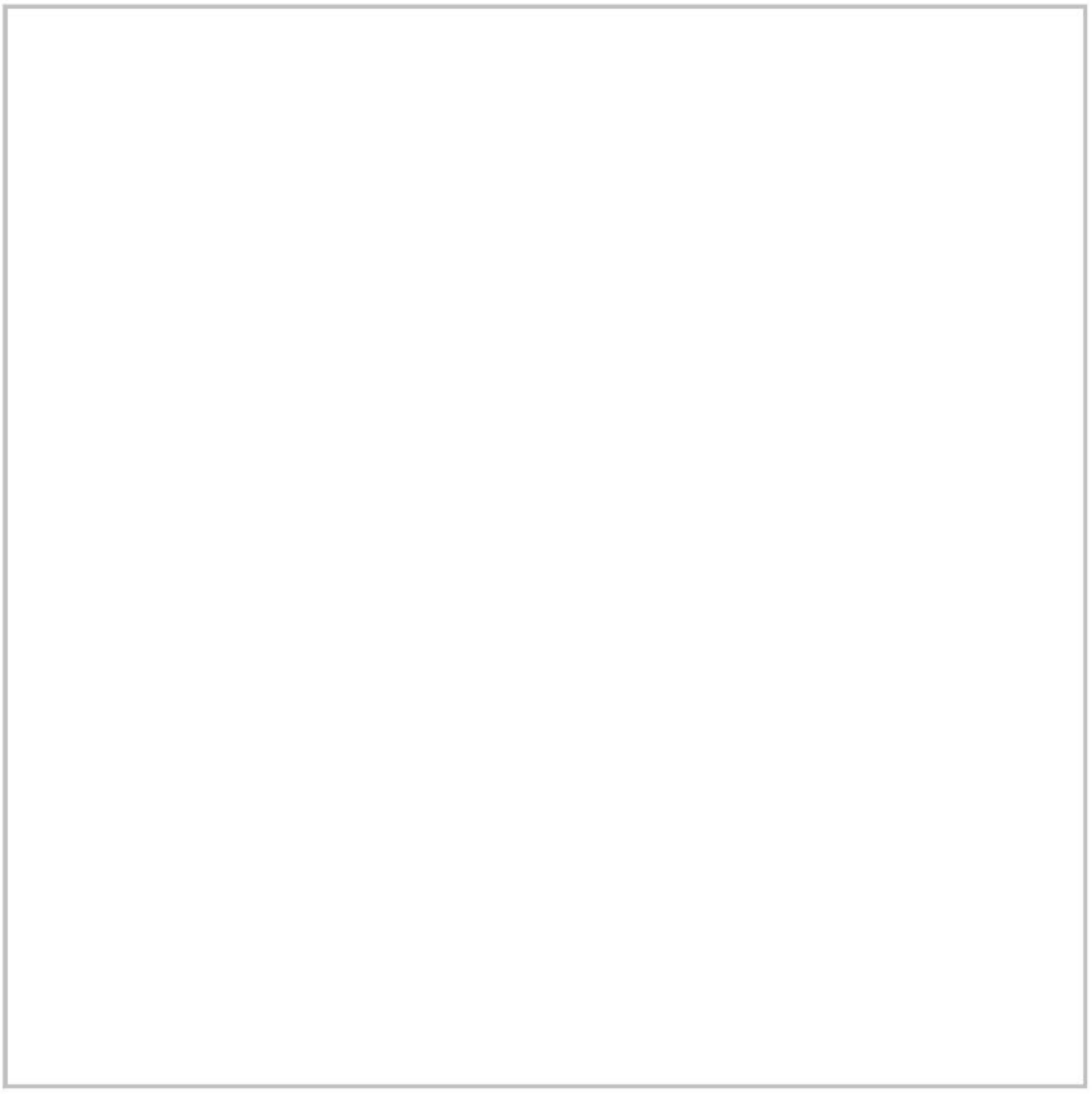
The Hill has reached out to Truscott for further comment.

His remarks come after hundreds of demonstrators, some of whom were armed, descended on the state Capitol last week to protest Michigan Gov. Gretchen Whitmer's (D) stay-at-home order.

In footage of the demonstration, which was dubbed the "American Patriot Rally," protesters could be seen carrying firearms inside the statehouse and calling for lawmakers to reopen businesses that had been closed temporarily during the pandemic. Some protesters also could be seen with Confederate flags and swastikas.

Whitmer on Sunday condemned the protests, which she said "depicted some of the worst racism and awful parts of our history in this country."

"The behavior you've seen in all of the clips is not representative of who we are in Michigan," she also said.



Law enforcement left in limbo during legal battle between Whitmer, legislature

There is nothing normal about the times we are living in as a result of the COVID-19 pandemic and now law enforcement has had another curveball throw at them.

Gov. Gretchen Whitmer late Thursday issued directives both proclaiming that the coronavirus emergency continues under a 1945 law and declaring new states of emergency and disaster under a 1976 law after lawmakers refused her request for a 28-day extension. The declarations are the foundation of her stay-home order and other measures to curb the spread of the virus.

Republicans, who want more input on gradually restarting the economy and say a ban on elective medical and dental procedures should be lifted, also voted to

authorize a lawsuit challenging her authority and actions. They question the legality of her stay-home measure since the Legislature did not lengthen the state of emergency.

But Whitmer said the stay-home order rests on gubernatorial powers in the 1945 law, which does not require legislative consent nor an extension.

"If the 1976 law supersedes the '45 law, they would have repealed it. It was an intentional decision to keep both of these sources of authority for the chief executive of the state of Michigan," she said. "It is for times like these that that authority is really important, when lives are on the line."

The later law has a provision saying it should not be construed to "limit, modify, or abridge" a governor's authority to proclaim an emergency under the earlier law or to exercise powers vested by the state constitution.

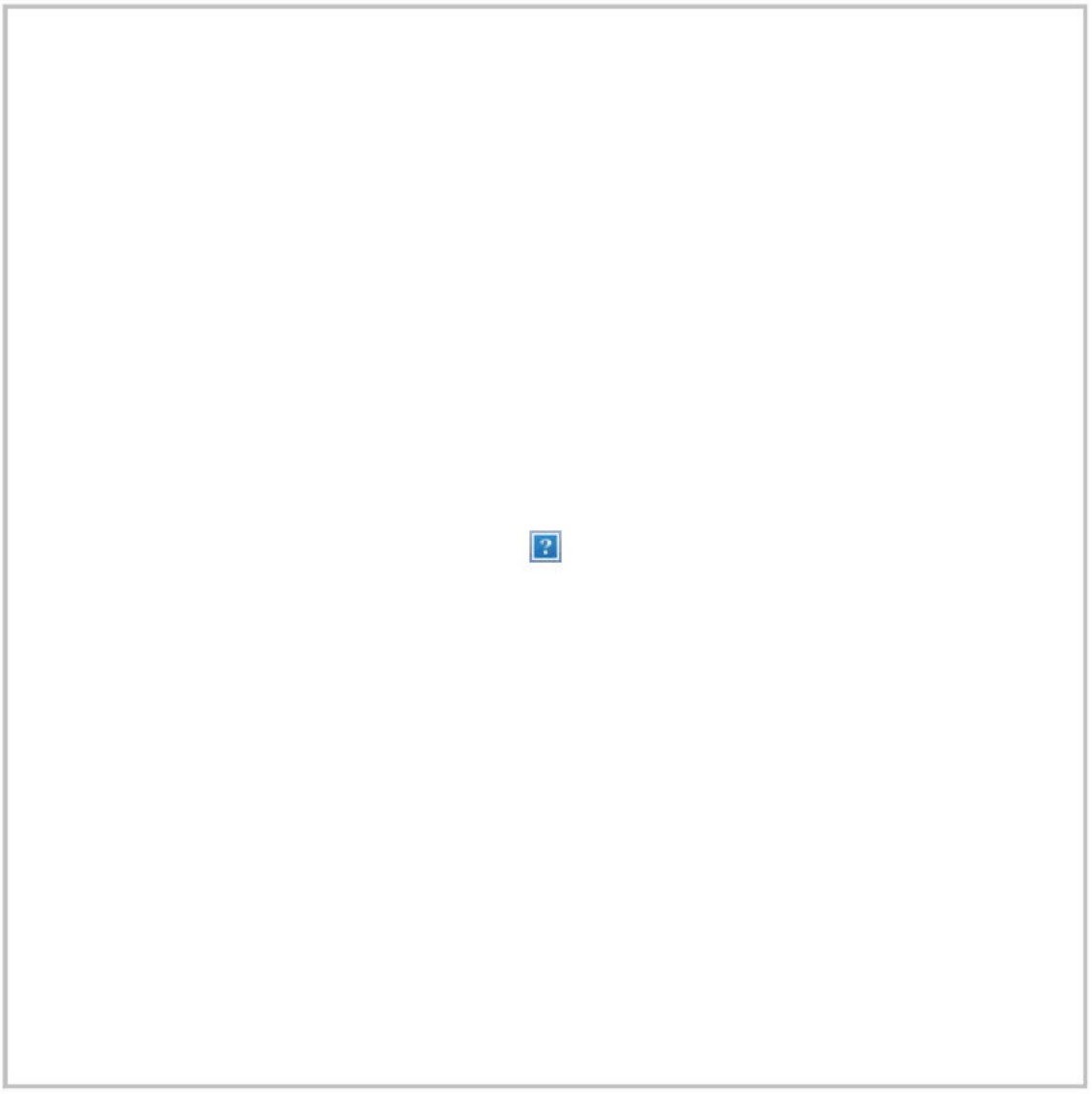
House Speaker Lee Chatfield, a Republican, said "the judiciary will have the final say."

While this political and legal showdown will unfold in the coming weeks, with the uncertainty Michigan Attorney General Dana Nessel is advising law enforcement to use their best judgment regarding enforcement of Stay Home, Safe Safe violations until the issue is resolved in court.

For Wexford County Prosecutor Jason Elmore, this doesn't help clarify how law enforcement should proceed.

The orders were issued under section 1 of article 5 of the Michigan Constitution of 1963, the Emergency Management Act, 1976 PA 390, as amended, MCL 30.401 et seq., and the Emergency Powers of the Governor Act of 1945, 1945 PA 302, as amended, MCL 10.31 et seq. The issue to be determined in the court is the authority to extend beyond 28 days. This is the separation of powers between legislative, executive, and judicial branches of state government In action.

"Those in law enforcement have taken oaths to enforce the laws," he said. "Typically, our laws are passed by our legislature and signed into law by our executive. They are tested over the years by our judiciary. This is a different situation."



The Coronavirus Becomes a Battle Cry for U.S. Extremists

America's extremists are attempting to turn the coronavirus pandemic into a potent recruiting tool both in the deep corners of the internet and on the streets of state capitals by twisting the public health crisis to bolster their white supremacist, anti-government agenda.

Although the protests that have broken out across the country have drawn out a wide variety of people pressing to lift stay-at-home orders, the presence of extremists cannot be missed, with their anti-immigrant and anti-Semitic signs and coded messages aimed at inspiring the faithful, say those who track such movements.

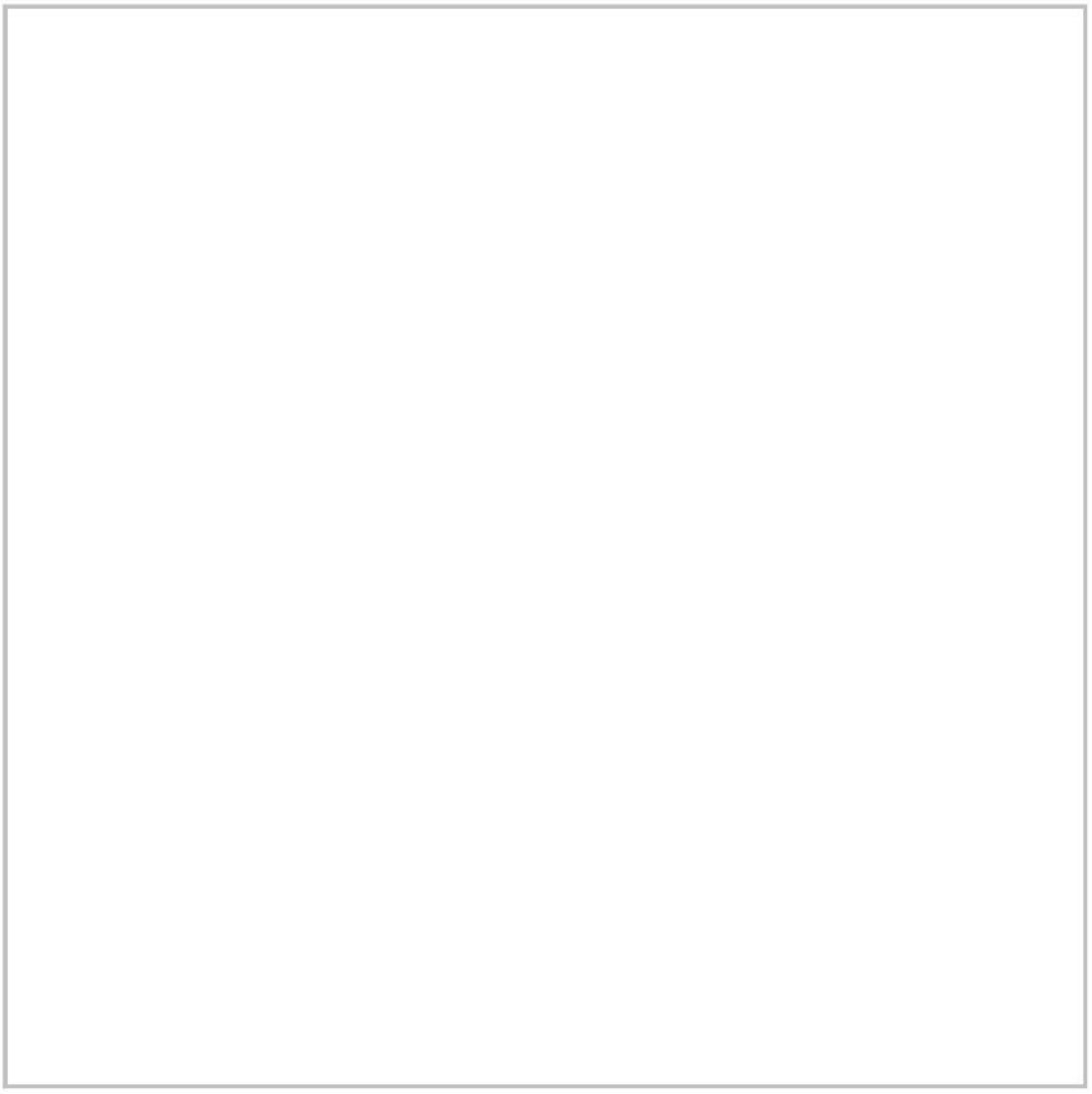
April is typically a busy month for white supremacists. There is Hitler's birthday,

which they contort into a celebration. There is the anniversary of the Oklahoma City bombing, the domestic attack 25 years ago that killed 168 people and still serves as a rallying call for new extremist recruits.But this April, something else overshadowed those chilling milestones. It was the coronavirus, and the disruption it wreaked on society, that became the extremists' battle cry.

Embellishing Covid-19 developments to fit their usual agenda, extremists spread disinformation on the transmission of the virus and disparage stay-at-home orders as "medical martial law" — the long-anticipated advent of a totalitarian state.

"They are being very effective in capitalizing on the pandemic," said Devin Burghart, a veteran researcher of white nationalists who runs the Institute for Research and Education on Human Rights, a Seattle-based research center on far right movements.

What success the groups have had in finding fresh recruits is not yet clear, but new research indicates a significant jump in people consuming extremist material while under lockdown. Various violent incidents have been linked to white supremacist or anti-government perpetrators enraged over aspects of the pandemic.

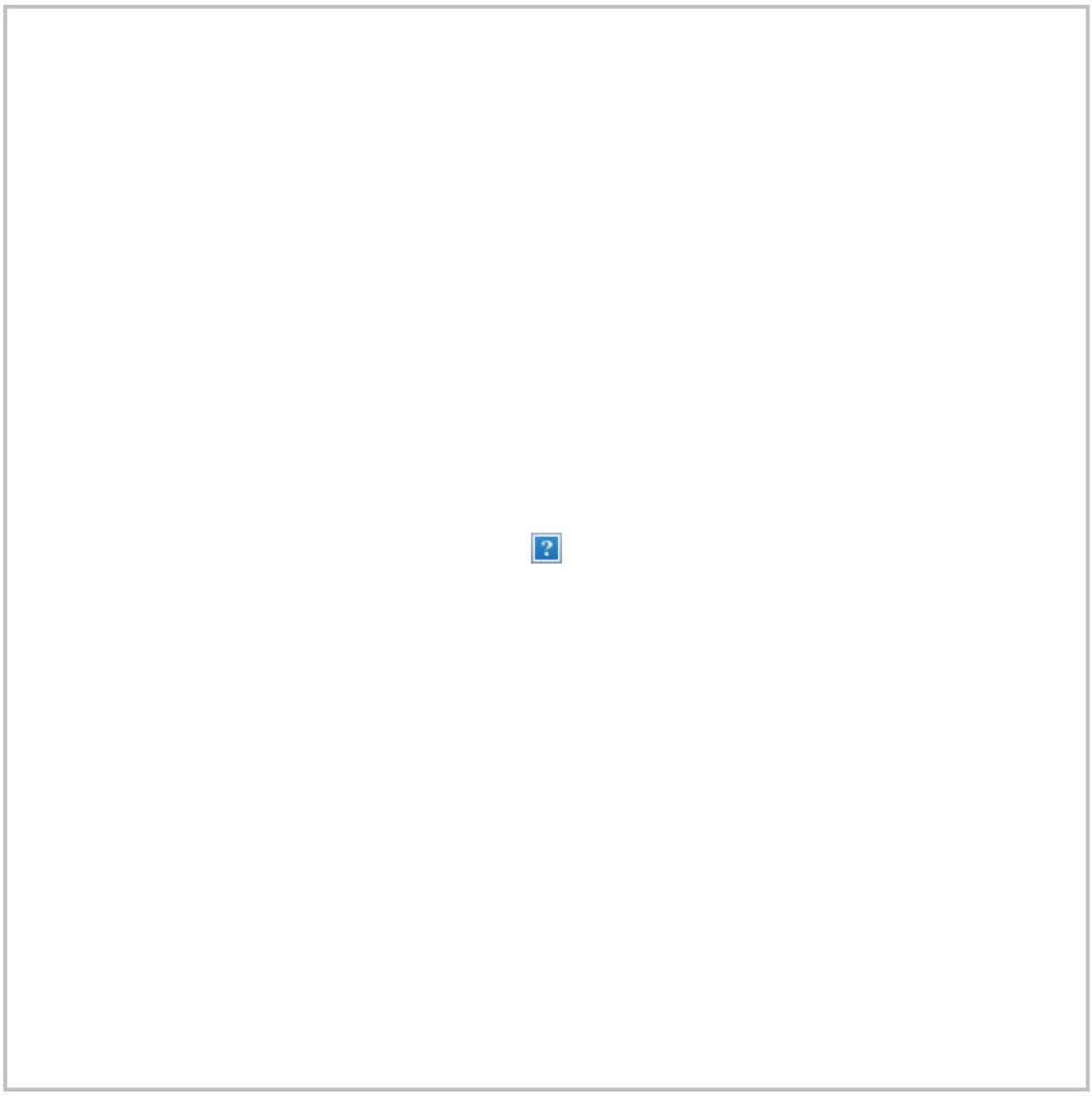


NY police union warns city will 'fall apart' if enforcement of social distancing does not end

The union representing New York City's police officers warned that the city will "fall apart" if the police force is used to enforce social distancing measures. "This situation is untenable: the [New York Police Department] needs to get cops out of the social distancing enforcement business altogether," Patrick Lynch, the president of the Police Benevolent Association of New York, said in a statement.

The NYPD's involvement in enforcing the city's social distancing orders has been thrust under scrutiny after video surfaced of an officer hitting a man in Manhattan while trying to separate people. Three men in total were arrested in

the incident, and an officer is on modified duty pending an internal review.
Lynch accused the city's leadership of providing the police force only "vague" guidelines over how to enforce the measures, and that the criticism of the NYPD's involvement in making sure people separate from each other was inevitable.
"The cowards who run this city have given us nothing but vague guidelines and mixed messages, leaving the cops on the street corners to fend for ourselves," he said. "Nobody has a right to interfere with a police action, but now that the inevitable backlash has arrived, they are once again throwing us under the bus.



Video of violent LAPD arrest in Boyle Heights sparks outrage, internal review

Footage of a Los Angeles police officer repeatedly punching a man during an arrest in Boyle Heights in late April has stoked outrage and prompted the launch of an internal review of the incident.

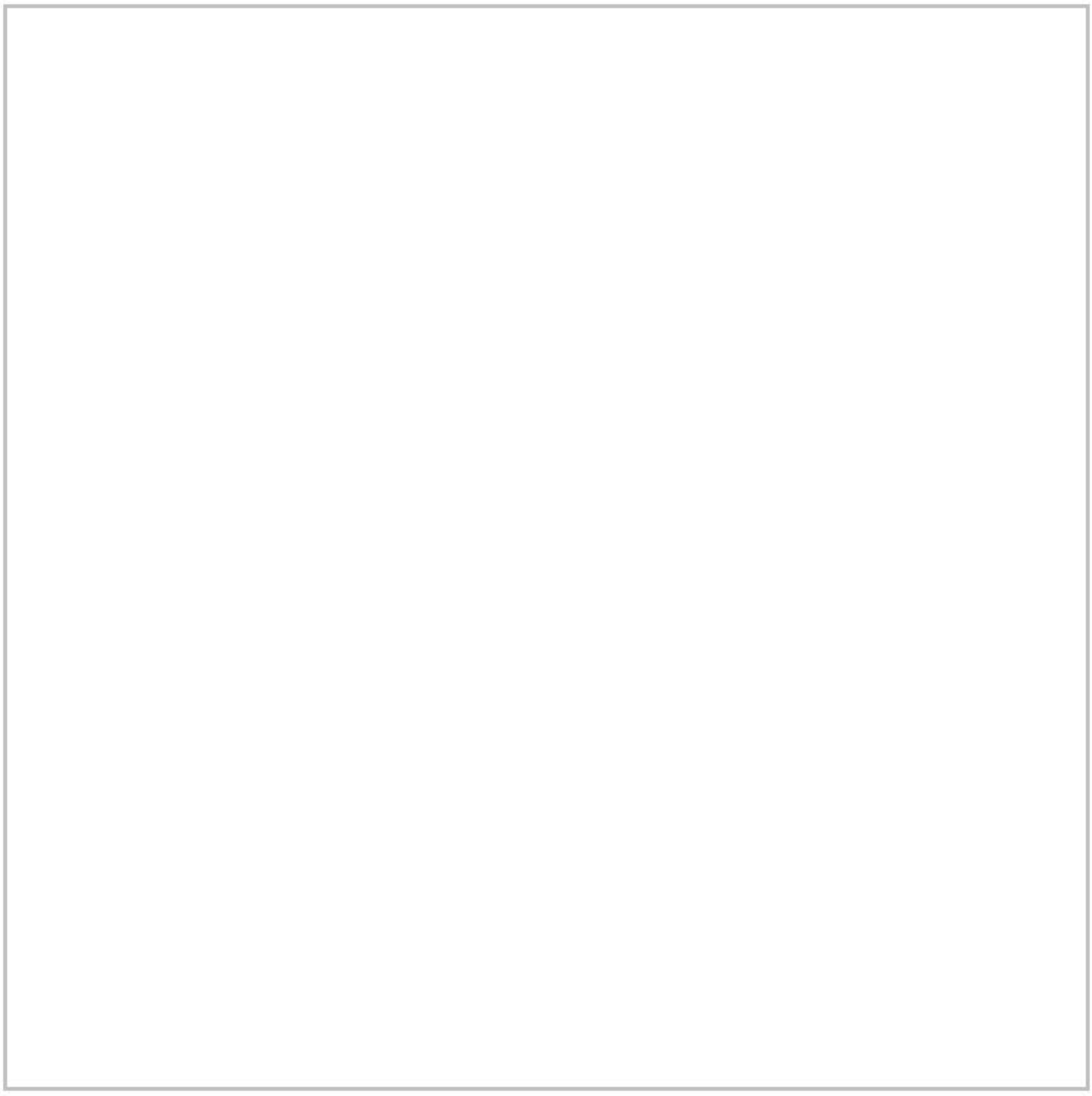
Officers were responding to a trespassing call in the 2400 block of Houston Street on April 27 and ordered a man to leave the property near the Church of God of Prophecy, according to a statement issued by the LAPD after footage of the incident began to gain traction online Monday night.

In a 50-second video, two officers can be seen ordering a man to turn around near a fence outside the church. A male officer tells the suspect to “stop fighting,” and the suspect responds, “Ain’t nobody fighting.”

The officer then begins throwing overhand punches to the back of the suspect’s head while shouting profanities. At one point, the suspect attempts to take a few steps away from the officer, who follows and continues to punch the man in the head and body. A female officer stands by, occasionally reaching her hand out but otherwise not intervening.

The LAPD statement described the incident as a “physical altercation” between the suspect and officer. The suspect sustained “abrasions to his head and face” but refused medical attention, according to the LAPD. The officer suffered a hand injury, the LAPD said.

Neither the officer nor the suspect were immediately identified. The man was ultimately released pending further investigation, the LAPD said in its statement.



5-year-old boy pulled over in Utah says he was on his way to California to buy a Lamborghini

A Utah Highway Patrol trooper got a pint-sized surprise when he pulled over a 5-year-old driver who was swerving so badly he thought the driver needed medical attention.

Trooper Rick Morgan said the driver did not respond to his lights but pulled over when Morgan hit his siren on Interstate 15 in Ogden on Monday.

“I approached the vehicle and I was expecting to find somebody who needed an ambulance or paramedics,” Morgan said.

But when the window came down Morgan said it was pretty clear that it was “a very underaged driver who was behind the wheel.”

The boy was sitting on the edge of his seat to reach the brake pedal, the trooper said.

When asked, Morgan said, the boy told the officer he was going to his sister's house — in California. The boy told another trooper that he wanted to buy a Lamborghini when he got there and then flashed open his wallet showing his cash to purchase his dream car: $3.

His parents were contacted and they arrived and took custody of their son and the vehicle.



Philippines orders its largest broadcaster off the air as nation fights virus

The Philippine government on Tuesday ordered the country's largest broadcasting network to halt operations, a blow to press freedom and the flow of information in the middle of a pandemic.

Media giant ABS-CBN signed off after its evening news broadcast, leaving the screens of millions of viewers black and the jobs of 11,000 employees in jeopardy.

A cease-and-desist order was issued by the National Telecommunications Commission earlier Tuesday, affecting television and radio operations. ABS-CBN's cable news channel and digital operations will continue, albeit with a limited reach.

Staff of ABS-CBN watch last moments of airtime after ordered to cease operations

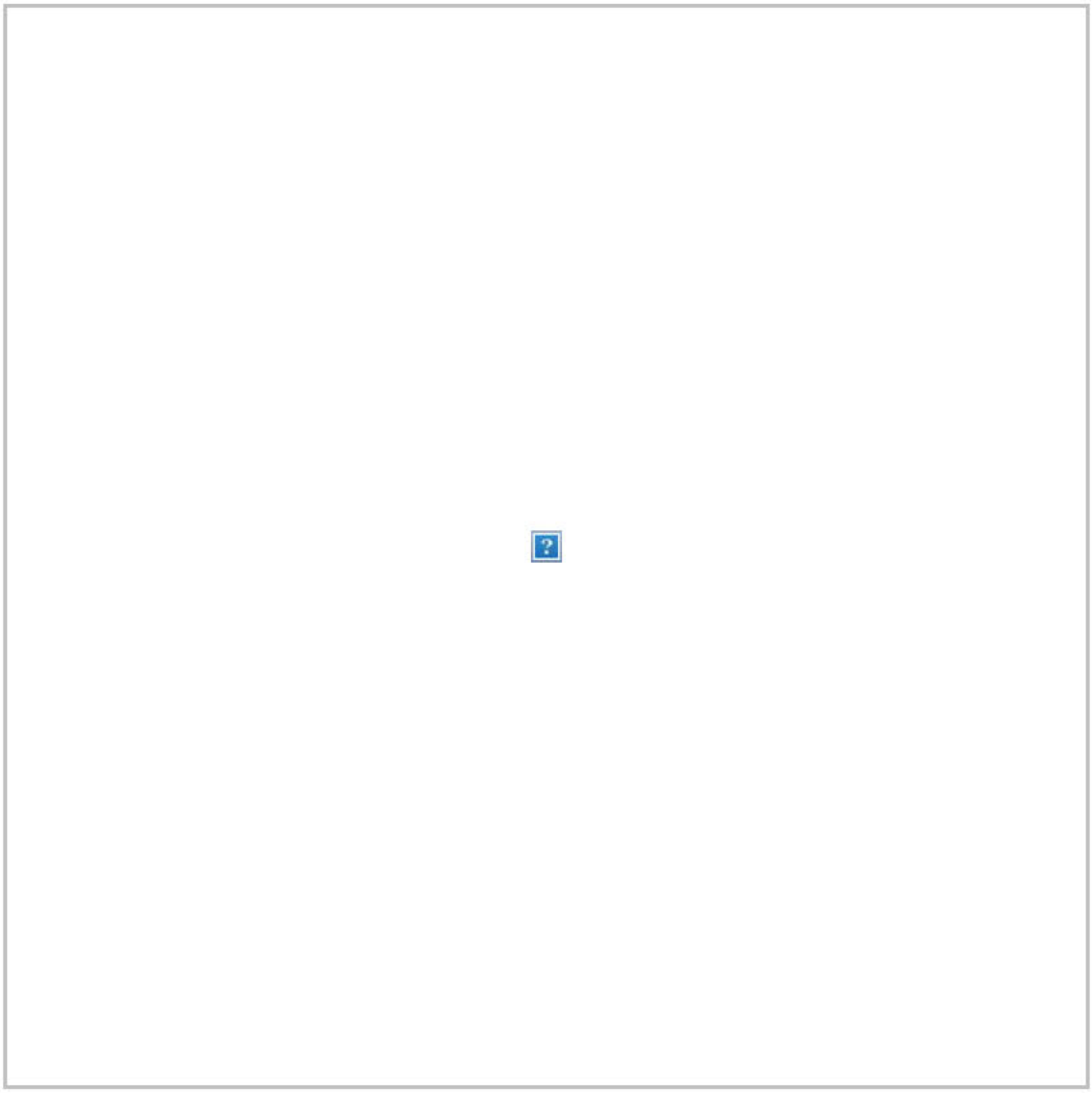
ABS-CBN, the Philippines' largest network, ceased operations May 5 after President Rodrigo Duterte's allies in congress refused to renew the station's license. (Nick Villavecer via Storyful)

President Rodrigo Duterte has repeatedly threatened to close down the

network in the past. His office denied that he had a hand in the order, saying the decision was entirely up to the commission.

“ABS-CBN is free to exhaust all legal remedies available to it,” said presidential spokesperson Harry Roque. Duterte “accepted the apology of the network and left its fate to both houses of Congress,” he added.

Duterte and his allies have accused ABS-CBN of not carrying his advertisements during the 2016 election campaign, instead airing those of his opponents. The network’s president, Carlo Katigbak, apologized to Duterte in February, clarifying the operations surrounding how the advertisements were aired.



Intel chief nominee says he won't be swayed by politics

Rep. John Ratcliffe, President Donald Trump's nominee to be director of national intelligence, pledged at his confirmation hearing Tuesday to deliver intelligence free of bias or political influence, even as skeptical Democrats repeatedly pressed the Texas Republican on whether he could stand up to the president and defend the agencies he would oversee.

The comments from Ratcliffe were aimed at quelling concerns that the ardent Trump loyalist would be swayed by political pressure from a president who has been openly dismissive of the government's spy agencies and once derided them as being "run amok."

The confirmation hearing, the first in-person one held under drastic new distancing rules to protect Capitol Hill from the coronavirus, comes as Trump faces persistent criticism for politicizing intelligence issues. It's also been a tumultuous time: At least a half dozen intelligence leaders have been replaced over the last year and agencies already confronting the threat of Russian interference in November's election are now investigating the politically charged question of whether the coronavirus pandemic originated in a Chinese market or a laboratory.

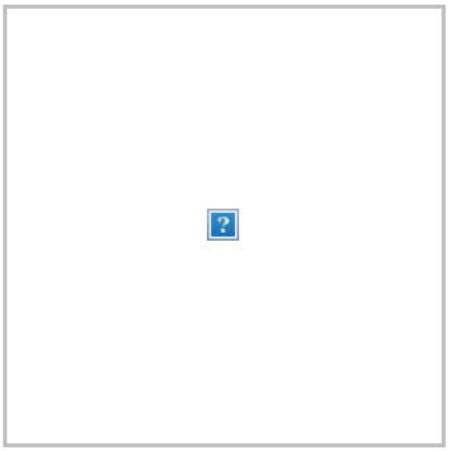
Ratcliffe's path to the job has been similarly topsy-turvy, with the original nomination withdrawn after bipartisan criticism that one of the president's most ardent defenders during the Russia investigations and Trump's impeachment was unqualified to oversee 17 U.S. spy agencies. Trump unexpectedly renominated him in February. His chances of securing the job appear better, but confirmation is not guaranteed.

Democrats laid bare their skepticism in occasionally contentious questioning, with Sen. Dianne Feinstein of California pressing him over past comments about whistleblowers and New Mexico Sen. Martin Heinrich asking for instances of when Ratcliffe had ever "spoken truth to power," particularly involving the president.

"I have to say that while I am willing to give you the benefit of the doubt at this hearing, I don't see what has changed since last summer when the president decided not to proceed with your nomination," said Virginia Sen. Mark Warner, the panel's top Democrat.

Ratcliffe took pains to break with the president, saying he did not know what Trump meant last summer when he said intelligence agencies had "run amok."

He refused to endorse Trump's assertion of a "deep state" inside the intelligence community and insisted that he would not shade intelligence findings to meet the desires of anyone, including the president.



Feds arrest 2 men in first fraud case involving PPP loan program for small businesses hurt by coronavirus

Two New England businessmen have been charged with illegally trying to procure hundreds of thousands of dollars in federal Paycheck Protection Program loans, the first fraud case in the nation involving the massive effort to rescue small businesses from the coronavirus crisis.

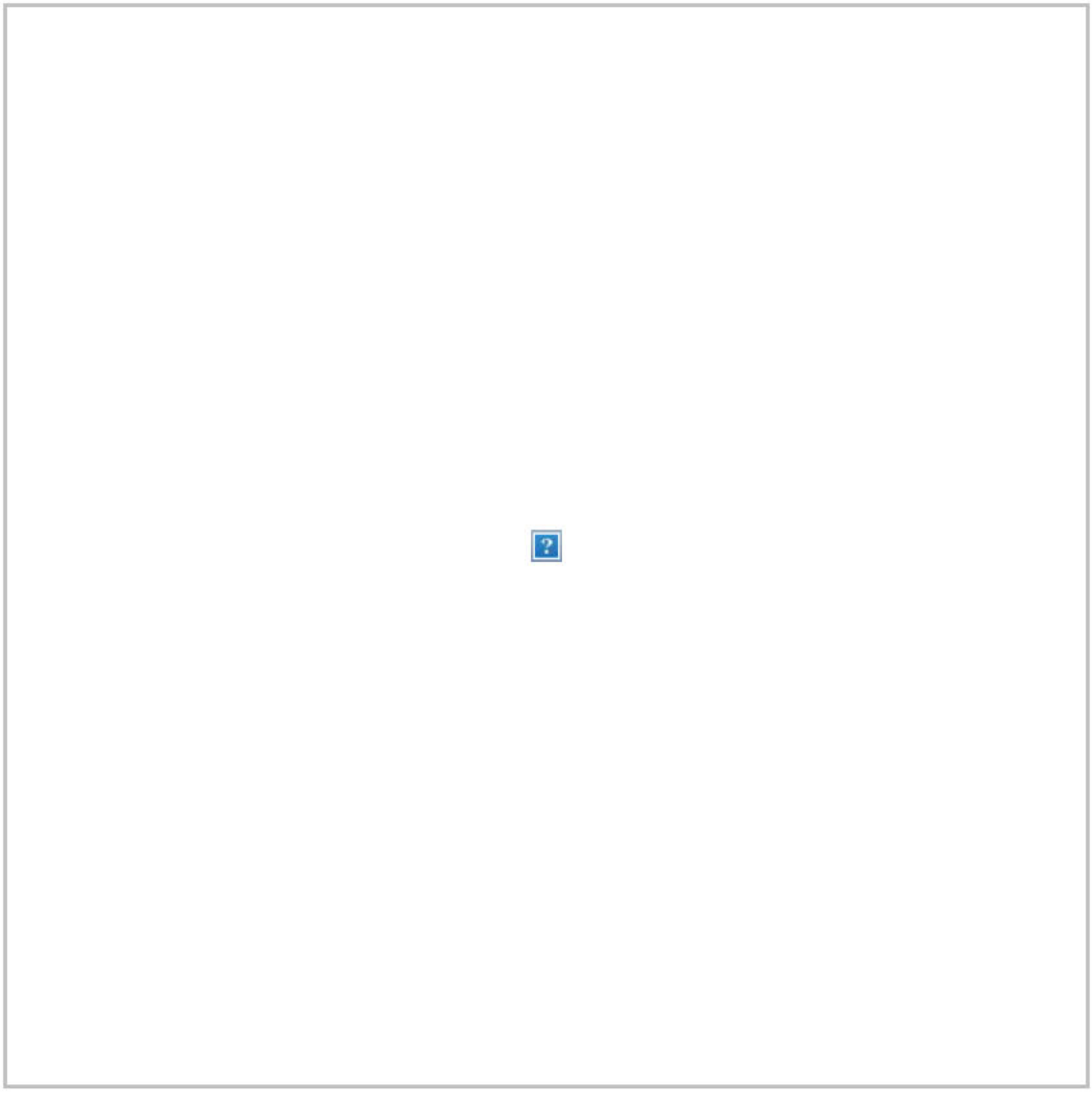
And the chief of the U.S. Justice Department's Criminal Division said he expects more cases in the future. Tuesday's case, filed in Rhode Island, is the first of several investigations launched by federal authorities since the start of the massive program, he said.

"What we see coming out of Rhode Island is what's happening across the country," Assistant Attorney General Brian A. Benczkowski, told USA TODAY. "We have a lot of leads."

On Tuesday, prosecutors charged David A. Staveley, 52, of Andover, Massachusetts, and David Butziger, 51, of Warwick, Rhode Island, with conspiring to seek forgivable loans guaranteed by the Small Business Administration. The loans amounted to nearly $544,000, according to the U.S. Department of Justice.

They claimed to have dozens of employees earning wages at four different entities when, in fact, there were no employees working for any of the

businesses, according to a DOJ news release issued Tuesday.Congress created the PPP in March as part of the CARES Act, the federal response to the COVID-19 pandemic, which has forced social distancing steps that have forced millions of small businesses to contract or close entirely. They have allocated more than $660 billion for the program, which has approved loans for some 4 million businesses.



Michigan man arrested after wiping face on store clerk who told him to wear a mask, police say

A 68-year-old Michigan man is expected to face charges after he was captured

on surveillance video wiping his nose and face on a Dollar Tree employee's sleeve rather than wear a mask.

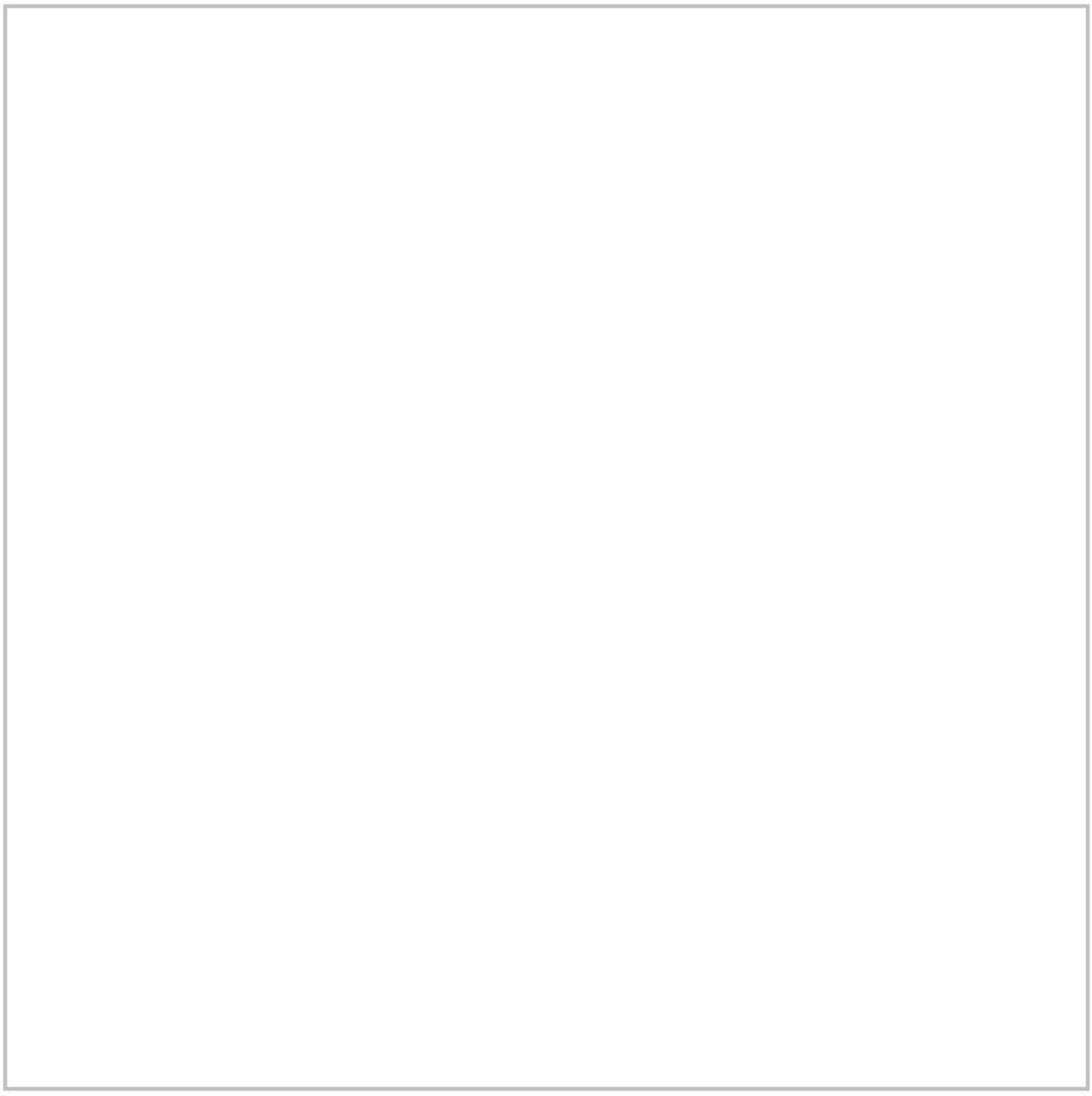
Police said they were tipped off to the identity of the Linden, Michigan, man by a viewer who saw the footage, and the case has been referred to the Oakland County Prosecutor's Office for charges.

The incident happened at 1:30 p.m. local time Saturday at the store in Holly, Michigan, and was captured on surveillance footage.

According to the Holly Police Department, the suspect walked past door signs indicating all customers entering the store were required to wear a face mask and reacted when a young female clerk reminded him of the new store policy.

"Here, I will just use this as a mask," the suspect said as he wiped his face on the clerk's sleeve.

Police said the man continued to be loud and disruptive inside the store before leaving in a white van.



Hand sanitizer is still considered contraband in some prisons around the country

When a half-dozen inmates reported in for their prison jobs in Nebraska in late March, they found themselves with a new assignment: turning vats of ethanol into 2,500 gallons of coronavirus-killing hand sanitizer, for a wage of $1.08 an hour.

But while their work has helped the state government stave off a sanitizer shortage, the inmates on the production line -- and more than 5,000 others in prisons around Nebraska -- are banned from using the hand gel they helped make, according to the state corrections department.

They're not alone. Even as correctional facilities have emerged as some of the country's largest sources of coronavirus outbreaks, hand sanitizer is still

considered contraband in all federal prisons as well as state prisons in more than a dozen states, a CNN review of department policies found.

"They have the capability to protect us, but they are failing to do it," Ryan Kubik, an inmate at the Nebraska State Penitentiary, told CNN. He said he was "scared to death" of catching the virus in his overcrowded prison. "People are going to die in here."

Hand sanitizer has long been banned in most prisons due to its alcohol content, based on fears that inmates would drink it or use it to start fires. But during the pandemic, the Centers for Disease Control and Prevention has recommended that correctional facilities "consider relaxing restrictions" on alcohol-based sanitizer "where security concerns allow." A CDC spokesperson said that the extent to which the rules could be relaxed "will depend on the security level of the facility and other aspects of the operational environment."

Many states have followed the advice: At least 30 corrections departments are allowing inmates to use alcohol-based hand sanitizer, either letting prisoners have their own bottles or dispensing it to them in a more controlled method. Most had banned the substance before the pandemic broke out.

But 17 state corrections departments -- including six of the 10 with the largest inmate populations -- said they were maintaining their bans for now, many arguing that the alcohol in sanitizer made it a safety risk. And inmates in federal prisons around the country are also prohibited from using hand sanitizer, the federal Bureau of Prisons said in a statement.



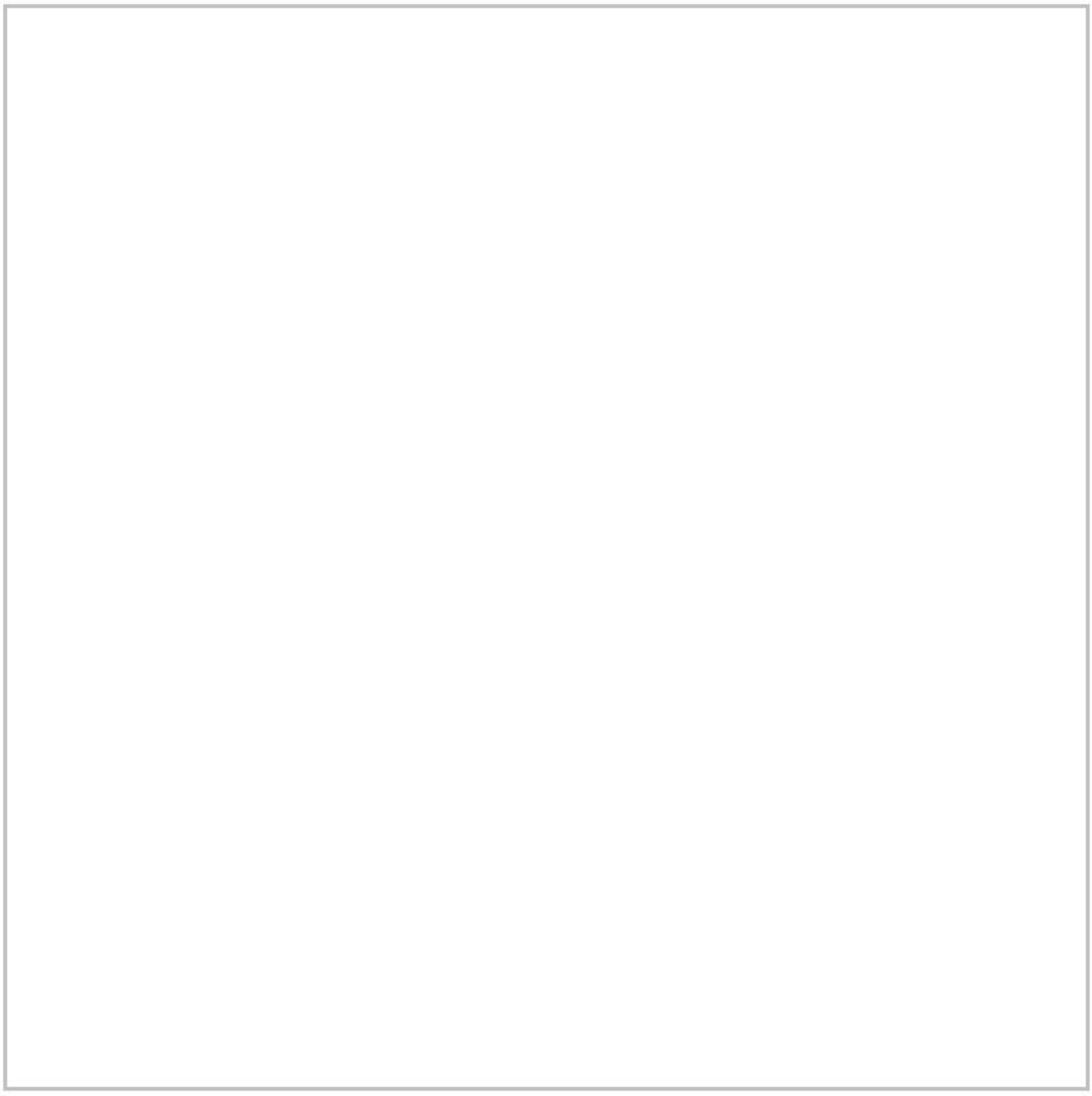
Venezuela’s Maduro says two Americans captured in failed invasion attempt

President Nicolás Maduro said his government had captured two American “mercenaries” Monday in a murky operation allegedly intended to infiltrate Venezuela, incite rebellion and apprehend its leaders, adding a fresh

complication to escalating tensions between Washington and Caracas. The socialist leader said the plan was to kill him.

In a lengthy speech Monday night, Maduro decried an ongoing “terrorist” assault on Venezuela that he said had led him to dispatch 25,000 reservists to the coasts. He displayed images that apparently depicted the two apprehended Americans in a lineup, one of them forced to lower his head by a captor.U.S. officials and the mainstream Venezuelan opposition headed by Juan Guaidó have strongly denied any connection with the operation, which allegedly involved several dozen men, most of them defectors from the Venezuelan military who had been living hand-to-mouth in camps in Colombia. Former Venezuelan National Guard officer Javier Nieto Quintero and former U.S. Army Green Beret Jordan Goudreau, head of a Florida company that says it offers paid strategic security services, released a video Sunday announcing the start of “Operation Gideon” and calling on Venezuelan soldiers to join them.

Goudreau, in an interview with The Washington Post, confirmed that two Americans in what he says was a force of about 60 men were captured Monday along with six Venezuelans. He identified the Americans as Airan Berry and Luke Denman. Also captured was one of the operation’s leaders, former Capt. Antonio Sequea.The Americans, Goudreau said, were fellow former Special Forces members he had known for years who had joined the operation as “supervisors.” He said he has engaged a lawyer in Venezuela and was reaching out to the State Department to try to secure their release.



FBI: Cyber crimes on the rise during coronavirus pandemic

The Federal Bureau of Investigation wants you to be careful when you go online: The agency says cyber crimes are on the rise in the time of COVID-19.
“It’s really too early to tell the exact numbers but I can assure you the trend is up,” said FBI Public Affairs Officer Don Wood.
Wood told 7News cyber criminals have tailored some traps to trick those thinking about the coronavirus pandemic.
“People will be looking for more information on coronavirus,” he said. “They may be sent a fraudulent link to the CDC website.”
That fake CDC website could then prompt visitors into clicking more links. For example, it could offer free personal protective equipment just by following a

link.

“Once you click the link, you could be downloading a virus,” Wood said. “You’ll definitely be taken to a site that is not legitimate that has its purpose set up to get your personal information and financial information.”

That is just one example.

A more classic scam that is still tricking many Americans is the email extortion scam. These emails will threaten the recipient to pay a sum of money or run the risk of the sender leaking compromising photos, personal data or financial information.

“They’re blackmailing you over the internet,” Wood said.

There is good news, though. All of these crimes are preventable if you remain cautious, Wood said. He provided some tips to protect yourself from online criminals:

Do not download email attachments from senders whom you do not recognize.

Do not follow links sent to you from senders you do not recognize.

Be cautious about offers for free services. If it sounds too good to be true, it likely is.

Update your computer regularly.

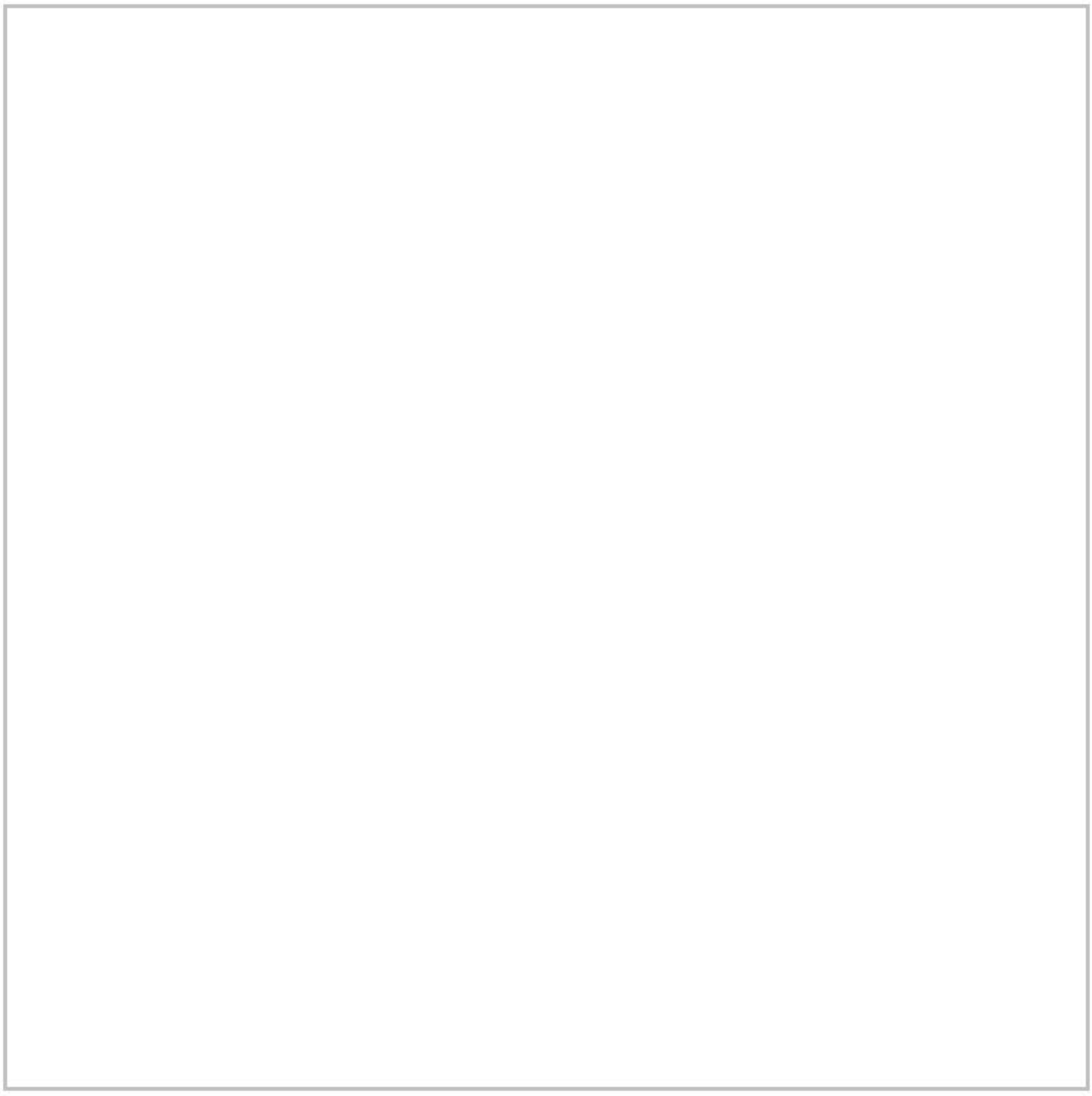
Update your computer’s security software regularly.

Do not use the same password for multiple accounts or websites.

Change passwords frequently.

Change your Wi-Fi’s password semi-frequently.

Monitor your bank statements for suspicious activity.



Suspect Drops Nearly $1M in Cash on Road During California Vehicle Pursuit

Nearly $1 million in cash was dropped on the side of the road during a vehicle pursuit Friday in Merced County, according to the California Highway Patrol.

At about 6:26 p.m. an officer, who was traveling with his K-9 ‘Beny,’ observed three SUVs that appeared to be traveling together on northbound Interstate 5 near Highway 165, just south of Los Banos, according to CHP Officer Eric Zuniga.

When the officer attempted to make an enforcement stop on one of the vehicles — a black 2020 Chevrolet Suburban — the vehicle failed to yield and attempted to flee, the CHP said.

The officer pursued the vehicle southbound on I-5 to the area of Nees Avenue.

The pursuit then headed northbound and ended near the John Erreca Rest Area, according to the CHP.

As the officer pursued the vehicle, one of the other SUVs, a black Ford Expedition, attempted to block the officer's vehicle by straddling the lanes. Authorities said the officer was able to out-maneuver the Expedition and continued the pursuit with the Suburban. The CHP said the driver of the Suburban stopped on the right shoulder of the road during the pursuit, exited the vehicle and dropped two cardboard boxes before returning to the vehicle and continuing to flee from authorities.

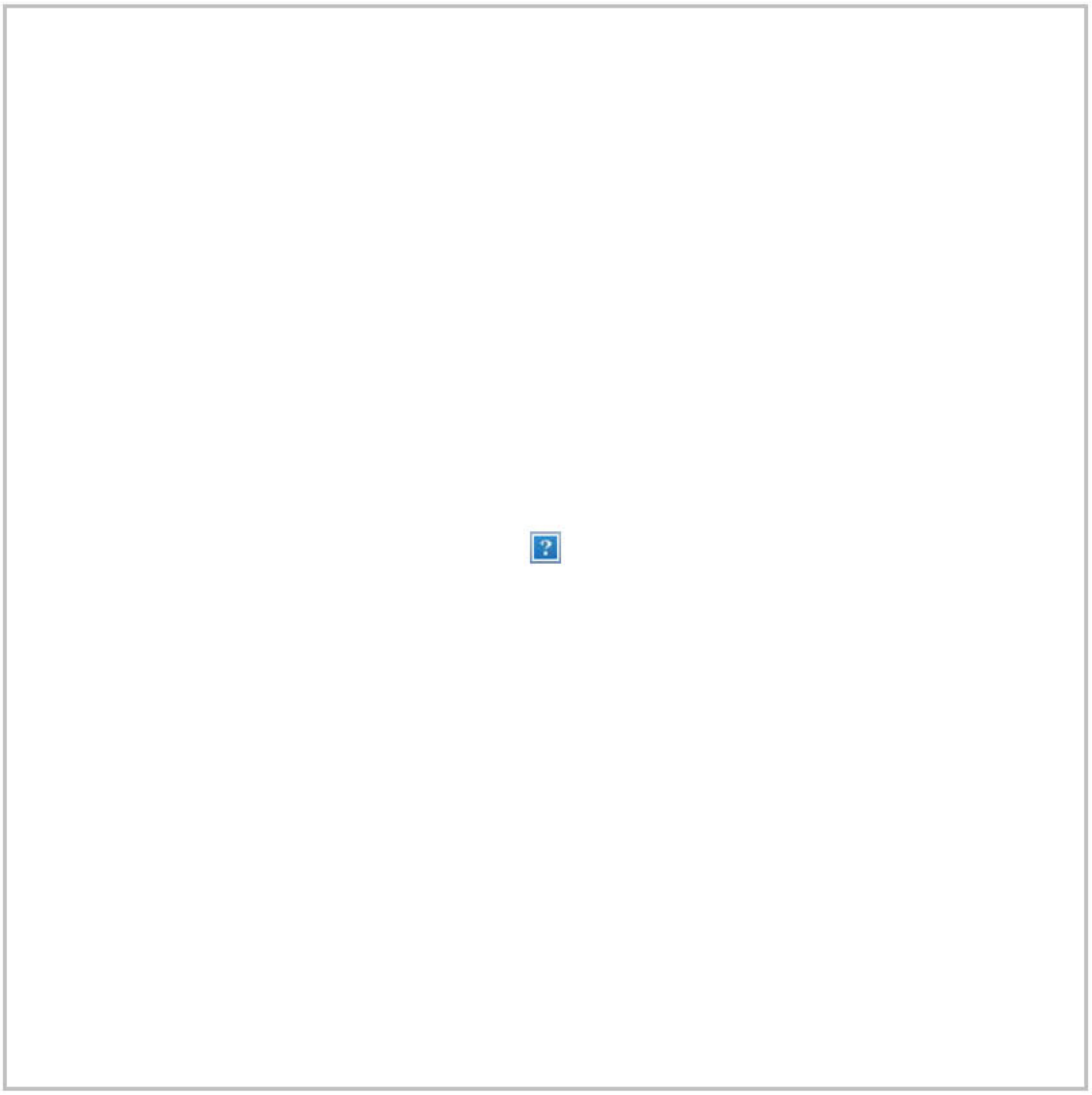
The driver of the Suburban then stopped the vehicle and surrendered to authorities shortly after dropping the boxes. The driver of the third SUV — a black Chevrolet Tahoe — stopped the vehicle in traffic. Both drivers were taken into custody.

Authorities identified the driver of the Suburban as Frank Capraro, 23, of Medford, New York and the driver of the Tahoe as Desmond McDay, 25, also from Medford, New York.

Authorities said the driver of the Ford changed directions during the pursuit and was not located.

The CHP said the Merced Communications Center received several calls during the incident regarding the cardboard boxes dropped on the shoulder of the road.

Officers retrieved the boxes and located about $915,000 cash. Officers also located walkie talkies in the suspect vehicles. It was later determined the three drivers were using them to communicate during the pursuit



Layoffs widen rift between police chief, administration

While council met Monday night, Mayor Greg Bricker took the opportunity to distribute a lengthy letter, expressing his displeasure with the city's police chief. At a Finance Committee meeting last week, Police Chief John Lane suggested that committee members look at some different cost-cutting measures than laying off the two lowest ranking patrolmen in the department.

Last month, Safety Service Director David Dawson had hand delivered layoff notices to Jay Lane, the chief's son, and Hunter Maze. Both men were the department's last hires.

Chief Lane had passed along a suggestion from the Fraternal Order Of Police that offering senior ranking officers buyouts, especially if they are contemplating

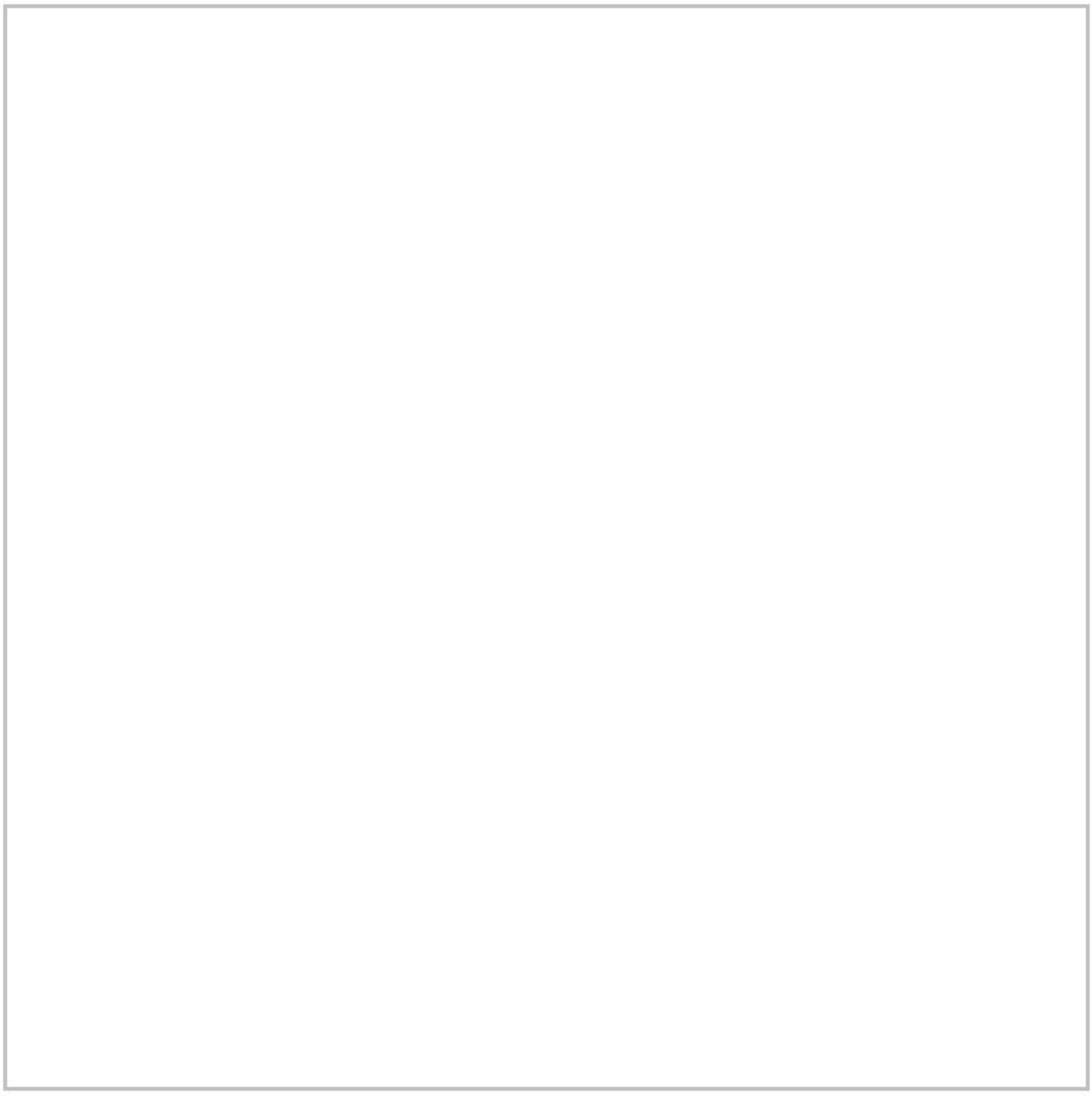
retirement anyway, can generate more savings than laying off lower level patrolmen.

This statement inadvertently offended many officers and their friends and family, who might be eligible for such a buyout, Chief Lane said Monday night before offering apologies to those who felt wronged.

However, it was the letter from Bricker that detailed so-called offenses from the chief, although the source of the information is not specified.

Mayor Bricker talks about the first months of his tenure and how he had organized regular meetings with department heads *"to understand current priorities and develop a strategic plan,"* especially since the city faces a deficit of $420,000 and a half million dollar debt to its health care provider. He anticipates that deficit will only grow due to tax losses stemming from the coronavirus pandemic.

In his letter, Bricker not only alleges that Chief Lane has "not been active in providing updates and implementing important initiatives (beyond purchase of additional cruisers), the mayor also details the poor morale in his department.



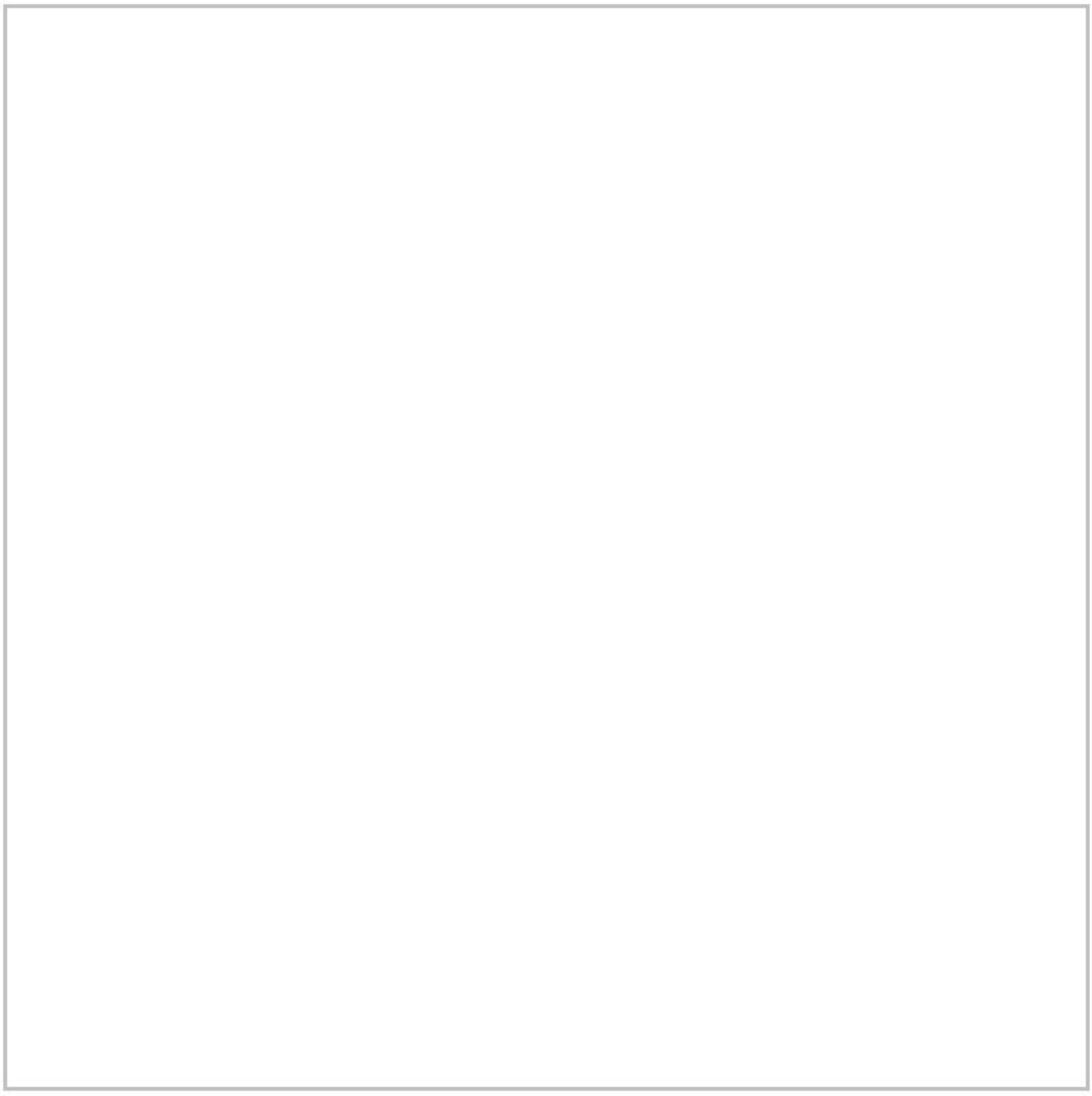
Courts Issue Rulings in Two Cases Challenging Law Enforcement Searches of License Plate Databases

This week, the Ninth Circuit Court of Appeals issued an opinion in *United States v. Yang*, a case challenging the search of an automated license plate reader database under the Fourth Amendment. Although the court, citing EFF's amicus brief, recognized ALPRs capture massive amounts of data on Americans across the country, it decided not to reach the search issue. Instead it held that because Yang was driving a rental car after his rental agreement ended when the search occurred, he didn't have the right to challenge the search.

The Ninth Circuit's decision follows an April opinion from Massachusetts's

highest court in another ALPR case, *Commonwealth v. McCarthy*. In *McCarthy*, the court held that, although ALPRs raise clear privacy issues under the Fourth Amendment and Massachusetts's Article 14, McCarthy hadn't introduced sufficient facts to show that the search at issue in his case rose to the level of a constitutional violation.

ALPRs are high-speed, computer-controlled camera systems that are attached to vehicles, such as police cars, or can be mounted on street poles, highway overpasses, or mobile trailers. Some models can photograph up to 1,800 license plates every minute, and every week, law enforcement agencies across the country use these cameras to collect data on millions of vehicles. The plate numbers, together with location, date, and time information, are uploaded to central servers, and made instantly available to other agencies. The location data generated by ALPRs is so precise it can place a vehicle in front of a specific home or business, as was the case in *Yang*, or within a specific lane on a bridge, as in *McCarthy*. Law enforcement agencies may maintain their own databases of ALPR data or store their data with private companies. In the *Yang* case, the law enforcement agency didn't collect its own ALPR data but instead accessed a commercial database that advertises it contains 6.5 billion plates collected both by law enforcement and by private contractors.



National Correctional Officers Week being observed through May 9

A tradition begun 36 years ago continues this week with the observation of the first full week of May (May 3-9) as National Correctional Officers Week.

This is done in recognition of the important role these officers play in our criminal justice system, the Genesee County Sheriff's Office said in a press release.

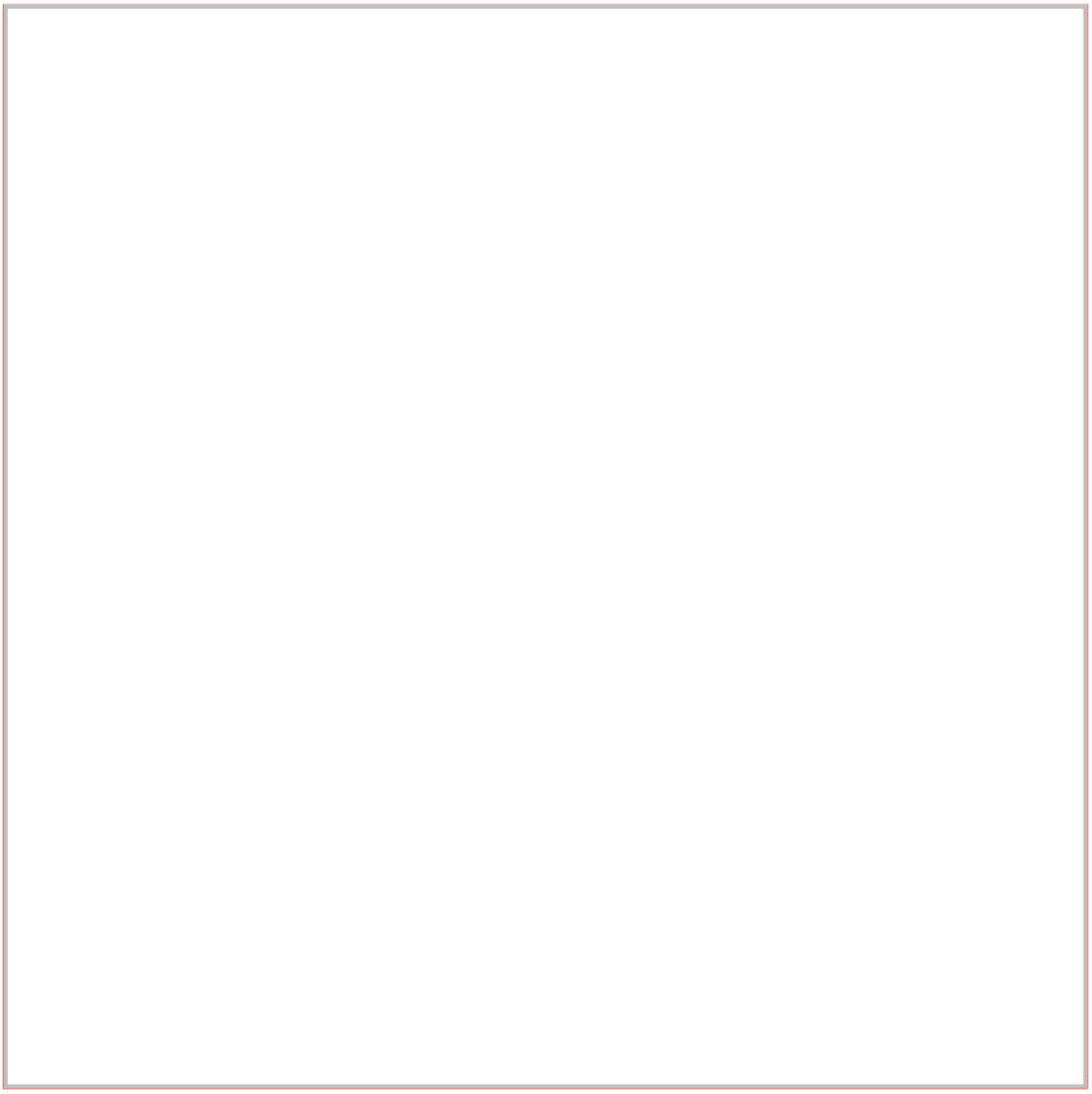
The position of correctional officer, once considered merely that of a "guard," has become increasingly more complex and demanding, involving simultaneously custodial, supervisory, rehabilitation, and counseling roles, and that complexity continues to grow, said Sheriff William A. Sheron Jr. He said

today, the officers continue to play that role in an ever-more-stressful environment due to the current COVID-19 pandemic sweeping the nation and the world.

“This week acknowledges the difficult job correction officers perform, locked within a facility for a large part of their day where they must securely, safely and humanely keep those committed to the jail, respecting the rights and dignity of all the inmates, including those who have been found guilty and those only awaiting adjudication,” Sheron said.

During the April 22 county Legislature meeting, Sheron and legislators recognized correction officers for their continued dedication, professionalism and commitment to public service. The Genesee County Legislature issued a proclamation recognizing May 3-9 as National Correctional Officers’ Week. The lights on the Old County Courthouse cupola have been changed to red, white and blue to acknowledge this week.

“The important and difficult role correctional officers fulfill is not always recognized by the general public,” said Sheron. “If you know a Correctional Officer, please join me in thanking these men and women for their exceptional service.”



The Law Enforcement News of the Day is a compilation of daily news articles selected from thousands of sources by the editors of Ness & Associates. Ness & Associates are not liable for the use of or reliance on any information contained in these articles. The presence of advertising does not endorse, nor imply endorsement of, any products or services by Ness & Associates.

Copyright © 2020 Ness & Associates

Have an interesting article you would like to share? email jness23@cox.net

Copyright © 2020 Ness Associates, All rights reserved.
You are receiving this email because you opted in via our website.

Our mailing address is:
Ness Associates
9241 E Grandview St
Mesa, AZ 85207-4318

Add us to your address book

Want to change how you receive these emails?
You can update your preferences or unsubscribe from this list.

From: Quinn, Dermot (POL)
To: Scott, Michael (POL); Wilcox, Christopher (POL); McCarthy, Steven (POL); Egnitz, Brian (POL); Warren, Rosemary (POL); OToole, Kevin (POL)
Subject: GoToMeeting Invitation - Westchester County PD ALPR

Westchester County PD ALPR
Tue, Oct 13, 2020 3:00 PM - 4:00 PM (EDT)

Please join my meeting from your computer, tablet or smartphone.

https://global.gotomeeting.com/join/336430861

You can also dial in using your phone.
(For supported devices, tap a one-touch number below to join instantly.)

United States: +1 (646) 749-3122
- One-touch: tel:+16467493122,,336430861# <tel:+16467493122,,336430861>

Access Code: 336-430-861

New to GoToMeeting? Get the app now and be ready when your first meeting starts: https://global.gotomeeting.com/install/336430861

From: Motorola Solutions
To: McCarthy, Steven (POL)
Subject: Grant Information: 2020 Byrne JAG
Date: Thursday, July 23, 2020 12:24:32 PM

FY20 $75.3 Million in Funds Available
View Online

$75.3M AVAILABLE FOR LAW ENFORCEMENT & TECH PROGRAMS

APPLY BY AUGUST 19

banner

For decades, the Byrne Justice Assistance Grant (JAG) program has funded key law enforcement initiatives allowing agencies to reduce crime and enhance citizen safety. The Bureau of Justice Assistance recently released its 2020 Byrne JAG solicitation. These funds can be used to invest in technologies that promote officer and community safety including mission-critical communications equipment, digital evidence solutions, public safety software, video security and analytics solutions, ALPR, and more.

FREE GRANT ASSISTANCE

Many Motorola Solutions products and solutions qualify for grant funding, but the grant application can be challenging to navigate. To help you, we've partnered with the grant experts at **PoliceGrantsHelp**. Their team can help answer your questions and offer insights on how to write an effective application.

2020 BYRNE JAG OVERVIEW

solution guide

DOWNLOAD NOW

MOTOROLA SOLUTIONS GRANT ASSISTANCE PROGRAM

grant assistance

Even if this grant is not a fit for your agency, the grant experts at **PoliceGrantsHelp** can help identify upcoming funding opportunities for which you may qualify.

DON'T DELAY: APPLICATIONS ARE DUE AUGUST 19

FREE GRANT HELP

DOWNLOAD OVERVIEW

Read and Subscribe to our Blog >

Follow Us:

Motorola Solutions values your privacy. See our Privacy Policy and Terms of Use. You can manage your communication preferences or unsubscribe at any time. You may also write to Motorola Solutions, Inc., Attention: Privacy Compliance Program, 500 W. Monroe, Chicago, IL USA 60661 or email privacy1@motorolasolutions.com.

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license.All other trademarks are the property of their respective owners. © 2020 Motorola Solutions, Inc. All rights reserved.

From: WatchGuard
To: McCarthy, Steven (POL)
Subject: IADLEST Certified Course: License Plate Recognition Technology & Best Practices
Date: Thursday, August 6, 2020 4:06:23 PM

Not rendering correctly? View this email as a web page here.

ALPR_4RE_WatchGuard_2_561x257

IADLEST Certified Course

License Plate Recognition Technology & Best Practices

Learn about the diverse uses of License Plate Recognition (LPR) technology and how to utilize the tool in real world scenarios. Led by former law enforcement members, this course will demonstrate how to integrate a cloud-based commercial LPR data platform into the existing traditional law enforcement deployment LPR model.

Session Dates and Times

08/11/2020 12-2:00PM CDT

08/18/2020 12-2:00PM CDT
08/25/2020 12-2:00PM CDT
09/01/2020 12-2:00PM CDT



- Week 1: Introduction, walk-through, take-home work
- Week 2: Week 1 overview – exam, legal aspects, Best Practices, advanced tools walk-through, take-home work
- Week 3: Week 2 overview – exam, hot lists, hot list advanced tools walk-through, take-home work
- Week 4: Week 3 overview – exam, LPR databases, investigative resources, documenting, additional tools/functions, full case walk-through, final LPR exam

This four part series will be taught in 2 hour blocks every Tuesday beginning August 11th to September 1st from 10AM PST – 12PM PST. As an IADLEST certified course, you must attend all four courses to receive course credit. See the Registration Page for more details.

WatchGuard Video
415 E Exchange Parkway
Allen, TX 75002
USA

You received this email because you are subscribed to Products from WatchGuard Video.

Update your email preferences to choose the types of emails you receive.

Unsubscribe from all future emails

From: PoliceGrantsHelp eNews
To: Irwin, Patrick (POL)
Subject: Impact of marijuana legalization on grants; 3 steps to the perfect grant application
Date: Tuesday, October 20, 2020 3:24:59 PM

October 20, 2020 | View as webpage

Dear PoliceGrantsHelp Member,

In this month's eNews, we look at the impact of marijuana legalization on grants that stem from marijuana sales. This article is part of Police1's analysis of a recent survey on policing in an era of legal marijuana.

Now is the time to start planning your 2021 grant projects and applications. Don't let the complex and sometimes difficult application process intimidate your efforts. Contact the grant experts at PoliceGrantsHelp for assistance writing and preparing your grant application. Contract for grant writing services in October and receive a full year subscription of GrantFinder – an online searchable database of federal, state, foundation and corporate grants available to your community.

— *The PoliceGrantsHelp Team*

FEATURED CONTENT

The impact of legalizing marijuana: Utilizing grant funding to support youth programs

By PoliceGrantsHelp Staff

Grants that stem from marijuana sales consist of an array of programs

GET GRANT ASSISTANCE

PoliceGrantsHelp offers customized grant assistance in several categories. Click on the links below to access free grant services including: research, consulting and application assistance.

- AEDs
- All Terrain Vehicles
- Armored Vehicles
- Boats
- Body Cameras
- CAD
- Citation Management
- Crime Analysis and Investigation Software
- Drones
- Drug and Alcohol Testing
- Evidence Management
- Explosives Detection
- Firearms Training
- Forensic 3D Laser Scanners
- In Car Video
- Less Lethal
- License Plate Readers
- Mobile Command Centers
- NG911
- Narcotics Identification
- Network Solutions
- Officer Wellness
- Online Training
- Personal Protective Equipment - PPE
- RMS
- Radiation Detection
- Radio Systems
- Radios
- Rapid DNA Analysis
- Risk Management
- Rugged Computers
- Specialty Vehicles
- Training Simulation
- Video Surveillance

ALL GRANTS HELP

Start Planning Your 2021 Grant Applications

Submitting a successful application requires a lot of resources and planning. Don't know where to start? Contact PoliceGrantsHelp for assistance writing and preparing your grant applications.

Get started today

Get Help With Grant Funding for Leica Geosystems

Leica Geosystems has partnered with the PoliceGrantsHelp team to offer free grant assistance for forensic 3D laser scanners.

Get free grant help

OTHER HIGHLIGHTS

3 easy steps to write the perfect grant application

By Linda Gilbertson

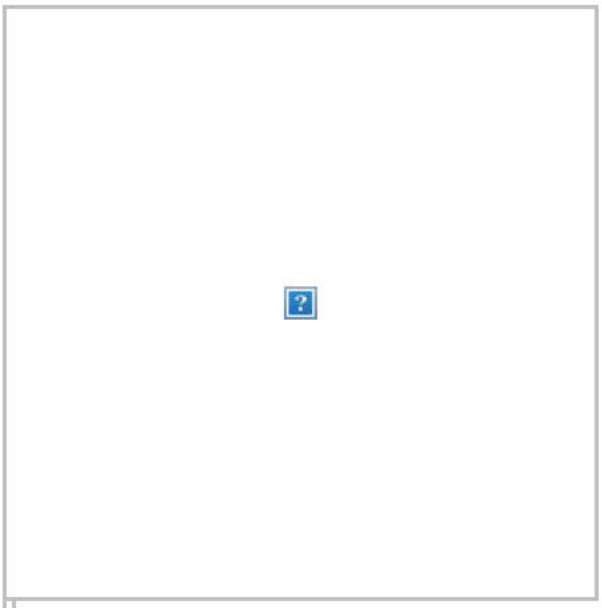
The good news is that you can, in fact, write a pretty great grant application if you apply yourself

A 7-Step Guide to Public Safety Grant Writing



At Lexipol, we've developed an easy-to-follow process to get you up to speed on the basics of identifying, applying for and securing public safety grants.

Download eBook



UPCOMING GRANTS

Grant	Grant Deadline
Combating Opioid Overdose though Community-level Intervention (Maryland)	11/2/2020
Child Sexual Abuse Treatment (CS) Program (California)	11/3/2020
Title II Formula Grant Program (Indiana)	11/4/2020
Neotropical Migratory Bird Conservation Act Grant (NMBCA)	11/5/2020
Community Violence Prevention/Reduction Grant Program (Pennsylvania)	11/10/2020
S.T.O.P. Violence Against Women Grant (VAWA Kansas)	11/10/2020

Interested in finding more grant opportunities?

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: PoliceGrantsHelp eNews
To: Ramsland, Erik (POL)
Subject: Impact of marijuana legalization on grants; 3 steps to the perfect grant application
Date: Tuesday, October 20, 2020 3:15:13 PM

October 20, 2020 | View as webpage

Dear PoliceGrantsHelp Member,

In this month's eNews, we look at the impact of marijuana legalization on grants that stem from marijuana sales. This article is part of Police1's analysis of a recent survey on policing in an era of legal marijuana.

Now is the time to start planning your 2021 grant projects and applications. Don't let the complex and sometimes difficult application process intimidate your efforts. Contact the grant experts at PoliceGrantsHelp for assistance writing and preparing your grant application. Contract for grant writing services in October and receive a full year subscription of GrantFinder – an online searchable database of federal, state, foundation and corporate grants available to your community.

— *The PoliceGrantsHelp Team*

FEATURED CONTENT

The impact of legalizing marijuana: Utilizing grant funding to support youth programs

By PoliceGrantsHelp Staff

Grants that stem from marijuana sales consist of an array of programs

GET GRANT ASSISTANCE

PoliceGrantsHelp offers customized grant assistance in several categories. Click on the links below to access free grant services including: research, consulting and application assistance.

- AEDs
- All Terrain Vehicles
- Armored Vehicles
- Boats
- Body Cameras
- CAD
- Citation Management
- Crime Analysis and Investigation Software
- Drones
- Drug and Alcohol Testing
- Evidence Management
- Explosives Detection
- Firearms Training
- Forensic 3D Laser Scanners
- In Car Video
- Less Lethal
- License Plate Readers
- Mobile Command Centers
- NG911
- Narcotics Identification
- Network Solutions
- Officer Wellness
- Online Training
- Personal Protective Equipment - PPE
- RMS
- Radiation Detection
- Radio Systems
- Radios
- Rapid DNA Analysis
- Risk Management
- Rugged Computers
- Specialty Vehicles
- Training Simulation
- Video Surveillance

ALL GRANTS HELP

Start Planning Your 2021 Grant Applications

Submitting a successful application requires a lot of resources and planning. Don't know where to start? Contact PoliceGrantsHelp for assistance writing and preparing your grant applications.

Get started today

Get Help With Grant Funding for Leica Geosystems

Leica Geosystems has partnered with the PoliceGrantsHelp team to offer free grant assistance for forensic 3D laser scanners.

Get free grant help

OTHER HIGHLIGHTS

3 easy steps to write the perfect grant application

By Linda Gilbertson

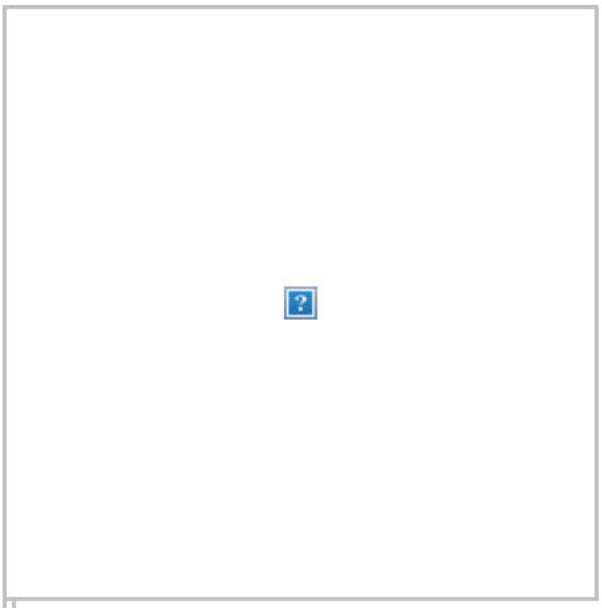
The good news is that you can, in fact, write a pretty great grant application if you apply yourself

A 7-Step Guide to Public Safety Grant Writing



At Lexipol, we've developed an easy-to-follow process to get you up to speed on the basics of identifying, applying for and securing public safety grants.

Download eBook



UPCOMING GRANTS

Grant	Grant Deadline
Combating Opioid Overdose though Community-level Intervention (Maryland)	11/2/2020
Child Sexual Abuse Treatment (CS) Program (California)	11/3/2020
Title II Formula Grant Program (Indiana)	11/4/2020
Neotropical Migratory Bird Conservation Act Grant (NMBCA)	11/5/2020
Community Violence Prevention/Reduction Grant Program (Pennsylvania)	11/10/2020
S.T.O.P. Violence Against Women Grant (VAWA Kansas)	11/10/2020

Interested in finding more grant opportunities?

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: PoliceGrantsHelp eNews
To: Cronin, John E (POL)
Subject: Impact of marijuana legalization on grants; 3 steps to the perfect grant application
Date: Tuesday, October 20, 2020 3:05:51 PM

October 20, 2020 | View as webpage

Dear PoliceGrantsHelp Member,

In this month's eNews, we look at the impact of marijuana legalization on grants that stem from marijuana sales. This article is part of Police1's analysis of a recent survey on policing in an era of legal marijuana.

Now is the time to start planning your 2021 grant projects and applications. Don't let the complex and sometimes difficult application process intimidate your efforts. Contact the grant experts at PoliceGrantsHelp for assistance writing and preparing your grant application. Contract for grant writing services in October and receive a full year subscription of GrantFinder – an online searchable database of federal, state, foundation and corporate grants available to your community.

— *The PoliceGrantsHelp Team*

FEATURED CONTENT

The impact of legalizing marijuana: Utilizing grant funding to support youth programs

By PoliceGrantsHelp Staff

Grants that stem from marijuana sales consist of an array of programs

GET GRANT ASSISTANCE

PoliceGrantsHelp offers customized grant assistance in several categories. Click on the links below to access free grant services including: research, consulting and application assistance.

- AEDs
- All Terrain Vehicles
- Armored Vehicles
- Boats
- Body Cameras
- CAD
- Citation Management
- Crime Analysis and Investigation Software
- Drones
- Drug and Alcohol Testing
- Evidence Management
- Explosives Detection
- Firearms Training
- Forensic 3D Laser Scanners
- In Car Video
- Less Lethal
- License Plate Readers
- Mobile Command Centers
- NG911
- Narcotics Identification
- Network Solutions
- Officer Wellness
- Online Training
- Personal Protective Equipment - PPE
- RMS
- Radiation Detection
- Radio Systems
- Radios
- Rapid DNA Analysis
- Risk Management
- Rugged Computers
- Specialty Vehicles
- Training Simulation
- Video Surveillance

ALL GRANTS HELP

Start Planning Your 2021 Grant Applications

Submitting a successful application requires a lot of resources and planning. Don't know where to start? Contact PoliceGrantsHelp for assistance writing and preparing your grant applications.

Get started today

Get Help With Grant Funding for Leica Geosystems

Leica Geosystems has partnered with the PoliceGrantsHelp team to offer free grant assistance for forensic 3D laser scanners.

Get free grant help

OTHER HIGHLIGHTS

3 easy steps to write the perfect grant application

By Linda Gilbertson

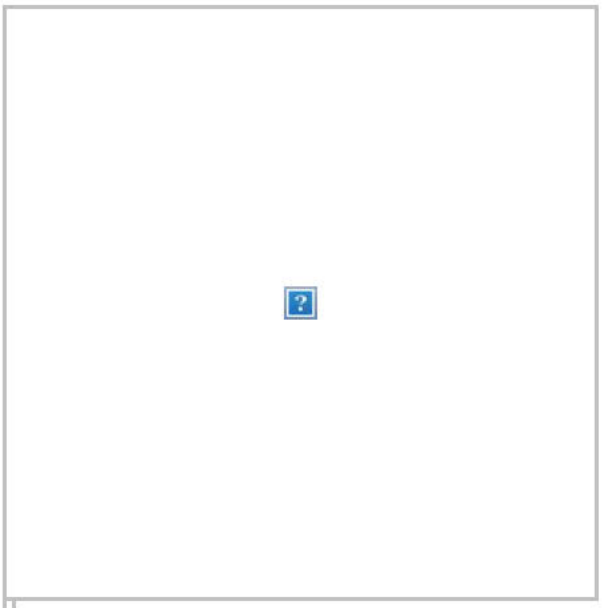
The good news is that you can, in fact, write a pretty great grant application if you apply yourself

A 7-Step Guide to Public Safety Grant Writing



At Lexipol, we've developed an easy-to-follow process to get you up to speed on the basics of identifying, applying for and securing public safety grants.

Download eBook



UPCOMING GRANTS

Grant	Grant Deadline
Combating Opioid Overdose though Community-level Intervention (Maryland)	11/2/2020
Child Sexual Abuse Treatment (CS) Program (California)	11/3/2020
Title II Formula Grant Program (Indiana)	11/4/2020
Neotropical Migratory Bird Conservation Act Grant (NMBCA)	11/5/2020
Community Violence Prevention/Reduction Grant Program (Pennsylvania)	11/10/2020
S.T.O.P. Violence Against Women Grant (VAWA Kansas)	11/10/2020

Interested in finding more grant opportunities?

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: PoliceGrantsHelp eNews
To: Silva, Patrick (POL)
Subject: Impact of marijuana legalization on grants; 3 steps to the perfect grant application
Date: Tuesday, October 20, 2020 2:54:46 PM

October 20, 2020 | View as webpage

Dear PoliceGrantsHelp Member,

In this month's eNews, we look at the impact of marijuana legalization on grants that stem from marijuana sales. This article is part of Police1's analysis of a recent survey on policing in an era of legal marijuana.

Now is the time to start planning your 2021 grant projects and applications. Don't let the complex and sometimes difficult application process intimidate your efforts. Contact the grant experts at PoliceGrantsHelp for assistance writing and preparing your grant application. Contract for grant writing services in October and receive a full year subscription of GrantFinder – an online searchable database of federal, state, foundation and corporate grants available to your community.

— *The PoliceGrantsHelp Team*

FEATURED CONTENT

The impact of legalizing marijuana: Utilizing grant funding to support youth programs

By PoliceGrantsHelp Staff

Grants that stem from marijuana sales consist of an array of programs

GET GRANT ASSISTANCE

PoliceGrantsHelp offers customized grant assistance in several categories. Click on the links below to access free grant services including: research, consulting and application assistance.

- AEDs
- All Terrain Vehicles
- Armored Vehicles
- Boats
- Body Cameras
- CAD
- Citation Management
- Crime Analysis and Investigation Software
- Drones
- Drug and Alcohol Testing
- Evidence Management
- Explosives Detection
- Firearms Training
- Forensic 3D Laser Scanners
- In Car Video
- Less Lethal
- License Plate Readers
- Mobile Command Centers
- NG911
- Narcotics Identification
- Network Solutions
- Officer Wellness
- Online Training
- Personal Protective Equipment - PPE
- RMS
- Radiation Detection
- Radio Systems
- Radios
- Rapid DNA Analysis
- Risk Management
- Rugged Computers
- Specialty Vehicles
- Training Simulation
- Video Surveillance

ALL GRANTS HELP

Start Planning Your 2021 Grant Applications

Submitting a successful application requires a lot of resources and planning. Don't know where to start? Contact PoliceGrantsHelp for assistance writing and preparing your grant applications.

Get started today

Get Help With Grant Funding for Leica Geosystems

Leica Geosystems has partnered with the PoliceGrantsHelp team to offer free grant assistance for forensic 3D laser scanners.

Get free grant help

OTHER HIGHLIGHTS

3 easy steps to write the perfect grant application

By Linda Gilbertson

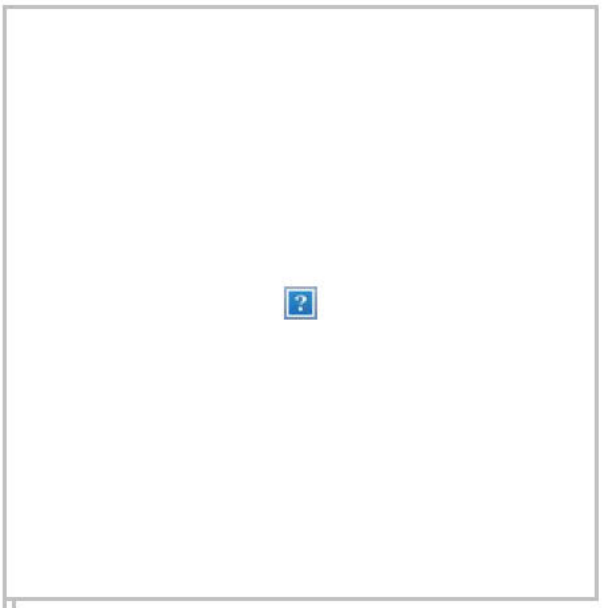
The good news is that you can, in fact, write a pretty great grant application if you apply yourself

A 7-Step Guide to Public Safety Grant Writing



At Lexipol, we've developed an easy-to-follow process to get you up to speed on the basics of identifying, applying for and securing public safety grants.

Download eBook



UPCOMING GRANTS

Grant	Grant Deadline
Combating Opioid Overdose though Community-level Intervention (Maryland)	11/2/2020
Child Sexual Abuse Treatment (CS) Program (California)	11/3/2020
Title II Formula Grant Program (Indiana)	11/4/2020
Neotropical Migratory Bird Conservation Act Grant (NMBCA)	11/5/2020
Community Violence Prevention/Reduction Grant Program (Pennsylvania)	11/10/2020
S.T.O.P. Violence Against Women Grant (VAWA Kansas)	11/10/2020

Interested in finding more grant opportunities?

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: PoliceGrantsHelp eNews
To: Conneely, Paul (POL)
Subject: Impact of marijuana legalization on grants; 3 steps to the perfect grant application
Date: Tuesday, October 20, 2020 3:34:51 PM

October 20, 2020 | View as webpage

Dear PoliceGrantsHelp Member,

In this month's eNews, we look at the impact of marijuana legalization on grants that stem from marijuana sales. This article is part of Police1's analysis of a recent survey on policing in an era of legal marijuana.

Now is the time to start planning your 2021 grant projects and applications. Don't let the complex and sometimes difficult application process intimidate your efforts. Contact the grant experts at PoliceGrantsHelp for assistance writing and preparing your grant application. Contract for grant writing services in October and receive a full year subscription of GrantFinder – an online searchable database of federal, state, foundation and corporate grants available to your community.

— *The PoliceGrantsHelp Team*

FEATURED CONTENT

The impact of legalizing marijuana: Utilizing grant funding to support youth programs

By PoliceGrantsHelp Staff

Grants that stem from marijuana sales consist of an array of programs

GET GRANT ASSISTANCE

PoliceGrantsHelp offers customized grant assistance in several categories. Click on the links below to access free grant services including: research, consulting and application assistance.

- AEDs
- All Terrain Vehicles
- Armored Vehicles
- Boats
- Body Cameras
- CAD
- Citation Management
- Crime Analysis and Investigation Software
- Drones
- Drug and Alcohol Testing
- Evidence Management
- Explosives Detection
- Firearms Training
- Forensic 3D Laser Scanners
- In Car Video
- Less Lethal
- License Plate Readers
- Mobile Command Centers
- NG911
- Narcotics Identification
- Network Solutions
- Officer Wellness
- Online Training
- Personal Protective Equipment - PPE
- RMS
- Radiation Detection
- Radio Systems
- Radios
- Rapid DNA Analysis
- Risk Management
- Rugged Computers
- Specialty Vehicles
- Training Simulation
- Video Surveillance

ALL GRANTS HELP

Start Planning Your 2021 Grant Applications

Submitting a successful application requires a lot of resources and planning. Don't know where to start? Contact PoliceGrantsHelp for assistance writing and preparing your grant applications.

Get started today

Get Help With Grant Funding for Leica Geosystems

Leica Geosystems has partnered with the PoliceGrantsHelp team to offer free grant assistance for forensic 3D laser scanners.

Get free grant help

OTHER HIGHLIGHTS

3 easy steps to write the perfect grant application

By Linda Gilbertson

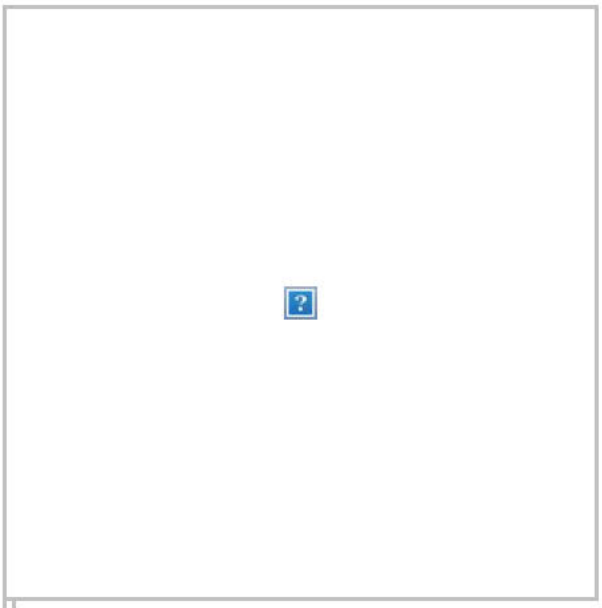
The good news is that you can, in fact, write a pretty great grant application if you apply yourself

A 7-Step Guide to Public Safety Grant Writing



At Lexipol, we've developed an easy-to-follow process to get you up to speed on the basics of identifying, applying for and securing public safety grants.

Download eBook



UPCOMING GRANTS

Grant	Grant Deadline
Combating Opioid Overdose though Community-level Intervention (Maryland)	11/2/2020
Child Sexual Abuse Treatment (CS) Program (California)	11/3/2020
Title II Formula Grant Program (Indiana)	11/4/2020
Neotropical Migratory Bird Conservation Act Grant (NMBCA)	11/5/2020
Community Violence Prevention/Reduction Grant Program (Pennsylvania)	11/10/2020
S.T.O.P. Violence Against Women Grant (VAWA Kansas)	11/10/2020

Interested in finding more grant opportunities?

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Plante, Michelle (POL)
To: Scott, Michael (POL)
Subject: job description for grant
Date: Wednesday, November 18, 2020 11:04:45 AM

Condensed job description you requested for the Heroin/Meth grant:
Intelligence Analyst II

Establish criminal profiles on drug trafficking organization members via sophisticated searches into several law enforcement databases, open source and social media databases and through use of investigative software including, but not limited to: TLO, CLEAR, ISO, Facial Recognition, ALPR, CJISWeb, InmateWeb, MIDNet and OSINT. Run historical ALPR queries and create "hot lists" in the ALPR system in order to track particular drug trafficking organization vehicles in real time and determine narcotics trafficking patterns. Determine the structure and operation of criminal groups on a tactical level and identify criminal associations and relationships by performing various kinds of analyses to support investigative work and produce intelligence products such as link analyses, telephone toll analyses, timeline analyses, and any analyses through which data are integrated to determine the existence of networks and patterns.

Justification for Cellebrite renewal:

Cellebrite is the leader in forensic cell phone extractions and as a trained and certified examiner, it is incumbent upon the CINRET West unit to utilize an in-house analyst to perform cell phone extractions in a time-efficient manner to gain access to valuable intelligence related to narcotics investigations. It is imperative that the license be renewed as the program is updated multiples times a month to keep up to date with the ever-changing software and applications used on mobile devices. If the license is not renewed, we will not be able to update the software with critical updates. This can either lead to not being able to extract complete data from a device, or not being able to extract from a device at all.

Justification for computer:

I was hired by MSP in May 2020 to perform specific duties providing intelligence and investigative field support to the CINRET West Unit. The unit did not have a computer for me to perform my duties and six months later still has not received approval for a computer for me to perform my duties despite being awarded a multi-million dollar grant. Detective Lieutenant Loiselle let me use his old Panasonic CF-54 that was issued to him when he was in IA. This was intended to be a *temporary* solution. The laptop is sufficient for basic duties using the internet, but is not sufficient for running I2 Analyst Notebook, RAMS, BOSS LPRs, and the internet at the same time. Since there were multiple previous users on this laptop, it was given to me with half of the available space.

Michelle Plante, Intelligence Analyst II

Massachusetts State Police
Commonwealth Interstate Narcotics Reduction Enforcement Team
CINRET - Western Region
53 Elliot Street
Springfield, Massachusetts 01105
Cell: [redacted]
michelle.plante@pol.state.ma.us

From: Police1 Weekend Roll Call
To: McCarthy, Steven (POL)
Subject: Judge drops 1 Chauvin charge, "white boys" demotion & other top stories
Date: Sunday, October 25, 2020 9:15:03 AM

October 25, 2020 | View as webpage

FEATURED CONTENT



Top Minneapolis PD official demoted over 'white boys' comment

The man was quoted referring to white officers in an interview that prompted internal backlash



Police release video of Phoenix ambush, OIS

Video shows the suspect firing at a state trooper, who was sitting in an unmarked vehicle



Judge drops 3rd-degree murder charge against Derek Chauvin

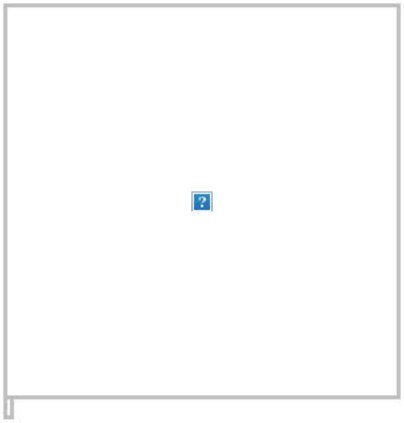
The former Minneapolis cop is still facing a second-degree murder charge in George Floyd's death

Decatur G3 Innovative Made in USA Police Radar



Made in USA speed & traffic calming products. G3™ police radar – save lives without financial pain! Request a complimentary test & evaluation!

Request now





Police: Good Samaritan rushed to aid Houston cop wounded in shooting

The man helped Officer Courtney Waller put on a tourniquet and escorted him to safety



Video: Atlanta Police use drone to arrest

suspect in actor's shooting death

The drone flies into an apartment where it contacts the suspect before he's taken into custody



Why 'shoot them in the leg' is not an effective strategy

By David Blake

When law enforcement practices become political fodder, both officers and civilians lose



Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: US 9th Circuit - Justia Daily Opinion Summaries
To: Grassia, Michael (POL)
Subject: Latest 4 Cases: Romero-Millan v. Barr (Criminal Law), United States v. Yang (Criminal Law), Bark v. United States Forest Service (Environmental Law)
Date: Tuesday, May 5, 2020 9:03:53 AM

If you are unable to see this message, click here to view it in a web browser.

Justia Daily Opinion Summaries

US Court of Appeals for the Ninth Circuit
May 5, 2020

Table of Contents

Romero-Millan v. Barr
Criminal Law

United States v. Yang
Criminal Law

Bark v. United States Forest Service
Environmental Law, Government & Administrative Law

John Doe #1 v. Trump
Immigration Law

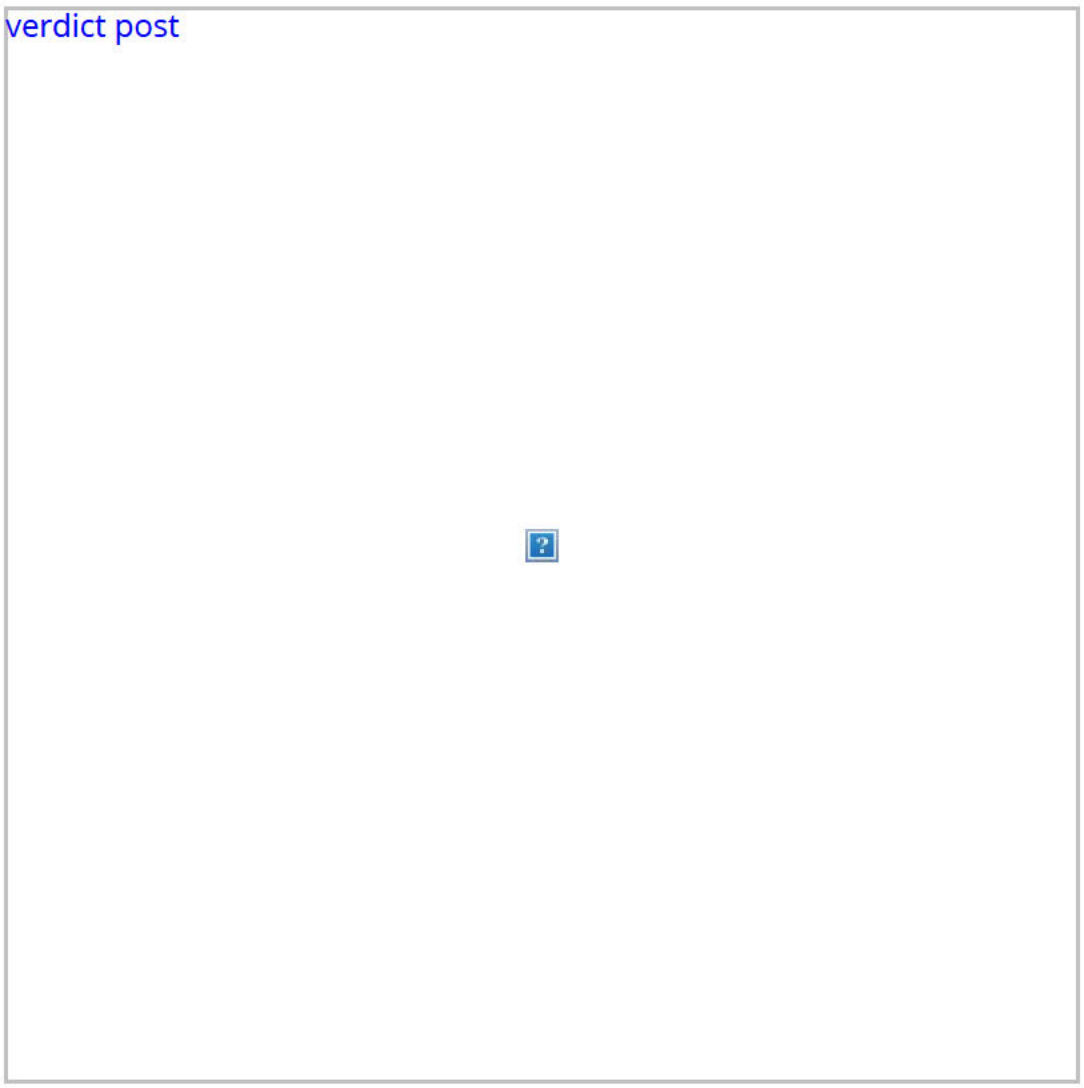
COVID-19 Updates: Law & Legal Resources Related to Coronavirus

Click here to remove Verdict from subsequent Justia newsletter(s).

New on Verdict
Legal Analysis and Commentary

Law in the Time of Corona
JOANNA L. GROSSMAN, LAWRENCE M. FRIEDMAN

verdict post



SMU Dedman School of Law professor Joanna L. Grossman and Stanford law professor Lawrence M. Friedman discuss the implications of COVID-19 on the execution of wills and marriage. Grossman and Friedman argue that the COVID-19 crisis demonstrates how quickly and universally Americans rush into court, demanding from judges legal solutions to ethical, political, and social issues.

Read More

US Court of Appeals for the Ninth Circuit Opinions

Romero-Millan v. Barr

Dockets: 16-73915, 17-72893, 18-71555

Opinion Date: May 4, 2020
Areas of Law: Criminal Law

The Ninth Circuit certified the following questions of state law to the Arizona Supreme Court: 1. Is Arizona's possession of drug paraphernalia statute, A.R.S. 13-3415, divisible as to drug type? 2. Is Arizona's drug possession statute, A.R.S. 13-3408, divisible as to drug type? 3. Put another way, is jury unanimity (or concurrence) required as to which drug or drugs listed in A.R.S. 13-3401(6), (19), (20), or (23) was involved in an offense under either statute?

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Yang

Docket: 18-10341
Opinion Date: May 4, 2020
Judge: Piersol
Areas of Law: Criminal Law

The Ninth Circuit affirmed the district court's denial of defendant's motion to suppress after he pleaded guilty to receipt of stolen mail and being a prohibited person in possession of a firearm. Defendant moved to suppress the evidence seized from his residence and the statements he made to law enforcement on the basis that the search warrant obtained by the Postal Inspection Service relied on evidence that was obtained illegally. The panel declined to address the potential Fourth Amendment privacy interests that may be implicated by the warrantless use of this Automatic License Plate Recognition (ALPR) technology, and held that defendant does not have a reasonable expectation of privacy in the historical location data of the Yukon under the facts of this case. The panel found no evidence in the record that Prestige Motors had a policy or practice of allowing lessees to keep cars beyond the rental period and Prestige had made affirmative attempts to repossess the vehicle by activating the GPS unit to locate and disable the vehicle. Therefore, defendant lacked standing to challenge the warrantless search of the database.

Read Opinion Are you a lawyer? **Annotate this case**.

Bark v. United States Forest Service

Docket: 19-35665
Opinion Date: May 4, 2020
Judge: Stephen Andrew Higginson
Areas of Law: Environmental Law, Government & Administrative Law

The Ninth Circuit granted the Forest Service's request to publish the unpublished Memorandum Disposition with modifications. The panel reversed the district court's grant of summary judgment for the Forest Service in an action alleging violations of the National Environmental Policy Act (NEPA) and National Forest Management Act (NFMA). The panel held that the Forest Service's determination that the Crystal Clear Restoration Project did not require an Environmental Impact Statement (EIS) was arbitrary and capricious for two independent reasons. First, the effects of the Project are highly controversial and uncertain, thus mandating the creation of an EIS. Second, the Forest Service failed to identify and meaningfully analyze the cumulative impacts of the Project. Because an EIS is required, and because the findings in the EIS could prompt the Forest Service to change the scope of the Project or the methods it plans to use, the panel did not reach the remaining claims. The panel reversed and remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

John Doe #1 v. Trump

Docket: 19-36020
Opinion Date: May 4, 2020
Judge: Sidney Runyan Thomas
Areas of Law: Immigration Law

The Ninth Circuit denied the government's motion for a stay pending appeal of the district court's preliminary injunction enjoining Presidential Proclamation No. 9945, Suspension of Entry of Immigrants Who Will Financially Burden the United States Health Care System. The Proclamation barred, with some exceptions, individuals seeking to enter the United States on an immigrant visa from entering unless they could demonstrate that they will be covered by certain approved health insurance within 30 days of entry or that they have the resources to cover foreseeable

healthcare costs. The panel held that the government has not established the requisite irreparable harm necessary to justify a stay pending appeal. In this case, the government's rights may be vindicated upon completion of this litigation; the alleged monetary harms to third parties upon which the government relies do not constitute irreparable harm; and the government did not meet its high burden to satisfy the other Nken factors. Therefore, the government has not demonstrated a likelihood of success. The panel also held that staying the injunction would injure both the plaintiff class and third parties, and the public interest weighs against entering a stay; the preliminary injunction preserves the status quo during the pendency of this appeal; and the district court did not abuse its discretion in determining the scope of the preliminary injunction.

Read Opinion Are you a lawyer? **Annotate this case**.

About Justia Opinion Summaries

Justia Daily Opinion Summaries is a free service, with 68 different newsletters, covering every federal appellate court and the highest courts of all US states.

Justia also provides weekly practice area newsletters in 63 different practice areas.

All daily and weekly Justia newsletters are free. Subscribe or modify your newsletter subscription preferences at daily.justia.com.

You may freely redistribute this email in whole.

About Justia

Justia is an online platform that provides the community with open access to the law, legal information, and lawyers.



Contact Us | Privacy Policy

Unsubscribe From This Newsletter

or unsubscribe from all Justia newsletters immediately **here.**



Justia | 1380 Pear Ave #2B, Mountain View, CA 94043

From:	Administrative Law - Justia Weekly Opinion Summaries
To:	Caravaggio, Suzanne (POL)
Subject:	Latest 29 Cases This Week: Spadaro v. United States Customs and Border Protection (2d Cir.), PDX North Inc v. Commissioner New Jersey Department ...
Date:	Friday, October 23, 2020 9:04:10 AM

If you are unable to see this message, click here to view it in a web browser.

Justia Weekly Opinion Summaries



Government & Administrative Law
October 23, 2020

Table of Contents

Spadaro v. United States Customs and Border Protection
Government & Administrative Law, Immigration Law
US Court of Appeals for the Second Circuit

PDX North Inc v. Commissioner New Jersey Department of Labor and Workforce Development

Civil Procedure, Government & Administrative Law
US Court of Appeals for the Third Circuit

Wise v. Circosta
Civil Rights, Constitutional Law, Election Law, Government & Administrative Law
US Court of Appeals for the Fourth Circuit

M.D. v. Abbott
Civil Procedure, Government & Administrative Law
US Court of Appeals for the Fifth Circuit

Richardson v. Texas Secretary of State
Civil Rights, Constitutional Law, Election Law, Government & Administrative Law
US Court of Appeals for the Fifth Circuit

EMW Women's Surgical Center, P.S.C. v. Friedlander
Civil Rights, Constitutional Law, Government & Administrative Law
US Court of Appeals for the Sixth Circuit

Boardman v. Inslee
Civil Rights, Constitutional Law, Government & Administrative Law, Labor & Employment Law
US Court of Appeals for the Ninth Circuit

California v. United States Environmental Protection Agency
Civil Procedure, Environmental Law, Government & Administrative Law
US Court of Appeals for the Ninth Circuit

Sensory NeuroStimulation, Inc. v. Azar
Government & Administrative Law, Health Law
US Court of Appeals for the Ninth Circuit

Speidell v. United States
Civil Procedure, Government & Administrative Law, Tax Law
US Court of Appeals for the Tenth Circuit

Monk v. Wilkie
Government & Administrative Law, Military Law, Public Benefits
US Court of Appeals for the Federal Circuit

Am. Chemistry Council v. Off. of Environ. Health Hazard Assessment
Civil Procedure, Environmental Law, Government & Administrative Law
California Courts of Appeal

Epstein v. Vision Service Plan
Arbitration & Mediation, Civil Rights, Government & Administrative Law
California Courts of Appeal

Paul Blanco's Good Car Co. Auto Group v. Superior Court
Civil Procedure, Government & Administrative Law
California Courts of Appeal

Rhoden, et al. v. Athens-Clarke County Bd. of Elections, et al.

Constitutional Law, Election Law, Government & Administrative Law
Supreme Court of Georgia

Schoeffel v. Idaho Dept. of Labor
Government & Administrative Law, Labor & Employment Law
Idaho Supreme Court - Civil

Goral v. Dart
Civil Procedure, Government & Administrative Law, Labor & Employment Law
Supreme Court of Illinois

Brown v. Indiana Department of Environmental Management
Government & Administrative Law, Labor & Employment Law
Supreme Court of Indiana

D90 Energy, LLC v. Jefferson Davis Parish Board of Review
Energy, Oil & Gas Law, Government & Administrative Law, Tax Law
Louisiana Supreme Court

Meiners v. St. Tammany Parish Fire Protection Dist. No. 4 et al.
Government & Administrative Law, Labor & Employment Law
Louisiana Supreme Court

Matter of Hehn
Government & Administrative Law
North Dakota Supreme Court

RFM-TREI Jefferson Apartments v. Stark County Board of Comm'rs
Civil Procedure, Government & Administrative Law, Real Estate & Property Law, Tax Law
North Dakota Supreme Court

Suelzle v. NDDOT
Criminal Law, Government & Administrative Law
North Dakota Supreme Court

WSI v. Tolman
Civil Procedure, Government & Administrative Law, Labor & Employment Law
North Dakota Supreme Court

Chernaik v. Brown
Civil Procedure, Environmental Law, Government & Administrative Law
Oregon Supreme Court

In re A.M. & G.M.
Family Law, Government & Administrative Law
Vermont Supreme Court

Dumfries-Triangle Rescue Squad v. Board of Supervisors
Government & Administrative Law
Supreme Court of Virginia

Neal v. Fairfax County Police

Government & Administrative Law
Supreme Court of Virginia

Reykdal v. Espinoza
Election Law, Government & Administrative Law
Washington Supreme Court

Associate Justice Ruth Bader Ginsburg

Mar. 15, 1933 - Sep. 18, 2020



In honor of the late Justice Ruth Bader Ginsburg, Justia has compiled a list of the **opinions she authored**.

For a list of cases argued before the Court as an advocate, **see her page on Oyez**.

Click here to remove Verdict from subsequent Justia newsletter(s).

New on Verdict

Legal Analysis and Commentary

He Said/She Said, Save Our Sons, and the Stories that Stick: Part Two of a Two-Part Series of Columns
SHERRY F. COLB

verdict post

In this second in a series of columns on the U.S. Department of Education's recent push toward a higher burden of proof in determinations of sexual harassment or assault under Title IX, Cornell Law professor Sherry F. Colb suggests that gendered narratives play a role in people's willingness to regard an acquaintance rape case as "he said/she said." Colb describes several examples in which people prefer a story that confirms a pre-existing bias over truth based on evidence.

Read More

Government & Administrative Law Opinions

Spadaro v. United States Customs and Border Protection

Court: US Court of Appeals for the Second Circuit
Docket: 19-1157
Opinion Date: October 20, 2020
Judge: Joseph F. Bianco
Areas of Law: Government & Administrative Law, Immigration Law

The Second Circuit affirmed the district court's judgment in favor of the government defendants in a Freedom of Information Act (FOIA) action brought by plaintiff, seeking documents related to the revocation of his visa. The court held that the contested documents were properly withheld under FOIA Exemption 3, and specifically INA 222(f), because they pertain to the issuance and refusal of a visa. Furthermore, officials properly invoked Exemption 3 to withhold revocation documents as they are related to visa issuances and refusals. Finally, plaintiff failed to meet his burden of demonstrating that the records are needed by a court "in the interest of the ends of justice," and the discretionary release of records under 8 U.S.C. 1202(f)(1) provides no basis for disclosure in this FOIA action. For the reasons set forth in a separate summary order addressing FOIA Exemption 5 filed simultaneously with this opinion, the court affirmed the judgment.

Read Opinion Are you a lawyer? **Annotate this case**.

PDX North Inc v. Commissioner New Jersey Department of Labor and Workforce Development

Court: US Court of Appeals for the Third Circuit
Docket: 19-2968
Opinion Date: October 22, 2020
Judge: Scirica
Areas of Law: Civil Procedure, Government & Administrative Law

PDX is a last-mile shipper of wholesale auto parts in New Jersey and other states. Depending on the volume and timing of its customers' shipping needs, PDX hires "independent owner-operators" on an "as-needed" basis. PDX long classified these drivers as independent contractors. In 2012, after completing an audit of PDX for 2006-2009, the New Jersey Department of Labor and Workforce Development determined that PDX had misclassified its drivers, finding they were employees, not independent contractors. The Department reached the same conclusion in two subsequent audits and sought payment of unemployment compensation taxes PDX filed suit,

contending New Jersey's statutory scheme for classifying workers was preempted by the Federal Aviation Administration Authorization Act of 1994 and was unconstitutional under the Interstate Commerce Clause. An action before the New Jersey Office of Administrative Law (OAL) was stayed at PDX's request. SLS, also a last-mile shipper, was audited by the Department and was allowed to intervene in the lawsuit. The Department's audit against SLS remains pending. The trial court dismissed the entire case as barred by the Younger abstention doctrine. The Third Circuit held that the trial court correctly dismissed PDX, but erred in dismissing SLS. PDX's OAL action is an ongoing judicial proceeding in which New Jersey has a strong interest and PDX may raise any constitutional claims while SLS is not subject to an ongoing state judicial proceeding.

Read Opinion Are you a lawyer? **Annotate this case**.

Wise v. Circosta

Court: US Court of Appeals for the Fourth Circuit
Dockets: 20-2104, 20-2107
Opinion Date: October 21, 2020
Judge: James Andrew Wynn, Jr.
Areas of Law: Civil Rights, Constitutional Law, Election Law, Government & Administrative Law

The Fourth Circuit declined to enjoin the North Carolina State Board of Elections's extension of its deadline for the receipt of absentee ballots for the ongoing general election. The court explained that the only issue it must address now is plaintiffs' request for an emergency injunction pending appeal regarding a single aspect of the procedures that the district court below refused to enjoin: an extension of the deadline for the receipt of mail-in ballots. The court explained that the change is simply an extension from three to nine days after Election Day for a timely ballot to be received and counted. Because plaintiffs have not established a likelihood of success on the merits of their equal protection claim—and because, in any event, Purcell v. Gonzalez, 549 U.S. 1 (2006), and Andino v. Middleton, No. 20A55, 2020 WL 5887393 (U.S. Oct. 5, 2020), require that the court not intervene at this late stage—the court declined to enter an injunction pending appeal. The court also held that plaintiffs lack standing to raise their Elections Clause challenge. Even if they did not lack standing, the Pullman

abstention doctrine strongly counsels the court against exercising jurisdiction over that claim. The court further held that all suggestions from the state courts point to the conclusion that the Board properly exercised its legislative delegation of authority, and there is no irreparable harm from a ballot extension. Finally, the balance of the equities is influenced heavily by Purcell and tilts against federal court intervention at this late stage, and Andino establishes that the appropriate status-quo framework is the status quo created by the state's actions, not by later federal court interventions.

Read Opinion Are you a lawyer? **Annotate this case**.

M.D. v. Abbott

Court: US Court of Appeals for the Fifth Circuit
Docket: 19-41015
Opinion Date: October 16, 2020
Judge: James C. Ho
Areas of Law: Civil Procedure, Government & Administrative Law

Plaintiffs, a certified class of minor children in the permanent managing conservatorship (PMC) of the Texas Department of Family Protective Services, filed 42 U.S.C. 1983 claims alleging that the Texas foster-care system violated their substantive due process right to be free from an unreasonable risk of harm. The district court issued a wide-ranging permanent injunction imposing sweeping changes on the Texas foster-care system. The Fifth Circuit vacated and remanded the injunction to the district court for modification; the district court made additional modifications to the injunction; and the state appealed again. The Fifth Circuit then instructed the district court to begin implementing, without further changes, the modified injunction with the alterations the court made. On remand, however, the district court expanded the injunction again by enjoining the state from moving any PMC child from their current placement as a result of enforcement of the court's requirement for 24-hour awake-night supervision unless application is made to the court prior to the proposed discharge. The Fifth Circuit reversed and held that it is black-letter law that a district court must comply with a mandate issued by an appellate court. The Fifth Circuit remanded to the district court to begin implementing, without further changes, the modified injunction with the alterations the court has made.

Read Opinion Are you a lawyer? **Annotate this case**.

Richardson v. Texas Secretary of State

Court: US Court of Appeals for the Fifth Circuit
Docket: 20-50774
Opinion Date: October 19, 2020
Judge: Jerry Edwin Smith
Areas of Law: Civil Rights, Constitutional Law, Election Law, Government & Administrative Law

After plaintiffs filed suit challenging Texas's absentee-ballot system in August 2019, the district court granted plaintiffs' summary judgment motion in part, issuing an injunction adopting many of plaintiffs' proposed changes to Texas's election procedures. The injunction included three main provisions regarding the 2020 election: first, the district court required the Secretary to issue an advisory, within ten days, notifying local election officials of the injunction, and the notification must inform them that rejecting ballots because of mismatching signatures is unconstitutional unless the officials take actions that go beyond those required by state law; second, the Secretary must either issue an advisory to local election officials requiring them to follow the district court's newly devised signature verification and voter-notification procedures, or else promulgate an advisory requiring that officials cease rejecting ballots with mismatched signatures altogether; and third, the district court mandated that the Secretary take action against any election officials who fail to comply with the district court's newly minted procedures. The Fifth Circuit considered the Nken factors and granted the Secretary's motion to stay the district court's injunction pending appeal, because the Secretary is likely to succeed in showing that Texas's signature-verification procedures are constitutional. The court held that the Secretary is likely to show that plaintiffs have alleged no cognizable liberty or property interest that could serve to make out a procedural due process claim. Given the failure of plaintiffs and the district court to assert that voting—or, for that matter, voting by mail—constitutes a liberty interest, along with the absence of circuit precedent supporting that position, the court stated that the Secretary is likely to prevail in showing that plaintiffs' motion for summary judgment on their due process claim should have been denied. The court rejected the district court's reasoning regarding any state-created liberty interest. Even if voting is a protected

liberty or property interest, the court held that the Secretary is likely to show that the district court used the wrong test for the due process claim. The court held that the Anderson/Burdick framework provides the appropriate test for plaintiffs' due process claims and Texas's signature-verification procedures are reasonable and nondiscriminatory, and they survive scrutiny under the Anderson/Burdick framework. In this case, Texas's important interest in reducing voter fraud—and specifically in stymying mail-in ballot fraud—justifies its use of signature verification. The court also held that the Secretary is likely to prevail in her defense that sovereign immunity bars the district court's injunction requiring that she issue particular advisories and take specific potential enforcement action against noncomplying officials. Finally, the remaining Nken factors counsel in favor of granting a stay pending appeal where the Secretary will be irreparably injured absent a stay, public interest favors granting a stay, and the balance of harms weighs in favor of the Secretary.

Read Opinion Are you a lawyer? **Annotate this case**.

EMW Women's Surgical Center, P.S.C. v. Friedlander

Court: US Court of Appeals for the Sixth Circuit
Docket: 18-6161
Opinion Date: October 16, 2020
Judge: Larsen
Areas of Law: Civil Rights, Constitutional Law, Government & Administrative Law

A 1998 Kentucky law requires abortion facilities to obtain transfer agreements with local hospitals and transport agreements with local ambulance services, Ky. Rev. Stat. (KRS) 216B.0435; 2017 regulations imposed stricter conditions on the agreements but also allowed successive, 90-day waivers for facilities unable to comply. EMW, at the time, Kentucky's only licensed abortion facility, challenged the requirements as imposing an undue burden on abortion access. They argued that it had become impossible for them to obtain the required agreements and that the law's enforcement would leave Kentucky without a licensed abortion facility. The district court found Kentucky's requirements were facially invalid and permanently enjoined them. The Sixth Circuit reversed in part, vacating the injunction. The district court erred in attempting to weigh the benefits of the Kentucky laws against their burdens; a court need only consider whether

the laws are reasonably related to a legitimate state interest and whether they impose a substantial obstacle. The laws are reasonably related to a legitimate government end. The court noted that Planned Parenthood received a provisional license for its Louisville facility in 2020 and currently performs abortions. To establish a substantial burden, the plaintiffs had to establish that both EMW and Planned Parenthood would be unable to operate on the basis of waivers even if they could reasonably expect to renew the waiver every 90 days. They failed to make that showing.

Read Opinion Are you a lawyer? **Annotate this case**.

Boardman v. Inslee

Court: US Court of Appeals for the Ninth Circuit
Docket: 19-35113
Opinion Date: October 22, 2020
Judge: N. R. Smith
Areas of Law: Civil Rights, Constitutional Law, Government & Administrative Law, Labor & Employment Law

Washington ballot initiative 1501 prohibits public access to certain government-controlled information, including the personal information of in-home care providers, but permits that information to be disclosed to the providers' certified exclusive bargaining representatives. The law was challenged under 42 U.S.C. 1983 by in-home providers, required by Washington law to participate in statewide collective bargaining, who are not members of their respective unions and do not pay agency fees. They wanted to inform other individual in-home providers of their right to not pay union agency fees and were unable to obtain the necessary contact information. The Ninth Circuit affirmed summary judgment in favor of the defendants. The First Amendment does not guarantee a general right of access to government-controlled information. Whether to disclose government-controlled information is generally left to the political processes but the First Amendment forbids a state from discriminating invidiously among viewpoints. A state does not engage in viewpoint discrimination by disclosing the personal information of public or quasi-public employees to the employees' certified bargaining representative while denying equal access to the public. Initiative 1501 does not implicate the plaintiffs' associational freedom; the plaintiffs lack standing to assert the rights of

other in-home care providers. Initiative 1501 does not violate the Equal Protection Clause; the challenged provisions satisfy rational-basis review. The state has a legitimate interest in protecting seniors and other vulnerable individuals from identity theft and other financial crimes. There was no evidence that those who voted in favor of Initiative 1501 were motivated by an irrational prejudice or desire to harm the plaintiffs or their message.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. United States Environmental Protection Agency

Court: US Court of Appeals for the Ninth Circuit
Docket: 19-17480
Opinion Date: October 22, 2020
Judge: Patrick J. Bumatay
Areas of Law: Civil Procedure, Environmental Law, Government & Administrative Law

The U.S. EPA promulgated new landfill emissions guidelines in 2016. Each state was required to submit a plan for implementing the new guidelines. The EPA was to approve or disapprove each state plan. For states that failed to submit a plan, the EPA had to promulgate a federal plan that would govern implementation in those states. The deadline for EPA issue the federal plan was set by regulation for November 2017. The EPA missed the deadline. Several states sued to force EPA to promulgate its federal plan. EPA responded to the suit and also began the rulemaking process to extend its regulatory deadline. While that rulemaking was underway, the district court entered an injunction requiring EPA to promulgate the federal plan within six months (November 2019). Months later, the EPA finalized the rulemaking process, extending its regulatory deadline by two years to August 2021. The district court declined to modify the injunction. The Ninth Circuit reversed. The district court abused its discretion in denying the EPA's request for relief because the new regulations constituted a change in law, and removed the legal basis for the court's deadline. A shift in the legal landscape that removed the basis for an order warranted modification of the injunction. The court rejected an argument that courts must look beyond the new regulations and conduct a broad, fact-specific inquiry into whether modification prevented inequity.

Read Opinion Are you a lawyer? **Annotate this case**.

Sensory NeuroStimulation, Inc. v. Azar

Court: US Court of Appeals for the Ninth Circuit
Docket: 19-55036
Opinion Date: October 16, 2020
Judge: Michael M. Baylson
Areas of Law: Government & Administrative Law, Health Law

The Ninth Circuit affirmed the district court's dismissal based on lack of jurisdiction of an action brought by Sensory NueroStimulation, a medical device supplier, seeking Medicare coverage of its product. The panel held that the district court correctly held that 42 U.S.C. 405(h)'s administrative channeling requirement applied and that it therefore had no subject matter jurisdiction to hear Sensory's claims. In this case, the lawsuit is subject to Medicare's administrative channeling requirements; Sensory has not met those requirements; there exists a way to satisfy those requirements; and these conclusions do not completely preclude judicial review so as to trigger a key exception to the channeling requirements.

Read Opinion Are you a lawyer? **Annotate this case**.

Speidell v. United States

Court: US Court of Appeals for the Tenth Circuit
Docket: 19-1214
Opinion Date: October 20, 2020
Judge: Mary Beck Briscoe
Areas of Law: Civil Procedure, Government & Administrative Law, Tax Law

The Appellants objected to the IRS's attempts to collect and audit information about their marijuana-related business practices, arguing: (1) the IRS investigation was quasi-criminal, exceeded the Agency's authority, and was being conducted for an illegitimate purpose; (2) even if the investigation had a legitimate purpose, the information sought was irrelevant; and (3) the investigation was in bad faith and constituted an abuse of process because (a) the IRS may share the information collected with federal law enforcement agents, (b) the IRS summonses are overly broad and require the creation of new reports, (c) the dispensaries had a reasonable expectation of privacy in the data they tender to state regulatory

authorities, and (d) those state authorities could not provide the requested information without violating Colorado law. The Appellants further contended the district court applied the wrong standard of review when it denied motions to quash and granted motions to enforce the summonses. Relying on the reasoning outlined in Standing Akimbo, LLC v. United States, 955 F.3d 1146, 1150–69 (10th Cir. 2020), the Tenth Circuit rejected Appellants' arguments and affirmed the district court's rulings in favor of the IRS.

Read Opinion Are you a lawyer? **Annotate this case**.

Monk v. Wilkie

Court: US Court of Appeals for the Federal Circuit
Docket: 19-1094
Opinion Date: October 20, 2020
Judge: Pauline Newman
Areas of Law: Government & Administrative Law, Military Law, Public Benefits

Veterans sought certification for the class of veterans whose disability claims had not been resolved by the Board of Veterans Appeals within one year of the filing of a Notice of Disagreement (NOD), requesting judicial action to compel the Secretary of Veterans Affairs to decide all pending appeals within one year of receipt of a timely NOD. The Veterans Court requested that they separate or limit the requested class action into issues that meet the Federal Rule of Civil Procedure 23(b)(2) “commonality” standard. The veterans declined, stating that “systemic delay” exists in the VA claims system, and broad judicial remedy is required. The Veterans Court denied the requested class certification. While the case was pending, the Veterans Appeals Improvement and Modernization Act of 2017, 131 Stat. 1105 purportedly improved processing times by allowing claimants to choose: higher-level review, a supplemental claim, board review with a hearing and opportunity to submit additional evidence, board review without a hearing, but with an opportunity to submit additional evidence, or board review without a hearing or additional evidence, based on their priorities on appeal. The Federal Circuit affirmed the denial of class certification, citing the lack of proof of commonality. When Congress has crafted a comprehensive remedial structure, that structure warrants evaluation in practice before judicial intervention is contemplated.

Read Opinion Are you a lawyer? **Annotate this case**.

Am. Chemistry Council v. Off. of Environ. Health Hazard Assessment

Court: California Courts of Appeal
Docket: C079078(Third Appellate District)
Opinion Date: October 19, 2020
Judge: Murray
Areas of Law: Civil Procedure, Environmental Law, Government & Administrative Law

Proposition 65 was enacted by the voters to protect the people of California and its water supply from harmful chemicals. Proposition 65 required the Governor to publish, at least annually, a list of chemicals known to the state to cause cancer or reproductive toxicity. Proposition 65 added Health and Safety Code section 25249.8, which provided the listing obligations and sets forth four independent "listing mechanisms" by which a chemical could be listed, including the "state's qualified expert" listing mechanism and the "authoritative body" listing mechanism. At issue in this case was whether the decision by the Office of Environmental Health Hazard Assessment (OEHHA) to list Bisphenol A (BPA) as a chemical known to cause reproductive toxicity under Proposition 65, was an abuse of discretion. BPA is used primarily to coat food and beverage packaging and containers. The American Chemistry Council (ACC) commenced this action seeking to enjoin OEHHA from listing BPA. In an amended complaint, ACC sought a peremptory writ of mandate directing OEHHA not to list BPA. The trial court denied the requested relief. ACC appealed, asserting that OEHHA abused its discretion in: (1) refusing to consider the arguments against listing BPA; (2) concluding that the National Toxicology Program (NTP) formally identified BPA as a reproductive toxicant in the monograph; and (3) determining that NTP concluded that studies in experimental animals indicated that there was sufficient data to establish that an association between adverse reproductive effects in humans and BPA is "biologically plausible" within the meaning of that term as it was used in OEHHA's own regulation. The Court of Appeal found OEHHA's position as to biological plausibility was based on, among other things, the presumption that chemicals that cause harm in experimental animals will also cause similar harm in humans in the absence of evidence to the contrary. The Court concluded OEHHA did not abuse its discretion in listing BPA based on the

monograph. Therefore, the Court concluded the trial court did not abuse its discretion in denying ACC the relief requested in the amended complaint.

Read Opinion Are you a lawyer? **Annotate this case**.

Epstein v. Vision Service Plan

Court: California Courts of Appeal
Docket: A155219(First Appellate District)
Opinion Date: October 22, 2020
Judge: Banke
Areas of Law: Arbitration & Mediation, Civil Rights, Government & Administrative Law

Epstein, an optometrist, entered into a VSP "Network Doctor Agreement." VSP audited of Epstein's claims for reimbursement, concluded he was knowingly purchasing lenses from an unapproved supplier, and terminated the provider agreement. The agreement included a two-step dispute resolution procedure: the "Fair Hearing" step provided for an internal "VSP Peer Review." If the dispute remained unresolved, the agreement required binding arbitration under the Federal Arbitration Act (FAA), under procedures set forth in the policy. A "Fair Hearing" panel upheld the termination. Instead of invoking the arbitration provision, Epstein filed an administrative mandamus proceeding, alleging the second step of the process was contrary to California law requiring certain network provider contracts to include a procedure for prompt resolution of disputes and expressly stating arbitration "shall not be deemed" such a mechanism. (28 Cal. Code Regs 1300.71.38.) He claimed that state law was not preempted by the FAA, citing the McCarran-Ferguson Act, which generally exempts from federal law, state laws enacted to regulate the business of insurance. The court of appeal affirmed the rejection of those challenges. State regulatory law requiring certain network provider agreements to include a dispute resolution process that is not arbitration pertains only to the first step of the dispute resolution process and does not foreclose the parties from agreeing to arbitration in lieu of subsequent judicial review. While the arbitration provision is procedurally unconscionable in minor respects, Epstein failed to establish that it is substantively unconscionable.

Read Opinion Are you a lawyer? **Annotate this case**.

Paul Blanco's Good Car Co. Auto Group v. Superior Court

Court: California Courts of Appeal
Docket: A159623(First Appellate District)
Opinion Date: October 21, 2020
Judge: Needham
Areas of Law: Civil Procedure, Government & Administrative Law

The state filed an unverified complaint against the entities and one of their principals, asserting unfair practices and false advertising. The defendants filed an unverified "Answer" with a general denial of the complaint's allegations and affirmative defenses. The judge struck the answer as to the entities because they failed to verify the answer as required by Code of Civil Procedure section 446 and asserted only a general denial in contravention of section 431.30(d). The court concluded that section 446(a)'s exception to the verification requirement was coextensive with the Fifth Amendment privilege against self-incrimination and a corporation may not invoke that privilege. In response to a "show cause order" following the defendants' petition for extraordinary writ relief, the court issued an order noting that the case had been reassigned. After a hearing, a new judge vacated the previous order. The court of appeal agreed that the exception applies to corporations and that the defendants could file a general denial under section 431.30(d), which requires a defendant to answer each material allegation of a verified complaint with specific admissions or denials, but allows a defendant to file a general denial if the complaint is not verified. There is no reason for deeming the state's complaint verified. The court also noted that an order to show cause, unlike an alternative writ, does not invite the trial court to change the challenged order and that superior court judges generally may not overturn the order of another judge unless the other judge is unavailable.

Read Opinion Are you a lawyer? **Annotate this case**.

Rhoden, et al. v. Athens-Clarke County Bd. of Elections, et al.

Court: Supreme Court of Georgia
Docket: S21A0030
Opinion Date: October 19, 2020
Judge: Bethel

Areas of Law: Constitutional Law, Election Law, Government & Administrative Law

Jerry NeSmith earned enough support to be placed on the ballot for the office of district commissioner for the Athens-Clarke County Unified Government. NeSmith died just three days before Election Day. In addition to the personal loss of his family and friends, NeSmith's death before Election Day ultimately resulted in an electoral loss for his supporters, a number of whom joined to bring suit in superior court challenging the results of the election. The Georgia Supreme Court found that because the applicable Georgia statutes dictated that votes cast on paper ballots for a candidate who died before Election Day were void, none of the votes cast for NeSmith had legal effect. Therefore, the Athens-Clarke County Board of Elections properly applied Georgia law by voiding votes cast for NeSmith and declaring Jesse Houle the commissioner-elect for Athens-Clarke County Commission. The superior court order dismissing appellants' election challenge was affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Schoeffel v. Idaho Dept. of Labor

Court: Idaho Supreme Court - Civil
Docket: 47101
Opinion Date: October 16, 2020
Judge: Brody
Areas of Law: Government & Administrative Law, Labor & Employment Law

Connie Schoeffel worked for Thorne Research, Inc. ("Thorne") as a kitchen manager. In 2016, Thorne announced that it would be moving its operations from Idaho to South Carolina. For those employees who would not be relocating to South Carolina, Thorne offered an employee retention program to encourage them to continue working at the Idaho facility until the South Carolina facility was ready. As part of this program, Thorne prepared a "Release of Claims Agreement" ("the Agreement") providing that Thorne would pay participating employees "bargained-for compensation" in exchange for giving up certain rights, including the right to quit before their positions were eliminated. Schoeffel signed this Agreement approximately six weeks before her last day of work. After her separation, Schoeffel filed for unemployment benefits without reporting the retention payments as

income. Around the time Schoeffel received her fourth benefit payment, the Department learned of the payments that Thorne owed Schoeffel under the Agreement. The Department determined that those payments constituted reportable “severance pay” under Idaho Code section 72-1367(4). Consequently, the Department determined that Schoeffel was receiving severance pay and was required to repay the unemployment benefits she had received. Schoeffel appealed to the Department’s Appeals Bureau, which initially ruled in her favor but affirmed the Department’s decision on reconsideration. Schoeffel then appealed to the Industrial Commission which affirmed the Appeals Bureau’s decision. The Idaho Supreme Court determined the payments were reportable severance pay, applying Parker v. Underwriters Labs, Inc., 96 P.3d 618 (2004). "[B]ecause the primary purpose of the Agreement was to secure the relinquishment of Schoeffel’s right to quit, rather than to compensate her for her past service to Thorne, they were not made 'as a result of' severance under Idaho Code section 72-1367(4). Therefore, the retention payments do not constitute reportable severance pay." The Commission's decision was reversed.

Read Opinion Are you a lawyer? **Annotate this case**.

Goral v. Dart

Court: Supreme Court of Illinois
Citation: 2020 IL 125085
Opinion Date: October 22, 2020
Judge: Neville
Areas of Law: Civil Procedure, Government & Administrative Law, Labor & Employment Law

Cook County Sheriff Dart instituted disciplinary proceedings against several Sheriff’s officers (plaintiffs) by filing charges with the Cook County Sheriff’s Merit Board under Counties Code, 55 ILCS 5/3-7011. The plaintiffs filed motions with the Board to dismiss the charges. While the administrative proceedings were pending, the plaintiffs filed suit, seeking declaratory, injunctive, and monetary relief against the Sheriff, Cook County, the Board, and the Cook County Board of Commissioners, asserting that the Board was not legally constituted because several of its members were appointed to or served terms that did not comply with the Code section 3-7002 requirements. The Illinois Supreme Court reversed the dismissal of the suit

for failure to exhaust administrative remedies. Because the plaintiffs challenged the authority of the Board to address the charges, the “authority” exception to the exhaustion requirement applied. The circuit court can adjudicate the requests for back pay and other claims, which do not fall within the particular expertise of the Board. The plaintiffs raised the issue before the Board, which refused to hear them until after the disciplinary proceedings were complete. Given that the Board had not taken any substantive action regarding the disciplinary charges before the filing of the lawsuit, the “de facto officer doctrine” does not apply.

Read Opinion Are you a lawyer? **Annotate this case**.

Brown v. Indiana Department of Environmental Management

Court: Supreme Court of Indiana
Docket: 20S-MI-609
Opinion Date: October 21, 2020
Judge: Per Curiam
Areas of Law: Government & Administrative Law, Labor & Employment Law

The Supreme Court vacated a portion of the court of appeals opinion affirming the judgment of the trial court denying Appellant's petition for judicial review of the summary judgment granted by the State Employees' Appeals Commission (SEAC) against Appellant on his claim that his alleged protected activity was related to his termination, holding that the court of appeals reached too broad a conclusion to resolve the issue in this case. Appellant appealed his termination, claiming he was a protected whistleblower. SEAC dismissed the complaint, but the superior court reversed. On remand, SEAC granted summary judgment in favor of Appellant's employer. Appellant sought judicial review, claiming that most of his employer's arguments were barred by the law-of-the-case doctrine. The trial court denied the petition, concluding that the law-of-the-case doctrine did not apply. The court of appeals affirmed, agreeing that the law-of-the-case doctrine did not apply but going further to find that the law-of-the-case doctrine "is applicable only when an appellate court determines a legal issue, not a trial court." The Supreme Court vacated that portion of the court of appeals' opinion and otherwise affirmed, holding that the court of appeals need not have reached so broad a conclusion to resolve the issue.

Read Opinion Are you a lawyer? **Annotate this case**.

D90 Energy, LLC v. Jefferson Davis Parish Board of Review

Court: Louisiana Supreme Court
Docket: 2020-C-00200
Opinion Date: October 20, 2020
Judge: Crain
Areas of Law: Energy, Oil & Gas Law, Government & Administrative Law, Tax Law

This dispute involved ad valorem taxes for the tax years 2013 through 2016. In October 2012, D90 Energy, LLC, purchased two gas wells and one saltwater disposal well. The wells were subject to ad valorem property taxation in Jefferson Davis Parish, Louisiana. Relying on a Commission regulation applicable to oil and gas wells, D90 argued that a purchase price in a valid sale is fair market value; therefore, the wells should be valued at $100,000.00 for each of these tax years. For each tax year, the Assessor rejected D90's documentation of the sale, explaining, in part, that his office never uses the sales price as fair market value for oil and gas wells. Rather, the Assessor used valuation tables provided by the Commission, which take into account age, depth, type, and production of the wells. D90 appealed each assessment to the Commission, presenting documentary evidence and live testimony to establish the $100,000.00 purchase price for the wells and the arms-length nature of the sale. It presented additional evidence to establish that the condition and value of the wells were virtually identical for each tax year. The district court affirmed the Commission's valuations for all four tax years. Reviewing only what was presented to the Assessor, the court of appeal reversed the district court and reinstated the Assessor's valuation. The Louisiana Supreme Court granted D90's writ application to determine the correctness of the assessments, the proper scope and standard of review, and the legal effect of D90's failure to pay taxes under protest. After review, the Court determined the district court was correct in affirming the Commission, thus reversing the appellate court's judgment.

Read Opinion Are you a lawyer? **Annotate this case**.

Meiners v. St. Tammany Parish Fire Protection Dist. No. 4 et al.

Court: Louisiana Supreme Court
Docket: 2020-CC-00491
Opinion Date: October 20, 2020
Judge: Per Curiam
Areas of Law: Government & Administrative Law, Labor & Employment Law

Frederick Meiners, III was employed as Assistant Fire Chief with the St. Tammany Parish Fire Protection District No. 4 ("District"). In early 2016, Meiners agreed to retrieve a repaired ambulance unit from Hattiesburg, but informed his supervisor, provisional fire chief Kenneth Moore, that he first had to attend a speaking engagement with a ladies' group that would last approximately thirty minutes. At 1:08 p.m. that day, Jennifer Glorioso, the wife of Fire Equipment Operator Glorioso (hereinafter referred to as "FEO Glorioso"), photographed Meiners sitting at a table at the La Madeleine restaurant with his wife and his lawyer. She later sent a text message containing this photograph to her husband. At 2:30 p.m., District Fire Chief Brady Anderson advised Chief Moore that Meiners was not yet back from his meeting and offered to pick up the ambulance himself. Chief Moore declined Anderson's offer. After being reassured by Meiners he was on his way back to the District, Chief Moore received a text from an unknown phone number that contained a photograph of Meiners taken at the restaurant. Chief Moore then provided a written notice of investigation to Meiners, stating that he was "initiating an investigation into an incident involving you in a matter which occurred on February 19, 2016, specifically, conflicting details regarding a speaking engagement while on duty." The notice of investigation also stated the "persons conducting this investigation will be Corianne Green and a PMI representative." Chief Moore then placed Meiners on administrative leave with pay. After a hearing, Meiners was terminated from his employment with the district based on his conduct on the date of the ambulance pickup. The termination was affirmed by the St. Tammany Parish Fire Protection District No. 4 Civil Service Board ("Board"). Upon review, a district court reversed and remanded, finding that untruthfulness alone, did not mandate termination, where the misconduct did not result in a detrimental effect on the efficient and orderly operation of the fire department. The Louisiana Supreme Court found the district court erred in remanding the case to the Board to impose discipline other than termination. The Court reversed judgment and reinstated the Board's decision.

Read Opinion Are you a lawyer? **Annotate this case**.

Matter of Hehn

Court: North Dakota Supreme Court
Citation: 2020 ND 226
Opinion Date: October 21, 2020
Judge: Lisa K. Fair McEvers
Areas of Law: Government & Administrative Law

Darl Hehn appealed a district court order denying his petition for discharge from civil commitment as a sexually dangerous individual. Because the North Dakota Supreme Court determined the district court failed to make sufficient findings, the case was remanded for the court make specific findings.

Read Opinion Are you a lawyer? **Annotate this case**.

RFM-TREI Jefferson Apartments v. Stark County Board of Comm'rs

Court: North Dakota Supreme Court
Citation: 2020 ND 204
Opinion Date: October 21, 2020
Judge: Jerod E. Tufte
Areas of Law: Civil Procedure, Government & Administrative Law, Real Estate & Property Law, Tax Law

RFM-TREI Jefferson Apartments, LLC; RFM-TREI Lincoln Apartments, LLC; Dickinson Homestay, LLC; and Lodgepros Dickinson, LLC (together "the Taxpayers") appealed district court judgments affirming the Stark County Board of Commissioners' ("the Board") denials of their applications for tax abatements or refunds. The Taxpayers collectively owned two apartment complexes and two hotels located in the City of Dickinson. The Taxpayers filed applications for abatement or refund of their 2016 property taxes. The Taxpayers' opinions of value for each property differed from the City's valuations by a range of roughly $1.8 million to $20.3 million. After holding a hearing, the City recommended the Board deny each application. The Board indeed denied the abatement applications in four separate written decisions. Using the same language in each, the Board concluded

the assessor's valuations were not "in error, invalid, inequitable, unjust, or arrived at in an arbitrary, capricious, or unreasonable manner." The decisions also explained the Board did not believe the Taxpayers provided "sufficient enough information relating to the subject properties, or the local market for competing properties, to lead us to the same value conclusions requested by the applicant." The district court affirmed each denial in separate, written orders and judgments. After review, the North Dakota Supreme Court concluded the Board acted arbitrarily and unreasonably in adopting assessments exceeding the true and full value of the property. The Court reversed the district court judgments and the Board's decisions denying the Taxpayers' abatement applications. The matters were remanded for a new hearing to determine the "true and full value" of the properties and reconsideration of the abatement applications.

Read Opinion Are you a lawyer? **Annotate this case**.

Suelzle v. NDDOT

Court: North Dakota Supreme Court
Citation: 2020 ND 206
Opinion Date: October 21, 2020
Judge: Jerod E. Tufte
Areas of Law: Criminal Law, Government & Administrative Law

Benjamin Suelzle appealed a district court judgment affirming a Department of Transportation hearing officer's decision revoking his driving privileges for two years. Suelzle argued the hearing officer erred: (1) by finding the arresting officer had reasonable grounds to arrest under N.D.C.C. 39-08-01; (2) by admitting a supplemental report and notice form; and (3) by failing to exclude evidence of his test refusal because he was not given a valid implied consent advisory. Specifically, he contended he could not be lawfully arrested under N.D.C.C. 39-08-01 because the alleged actual physical control occurred on the grassy yard of his private residence, which was an improved private residential lot and not a place to which the public has access. The hearing officer rejected Suelzle's argument that his vehicle was located on private property to which the officer could have no reasonable grounds to believe the public would have a right of access for vehicular use. The North Dakota Supreme Court concluded after review of the Department hearing and district court record that although there was

evidence in the record that Suelzle drove under the influence on areas where the public had a right of access before parking on his lawn, he was not charged with driving under the influence. He was charged only with actual physical control of his pickup where it was ultimately parked on his residential grass lawn. The hearing officer's finding was based on a misapplication of law, and it was not supported by evidence in the record sufficient to show the location of the actual physical control offense was within the scope of N.D.C.C. 39-08-01. The district court's judgment affirming the hearing officer's revocation of Suelzle's driving privileges was reversed.

Read Opinion Are you a lawyer? **Annotate this case**.

WSI v. Tolman

Court: North Dakota Supreme Court
Citation: 2020 ND 223
Opinion Date: October 21, 2020
Judge: Gerald W. VandeWalle
Areas of Law: Civil Procedure, Government & Administrative Law, Labor & Employment Law

Workforce Safety and Insurance ("WSI") appealed a district court judgment affirming an administrative law judge's ("ALJ") order that affirmed WSI's April 2018 order awarding permanent impairment benefits to Jason Tolman and that reversed WSI's July 2018 order denying benefits for his depression and anxiety conditions. In September 2014, Tolman was injured when he was driving a tanker truck and involved in a single vehicle roll-over accident. WSI accepted his claim for benefits. In April 2018, WSI issued an order awarding Tolman $4,905 in permanent impairment benefits based on a determination that he had sustained a 16 percent impairment of the whole body. In July 2018, WSI issued an order denying benefits in connection with his depression and anxiety, deciding these conditions were not caused by his physical injury and existed before the work injury. Tolman requested an administrative hearing on the orders, and a hearing was held before an independent ALJ in April 2019. The North Dakota Supreme Court concluded the ALJ erred in applying N.D.C.C. 65-01-02(10)(a)(6) and concluding Tolman established his depression and anxiety conditions were compensable. The Court affirmed that part of the ALJ's order affirming

WSI's April 2018 order; but reversed that part of the ALJ's order reversing WSI's July 2018 order, and reinstated WSI's July 2018 order.

Read Opinion Are you a lawyer? **Annotate this case**.

Chernaik v. Brown

Court: Oregon Supreme Court
Docket: S066564
Opinion Date: October 22, 2020
Judge: Nakamoto
Areas of Law: Civil Procedure, Environmental Law, Government & Administrative Law

Plaintiffs, two young Oregonians, concerned about the effects of climate change and their guardians, filed suit against the Governor and the State of Oregon (collectively, the State), contending the State was required to act as a trustee under the public trust doctrine to protect various natural resources in Oregon from substantial impairment due to greenhouse gas emissions and resultant climate change and ocean acidification. Among other things, plaintiffs asked the circuit court to specify the natural resources protected by the public trust doctrine and to declare that the State had a fiduciary duty, which it breached, to prevent substantial impairment of those resources caused by emissions of greenhouse gases. Plaintiffs also asked for an injunction ordering the State to: (1) prepare an annual accounting of Oregon's carbon dioxide emissions; and (2) implement a carbon reduction plan protecting the natural resources, which the court would supervise to ensure enforcement. The circuit court granted the State's motion for summary judgment and denied plaintiffs' motion for partial summary judgment, concluding the public trust doctrine did not encompass most of the natural resources that plaintiffs identified, and did not require the State to take the protective measures that plaintiffs sought. In 2015, the circuit court entered a general judgment dismissing the action, and the Court of Appeals vacated the judgment and remanded for the circuit court to enter a judgment, consistent the Court of Appeals opinion, declaring the parties' rights. Plaintiffs appealed, arguing that as a matter of common law, the public trust doctrine was not fixed and, that it must evolve to address the undisputed circumstances presented, namely, that climate change was damaging Oregon's natural resources. They argued the doctrine was not limited to the natural resources that the circuit court identified and, the

doctrine should cover other natural resources beyond those that have been traditionally protected. The Oregon Supreme Court held the public trust doctrine currently encompassed navigable waters and the submerged and submersible lands underlying those waters. "Although the public trust is capable of expanding to include more natural resources, we do not extend the doctrine to encompass other natural resources at this time." The Supreme Court also declined to adopt plaintiffs' position that, under the doctrine, the State had the same fiduciary duties that a trustee of a common-law private trust would have, such as a duty to prevent substantial impairment of trust resources. Accordingly, the Court affirmed the Court of Appeals, which vacated the judgment of the circuit court. The matter was remanded the circuit court to enter a judgment consistent with Supreme Court's judgment.

Read Opinion Are you a lawyer? **Annotate this case**.

In re A.M. & G.M.

Court: Vermont Supreme Court
Citation: 2020 VT 95
Opinion Date: October 16, 2020
Judge: Carroll
Areas of Law: Family Law, Government & Administrative Law

Parents appealed the termination of their rights in A.M. and G.M., ages five and four. Parents struggled with substance abuse and were incarcerated periodically during the underlying proceedings. In January 2018, the Department for Children and Families (DCF) filed a petition alleging the children were in need of care or supervision (CHINS) based on parental neglect, including squalid living conditions, and parental substance-abuse concerns. The children were initially placed with their maternal grandmother pursuant to a conditional custody order (CCO), and then with mother pursuant to a CCO. In April 2018, with parents' agreement, custody of the children was transferred to DCF. Parents stipulated that the children were CHINS, and following a June 2018 disposition hearing, the parties stipulated to continued DCF custody and to DCF's disposition case plan, which contemplated reunification by November 2018 or adoption. Parents were required to take various action steps to achieve reunification. The children did not see mother after June 2018 and they stopped seeing father before

that time. As of September 2018, the children were placed together in the same foster home. Appealing the ultimate termination of the parental rights to their children, Parents challenged the trial court's treatment of voluntary guardianship petitions filed during the pendency of the juvenile proceedings. Mother also argued the court erred in terminating her rights. Finding no abuse of discretion or other reversible error, the Vermont Supreme Court affirmed termination.

Read Opinion Are you a lawyer? **Annotate this case**.

Dumfries-Triangle Rescue Squad v. Board of Supervisors

Court: Supreme Court of Virginia
Docket: 191000
Opinion Date: October 22, 2020
Judge: Cleo E. Powell
Areas of Law: Government & Administrative Law

The Supreme Court reversed the judgment of the circuit court determining that the Board of County Supervisors of Prince William County, Virginia had the authority to dissolve the corporate status of Dumfries-Triangle Rescue Squad, Inc. (DTRS), holding that the circuit court erred in concluding that the Board had the power to dissolve the corporate status of DTRS . The Board filed a complaint for declaratory judgment asserting that the Board had the authority to dissolve DTRS's corporate status under Code 32.1-111.4:7(D). The circuit court determined that DTRS was subject to the corporate dissolution authority of the Board pursuant to section 32.1-111.4:7(D) and appointed a receiver to wind up DTRS's corporate affairs, as requested by the Board. The Supreme Court reversed, holding (1) because DTRS was not incorporated pursuant to section 32.1-111.4:7, the Board could not rely on that authority to dissolve its corporate status; and (2) DTRS was not the type of entity that was subject to dissolution under that section.

Read Opinion Are you a lawyer? **Annotate this case**.

Neal v. Fairfax County Police

Court: Supreme Court of Virginia

Docket: 191127
Opinion Date: October 22, 2020
Judge: McCullough
Areas of Law: Government & Administrative Law

The Supreme Court reversed the decision of the circuit court concluding that the Fairfax County Police Department's automated license plate recognition (ALPR) satisfied the definition of an "information system" under the Government Data Collection and Dissemination Practices Act (Data Act), Va. Code 2.2-3800 through -3809, holding that the ALPR system does not constitute an "information system" within the meaning of the Data Act. Specifically, the Supreme Court held (1) the ALPR system did not satisfy the statutory definition of an "information system" because it did not contain "the name, personal number, or other identifying particulars of a data subject," and therefore, the Police Department's passive use of the ALPR system was lawful under the Data Act; and (2) the resolution of this case favorably to the Police Department foreclosed the recovery of attorneys' fees.

Read Opinion Are you a lawyer? **Annotate this case**.

Reykdal v. Espinoza

Court: Washington Supreme Court
Docket: 98731-9
Opinion Date: October 22, 2020
Judge: Debra Stephens
Areas of Law: Election Law, Government & Administrative Law

Incumbent Superintendent of Public Instruction Chris Reykdal sued to have the Thurston County Superior Court order the removal of one allegedly defamatory line in the voters' guide pamphlet from challenger Maia Espinoza's candidate statement. The superior court agreed that there was a substantial likelihood Reykdal could succeed in a defamation suit based on Espinoza's statement. Using a supervisory power conferred by RCW 29A.32.090(3)(b), the superior court ordered the secretary of state to edit out the offending line. Espinoza sought accelerated direct review, which the Washington Supreme Court granted. Because Reykdal was a public figure, he had to show "actual malice" to succeed in a defamation suit. The Supreme Court found the superior court made no findings regarding actual malice, and thus granted Reykdal's request in error. Because there was no

likelihood that Reykdal could succeed in a defamation suit, the Supreme Court concluded the superior court erred in its application of the statute.

Read Opinion Are you a lawyer? **Annotate this case**.

About Justia Opinion Summaries

Justia Weekly Opinion Summaries is a free service, with 63 different newsletters, each covering a different practice area.

Justia also provides 68 daily jurisdictional newsletters, covering every federal appellate court and the highest courts of all US states.

All daily and weekly Justia newsletters are free. Subscribe or modify your newsletter subscription preferences at daily.justia.com.

You may freely redistribute this email in whole.

About Justia

Justia is an online platform that provides the community with open access to the law, legal information, and lawyers.

Contact Us | Privacy Policy

Unsubscribe From This Newsletter
or unsubscribe from all Justia newsletters immediately **here.**

Justia | 1380 Pear Ave #2B, Mountain View, CA 94043

From: Civil Rights - Justia Weekly Opinion Summaries
To: Caravaggio, Suzanne (POL)
Subject: Latest 34 Cases This Week: Ramos v. Louisiana (U.S.), Brandt v. Fitzpatrick (1st Cir.), Trahan v. Wayfair Maine LLC (1st Cir.)
Date: Friday, April 24, 2020 9:04:36 AM

If you are unable to see this message, click here to view it in a web browser.

Justia Weekly Opinion Summaries

Civil Rights
April 24, 2020

Table of Contents

Ramos v. Louisiana
Civil Rights, Constitutional Law, Criminal Law
US Supreme Court

Brandt v. Fitzpatrick
Civil Rights, Labor & Employment Law

US Court of Appeals for the First Circuit

Trahan v. Wayfair Maine LLC
Civil Rights, Labor & Employment Law
US Court of Appeals for the First Circuit

Ali v. Woodbridge Township School District
Civil Rights, Constitutional Law, Education Law, Labor & Employment Law
US Court of Appeals for the Third Circuit

Fogle v. Sokol
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Third Circuit

Hope v. Warden Pike County Correctional Facility
Civil Procedure, Civil Rights, Constitutional Law, Immigration Law
US Court of Appeals for the Third Circuit

James v. New Jersey State Police
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Third Circuit

In re: Greg Abbott
Civil Rights, Constitutional Law, Health Law
US Court of Appeals for the Fifth Circuit

Sanchez v. Young County
Civil Rights, Constitutional Law
US Court of Appeals for the Fifth Circuit

Singleton v. Cannizzaro
Civil Rights, Constitutional Law
US Court of Appeals for the Fifth Circuit

Valentine v. Collier
Civil Rights, Constitutional Law, Criminal Law, Government & Administrative Law, Health Law
US Court of Appeals for the Fifth Circuit

Williams v. Banks
Civil Rights, Constitutional Law
US Court of Appeals for the Fifth Circuit

Gary B. v. Whitmer
Civil Rights, Constitutional Law, Education Law
US Court of Appeals for the Sixth Circuit

Queen v. City of Bowling Green
Civil Rights, Constitutional Law, Labor & Employment Law
US Court of Appeals for the Sixth Circuit

Winburn v. Nagy
Civil Rights, Constitutional Law, Criminal Law

US Court of Appeals for the Sixth Circuit

Lund v. City of Rockford
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

Mayle v. Illinois
Civil Procedure, Civil Rights, Family Law, Government & Administrative Law
US Court of Appeals for the Seventh Circuit

In Re: Leslie Rutledge
Civil Rights, Constitutional Law, Health Law
US Court of Appeals for the Eighth Circuit

Lombardo v. City of St. Louis
Civil Rights, Constitutional Law
US Court of Appeals for the Eighth Circuit

Anthony v. TRAX International Corp.
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Ninth Circuit

Wilk v. Neven
Civil Rights, Constitutional Law
US Court of Appeals for the Ninth Circuit

Barnett v. Hall, Estill, Hardwick, Gable
Civil Procedure, Civil Rights
US Court of Appeals for the Tenth Circuit

Durham v. Rural/Metro Corp.
Civil Rights, Constitutional Law, Labor & Employment Law
US Court of Appeals for the Eleventh Circuit

Cave v. State
Civil Rights, Constitutional Law, Criminal Law
Arkansas Supreme Court

Thomas v. State
Civil Rights, Constitutional Law, Criminal Law
Arkansas Supreme Court

Pinter-Brown v. The Regents of the University of California
Civil Rights, Constitutional Law
California Courts of Appeal

Archer v. State
Civil Rights, Constitutional Law, Criminal Law
Florida Supreme Court

State v. Gibbs
Civil Rights, Constitutional Law, Criminal Law

Iowa Supreme Court

State v. Harris
Civil Rights, Constitutional Law, Criminal Law
Kansas Supreme Court

Commonwealth v. McCarthy
Civil Rights, Constitutional Law, Criminal Law
Massachusetts Supreme Judicial Court

State v. Reek
Civil Rights, Constitutional Law, Criminal Law
Minnesota Supreme Court

State v. Montoya
Civil Rights, Constitutional Law, Criminal Law
Nebraska Supreme Court

Morrisey v. West Virginia AFL-CIO
Civil Rights, Constitutional Law, Labor & Employment Law
Supreme Court of Appeals of West Virginia

State v. Taylor
Civil Rights, Constitutional Law, Criminal Law
Supreme Court of Appeals of West Virginia

COVID-19 Updates: Law & Legal Resources Related to Coronavirus

Click here to remove Verdict from subsequent Justia newsletter(s).

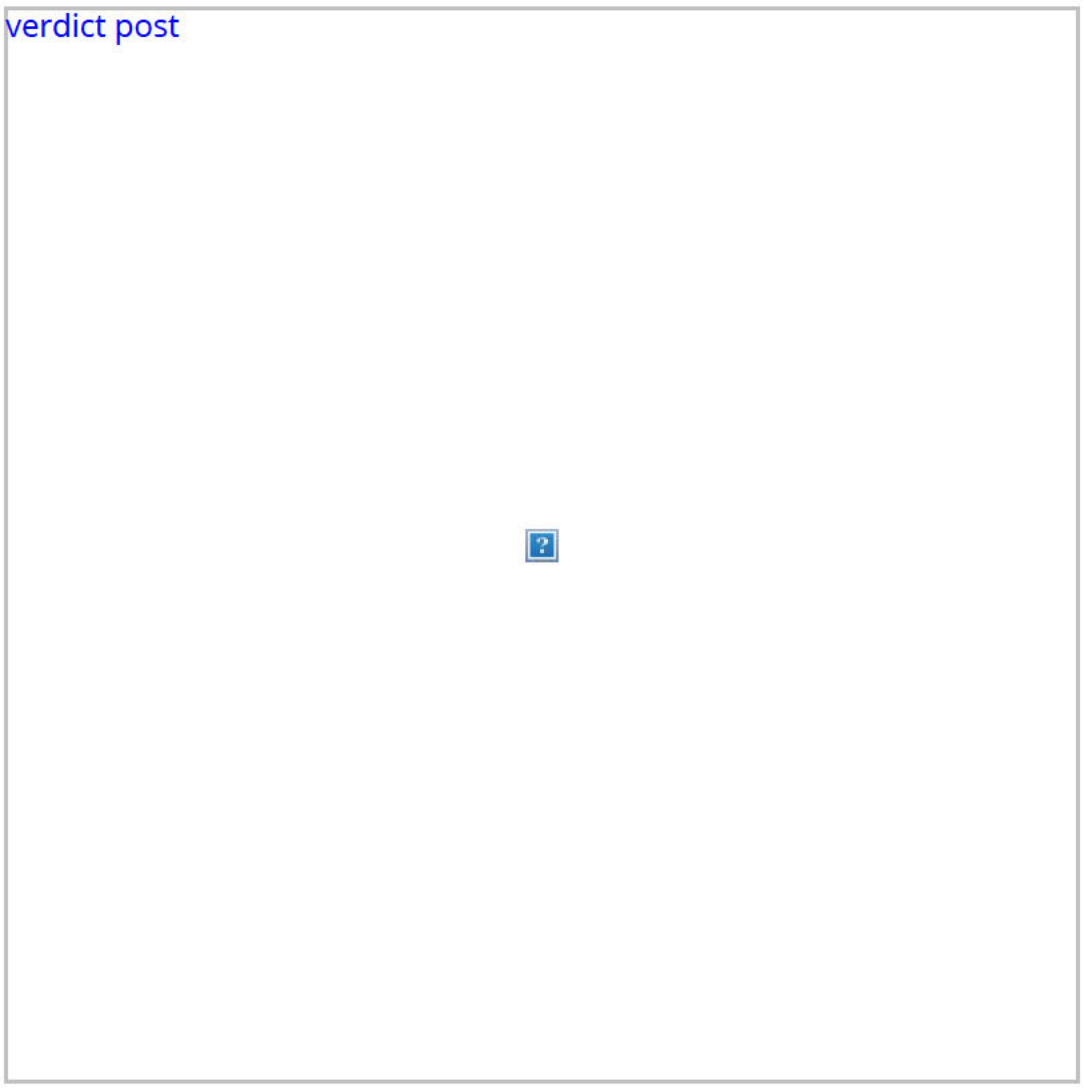
New on Verdict

Legal Analysis and Commentary

Rethinking Retroactivity in Light of the Supreme Court's Jury Unanimity Requirement

MICHAEL C. DORF

verdict post



In light of the U.S. Supreme Court's decision Monday in *Ramos v. Louisiana*, in which it held that the federal Constitution forbids states from convicting defendants except by a unanimous jury, Cornell law professor Michael C. Dorf discusses the Court's jurisprudence on retroactivity. Dorf highlights some costs and benefits of retroactivity and argues that the Court's refusal to issue advisory opinions limits its ability to resolve retroactivity questions in a way that responds to all the relevant considerations.

Read More

Civil Rights Opinions

Ramos v. Louisiana

Court: US Supreme Court
Docket: 18-5924
Opinion Date: April 20, 2020
Judge: Neil M. Gorsuch
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

In 48 states and in federal court, a single juror's vote to acquit is enough to prevent a conviction; Louisiana and Oregon punish people based on 10-to-2 verdicts. Ramos was convicted in a Louisiana court by a 10-to-2 jury verdict and was sentenced to life without parole. The Supreme Court reversed. The Sixth Amendment right to a jury trial, as incorporated against the states by the Fourteenth Amendment, requires a unanimous verdict to convict a defendant of a serious offense. Juror unanimity is a vital common law right. The Court rejected an "invitation" to "perform a cost-benefit analysis on the historic features of common law jury trials and to conclude that unanimity does not make the cut." In overturning its 1972 "Apodaca" decision, the Court stated that the reasoning, in that case, was "gravely mistaken" and "sits uneasily with 120 years of preceding case law." The fact that Louisiana and Oregon may need to retry defendants convicted of felonies by non-unanimous verdicts whose cases are still pending on direct appeal "will surely impose a cost, but new rules of criminal procedure usually do."

Read Opinion Are you a lawyer? **Annotate this case**.

Brandt v. Fitzpatrick

Court: US Court of Appeals for the First Circuit
Docket: 19-1174
Opinion Date: April 22, 2020
Judge: Ojetta Rogeriee Thompson
Areas of Law: Civil Rights, Labor & Employment Law

The First Circuit affirmed the district court's grant of summary judgment against Appellant and dismissing his race discrimination and retaliation claims against the Maine Department of Corrections (MDOC), holding that Appellant lacked the proof needed to reach trial. Appellant left his job with MDOC as a state corrections officer to apply for a position in the federal prison system. Appellant met the minimum qualification and interviewed for each open spot but was turned down each time. Appellant subsequently

reapplied for his former job, but MDOC refused to rehire him. Appellant sued MDOC in federal court for race discrimination and retaliation. The district court judge granted summary judgment for MDOC. The First Circuit affirmed, holding that a reasonable jury could not find that MDOC's rejection of Appellant's application for reinstatement was a product of unlawful discrimination or made in retaliation for his complaint to the Maine Human Rights Commission.

Read Opinion Are you a lawyer? **Annotate this case**.

Trahan v. Wayfair Maine LLC

Court: US Court of Appeals for the First Circuit
Docket: 19-1961
Opinion Date: April 21, 2020
Judge: Selya
Areas of Law: Civil Rights, Labor & Employment Law

The First Circuit affirmed the decision of the district court granting summary judgment in favor of Employer in this disability discrimination case brought by Plaintiff, a former employee, holding that the district court did not err in entering summary judgment against Plaintiff on her claims. Plaintiff was a military veteran who suffers from post-traumatic stress disorder (PTSD). After she was discharged from her employment, Plaintiff sued Employer for disability discrimination under the Americans with Disabilities Act (ADA), 42 U.S.C. 12101-12213, and the Maine Human Rights Act, Me. Stat. tit. 5 4551-4634, alleging that she was wrongfully discharged based on her PTSD. Plaintiff also claimed that Employer unlawfully failed to accommodate her disability. The district court granted summary judgment for Employer. The First Circuit affirmed, holding that the district court properly granted summary judgment for Employer on Plaintiff's discriminatory discharge claim and failure to accommodate claim.

Read Opinion Are you a lawyer? **Annotate this case**.

Ali v. Woodbridge Township School District

Court: US Court of Appeals for the Third Circuit
Docket: 19-2217

Opinion Date: April 22, 2020
Judge: Greenaway
Areas of Law: Civil Rights, Constitutional Law, Education Law, Labor & Employment Law

Ali, a non-practicing Muslim of Egyptian descent, was a non-tenured high school teacher. His supervisor received complaints about Ali's instruction on the Holocaust. One English teacher reported that her students were questioning historical accounts of the Holocaust, opining that Hitler didn't hate the Jews and that the death counts were exaggerated. Students' written assignments confirmed those accounts. Ali also presented a lesson on the September 11 terrorist attacks, requiring students to read online articles translated by the Middle Eastern Media Research Institute (MEMRI). Ali posted links to the articles on a school-sponsored website: "U.S. Planned, Carried Out 9/11 Attacks—But Blames Others" and "U.S. Planning 9/11 Style Attack Using ISIS in Early 2015." The MEMRI articles also contained links to other articles, such as "The Jews are Like a Cancer, Woe to the World if they Become Strong." A reporter questioned Principal Lottman and Superintendent Zega. Lottman directed Ali to remove the MEMRI links from the school's website. The following morning, Ali met with Zega and Lottman; his employment was terminated. Ali sued under New Jersey law and 42 U.S.C. 1981, claiming that Lottman referred to him as "Mufasa," asked Ali if "they had computers in Egypt," and remarked on his ethnicity during the meetings that resulted in Ali's termination. He alleged discrimination, hostile work environment, free speech and academic freedom violations, and defamation. The Third Circuit affirmed summary judgment in favor of the defendants. Ali cannot show that his termination for teaching anti-Semitic views was a pretext for discrimination.

Read Opinion Are you a lawyer? **Annotate this case**.

Fogle v. Sokol

Court: US Court of Appeals for the Third Circuit
Docket: 19-1066
Opinion Date: April 21, 2020
Judge: Matey
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

In 1976, the body of 15-year-old "Kathy" was found near her Indiana

County, Pennsylvania home. Kathy's death involved a brutal assault, rape, and a gunshot to the head. Kathy's sisters, ages nine and 12, stated that she had gotten into a car with a man with blue eyes, black hair that came below his ears and curled at the ends, sideburns, heavy eyebrows, and a heavy mustache. Fogle had "straight reddish-blonde hair that dropped down his back and a matching, full beard that reached his waist." After three years, Fogle became a suspect because a psychiatric patient described seeing Kathy get in a car with Fogle and his brother. The story was largely inconsistent with statements by Kathy's sisters. Jailhouse informants were recruited and counseled by law enforcement with promises of leniency. The prosecutors "either knew about, encouraged, or permitted" this strategy. A jury found Fogle guilty of second-degree murder. In 2015, Fogle obtained DNA evidence excluding both himself and his brother as the source of semen collected from Kathy. His conviction was vacated. The Commonwealth declined to pursue new charges, describing the case as lacking "prosecutorial merit." Fogle, having spent three decades in prison, sued the prosecutors and Indiana County under 42 U.S.C. 1983. The Third Circuit affirmed the denial of their motions to dismiss based on absolute immunity. Only truly prosecutorial functions, not investigative conduct, justify complete protection from suit. Fogle's complaint alleges actions that fall outside the narrow doctrine of absolute immunity.

Read Opinion Are you a lawyer? **Annotate this case**.

Hope v. Warden Pike County Correctional Facility

Court: US Court of Appeals for the Third Circuit
Docket: 20-1784
Opinion Date: April 21, 2020
Judge: Smith
Areas of Law: Civil Procedure, Civil Rights, Constitutional Law, Immigration Law

On April 3, 2020, 20 immigration detainees filed a habeas petition (28 U.S.C. 2241), seeking immediate release, claiming that due to underlying health conditions, their continued detention during the COVID-19 pandemic puts them at imminent risk of death or serious injury. The district court found that the petitioners face irreparable harm and are likely to succeed on the merits, that the government would "face very little potential harm" from their immediate release, and that "the public interest strongly encourages

Petitioners' release." Without waiting for a response from the government, the court granted a temporary restraining order (TRO) requiring the release. The government moved for reconsideration, submitting a declaration describing conditions at the facilities, with details of the petitioners' criminal histories. The court denied reconsideration, stating that the government had failed to demonstrate a change in controlling law, provide previously unavailable evidence, or show a clear error of law or the need to prevent manifest injustice. The court extended the release period until the COVID-19 state of emergency is lifted but attached conditions to the petitioners' release. The government reports that 19 petitioners were released; none have been re-detained. The Third Circuit granted an immediate appeal, stating that the order cannot evade prompt appellate review simply by virtue of the label "TRO." A purportedly non-appealable TRO that goes beyond preservation of the status quo and mandates affirmative relief may be immediately appealable under 28 U.S.C. 1292(a)(1).

Read Opinion Are you a lawyer? **Annotate this case**.

James v. New Jersey State Police

Court: US Court of Appeals for the Third Circuit
Docket: 18-1432
Opinion Date: April 21, 2020
Judge: Porter
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Stephens called 911 and reported that Gibbons hit her and had a gun in his truck. The police responded. Stephens obtained a temporary restraining order, prohibiting Gibbons from possessing firearms and from returning to Stephens's house. The next day, Gibbons went to Stephens's house. Stephens was talking on the phone; the friend called the police. Gibbons left Stephens's house. Trooper Conza arrived. Stephens stated that Gibbons had waved a gun throughout their argument. Conza told Stephens to go to the police barracks and reported over the radio that Gibbons had brandished a firearm. Conza, with Troopers Bartelt and Korejko, visited the nearby home of Gibbons's mother, James. James stated that she did not know where Gibbons was and that he might be off his schizophrenia medication. While driving to the barracks, Stephens saw Gibbons walking alongside the road and called 911. The Troopers responded. Bartelt parked

his car and, exiting, observed that Gibbons was pointing a gun at his own head. Bartelt drew his weapon, stood behind his car door, and twice told Gibbons to drop his weapon. Gibbons did not comply. Bartelt shot Gibbons twice within seconds of stopping his car. Gibbons died that night. In James' suit under 42 U.S.C. 1983, the Third Circuit held that Bartelt is entitled to qualified immunity because he did not violate Gibbons's clearly established rights. Bartelt's pre-standoff knowledge of Gibbons differs from that of officers involved in cited cases. Bartelt could reasonably conclude that Gibbons posed a threat to others.

Read Opinion Are you a lawyer? **Annotate this case**.

In re: Greg Abbott

Court: US Court of Appeals for the Fifth Circuit
Docket: 20-50296
Opinion Date: April 20, 2020
Judge: Jennifer Walker Elrod
Areas of Law: Civil Rights, Constitutional Law, Health Law

On April 7, 2020, the Fifth Circuit issued a writ of mandamus vacating the district court's temporary restraining order (TRO) that exempted abortions from GA-09, an emergency measure temporarily postponing non-essential medical procedures during the COVID-19 pandemic. On April 9, 2020, the district court entered a second TRO exempting various categories of abortion from GA-09. At issue in this mandamus petition is the April 9 TRO. The court held that the district court disregarded the court's mandate in Abbott II and failed to apply the framework governing emergency exercises of state authority during a public health crisis, established over 100 years ago in Jacobson v. Commonwealth of Massachusetts, 197 U.S. 11 (1905). Furthermore, the district court second-guessed the basic mitigation strategy underlying GA-09 (the concept of "flattening the curve"), and also acted without knowing critical facts such as whether, during this pandemic, abortion providers do (or should) wear masks or other protective equipment when meeting with patients. The court concluded that these errors resulted in an overbroad TRO that exceeds the district court's jurisdiction, reaches patently erroneous results, and usurps the state's authority to craft emergency public health measures "during the escalating COVID-19 pandemic." Therefore, the court granted the writ in part and directed the

district court to vacate parts of the April 9 TRO.

Read Opinion Are you a lawyer? **Annotate this case**.

Sanchez v. Young County

Court: US Court of Appeals for the Fifth Circuit
Docket: 19-10222
Opinion Date: April 22, 2020
Judge: Edith Brown Clement
Areas of Law: Civil Rights, Constitutional Law

After Diana Simpson died of a drug overdose while she was a pretrial detainee at the Young County Jail, her family filed suit under 42 U.S.C. 1983, alleging Eighth and Fourteenth Amendment violations, as well as a claim under the Texas Tort Claims Act. The Fifth Circuit previously affirmed summary judgment for the County in part, and remanded in part for the district court to evaluate plaintiffs' conditions-of-confinement theory in the first instance. On remand, the district court granted summary judgment on that theory and plaintiffs appealed. The court affirmed the district court's dismissal of plaintiffs' claims based on a failure to train based on the law-of-the-case doctrine. The court held that the district court erred in dismissing plaintiffs' claims based on a failure to monitor because plaintiffs' evidence, when viewed in the light most favorable to them, creates several disputes of material fact about whether the jail has a de facto policy of inadequately monitoring detainees. Furthermore, plaintiffs offered sufficient evidence to create fact issues over whether the County failed to assess pretrial detainees' medical needs and whether this caused plaintiff to be denied needed medical care. Accordingly, the court reversed in part and affirmed in part, remanding for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

Singleton v. Cannizzaro

Court: US Court of Appeals for the Fifth Circuit
Docket: 19-30197
Opinion Date: April 21, 2020
Judge: Catharina Haynes

Areas of Law: Civil Rights, Constitutional Law

Plaintiffs allege that for years, prosecutors at the Orleans Parish District Attorney's Office, under the direction of District Attorney Leon Cannizzaro, used fake "subpoenas" to pressure crime victims and witnesses to meet with them. The Fifth Circuit held that (1) at this early, motion to dismiss stage, the individual defendants are not entitled to absolute immunity for plaintiffs' subpoena-related state-law claims and (2) the court lacked jurisdiction to consider the merits of plaintiffs' claims. Accordingly, the court affirmed the district court's holding that the individual defendants are not entitled to absolute immunity for their alleged creation and use of fraudulent subpoenas, but dismissed the remainder of defendants' appeal for lack of jurisdiction.

Read Opinion Are you a lawyer? **Annotate this case**.

Valentine v. Collier

Court: US Court of Appeals for the Fifth Circuit
Docket: 20-20207
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Criminal Law, Government & Administrative Law, Health Law

Plaintiffs filed suit alleging that TDCJ's adoption and implementation of measures guided by changing CDC recommendations in regards to the COVID-19 pandemic do not go far enough. Plaintiffs filed a class action alleging violations of the Eighth Amendment's prohibition against cruel and unusual punishment, and the Americans with Disabilities Act, seeking a preliminary injunction. The Fifth Circuit granted TDCJ's motion to stay the district court's preliminary injunction, which regulates the cleaning intervals for common areas, the types of bleach-based disinfectants the prison must use, the alcohol content of hand sanitizer that inmates must receive, mask requirements for inmates, and inmates' access to tissues (amongst many other things). The court held that TDCJ is likely to prevail on the merits of its appeal because: (1) after accounting for the protective measures TDCJ has taken, plaintiffs have not shown a "substantial risk of serious harm" that amounts to "cruel and unusual punishment"; and (2) the district court

committed legal error in its application of Farmer v. Brennan, by treating inadequate measures as dispositive of defendants' mental state. In this case, even assuming that there is a substantial risk of serious harm, plaintiffs lack evidence of defendants' subjective deliberate indifference to that harm. The court also held that TDCJ has shown that it will be irreparably injured absent a stay, and that the balance of the harms and the public interest favor a stay. Finally, the court held that plaintiffs have not exhausted their administrative remedies as required in the Prison Litigation Reform Act (PLRA), and the district court's injunction goes well beyond the limits of what the PLRA would allow even if plaintiffs had properly exhausted their claims.

Read Opinion Are you a lawyer? **Annotate this case**.

Williams v. Banks

Court: US Court of Appeals for the Fifth Circuit
Docket: 17-60716
Opinion Date: April 23, 2020
Judge: Priscilla R. Owen
Areas of Law: Civil Rights, Constitutional Law

The Fifth Circuit affirmed the district court's grant of summary judgment to prison officials in a 42 U.S.C. 1983 action brought by plaintiff, an inmate in custody at the MDOC, alleging that defendants violated the Eighth and Fourteenth Amendments by being deliberately indifferent to the risk that another inmate would harm plaintiff. The court held that plaintiff's claims against defendants in their official capacities are barred under sovereign immunity. The court also held that the magistrate judge correctly granted summary judgment on plaintiff's theory that defendants failed to protect him from the other inmate, where there is no evidence in the record to suggest that defendants knew the inmate was a member of a gang or otherwise posed a specific threat to plaintiff when they moved him into plaintiff's zone. Furthermore, the magistrate judge correctly granted summary judgment on plaintiff's theory that defendants violated plaintiff's constitutional rights because they placed the inmate into plaintiff's protective custody zone instead of following MDOC policy and placing the inmate in lockdown. In this case, defendants did not disregard an excessive risk to inmate health or safety.

Read Opinion Are you a lawyer? **Annotate this case**.

Gary B. v. Whitmer

Court: US Court of Appeals for the Sixth Circuit
Dockets: 18-1855, 18-1871
Opinion Date: April 23, 2020
Judge: Eric L. Clay
Areas of Law: Civil Rights, Constitutional Law, Education Law

Students at several of Detroit's worst-performing public schools were subject to poor conditions within their classrooms, missing or unqualified teachers, physically dangerous facilities, and inadequate books and materials. In 2016, the plaintiffs filed suit under 42 U.S.C. 1983, claiming that these conditions deprive them of a basic minimum education that provides a chance at foundational literacy, in violation of the due process and equal protection clauses. They sought recognition of a fundamental right to a basic education. They argued that the schools they are forced to attend are schools in name only, so the state cannot justify the restriction on their liberty imposed by compulsory attendance. They sued state officials, rather than local entities, based on the state's general supervision of all public education and the state's specific interventions in Detroit's public schools. The state argued that it recently returned control to local officials. The district court found that the state defendants were the proper parties to sue but dismissed the complaint on the merits. The Sixth Circuit reversed in part. Though the plaintiffs failed to adequately plead their equal protection and compulsory attendance claims, the court reinstated claims that they have been denied a basic minimum education, and have been deprived of access to literacy. Application of the principles in the Supreme Court's education cases to a substantive due process framework demonstrates that a basic minimum education should be recognized as a fundamental right.

Read Opinion Are you a lawyer? **Annotate this case**.

Queen v. City of Bowling Green

Court: US Court of Appeals for the Sixth Circuit
Docket: 18-5840

Opinion Date: April 22, 2020
Judge: Bush
Areas of Law: Civil Rights, Constitutional Law, Labor & Employment Law

Queen, a Bowling Green firefighter, 2011-2016, was subject to harassment because he is an atheist. According to Queen, he was forced to participate in Bible studies; his co-workers and supervisors badgered him regarding his sexuality and regularly disparaged minorities. In 2012, Queen complained to his supervisor, Rockrohr, who "responded in hostility." Rockrohr later told Queen that he had discussed the matter with the fire chief and they both believed that Queen "needed to get employment somewhere else." Queen apologized. Queen's employment conditions did not improve. Queen was intentionally tripped while retrieving his gear and was regularly subject to disparaging remarks. Stress and anxiety caused Queen to take a leave of absence. While on leave, Queen received many phone calls from his supervisors asking why he was absent. Queen resigned and filed suit under the Kentucky Civil Rights Act, alleging hostile work environment based on religion and gender, constructive discharge, retaliation, and violations of the Family and Medical Leave Act. The district court granted the defendants summary judgment on hostile work environment based on religion and gender and the FMLA claims. On interlocutory appeal, the Sixth Circuit affirmed the denial of qualified immunity to the city on the claims for hostile work environment based on religion and for retaliation and denial of qualified immunity to Rockrohr for the retaliation claim.

Read Opinion Are you a lawyer? **Annotate this case**.

Winburn v. Nagy

Court: US Court of Appeals for the Sixth Circuit
Dockets: 19-2399, 19-2398
Opinion Date: April 23, 2020
Judge: Jeffrey S. Sutton
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Winburn represented himself at his trial for armed robbery, home invasion, and conspiracy. Based on Winburn's disruptive behavior, the judge removed him from the courtroom and revoked Winburn's permission to represent himself, then granted a competency evaluation and a mistrial. While Winburn awaited his second trial, the judge permitted Winburn's stand-by

attorney to withdraw because Winburn had sued her and enjoined Winburn from filing complaints or grievances against his new attorney, except to discharge her. Although represented by a new attorney, Winburn moved pro se to dismiss his charges on double jeopardy grounds. The trial judge denied the motion because Winburn's attorney had not filed it. Winburn filed a habeas petition under 28 U.S.C. 2241 challenging his retrial and another section 2241 petition challenging the injunction. The district judges denied both and declined to issue certificates of appealability. Winburn filed a notice of appeal for one petition and sought a certificate of appealability for the other. The Sixth Circuit held that state pretrial detainees proceeding under section 2241 may not appeal without certificates of appealability and granted Winburn a certificate on the injunction claim. A reasonable jurist could conclude that the unusual order was constitutionally infirm. The court denied relief with respect to double jeopardy. Winburn failed to exhaust his state-court remedies by a motion to dismiss.

Read Opinion Are you a lawyer? **Annotate this case**.

Lund v. City of Rockford

Court: US Court of Appeals for the Seventh Circuit
Docket: 19-1945
Opinion Date: April 20, 2020
Judge: ROVNER
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Lund, a reporter for the Rockford Scanner, heard, by police scanner, of multiple traffic stops in Midtown. He did not have a driver's license, so he rode a motorized bicycle to Midtown to take photographs. He suspected a prostitution sting operation. An officer noticed Lund and radioed the team. Officers Welsh and Campbell knew of Lund's previous anti-police speech. They directed Lund to "move on." Lund asked if he was breaking any laws. Campbell informed him that he was not, but that his continued presence would constitute obstruction of a police detail and result in arrest. Lund started his bicycle and called out, loudly, "goodbye officers." Concerned that Lund might post pictures on social media while the sting operation was ongoing and create a danger for unarmed undercover officers, the officers followed Lund and arrested him for driving the wrong way on a one-way street, operating a vehicle without insurance, obstructing a police officer,

felony aggravated driving on a revoked license, and operating a motor vehicle without a valid drivers' license. News stories listed Lund's name as an arrestee in the prostitution sting. The charges against Lund were dismissed. Lund sued the officers and the city under 42 U.S.C. 1983. The Seventh Circuit affirmed summary judgment for the defendants on First Amendment retaliation and malicious prosecution under Illinois law, citing the Supreme Court's intervening "Nieves" (2019) holding, that, in most cases, probable cause to arrest defeats a claim of retaliatory arrest. There was probable cause to arrest Lund.

Read Opinion Are you a lawyer? **Annotate this case**.

Mayle v. Illinois

Court: US Court of Appeals for the Seventh Circuit
Docket: 19-1691
Opinion Date: April 23, 2020
Judge: HAMILTON
Areas of Law: Civil Procedure, Civil Rights, Family Law, Government & Administrative Law

Mayle, a self-proclaimed Satanist, is a follower of The Law of Thelema, a set of beliefs developed in the early 1900s by Aleister Crowley. As part of this religion, Mayle participates in what he calls "sex magick rituals" that he believes violate Illinois laws forbidding adultery and fornication. He claims that he reasonably fears prosecution for practicing his beliefs. He also says that he wants to marry more than one person at the same time and that if he were to do so, he would violate an Illinois law against bigamy. Mayle's first challenge to the laws was dismissed. Mayle did not appeal, but the next year he filed another suit challenging the same statutes. The Seventh Circuit affirmed the dismissal of the second suit, first rejecting a challenge to the district court's grant of a two-day extension to allow Mayle to file a notice of appeal. Mayle's bigamy claim was precluded by the 2017 final judgment on the merits. Mayle lacked standing to challenge the state's adultery and fornication laws because he still showed no reasonable fear of prosecution; those laws are no longer enforced.

Read Opinion Are you a lawyer? **Annotate this case**.

In Re: Leslie Rutledge

Court: US Court of Appeals for the Eighth Circuit
Docket: 20-1791
Opinion Date: April 22, 2020
Judge: Bobby E. Shepherd
Areas of Law: Civil Rights, Constitutional Law, Health Law

The Eighth Circuit granted a writ of mandamus in part and directed the district court to dissolve a Temporary Restraining Order (TRO) enjoining the State from enforcing a COVID-19-related health directive against a provider of surgical abortions. The Arkansas Department of Health (ADH) issued a directive requiring that all non-medically necessary surgeries be postponed in response to Executive Order 20-03, directing the ADH to do everything reasonably possible to respond to and recover from the COVID-19 virus. After adopting the Fifth Circuit's reasoning in In re Abbott, No. 20-50264, 2020 WL 1685929 (5th Cir. April 7, 2020), the court held that the State is entitled to mandamus relief because it has satisfied its burden in demonstrating that it has no other means to obtain the relief that it seeks, the State is clearly and indisputably entitled to the writ, and entry of the writ is appropriate under the circumstances. In Jacobson v. Massachusetts, 197 U.S. 11 (1905), the Supreme Court held that, when faced with a public health crisis, a state may implement measures that infringe on constitutional rights, subject to certain limitations. The court found that the district court's failure to apply the Jacobson framework produced a patently erroneous result. In this case, the directive bears a real and substantial relation to the State's interest in protecting public health in the face of the COVID-19 pandemic; the directive is not, beyond all question, a prohibition of pre-viability abortion in violation of the Constitution because it is a delay, not a ban, and contains emergency exceptions; and the district court clearly abused its discretion in finding that the provider is likely to prevail on its argument that the directive will likely operate as a substantial obstacle to a woman's choice to undergo an abortion in a large fraction of the cases in which the directive is relevant. The court declined to exercise its mandamus power to direct the district court to dismiss the supplemental complaint, and denied the emergency motion to stay the ex parte TRO and for a temporary administrative stay as moot.

Read Opinion Are you a lawyer? **Annotate this case**.

Lombardo v. City of St. Louis

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1469
Opinion Date: April 20, 2020
Judge: Bobby E. Shepherd
Areas of Law: Civil Rights, Constitutional Law

The Eighth Circuit affirmed the magistrate judge's grant of summary judgment in favor of law enforcement officers and the City, in a 42 U.S.C. 1983 action brought by plaintiff after the death of her son. The court held that the officers' actions did not amount to constitutionally excessive force. In this case, the undisputed facts show that the officers discovered the son acting erratically, and even though the son was held in a secure cell, it was objectively reasonable for the officers to fear that he would intentionally or inadvertently physically harm himself. Furthermore, the son actively resisted the officers' attempts to subdue him, and officers held him in the prone position only until he stopped actively fighting against the restraints and the officers. Therefore, the court held that the officers are entitled to qualified immunity on plaintiff's excessive force claim.

Read Opinion Are you a lawyer? **Annotate this case**.

Anthony v. TRAX International Corp.

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-15662
Opinion Date: April 17, 2020
Judge: Kim McLane Wardlaw
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Ninth Circuit affirmed the district court's grant of summary judgment to TRAX in a disability discrimination action brought by plaintiff under Title I of the Americans with Disabilities Act (ADA). After TRAX terminated plaintiff from her position as a Technical Writer allegedly due to an inability or unwillingness to accommodate her disability, TRAX discovered during the course of litigation that plaintiff lacked the requisite bachelor's degree for her position. The panel held that, although McKennon v. Nashville Banner Publishing Co., 513 U.S. 352 (1995), held that after-acquired evidence

cannot establish a superseding, non-discriminatory justification for an employer's challenged actions, after-acquired evidence remains available for other purposes, including to show that an individual is not qualified under the ADA. Because plaintiff did not satisfy one of the prerequisites for her position, she is not "otherwise qualified," and TRAX was not obligated to engage in the interactive process.

Read Opinion Are you a lawyer? **Annotate this case**.

Wilk v. Neven
Court: US Court of Appeals for the Ninth Circuit
Docket: 17-17355
Opinion Date: April 23, 2020
Judge: William A. Fletcher
Areas of Law: Civil Rights, Constitutional Law

The Ninth Circuit reversed the district court's grant of summary judgment for prison officials in a 42 U.S.C. 1983 action alleging that defendants violated plaintiff's right to be free from cruel and unusual punishment when they failed to protect him from an attack by another inmate. The panel held that defendants violated plaintiff's Eighth Amendment right to be protected from serious harm while incarcerated. The panel also held that a reasonable fact-finder would be able to conclude that defendants were subjectively aware of the substantial risk of serious harm to plaintiff, and failed to respond reasonably; any reasonable prison official in the defendants' position would know that the actions defendants took, and failed to take, violated the Eighth Amendment; none of the defendants can claim ignorance to a prisoner's right to be protected from violence at the hands of other inmates where that right has been clearly established in Farmer v. Brennan, 511 U.S. at 833 (1994). Finally, the panel noted that throughout proceedings in the district court plaintiff struggled to obtain discovery from defendants. On remand, plaintiff should have another opportunity to seek the materials he requested previously, and the panel encouraged the district court to appoint him counsel.

Read Opinion Are you a lawyer? **Annotate this case**.

Barnett v. Hall, Estill, Hardwick, Gable

Court: US Court of Appeals for the Tenth Circuit
Docket: 18-5090
Opinion Date: April 20, 2020
Judge: Harris L. Hartz
Areas of Law: Civil Procedure, Civil Rights

Plaintiff Christopher Barnett appealed the dismissal with prejudice his federal civil-rights claims for failure to state a claim and dismissing with prejudice his state-law claims because they did not survive the restrictions imposed by the Oklahoma Citizens Participation Act (OCPA), Okla. Stat. tit. 12, sections 1430–40 . Defendants cross-appealed the district court's denial of attorney fees under the OCPA, contending that an award of attorney fees was mandatory. Barnett's complaint bases his claims on an incident on January 4, 2018, related to a hearing in Oklahoma state court on an open-records case he had brought against Tulsa Community College. According to Barnett, two lawyers in the firm of Hall, Estill, Hardwick, Gable, Golden & Nelson, P.C., (Hall Estill) falsely reported to the office of the state attorney general (AG) that Barnett had made a threat. The AG's office then relayed this report to the county sheriff. When Barnett arrived at the courtroom for the hearing, the state-court judge instructed him to speak with a deputy sheriff. After Barnett denied making any threat, the deputy told him to stay inside the courtroom until he received permission to leave. At some point the AG's office arrived with its own security detail. When the proceedings began, the state-court judge discussed the report in open court. Barnett filed suit in state court the next day against Hall Estill, and Tulsa University (TU), alleging federal civil-rights claims under 42 U.S.C. 1983 and state tort claims because he had been unlawfully seized when he was forbidden to leave the courtroom, had been cast in a false light by the public airing of the alleged threat, and had been retaliated against by Defendants for his exercise of his rights to free speech and access to the courts. After review, the Tenth Circuit affirmed dismissal of the federal-law claims, agreeing with the district court that the complaint did not adequately allege that any of the Defendants acted under color of state law. But the Court reversed judgment on the state-law claims and remanded to the district court with instructions to dismiss the claims without prejudice or remand them to the state court.

Read Opinion Are you a lawyer? **Annotate this case**.

Durham v. Rural/Metro Corp.

Court: US Court of Appeals for the Eleventh Circuit
Docket: 18-14687
Opinion Date: April 17, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Labor & Employment Law

After plaintiff asked her employer, Rural, for a temporary light-duty or dispatcher assignment for the duration of her pregnancy because her physician advised her to refrain from lifting more than 50 pounds while pregnant, Rural declined plaintiff's request for accommodation. Plaintiff filed suit against Rural, alleging discrimination under the Pregnancy Discrimination Act (PDA). The Eleventh Circuit vacated the district court's grant of Rural's motion for summary judgment, holding that the district court erroneously factored into the "similar in their ability or inability to work" evaluation the distinct, post-prima-facie-case consideration of Rural's purported legitimate, non-discriminatory reasons for treating plaintiff and the non-pregnant employees differently. The court explained that neither a non-pregnant EMT who is limited to lifting 10 or 20 pounds nor a pregnant EMT who is restricted to lifting 50 pounds or less can lift the required 100 pounds to serve as an EMT. Consequently, neither can meet the lifting requirement and are thus the same in their "inability to work" as an EMT. The court held that plaintiff's prima facie requirement to establish that she was similarly situated to other employees in their ability or inability to work was satisfied. The court remanded for the district court to determine the remaining issues in the first instance.

Read Opinion Are you a lawyer? **Annotate this case**.

Cave v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 356
Opinion Date: April 23, 2020
Judge: Josephine L. Hart
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's pro se petition for writ of habeas corpus, holding that the circuit

court did not err in denying the petition. Appellant was found guilty of two counts of delivery of a controlled substance and one count of maintaining a drug premises. In his habeas petition, Appellant argued that he was actually innocent because his arrest and conviction was based on the false testimony of a witness who had a lengthy criminal history. Appellant further argued that the writ should issue because he was not afforded effective assistance of counsel. The circuit court denied the petition. The Supreme Court affirmed, holding (1) Appellant's claims regarding the witness's credibility do not constitute a valid assertion that he was being unlawfully detained; and (2) Appellant did not actually connect an allegation of ineffective assistance of counsel to his allegation that he was unlawfully detained.

Read Opinion Are you a lawyer? **Annotate this case**.

Thomas v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 354
Opinion Date: April 23, 2020
Judge: Josephine L. Hart
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Appellant's conviction of capital murder, holding that the evidence was sufficient to sustain the conviction and that the circuit court did not err in denying Appellant's motion to suppress tracking data generated by his cellphone. On appeal, Appellant argued that the trial court erred by denying his directed-verdict motion because the evidence supported the defense's theory of the case that he did not intend to shoot the victim. Further, Appellant argued that the court abused its discretion in denying his motion to suppress evidence obtained from the seizure of AT&T phone records. The Supreme Court disagreed, holding (1) the evidence was sufficient to support the capital murder conviction; and (2) the circuit court correctly denied the motion to suppress.

Read Opinion Are you a lawyer? **Annotate this case**.

Pinter-Brown v. The Regents of the University of California

Court: California Courts of Appeal
Docket: B290086(Second Appellate District)
Opinion Date: April 23, 2020
Judge: Stratton
Areas of Law: Civil Rights, Constitutional Law

Plaintiff filed suit against The Regents for gender discrimination based on a series of events that took place while she was a Professor of Medicine at UCLA. The jury found in favor of plaintiff, awarding her economic and noneconomic damages. The Court of Appeal reversed and held that the trial court committed a series of grave errors that significantly prejudiced The Regents' right to a fair trial by an impartial judge. In this case, the trial court delivered a presentation to the jury highlighting major figures in the civil rights movement, and told the jury their duty was to stand in the shoes of Dr. Martin Luther King and bend the arc of the moral universe toward justice; the trial court allowed the jury to hear about and view a long list of discrimination complaints from across the entire University of California system that were not properly connected to plaintiff's circumstances or her theory of the case; the trial court allowed the jury to learn of the contents and conclusions of the Moreno Report, which documented racial discrimination occurring throughout the entire UCLA campus; and the trial court allowed plaintiff to resurrect a retaliation claim after the close of evidence despite having summarily adjudicated that very claim prior to trial. The court held that these errors were cumulative and highly prejudicial, and were evidence of the trial court's inability to remain impartial, creating the impression that the trial court was partial to plaintiff's claims.

Read Opinion Are you a lawyer? **Annotate this case**.

Archer v. State

Court: Florida Supreme Court
Docket: SC19-841
Opinion Date: April 23, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the order of the circuit court denying Appellant's successive motion to vacate his sentence of death under Fla. R. Crim. P. 3.851, holding that the circuit court did not err in denying the Rule

3.851 motion. Appellant was convicted of first-degree murder, armed robbery, and grand theft. Appellant was sentenced to death for the murder. The Supreme Court affirmed the convictions but reversed Appellant's death sentence and remanded the case for a new penalty phase. After a new penalty phase, Appellant was again sentenced to death. In his successive Rule 3.851 motion, Appellant raised three claims. The circuit court denied relief. The Supreme Court affirmed, holding that the circuit court (1) properly denied Appellant's claim that his death sentence violated the Sixth and Eighth Amendments in light of Hurst v. Florida, 136 S. Ct. 616 (2016), and Hurst v. State, 202 So. 3d 40 (Fla. 2016); (2) correctly denied Appellant's claim that his sentence violated the Eighth Amendment; and (3) did not err in denying Appellant's claim of newly discovered evidence.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Gibbs

Court: Iowa Supreme Court
Docket: 18-1298
Opinion Date: April 17, 2020
Judge: Edward M. Mansfield
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction of murder in the second degree, holding that Defendant's Fifth Amendment rights were invaded when the trial judge instructed the jury that Defendant was required to notify law enforcement of his use of deadly force, but the error was harmless. During trial, Defendant asserted the defense of justification in his shooting of the victim. At issue on appeal was whether the district court abused its discretion by giving a jury instruction incorporating the terms of Iowa Code 704.2B. The instruction included a statement that a person using deadly force is required to notify law enforcement about his use of deadly force. Defendant argued before the Supreme Court that both section 704.2B and the jury instruction incorporating that section violated his Fifth Amendment rights. The Supreme Court affirmed, holding (1) instructing the jury that a homicide defendant is required to notify a law enforcement agency of his use of deadly force violates the defendant's Fifth Amendment rights; but (2) any error in this case was harmless beyond a reasonable doubt.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Harris

Court: Kansas Supreme Court
Docket: 117362
Opinion Date: April 17, 2020
Judge: Wilson
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court reversed the judgment of the court of appeals affirming Defendant's conviction of possession fo marijuana, holding that Defendant's waiver of jury trial was legally insufficient. On appeal, Defendant argued that he did not properly waive his right to a jury and asserted three other issues. The Supreme Court reversed the judgment of the court of appeals affirming Defendant's convictions without addressing the three remaining issues, holding that because the district court failed properly to apprise Defendant of his right to a jury trial and failed to ensure that Defendant understood the nature of the right he was giving up, Defendant's constitutional right to a jury trial was violated in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. McCarthy

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12750
Opinion Date: April 16, 2020
Judge: Gaziano
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Judicial Court affirmed the judgment of the district court denying Defendant's motions to suppress, holding that the limited use of automatic license plate readers (ALPRs) in this case did not implicate constitutional protections against unreasonable searches. While police were investigating Defendant on suspicion of drug distribution they used ALPRs on two bridges to track Defendant's movements. The police accessed historical data via ALPR technology and received real-time alerts, the last of

which led to Defendant's arrest. Defendant filed motions to suppress the ALPR data and the fruits of the arrest. The superior court denied the motions. The Supreme Judicial Court affirmed, holding that while the widespread use of ALPRs in the Commonwealth could implicate a defendant's constitutional protected expectation of privacy in the whole of his public movements, that interest was not invaded by the limited extent and use of the ALPR data in the instant case.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Reek

Court: Minnesota Supreme Court
Docket: A19-0153
Opinion Date: April 22, 2020
Judge: G. Barry Anderson
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction for first-degree murder, holding that there was no error in the proceedings below. Specifically, the Supreme Court held (1) Appellant's right to a fair trial before an impartial tribunal was not violated when the district court stated that it might reconsider its prior Spreigl ruling if the defense presented certain witnesses; (2) the jury instructions on accomplice liability were plainly erroneous, but Appellant failed to establish that there was a reasonable likelihood that the error had a significant effect on the verdict; (3) the prosecutor did not commit misconduct in his closing arguments regarding the law of accomplice liability; (4) the district court did not abuse its discretion by granting the State's motion to admit evidence of appellant's past convictions for impeachment purposes, including by allowing the specific convictions to be disclosed to the jury; and (5) Appellant's pro se arguments were without merit.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Montoya

Court: Nebraska Supreme Court
Citation: 305 Neb. 581

Opinion Date: April 17, 2020
Judge: Freudenberg
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the judgment of the district court affirming Defendant's conviction and sentence for driving under the influence, holding that there was no error in the challenged rulings by the trial court. Specifically, the Supreme Court held that the district court did not err by (1) affirming the county court's order denying Defendant's motion to suppress fruits of the stop; (2) affirming the county court's order that denied Defendant's motion to suppress the fruits of his arrest; (3) affirming the county court's order that denied Defendant's motion to suppress the results of the test of his breath alcohol content; (4) finding sufficient evidence to support the conviction; and (5) finding that Defendant's sentence was not excessive.

Read Opinion Are you a lawyer? **Annotate this case**.

Morrisey v. West Virginia AFL-CIO

Court: Supreme Court of Appeals of West Virginia
Docket: 19-0298
Opinion Date: April 21, 2020
Judge: Jenkins
Areas of Law: Civil Rights, Constitutional Law, Labor & Employment Law

The Supreme Court reversed the rulings of the circuit court finding that the Workplace Freedom Act (the Act) infringes upon the rights to associate, as well as the liberty and property rights, of labor unions that are member organizations of the AFL-CIO (Labor Unions), holding that the Act does not violate constitutional rights at issue. In 2016, the Legislature enacted the Act, which prohibits collective bargaining agreements that require an employee to pay any dues, fees, assessments, or other similar charges as a condition of employment, or as a condition for the continuation of employment, when the employee has chosen not to join a union. On remand, the circuit court ruled that the Act unconstitutionally fringes on the rights of the Labor Unions, who represent both private and government workers in West Virginia. The Supreme Court reversed, holding that the Act does not violate the West Virginia Constitution's protections of association, property, and liberty rights.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Taylor

Court: Supreme Court of Appeals of West Virginia
Docket: 18-0502
Opinion Date: April 21, 2020
Judge: Walker
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the judgment of the circuit court giving Petitioner credit for twelve days of time served toward the sentence he received for his felony conviction although Petitioner spent additional time in confinement for other charges that were dismissed in the universal plea agreement, holding that to grant Petitioner additional credit for time served would do little more than reward Petitioner for habitual criminal behavior. Petitioner was charged with several crimes and agreed to resolve the pending charges against him in a universal plea agreement. Under the terms of the agreement, Petitioner agreed to plea guilty to the charge of felony carrying a concealed firearm by a prohibited person. In exchange, the State agreed to drop the remaining charges. After he was sentenced, Petitioner argued that, in addition to the twelve days of credit for time served he was granted, he was constitutionally entitled to credit for time served while he was incarcerated for charges that were resolved in the universal plea agreement. The Supreme Court affirmed, holding that Petitioner's circumstances implicated neither double jeopardy nor equal protection of the law such that additional credit for time served was constitutionally mandated.

Read Opinion Are you a lawyer? **Annotate this case**.

About Justia Opinion Summaries

Justia Weekly Opinion Summaries is a free service, with 63 different newsletters, each covering a different practice area.

Justia also provides 68 daily jurisdictional newsletters, covering every

federal appellate court and the highest courts of all US states.

All daily and weekly Justia newsletters are free. Subscribe or modify your newsletter subscription preferences at daily.justia.com.

You may freely redistribute this email in whole.

About Justia

Justia is an online platform that provides the community with open access to the law, legal information, and lawyers.

Contact Us | Privacy Policy

Unsubscribe From This Newsletter
or unsubscribe from all Justia newsletters immediately **here.**

Justia | 1380 Pear Ave #2B, Mountain View, CA 94043

From: Constitutional Law - Justia Weekly Opinion Summaries
To: Caravaggio, Suzanne (POL)
Subject: Latest 65 Cases This Week: Ramos v. Louisiana (U.S.), Ali v. Woodbridge Township School District (3d Cir.), Fogle v. Sokol (3d Cir.)
Date: Friday, April 24, 2020 9:07:02 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

If you are unable to see this message, click here to view it in a web browser.

Justia Weekly Opinion Summaries

Constitutional Law
April 24, 2020

Table of Contents

Ramos v. Louisiana
Civil Rights, Constitutional Law, Criminal Law
US Supreme Court

Ali v. Woodbridge Township School District
Civil Rights, Constitutional Law, Education Law, Labor & Employment Law
US Court of Appeals for the Third Circuit

Fogle v. Sokol
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Third Circuit

Hope v. Warden Pike County Correctional Facility
Civil Procedure, Civil Rights, Constitutional Law, Immigration Law
US Court of Appeals for the Third Circuit

James v. New Jersey State Police
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Third Circuit

In re: Greg Abbott
Civil Rights, Constitutional Law, Health Law
US Court of Appeals for the Fifth Circuit

Sanchez v. Young County
Civil Rights, Constitutional Law
US Court of Appeals for the Fifth Circuit

Singleton v. Cannizzaro
Civil Rights, Constitutional Law
US Court of Appeals for the Fifth Circuit

Valentine v. Collier
Civil Rights, Constitutional Law, Criminal Law, Government & Administrative Law, Health Law
US Court of Appeals for the Fifth Circuit

Williams v. Banks
Civil Rights, Constitutional Law
US Court of Appeals for the Fifth Circuit

Gary B. v. Whitmer
Civil Rights, Constitutional Law, Education Law
US Court of Appeals for the Sixth Circuit

Lebamoff Enterprises, Inc., v. Whitmer
Constitutional Law, Government & Administrative Law
US Court of Appeals for the Sixth Circuit

Queen v. City of Bowling Green
Civil Rights, Constitutional Law, Labor & Employment Law
US Court of Appeals for the Sixth Circuit

Winburn v. Nagy
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Sixth Circuit

Lund v. City of Rockford
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

In Re: Leslie Rutledge
Civil Rights, Constitutional Law, Health Law
US Court of Appeals for the Eighth Circuit

Lombardo v. City of St. Louis
Civil Rights, Constitutional Law
US Court of Appeals for the Eighth Circuit

Anthony v. TRAX International Corp.
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Ninth Circuit

Wilk v. Neven
Civil Rights, Constitutional Law
US Court of Appeals for the Ninth Circuit

United States v. Manzanares
Constitutional Law, Criminal Law
US Court of Appeals for the Tenth Circuit

Durham v. Rural/Metro Corp.
Civil Rights, Constitutional Law, Labor & Employment Law
US Court of Appeals for the Eleventh Circuit

Gadsden Industrial Park, LLC v. United States
Constitutional Law, Environmental Law, Real Estate & Property Law, Zoning, Planning & Land Use
US Court of Appeals for the Federal Circuit

Anderson v Alaska Housing Finance Corporation
Constitutional Law, Real Estate & Property Law
Alaska Supreme Court

Cave v. State
Civil Rights, Constitutional Law, Criminal Law
Arkansas Supreme Court

Thomas v. State
Civil Rights, Constitutional Law, Criminal Law
Arkansas Supreme Court

Williams v. Baptist Health
Constitutional Law, Labor & Employment Law, Personal Injury
Arkansas Supreme Court

California v. Landowski
Constitutional Law, Criminal Law
California Courts of Appeal

California v. May
Constitutional Law, Criminal Law
California Courts of Appeal

California v. Perez
Constitutional Law, Criminal Law
California Courts of Appeal

Pinter-Brown v. The Regents of the University of California
Civil Rights, Constitutional Law
California Courts of Appeal

Colorado v. Lujan
Constitutional Law, Criminal Law
Colorado Supreme Court

Archer v. State
Civil Rights, Constitutional Law, Criminal Law
Florida Supreme Court

Collins v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Heyward v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Howard v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Keller v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Mills v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Moore v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Morris v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Rickman v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Robinson v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Santana v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Sullivan v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Turner v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Valrie v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Williams v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Idaho v. Burke
Constitutional Law, Criminal Law
Idaho Supreme Court - Criminal

State v. Gibbs
Civil Rights, Constitutional Law, Criminal Law
Iowa Supreme Court

State v. Harris
Civil Rights, Constitutional Law, Criminal Law
Kansas Supreme Court

State v. Paquin
Constitutional Law, Criminal Law
Maine Supreme Judicial Court

Commonwealth v. McCarthy
Civil Rights, Constitutional Law, Criminal Law
Massachusetts Supreme Judicial Court

Goldstein v. Secretary of the Commonwealth
Constitutional Law, Election Law
Massachusetts Supreme Judicial Court

State v. Reek
Civil Rights, Constitutional Law, Criminal Law
Minnesota Supreme Court

State v. Montoya
Civil Rights, Constitutional Law, Criminal Law
Nebraska Supreme Court

Multnomah County v. Mehrwein
Constitutional Law, Election Law, Government & Administrative Law
Oregon Supreme Court

Pennsylvania v. Britton
Constitutional Law, Criminal Law
Supreme Court of Pennsylvania

Pennsylvania v. Copenhaver
Constitutional Law, Criminal Law
Supreme Court of Pennsylvania

Pennsylvania v. Tedford
Constitutional Law, Criminal Law
Supreme Court of Pennsylvania

Pennsylvania v. Trahey
Constitutional Law, Criminal Law
Supreme Court of Pennsylvania

In re Greg Abbott
Constitutional Law, Criminal Law
Supreme Court of Texas

Stahmann v. Texas
Constitutional Law, Criminal Law
Texas Court of Criminal Appeals

Washington v. Escalante
Constitutional Law, Criminal Law
Washington Supreme Court

Washington v. Haggard
Constitutional Law, Criminal Law
Washington Supreme Court

Morrisey v. West Virginia AFL-CIO
Civil Rights, Constitutional Law, Labor & Employment Law
Supreme Court of Appeals of West Virginia

State v. Taylor
Civil Rights, Constitutional Law, Criminal Law
Supreme Court of Appeals of West Virginia

COVID-19 Updates: Law & Legal Resources Related to Coronavirus

Click here to remove Verdict from subsequent Justia newsletter(s).

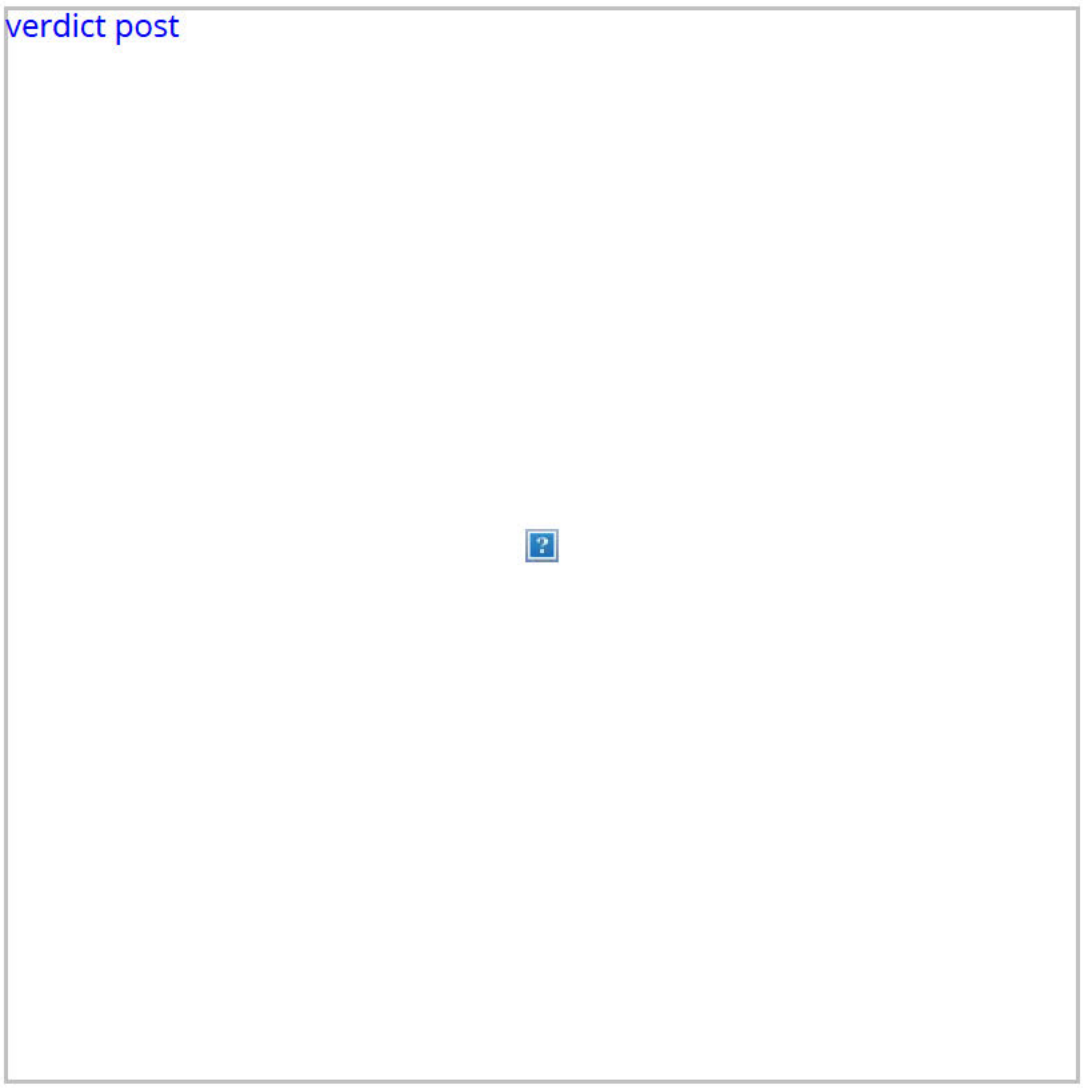
New on Verdict

Legal Analysis and Commentary

Rethinking Retroactivity in Light of the Supreme Court's Jury Unanimity Requirement

MICHAEL C. DORF

verdict post



In light of the U.S. Supreme Court's decision Monday in *Ramos v. Louisiana*, in which it held that the federal Constitution forbids states from convicting defendants except by a unanimous jury, Cornell law professor Michael C. Dorf discusses the Court's jurisprudence on retroactivity. Dorf highlights some costs and benefits of retroactivity and argues that the Court's refusal to issue advisory opinions limits its ability to resolve retroactivity questions in a way that responds to all the relevant considerations.

Read More

Constitutional Law Opinions

Ramos v. Louisiana

Court: US Supreme Court
Docket: 18-5924
Opinion Date: April 20, 2020
Judge: Neil M. Gorsuch
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

In 48 states and in federal court, a single juror's vote to acquit is enough to prevent a conviction; Louisiana and Oregon punish people based on 10-to-2 verdicts. Ramos was convicted in a Louisiana court by a 10-to-2 jury verdict and was sentenced to life without parole. The Supreme Court reversed. The Sixth Amendment right to a jury trial, as incorporated against the states by the Fourteenth Amendment, requires a unanimous verdict to convict a defendant of a serious offense. Juror unanimity is a vital common law right. The Court rejected an "invitation" to "perform a cost-benefit analysis on the historic features of common law jury trials and to conclude that unanimity does not make the cut." In overturning its 1972 "Apodaca" decision, the Court stated that the reasoning, in that case, was "gravely mistaken" and "sits uneasily with 120 years of preceding case law." The fact that Louisiana and Oregon may need to retry defendants convicted of felonies by non-unanimous verdicts whose cases are still pending on direct appeal "will surely impose a cost, but new rules of criminal procedure usually do."

Read Opinion Are you a lawyer? **Annotate this case**.

Ali v. Woodbridge Township School District

Court: US Court of Appeals for the Third Circuit
Docket: 19-2217
Opinion Date: April 22, 2020
Judge: Greenaway
Areas of Law: Civil Rights, Constitutional Law, Education Law, Labor & Employment Law

Ali, a non-practicing Muslim of Egyptian descent, was a non-tenured high school teacher. His supervisor received complaints about Ali's instruction on the Holocaust. One English teacher reported that her students were questioning historical accounts of the Holocaust, opining that Hitler didn't hate the Jews and that the death counts were exaggerated. Students' written assignments confirmed those accounts. Ali also presented a lesson

on the September 11 terrorist attacks, requiring students to read online articles translated by the Middle Eastern Media Research Institute (MEMRI). Ali posted links to the articles on a school-sponsored website: "U.S. Planned, Carried Out 9/11 Attacks—But Blames Others" and "U.S. Planning 9/11 Style Attack Using ISIS in Early 2015." The MEMRI articles also contained links to other articles, such as "The Jews are Like a Cancer, Woe to the World if they Become Strong." A reporter questioned Principal Lottman and Superintendent Zega. Lottman directed Ali to remove the MEMRI links from the school's website. The following morning, Ali met with Zega and Lottman; his employment was terminated. Ali sued under New Jersey law and 42 U.S.C. 1981, claiming that Lottman referred to him as "Mufasa," asked Ali if "they had computers in Egypt," and remarked on his ethnicity during the meetings that resulted in Ali's termination. He alleged discrimination, hostile work environment, free speech and academic freedom violations, and defamation. The Third Circuit affirmed summary judgment in favor of the defendants. Ali cannot show that his termination for teaching anti-Semitic views was a pretext for discrimination.

Read Opinion Are you a lawyer? **Annotate this case**.

Fogle v. Sokol

Court: US Court of Appeals for the Third Circuit
Docket: 19-1066
Opinion Date: April 21, 2020
Judge: Matey
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

In 1976, the body of 15-year-old "Kathy" was found near her Indiana County, Pennsylvania home. Kathy's death involved a brutal assault, rape, and a gunshot to the head. Kathy's sisters, ages nine and 12, stated that she had gotten into a car with a man with blue eyes, black hair that came below his ears and curled at the ends, sideburns, heavy eyebrows, and a heavy mustache. Fogle had "straight reddish-blonde hair that dropped down his back and a matching, full beard that reached his waist." After three years, Fogle became a suspect because a psychiatric patient described seeing Kathy get in a car with Fogle and his brother. The story was largely inconsistent with statements by Kathy's sisters. Jailhouse informants were recruited and counseled by law enforcement with promises of leniency. The

prosecutors "either knew about, encouraged, or permitted" this strategy. A jury found Fogle guilty of second-degree murder. In 2015, Fogle obtained DNA evidence excluding both himself and his brother as the source of semen collected from Kathy. His conviction was vacated. The Commonwealth declined to pursue new charges, describing the case as lacking "prosecutorial merit." Fogle, having spent three decades in prison, sued the prosecutors and Indiana County under 42 U.S.C. 1983. The Third Circuit affirmed the denial of their motions to dismiss based on absolute immunity. Only truly prosecutorial functions, not investigative conduct, justify complete protection from suit. Fogle's complaint alleges actions that fall outside the narrow doctrine of absolute immunity.

Read Opinion Are you a lawyer? **Annotate this case**.

Hope v. Warden Pike County Correctional Facility

Court: US Court of Appeals for the Third Circuit
Docket: 20-1784
Opinion Date: April 21, 2020
Judge: Smith
Areas of Law: Civil Procedure, Civil Rights, Constitutional Law, Immigration Law

On April 3, 2020, 20 immigration detainees filed a habeas petition (28 U.S.C. 2241), seeking immediate release, claiming that due to underlying health conditions, their continued detention during the COVID-19 pandemic puts them at imminent risk of death or serious injury. The district court found that the petitioners face irreparable harm and are likely to succeed on the merits, that the government would "face very little potential harm" from their immediate release, and that "the public interest strongly encourages Petitioners' release." Without waiting for a response from the government, the court granted a temporary restraining order (TRO) requiring the release. The government moved for reconsideration, submitting a declaration describing conditions at the facilities, with details of the petitioners' criminal histories. The court denied reconsideration, stating that the government had failed to demonstrate a change in controlling law, provide previously unavailable evidence, or show a clear error of law or the need to prevent manifest injustice. The court extended the release period until the COVID-19 state of emergency is lifted but attached conditions to the petitioners' release. The government reports that 19 petitioners were released; none

have been re-detained. The Third Circuit granted an immediate appeal, stating that the order cannot evade prompt appellate review simply by virtue of the label "TRO." A purportedly non-appealable TRO that goes beyond preservation of the status quo and mandates affirmative relief may be immediately appealable under 28 U.S.C. 1292(a)(1).

Read Opinion Are you a lawyer? **Annotate this case**.

James v. New Jersey State Police

Court: US Court of Appeals for the Third Circuit
Docket: 18-1432
Opinion Date: April 21, 2020
Judge: Porter
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Stephens called 911 and reported that Gibbons hit her and had a gun in his truck. The police responded. Stephens obtained a temporary restraining order, prohibiting Gibbons from possessing firearms and from returning to Stephens's house. The next day, Gibbons went to Stephens's house. Stephens was talking on the phone; the friend called the police. Gibbons left Stephens's house. Trooper Conza arrived. Stephens stated that Gibbons had waved a gun throughout their argument. Conza told Stephens to go to the police barracks and reported over the radio that Gibbons had brandished a firearm. Conza, with Troopers Bartelt and Korejko, visited the nearby home of Gibbons's mother, James. James stated that she did not know where Gibbons was and that he might be off his schizophrenia medication. While driving to the barracks, Stephens saw Gibbons walking alongside the road and called 911. The Troopers responded. Bartelt parked his car and, exiting, observed that Gibbons was pointing a gun at his own head. Bartelt drew his weapon, stood behind his car door, and twice told Gibbons to drop his weapon. Gibbons did not comply. Bartelt shot Gibbons twice within seconds of stopping his car. Gibbons died that night. In James' suit under 42 U.S.C. 1983, the Third Circuit held that Bartelt is entitled to qualified immunity because he did not violate Gibbons's clearly established rights. Bartelt's pre-standoff knowledge of Gibbons differs from that of officers involved in cited cases. Bartelt could reasonably conclude that Gibbons posed a threat to others.

Read Opinion Are you a lawyer? **Annotate this case**.

In re: Greg Abbott

Court: US Court of Appeals for the Fifth Circuit
Docket: 20-50296
Opinion Date: April 20, 2020
Judge: Jennifer Walker Elrod
Areas of Law: Civil Rights, Constitutional Law, Health Law

On April 7, 2020, the Fifth Circuit issued a writ of mandamus vacating the district court's temporary restraining order (TRO) that exempted abortions from GA-09, an emergency measure temporarily postponing non-essential medical procedures during the COVID-19 pandemic. On April 9, 2020, the district court entered a second TRO exempting various categories of abortion from GA-09. At issue in this mandamus petition is the April 9 TRO. The court held that the district court disregarded the court's mandate in Abbott II and failed to apply the framework governing emergency exercises of state authority during a public health crisis, established over 100 years ago in Jacobson v. Commonwealth of Massachusetts, 197 U.S. 11 (1905). Furthermore, the district court second-guessed the basic mitigation strategy underlying GA-09 (the concept of "flattening the curve"), and also acted without knowing critical facts such as whether, during this pandemic, abortion providers do (or should) wear masks or other protective equipment when meeting with patients. The court concluded that these errors resulted in an overbroad TRO that exceeds the district court's jurisdiction, reaches patently erroneous results, and usurps the state's authority to craft emergency public health measures "during the escalating COVID-19 pandemic." Therefore, the court granted the writ in part and directed the district court to vacate parts of the April 9 TRO.

Read Opinion Are you a lawyer? **Annotate this case**.

Sanchez v. Young County

Court: US Court of Appeals for the Fifth Circuit
Docket: 19-10222
Opinion Date: April 22, 2020
Judge: Edith Brown Clement

Areas of Law: Civil Rights, Constitutional Law

After Diana Simpson died of a drug overdose while she was a pretrial detainee at the Young County Jail, her family filed suit under 42 U.S.C. 1983, alleging Eighth and Fourteenth Amendment violations, as well as a claim under the Texas Tort Claims Act. The Fifth Circuit previously affirmed summary judgment for the County in part, and remanded in part for the district court to evaluate plaintiffs' conditions-of-confinement theory in the first instance. On remand, the district court granted summary judgment on that theory and plaintiffs appealed. The court affirmed the district court's dismissal of plaintiffs' claims based on a failure to train based on the law-of-the-case doctrine. The court held that the district court erred in dismissing plaintiffs' claims based on a failure to monitor because plaintiffs' evidence, when viewed in the light most favorable to them, creates several disputes of material fact about whether the jail has a de facto policy of inadequately monitoring detainees. Furthermore, plaintiffs offered sufficient evidence to create fact issues over whether the County failed to assess pretrial detainees' medical needs and whether this caused plaintiff to be denied needed medical care. Accordingly, the court reversed in part and affirmed in part, remanding for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

Singleton v. Cannizzaro

Court: US Court of Appeals for the Fifth Circuit
Docket: 19-30197
Opinion Date: April 21, 2020
Judge: Catharina Haynes
Areas of Law: Civil Rights, Constitutional Law

Plaintiffs allege that for years, prosecutors at the Orleans Parish District Attorney's Office, under the direction of District Attorney Leon Cannizzaro, used fake "subpoenas" to pressure crime victims and witnesses to meet with them. The Fifth Circuit held that (1) at this early, motion to dismiss stage, the individual defendants are not entitled to absolute immunity for plaintiffs' subpoena-related state-law claims and (2) the court lacked jurisdiction to consider the merits of plaintiffs' claims. Accordingly, the court affirmed the district court's holding that the individual defendants are not

entitled to absolute immunity for their alleged creation and use of fraudulent subpoenas, but dismissed the remainder of defendants' appeal for lack of jurisdiction.

Read Opinion Are you a lawyer? **Annotate this case**.

Valentine v. Collier

Court: US Court of Appeals for the Fifth Circuit
Docket: 20-20207
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Criminal Law, Government & Administrative Law, Health Law

Plaintiffs filed suit alleging that TDCJ's adoption and implementation of measures guided by changing CDC recommendations in regards to the COVID-19 pandemic do not go far enough. Plaintiffs filed a class action alleging violations of the Eighth Amendment's prohibition against cruel and unusual punishment, and the Americans with Disabilities Act, seeking a preliminary injunction. The Fifth Circuit granted TDCJ's motion to stay the district court's preliminary injunction, which regulates the cleaning intervals for common areas, the types of bleach-based disinfectants the prison must use, the alcohol content of hand sanitizer that inmates must receive, mask requirements for inmates, and inmates' access to tissues (amongst many other things). The court held that TDCJ is likely to prevail on the merits of its appeal because: (1) after accounting for the protective measures TDCJ has taken, plaintiffs have not shown a "substantial risk of serious harm" that amounts to "cruel and unusual punishment"; and (2) the district court committed legal error in its application of Farmer v. Brennan, by treating inadequate measures as dispositive of defendants' mental state. In this case, even assuming that there is a substantial risk of serious harm, plaintiffs lack evidence of defendants' subjective deliberate indifference to that harm. The court also held that TDCJ has shown that it will be irreparably injured absent a stay, and that the balance of the harms and the public interest favor a stay. Finally, the court held that plaintiffs have not exhausted their administrative remedies as required in the Prison Litigation Reform Act (PLRA), and the district court's injunction goes well beyond the limits of what the PLRA would allow even if plaintiffs had properly exhausted

their claims.

Read Opinion Are you a lawyer? **Annotate this case**.

Williams v. Banks

Court: US Court of Appeals for the Fifth Circuit
Docket: 17-60716
Opinion Date: April 23, 2020
Judge: Priscilla R. Owen
Areas of Law: Civil Rights, Constitutional Law

The Fifth Circuit affirmed the district court's grant of summary judgment to prison officials in a 42 U.S.C. 1983 action brought by plaintiff, an inmate in custody at the MDOC, alleging that defendants violated the Eighth and Fourteenth Amendments by being deliberately indifferent to the risk that another inmate would harm plaintiff. The court held that plaintiff's claims against defendants in their official capacities are barred under sovereign immunity. The court also held that the magistrate judge correctly granted summary judgment on plaintiff's theory that defendants failed to protect him from the other inmate, where there is no evidence in the record to suggest that defendants knew the inmate was a member of a gang or otherwise posed a specific threat to plaintiff when they moved him into plaintiff's zone. Furthermore, the magistrate judge correctly granted summary judgment on plaintiff's theory that defendants violated plaintiff's constitutional rights because they placed the inmate into plaintiff's protective custody zone instead of following MDOC policy and placing the inmate in lockdown. In this case, defendants did not disregard an excessive risk to inmate health or safety.

Read Opinion Are you a lawyer? **Annotate this case**.

Gary B. v. Whitmer

Court: US Court of Appeals for the Sixth Circuit
Dockets: 18-1855, 18-1871
Opinion Date: April 23, 2020
Judge: Eric L. Clay
Areas of Law: Civil Rights, Constitutional Law, Education Law

Students at several of Detroit's worst-performing public schools were subject to poor conditions within their classrooms, missing or unqualified teachers, physically dangerous facilities, and inadequate books and materials. In 2016, the plaintiffs filed suit under 42 U.S.C. 1983, claiming that these conditions deprive them of a basic minimum education that provides a chance at foundational literacy, in violation of the due process and equal protection clauses. They sought recognition of a fundamental right to a basic education. They argued that the schools they are forced to attend are schools in name only, so the state cannot justify the restriction on their liberty imposed by compulsory attendance. They sued state officials, rather than local entities, based on the state's general supervision of all public education and the state's specific interventions in Detroit's public schools. The state argued that it recently returned control to local officials. The district court found that the state defendants were the proper parties to sue but dismissed the complaint on the merits. The Sixth Circuit reversed in part. Though the plaintiffs failed to adequately plead their equal protection and compulsory attendance claims, the court reinstated claims that they have been denied a basic minimum education, and have been deprived of access to literacy. Application of the principles in the Supreme Court's education cases to a substantive due process framework demonstrates that a basic minimum education should be recognized as a fundamental right.

Read Opinion Are you a lawyer? **Annotate this case**.

Lebamoff Enterprises, Inc., v. Whitmer

Court: US Court of Appeals for the Sixth Circuit
Dockets: 18-2199, 18-2200
Opinion Date: April 21, 2020
Judge: Jeffrey S. Sutton
Areas of Law: Constitutional Law, Government & Administrative Law

The Twenty-first Amendment permits the states to regulate the sales of alcohol within their borders. Michigan is among several states with a three-tier system that forbids alcohol producers (first tier) to sell directly to retailers or consumers. Producers must sell to wholesalers within the state (second tier); those wholesalers sell exclusively to in-state retailers, who sell to consumers. Businesses at each tier must be independently owned; no one may operate more than one tier, Michigan imposes minimum prices and

prohibits wholesalers from offering volume discounts or selling on credit. For liquor (not wine and beer), the state is the wholesaler in Michigan. In 2016, Michigan amended its law to allow in-state retailers to deliver directly to consumers using state-licensed "third party facilitators" or common carriers like FedEx or UPS. A wine retailer based in Fort Wayne, Indiana and Michigan wine consumers alleged that the new law violated the Commerce Clause and the Privileges and Immunities Clause. The district court extended delivery rights to out-of-state retailers. Michigan obtained a stay. The Sixth Circuit reversed. The Twenty-first Amendment permits Michigan to treat in-state retailers differently from out-of-state retailers. There is no inherent right to sell intoxicating liquors by retail. Some reduction in consumer choice is inevitable in a three-tier system, which is intended to make it harder to sell alcohol.

Read Opinion Are you a lawyer? **Annotate this case**.

Queen v. City of Bowling Green

Court: US Court of Appeals for the Sixth Circuit
Docket: 18-5840
Opinion Date: April 22, 2020
Judge: Bush
Areas of Law: Civil Rights, Constitutional Law, Labor & Employment Law

Queen, a Bowling Green firefighter, 2011-2016, was subject to harassment because he is an atheist. According to Queen, he was forced to participate in Bible studies; his co-workers and supervisors badgered him regarding his sexuality and regularly disparaged minorities. In 2012, Queen complained to his supervisor, Rockrohr, who "responded in hostility." Rockrohr later told Queen that he had discussed the matter with the fire chief and they both believed that Queen "needed to get employment somewhere else." Queen apologized. Queen's employment conditions did not improve. Queen was intentionally tripped while retrieving his gear and was regularly subject to disparaging remarks. Stress and anxiety caused Queen to take a leave of absence. While on leave, Queen received many phone calls from his supervisors asking why he was absent. Queen resigned and filed suit under the Kentucky Civil Rights Act, alleging hostile work environment based on religion and gender, constructive discharge, retaliation, and violations of the Family and Medical Leave Act. The district court granted the defendants

summary judgment on hostile work environment based on religion and gender and the FMLA claims. On interlocutory appeal, the Sixth Circuit affirmed the denial of qualified immunity to the city on the claims for hostile work environment based on religion and for retaliation and denial of qualified immunity to Rockrohr for the retaliation claim.

Read Opinion Are you a lawyer? **Annotate this case**.

Winburn v. Nagy

Court: US Court of Appeals for the Sixth Circuit
Dockets: 19-2399, 19-2398
Opinion Date: April 23, 2020
Judge: Jeffrey S. Sutton
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Winburn represented himself at his trial for armed robbery, home invasion, and conspiracy. Based on Winburn's disruptive behavior, the judge removed him from the courtroom and revoked Winburn's permission to represent himself, then granted a competency evaluation and a mistrial. While Winburn awaited his second trial, the judge permitted Winburn's stand-by attorney to withdraw because Winburn had sued her and enjoined Winburn from filing complaints or grievances against his new attorney, except to discharge her. Although represented by a new attorney, Winburn moved pro se to dismiss his charges on double jeopardy grounds. The trial judge denied the motion because Winburn's attorney had not filed it. Winburn filed a habeas petition under 28 U.S.C. 2241 challenging his retrial and another section 2241 petition challenging the injunction. The district judges denied both and declined to issue certificates of appealability. Winburn filed a notice of appeal for one petition and sought a certificate of appealability for the other. The Sixth Circuit held that state pretrial detainees proceeding under section 2241 may not appeal without certificates of appealability and granted Winburn a certificate on the injunction claim. A reasonable jurist could conclude that the unusual order was constitutionally infirm. The court denied relief with respect to double jeopardy. Winburn failed to exhaust his state-court remedies by a motion to dismiss.

Read Opinion Are you a lawyer? **Annotate this case**.

Lund v. City of Rockford

Court: US Court of Appeals for the Seventh Circuit
Docket: 19-1945
Opinion Date: April 20, 2020
Judge: ROVNER
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Lund, a reporter for the Rockford Scanner, heard, by police scanner, of multiple traffic stops in Midtown. He did not have a driver's license, so he rode a motorized bicycle to Midtown to take photographs. He suspected a prostitution sting operation. An officer noticed Lund and radioed the team. Officers Welsh and Campbell knew of Lund's previous anti-police speech. They directed Lund to "move on." Lund asked if he was breaking any laws. Campbell informed him that he was not, but that his continued presence would constitute obstruction of a police detail and result in arrest. Lund started his bicycle and called out, loudly, "goodbye officers." Concerned that Lund might post pictures on social media while the sting operation was ongoing and create a danger for unarmed undercover officers, the officers followed Lund and arrested him for driving the wrong way on a one-way street, operating a vehicle without insurance, obstructing a police officer, felony aggravated driving on a revoked license, and operating a motor vehicle without a valid drivers' license. News stories listed Lund's name as an arrestee in the prostitution sting. The charges against Lund were dismissed. Lund sued the officers and the city under 42 U.S.C. 1983. The Seventh Circuit affirmed summary judgment for the defendants on First Amendment retaliation and malicious prosecution under Illinois law, citing the Supreme Court's intervening "Nieves" (2019) holding, that, in most cases, probable cause to arrest defeats a claim of retaliatory arrest. There was probable cause to arrest Lund.

Read Opinion Are you a lawyer? **Annotate this case**.

In Re: Leslie Rutledge

Court: US Court of Appeals for the Eighth Circuit
Docket: 20-1791
Opinion Date: April 22, 2020
Judge: Bobby E. Shepherd

Areas of Law: Civil Rights, Constitutional Law, Health Law

The Eighth Circuit granted a writ of mandamus in part and directed the district court to dissolve a Temporary Restraining Order (TRO) enjoining the State from enforcing a COVID-19-related health directive against a provider of surgical abortions. The Arkansas Department of Health (ADH) issued a directive requiring that all non-medically necessary surgeries be postponed in response to Executive Order 20-03, directing the ADH to do everything reasonably possible to respond to and recover from the COVID-19 virus. After adopting the Fifth Circuit's reasoning in In re Abbott, No. 20-50264, 2020 WL 1685929 (5th Cir. April 7, 2020), the court held that the State is entitled to mandamus relief because it has satisfied its burden in demonstrating that it has no other means to obtain the relief that it seeks, the State is clearly and indisputably entitled to the writ, and entry of the writ is appropriate under the circumstances. In Jacobson v. Massachusetts, 197 U.S. 11 (1905), the Supreme Court held that, when faced with a public health crisis, a state may implement measures that infringe on constitutional rights, subject to certain limitations. The court found that the district court's failure to apply the Jacobson framework produced a patently erroneous result. In this case, the directive bears a real and substantial relation to the State's interest in protecting public health in the face of the COVID-19 pandemic; the directive is not, beyond all question, a prohibition of pre-viability abortion in violation of the Constitution because it is a delay, not a ban, and contains emergency exceptions; and the district court clearly abused its discretion in finding that the provider is likely to prevail on its argument that the directive will likely operate as a substantial obstacle to a woman's choice to undergo an abortion in a large fraction of the cases in which the directive is relevant. The court declined to exercise its mandamus power to direct the district court to dismiss the supplemental complaint, and denied the emergency motion to stay the ex parte TRO and for a temporary administrative stay as moot.

Read Opinion Are you a lawyer? **Annotate this case**.

Lombardo v. City of St. Louis
Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1469
Opinion Date: April 20, 2020

Judge: Bobby E. Shepherd
Areas of Law: Civil Rights, Constitutional Law

The Eighth Circuit affirmed the magistrate judge's grant of summary judgment in favor of law enforcement officers and the City, in a 42 U.S.C. 1983 action brought by plaintiff after the death of her son. The court held that the officers' actions did not amount to constitutionally excessive force. In this case, the undisputed facts show that the officers discovered the son acting erratically, and even though the son was held in a secure cell, it was objectively reasonable for the officers to fear that he would intentionally or inadvertently physically harm himself. Furthermore, the son actively resisted the officers' attempts to subdue him, and officers held him in the prone position only until he stopped actively fighting against the restraints and the officers. Therefore, the court held that the officers are entitled to qualified immunity on plaintiff's excessive force claim.

Read Opinion Are you a lawyer? **Annotate this case**.

Anthony v. TRAX International Corp.

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-15662
Opinion Date: April 17, 2020
Judge: Kim McLane Wardlaw
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Ninth Circuit affirmed the district court's grant of summary judgment to TRAX in a disability discrimination action brought by plaintiff under Title I of the Americans with Disabilities Act (ADA). After TRAX terminated plaintiff from her position as a Technical Writer allegedly due to an inability or unwillingness to accommodate her disability, TRAX discovered during the course of litigation that plaintiff lacked the requisite bachelor's degree for her position. The panel held that, although McKennon v. Nashville Banner Publishing Co., 513 U.S. 352 (1995), held that after-acquired evidence cannot establish a superseding, non-discriminatory justification for an employer's challenged actions, after-acquired evidence remains available for other purposes, including to show that an individual is not qualified under the ADA. Because plaintiff did not satisfy one of the prerequisites for her position, she is not "otherwise qualified," and TRAX was not obligated to

engage in the interactive process.

Read Opinion Are you a lawyer? **Annotate this case**.

Wilk v. Neven

Court: US Court of Appeals for the Ninth Circuit
Docket: 17-17355
Opinion Date: April 23, 2020
Judge: William A. Fletcher
Areas of Law: Civil Rights, Constitutional Law

The Ninth Circuit reversed the district court's grant of summary judgment for prison officials in a 42 U.S.C. 1983 action alleging that defendants violated plaintiff's right to be free from cruel and unusual punishment when they failed to protect him from an attack by another inmate. The panel held that defendants violated plaintiff's Eighth Amendment right to be protected from serious harm while incarcerated. The panel also held that a reasonable fact-finder would be able to conclude that defendants were subjectively aware of the substantial risk of serious harm to plaintiff, and failed to respond reasonably; any reasonable prison official in the defendants' position would know that the actions defendants took, and failed to take, violated the Eighth Amendment; none of the defendants can claim ignorance to a prisoner's right to be protected from violence at the hands of other inmates where that right has been clearly established in Farmer v. Brennan, 511 U.S. at 833 (1994). Finally, the panel noted that throughout proceedings in the district court plaintiff struggled to obtain discovery from defendants. On remand, plaintiff should have another opportunity to seek the materials he requested previously, and the panel encouraged the district court to appoint him counsel.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Manzanares

Court: US Court of Appeals for the Tenth Circuit
Docket: 18-2010
Opinion Date: April 17, 2020
Judge: Mary Beck Briscoe

Areas of Law: Constitutional Law, Criminal Law

Defendant-Appellant Archie Manzanares appealed a district court's denial of his 28 U.S.C. 2255 motion challenging his sentence under the Armed Career Criminal Act (ACCA). Under the ACCA, an offense qualified as a violent felony by satisfying at least one of three definitions, which have come to be known as the Elements Clause, the Enumerated Clause, and the Residual Clause. Manzanares asserted that without the Residual Clause, his underlying New Mexico convictions (armed robbery, aggravated assault with a deadly weapon, and aggravated battery) no longer qualified as violent felonies. The district court denied the motion, concluding that all three underlying convictions satisfied the Elements Clause. Manzanares appealed the classification of the armed robbery conviction as a violent felony to the Tenth Circuit, and sought to expand the certificate of appealability to allow him to appeal the decision regarding the aggravated assault with a deadly weapon and aggravated battery convictions. After review, the Tenth Circuit affirmed the district court's denial of Manzanares's 2255 motion, and denied his motion to expand the COA.

Read Opinion Are you a lawyer? **Annotate this case**.

Durham v. Rural/Metro Corp.

Court: US Court of Appeals for the Eleventh Circuit
Docket: 18-14687
Opinion Date: April 17, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Labor & Employment Law

After plaintiff asked her employer, Rural, for a temporary light-duty or dispatcher assignment for the duration of her pregnancy because her physician advised her to refrain from lifting more than 50 pounds while pregnant, Rural declined plaintiff's request for accommodation. Plaintiff filed suit against Rural, alleging discrimination under the Pregnancy Discrimination Act (PDA). The Eleventh Circuit vacated the district court's grant of Rural's motion for summary judgment, holding that the district court erroneously factored into the "similar in their ability or inability to work" evaluation the distinct, post-prima-facie-case consideration of Rural's purported legitimate, non-discriminatory reasons for treating plaintiff and the

non-pregnant employees differently. The court explained that neither a non-pregnant EMT who is limited to lifting 10 or 20 pounds nor a pregnant EMT who is restricted to lifting 50 pounds or less can lift the required 100 pounds to serve as an EMT. Consequently, neither can meet the lifting requirement and are thus the same in their "inability to work" as an EMT. The court held that plaintiff's prima facie requirement to establish that she was similarly situated to other employees in their ability or inability to work was satisfied. The court remanded for the district court to determine the remaining issues in the first instance.

Read Opinion Are you a lawyer? **Annotate this case**.

Gadsden Industrial Park, LLC v. United States

Court: US Court of Appeals for the Federal Circuit
Docket: 18-2132
Opinion Date: April 22, 2020
Judge: Stoll
Areas of Law: Constitutional Law, Environmental Law, Real Estate & Property Law, Zoning, Planning & Land Use

GIP purchased property from a steel mill's bankruptcy estate, omitting the "Eastern Excluded Property" (EEP). GIP purchased some personal property located on the EEP, which contains two piles comprising slag (a steel manufacturing byproduct), kish (a byproduct of a blast furnace operation), and scrap. Each pile occupied more than 10 acres and was more than 80 feet high. GIP's "Itemization of Excluded Item from Sale" referred to: "All by-products of production other than kish and 420,000 cubic yards of slag" on the EEP "with a reasonable period of time to remove such items." The EPA began investigating contaminants leaching from the piles. While GIP was negotiating for the separation of recoverable metals, the EPA decided to reduce the size of the piles. In 2009-2013, EPA contractors recovered and sold 245,890 tons of material and recovered and used 92,500 cubic yards of slag onsite for environmental remediation; they processed approximately 50% of the piles, spending about $14.5 million, about a million more than income from sales. The EPA compacted the materials to minimize leachate, leaving further remediation to state environmental authorities. GIP did not attempt its own recovery operation during the EPA remediation. GIP sued, alleging "takings" of the slag, kish, and scrap. The trial court awarded GIP

$755,494 for the slag but awarded zero damages for the kish and scrap. The Federal Circuit vacated in part. GIP had no claim to any particular subset of slag. The trial court erred in finding that the EPA somehow prevented GIP from recovering its full allotment of slag; GIP cannot establish a cognizable property interest in the slag that was recovered. The court affirmed in part. GIP's unreliable calculations left the trial court without competent evidence relating to a critical component of the damages calculation with respect to the kish and scrap.

Read Opinion Are you a lawyer? **Annotate this case**.

Anderson v Alaska Housing Finance Corporation

Court: Alaska Supreme Court
Docket: S-17077
Opinion Date: April 17, 2020
Judge: Daniel E. Winfree
Areas of Law: Constitutional Law, Real Estate & Property Law

Alaska Housing Finance Corporation (AHFC) held a promissory note and deed of trust executed in connection with a borrower's purchase of his home. AHFC non-judicially foreclosed on the deed of trust without first providing the borrower an opportunity to present to a decision-maker his argument why under AHFC's policies and procedures he was entitled to loan assistance to prevent the foreclosure. The borrower brought suit, alleging among other things, that he was denied procedural due process protections before AHFC took his property by foreclosure. The superior court rejected his due process argument and granted AHFC summary judgment on all issues. The sole issue presented to the Alaska Supreme Court on appeal was the due process question. The Court concluded that AHFC, a public corporation, was a "state actor," that the foreclosure effected a deprivation of the borrower's property, and that the borrower was not afforded a constitutionally required pre deprivation opportunity to be heard. The Court therefore reversed the superior court's summary judgment decision on the due process question and remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

Cave v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 356
Opinion Date: April 23, 2020
Judge: Josephine L. Hart
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's pro se petition for writ of habeas corpus, holding that the circuit court did not err in denying the petition. Appellant was found guilty of two counts of delivery of a controlled substance and one count of maintaining a drug premises. In his habeas petition, Appellant argued that he was actually innocent because his arrest and conviction was based on the false testimony of a witness who had a lengthy criminal history. Appellant further argued that the writ should issue because he was not afforded effective assistance of counsel. The circuit court denied the petition. The Supreme Court affirmed, holding (1) Appellant's claims regarding the witness's credibility do not constitute a valid assertion that he was being unlawfully detained; and (2) Appellant did not actually connect an allegation of ineffective assistance of counsel to his allegation that he was unlawfully detained.

Read Opinion Are you a lawyer? **Annotate this case**.

Thomas v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 354
Opinion Date: April 23, 2020
Judge: Josephine L. Hart
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Appellant's conviction of capital murder, holding that the evidence was sufficient to sustain the conviction and that the circuit court did not err in denying Appellant's motion to suppress tracking data generated by his cellphone. On appeal, Appellant argued that the trial court erred by denying his directed-verdict motion because the evidence supported the defense's theory of the case that he did not intend to shoot the victim. Further, Appellant argued that the court abused its

discretion in denying his motion to suppress evidence obtained from the seizure of AT&T phone records. The Supreme Court disagreed, holding (1) the evidence was sufficient to support the capital murder conviction; and (2) the circuit court correctly denied the motion to suppress.

Read Opinion Are you a lawyer? **Annotate this case**.

Williams v. Baptist Health

Court: Arkansas Supreme Court
Citation: 2020 Ark. 350
Opinion Date: April 23, 2020
Judge: Kemp
Areas of Law: Constitutional Law, Labor & Employment Law, Personal Injury

The Supreme Court affirmed in part and reversed in part the judgment of the circuit court dismissing Appellant's action against Baptist Health appellees and John Hearnsberger, M.D., holding that the circuit court abused its discretion in denying Appellant's motions to compel production of two types of disputed discovery. Appellant, a surgeon, was on the medical staff of Baptist Health from 2003 until 2011, when his appointment and clinic privileges at Baptist Health Medical Center-Little Rock were terminated, effective immediately. Baptist Health also reported the suspension of Appellant's clinical privileges to the Arkansas State Medical Board, which, in 2014, revoked Appellant's license. Appellant appealed the revocation, and his license was reinstated. In 2011, Appellant filed a lawsuit against Baptist Health and several individuals, asserting several claims. The circuit court entered a consent order dismissing the Medical Board and Dr. Hearnsberger in his official capacity. The circuit court then granted summary judgment on Appellant's remaining claims. The Supreme Court reversed in part, holding that the circuit court abused its discretion in denying Appellant's motions to compel production of two types of discovery, and the discovery error was not harmless as to Appellant's discrimination and tortious-interference claims.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. Landowski

Court: California Courts of Appeal
Docket: C080210(Third Appellate District)
Opinion Date: April 23, 2020
Judge: Andrea Lynn Hoch
Areas of Law: Constitutional Law, Criminal Law

Defendant Michael Reyes, Jr., an active Norteno gang member (from the Broderick Boys subset), confronted a former Norteno gang member (from the Franklin Boys subset), "S.," about a physical altercation that occurred between S. and Reyes's stepfather over a debt. That earlier altercation had taken place in front of Reyes's autistic younger brother. Reyes pulled out a handgun and asked S. if he had a problem. S., who was riding his bicycle with his wife, "R.," when Reyes confronted him with the gun, stopped briefly, told Reyes to put the gun down if he wanted to fight, and then started to ride away. This angered Reyes, prompting him to fire six rounds at S. from behind. S. Was hit but survived. R. Was a short distance in front of S., but was not hit. Defendants Liberty Landowski and Lisa Humble were with Reyes at the time of the shooting and aided in his efforts to avoid being apprehended by law enforcement authorities. Reyes, Landowski, and Humble were tried together before the same jury. Reyes was convicted of one count of attempted murder (Count 1), two counts of assault with a semiautomatic firearm (Counts 2 and 4), one count of possession of a firearm by a convicted felon (Count 5), and one count of possession of ammunition by a convicted felon (Count 6). In addition to various firearm and other enhancements, the jury found Reyes committed the crimes for the benefit of, at the direction of, or in association with a criminal street gang with the specific intent to promote, further, or assist in criminal conduct by gang members. The jury convicted Landowski and Humble of being accessories to Reyes's criminal conduct (Count 9) and also found true gang enhancement allegations attached to that crime. Reyes challenged the sufficiency of the firearm evidence presented to support his conviction, and all defendants challenged the sufficiency of the evidence supporting their gang enhancements. The Court of Appeal determined Senate Bill 620 (2017-2018 Reg. Sess.) gave the trial court discretion to strike firearm enhancements in the interest of justice and applied retroactively; and Senate Bill 136 (2019-2020 Reg. Sess.) eliminated such enhancements, and also applied retroactively. To these issues, the Court remanded for the trial court's consideration. The Court affirmed the trial court in all other respects.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. May

Court: California Courts of Appeal
Docket: C084302(Third Appellate District)
Opinion Date: April 20, 2020
Judge: Ronald B. Robie
Areas of Law: Constitutional Law, Criminal Law

Defendant Raymond May was found guilty by jury of possessing an assault weapon and a machine gun based on his possession of a single AK-47 assault rifle while guarding a marijuana plantation. He was sentenced to probation, which included an electronic search condition. On appeal, defendant argued there was a lack of sufficient evidence corroborating his accomplice's testimony and demonstrating he knew of the firearm's illegal character. He further alleged the trial court erred in instructing the jury: that the accomplice instruction should have included language specifying that the accomplice testimony needed to prove more than defendant's mere presence or access to the firearm. Furthermore, defendant argued the electronic search condition imposed as part of his probation failed under the standards announced in California v. Lent, 15 Cal.3d 481 (1975). The Court of Appeal agreed defendant's electronic search condition should have been stricken, but otherwise affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. Perez

Court: California Courts of Appeal
Docket: E072260(Fourth Appellate District)
Opinion Date: April 20, 2020
Judge: Miller
Areas of Law: Constitutional Law, Criminal Law

In 2009, defendant-appellant Rudy Perez pled guilty to active gang participation under Penal Code section 186.22(a), and unlawful possession of a firearm under section 12025(b)(6). In 2010, defendant pled guilty to residential burglary under section 459, and active gang participation under

section 186.22(a). In August of 2018, the State filed a new felony complaint, alleging one of the prior gang participation convictions as a strike prior. In 2018, defendant moved to vacate the two prior gang participation convictions based upon changes in the law that rendered them invalid. The trial court denied defendant's motion. In 2019, defendant asked for reconsideration, which was again denied. Thereafter, defendant filed a timely notice of appeal from the denial of his motion to vacate the convictions. The Court of Appeal found that defendant pled guilty to street terrorism under Penal Code section 186.22(a) in 2009 and 2010, and it was undisputed that while committing these offenses, defendant acted alone. However, subsequent to defendant's guilty pleas, in 2012, the California Supreme Court held that a defendant had to act in concert with a fellow gang member in order to be guilty of street terrorism. At that time, defendant could have filed a state habeas petition requesting relief, but failed to do so. "Defendants can lose remedies that are established by law when they fail to invoke such remedies in time." Section 1473.7 became effective in 2017. In defendant's motion filed in the trial court, defendant failed to state what new evidence was discovered, instead arguing that the trial court was allowed "to vacate a conviction where the defendant is innocent as a matter of law or where vacating the conviction is in the interest of justice, even though the defendant is no longer in custody or otherwise restrained by the conviction." The Court of Appeal concurred with the trial court's reason to deny relief, determining that "while the outcome in this case may be unfortunate for defendant, we are not here to rewrite legislation. The Legislature could amend section 1473.7 to address issues raised in this case. However, under the laws, as written, we must uphold the trial court's order."

Read Opinion Are you a lawyer? **Annotate this case**.

Pinter-Brown v. The Regents of the University of California

Court: California Courts of Appeal
Docket: B290086(Second Appellate District)
Opinion Date: April 23, 2020
Judge: Stratton
Areas of Law: Civil Rights, Constitutional Law

Plaintiff filed suit against The Regents for gender discrimination based on a series of events that took place while she was a Professor of Medicine at

UCLA. The jury found in favor of plaintiff, awarding her economic and noneconomic damages. The Court of Appeal reversed and held that the trial court committed a series of grave errors that significantly prejudiced The Regents' right to a fair trial by an impartial judge. In this case, the trial court delivered a presentation to the jury highlighting major figures in the civil rights movement, and told the jury their duty was to stand in the shoes of Dr. Martin Luther King and bend the arc of the moral universe toward justice; the trial court allowed the jury to hear about and view a long list of discrimination complaints from across the entire University of California system that were not properly connected to plaintiff's circumstances or her theory of the case; the trial court allowed the jury to learn of the contents and conclusions of the Moreno Report, which documented racial discrimination occurring throughout the entire UCLA campus; and the trial court allowed plaintiff to resurrect a retaliation claim after the close of evidence despite having summarily adjudicated that very claim prior to trial. The court held that these errors were cumulative and highly prejudicial, and were evidence of the trial court's inability to remain impartial, creating the impression that the trial court was partial to plaintiff's claims.

Read Opinion Are you a lawyer? **Annotate this case**.

Colorado v. Lujan

Court: Colorado Supreme Court
Citation: 2020 CO 26
Opinion Date: April 20, 2020
Judge: Brian D. Boatright
Areas of Law: Constitutional Law, Criminal Law

Abel Lujan was charged with first-degree murder for the death of his girlfriend after she was found beaten and strangled behind a friend's house. At trial, two women testified for the State about Lujan's prior violent behavior towards them. Prior to admitting this evidence, the trial court read a limiting instruction, telling the jury that it could only consider the evidence for the purposes of establishing Lujan's motive, intent, or common plan. A copy of this instruction was not given to the jury for deliberations; however, the jury did receive an instruction at the close of the evidence explaining that certain evidence could only be considered for the limited purposes for which it was admitted. While deliberating, the jury submitted a question seeking

clarification about the limiting instruction. Over defense counsel's objection, the trial court cleared the courtroom of the public and parties, leaving only the judge, bailiff, and court reporter; the judge then brought in the jury and reread the limiting instruction that it had previously read twice in open court. The jury ultimately found Lujan guilty of second-degree murder. Lujan appealed, arguing that the court's actions when rereading the jury instruction constituted a courtroom closure that violated his Sixth Amendment right to a public trial. A division of the court of appeals agreed and reversed Lujan's conviction. The State argued on certiorari review that the Colorado Supreme Court adopt a triviality standard, under which a defendant's constitutional right to a public trial was not violated when the closure at issue was trivial. In so doing, the State argued that the brief courtroom closure here was trivial and therefore did not violate Lujan's public trial right. The Court concurred with the State, adopted the standard and reversed the appellate court's decision.

Read Opinion Are you a lawyer? **Annotate this case**.

Archer v. State

Court: Florida Supreme Court
Docket: SC19-841
Opinion Date: April 23, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the order of the circuit court denying Appellant's successive motion to vacate his sentence of death under Fla. R. Crim. P. 3.851, holding that the circuit court did not err in denying the Rule 3.851 motion. Appellant was convicted of first-degree murder, armed robbery, and grand theft. Appellant was sentenced to death for the murder. The Supreme Court affirmed the convictions but reversed Appellant's death sentence and remanded the case for a new penalty phase. After a new penalty phase, Appellant was again sentenced to death. In his successive Rule 3.851 motion, Appellant raised three claims. The circuit court denied relief. The Supreme Court affirmed, holding that the circuit court (1) properly denied Appellant's claim that his death sentence violated the Sixth and Eighth Amendments in light of Hurst v. Florida, 136 S. Ct. 616 (2016), and Hurst v. State, 202 So. 3d 40 (Fla. 2016); (2) correctly denied Appellant's

claim that his sentence violated the Eighth Amendment; and (3) did not err in denying Appellant's claim of newly discovered evidence.

Read Opinion Are you a lawyer? **Annotate this case**.

Collins v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0158
Opinion Date: April 20, 2020
Judge: David E. Nahmias
Areas of Law: Constitutional Law, Criminal Law

Appellant Tommy Collins was convicted of felony murder in connection with the stabbing death of 14-year-old Rueben Hand. Friends gathered to watch the Peach Drop on New Year's Eve 2010; a disagreement ensued and Hand was stabbed near the Five Points MARTS station shortly after midnight. Appellant's only argument on appeal was that the trial court plainly erred when it gave the jury the State's requested instruction on "revenge for a prior wrong." Seeing no error, "much less plain error," the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Heyward v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0399
Opinion Date: April 20, 2020
Judge: Peterson
Areas of Law: Constitutional Law, Criminal Law

Larmell Heyward was convicted by jury of malice murder and possession of a firearm during the commission of a felony in connection with the 2007 shooting death of Ramon Rogers. Heyward argued on appeal of those convictions that the trial court erred in denying his request to charge the jury on voluntary manslaughter. After review, the Georgia Supreme Court determined the trial court's refusal to give the charge was harmless, since, in the Court's estimation, there was no realistic probability that the jury would have accepted the "slight" evidence of voluntary manslaughter in the

light of the strong evidence of malice murder.

Read Opinion Are you a lawyer? **Annotate this case**.

Howard v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0819
Opinion Date: April 20, 2020
Judge: Keith R. Blackwell
Areas of Law: Constitutional Law, Criminal Law

Kenneth Howard was tried by jury and convicted of the murder of Emily Ann Smith Newbegin. Howard appealed, contending that the evidence was legally insufficient to sustain his conviction. Upon its review of the record and briefs, the Georgia Supreme Court found no merit in Howard's claim of error, and affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Keller v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0006
Opinion Date: April 20, 2020
Judge: Boggs
Areas of Law: Constitutional Law, Criminal Law

Randall Keller was convicted of felony murder and related crimes arising out of the beating death of his ex-wife's two-year-old son, William Powell. On appeal, Keller raised numerous claims of error, including ineffective assistance of counsel, the trial court's rulings on motions before and during trial, several evidentiary rulings, and alleged bias on the part of the trial judge. However, finding no reversible error, the Georgia Supreme Court affirmed Keller's convictions.

Read Opinion Are you a lawyer? **Annotate this case**.

Mills v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0364
Opinion Date: April 20, 2020
Judge: Ellington
Areas of Law: Constitutional Law, Criminal Law

Roger Mills was found guilty by jury of malice murder and aggravated assault in connection with the death of Masuto Garrett. Mills contended that the trial court erred when, during jury deliberations, it excused a holdout juror without sufficient inquiry or good cause. After review, the Georgia Supreme Court concurred with that contention, and reversed Mills's convictions. The Court also concluded the evidence presented at trial was legally sufficient to support the convictions, so the State could retry Mills if it chose.

Read Opinion Are you a lawyer? **Annotate this case**.

Moore v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0344
Opinion Date: April 20, 2020
Judge: David E. Nahmias
Areas of Law: Constitutional Law, Criminal Law

Appellant Carzell Moore, proceeding pro se, appealed a trial court's denial of his motion to set aside a September 2017 order denying his motion for an out-of-time appeal of his 2002 resentencing on his 1977 convictions for murder and rape. Moore contended the trial court abused its discretion by denying his motion to set aside because he was not given proper notice of the September 2017 order. Finding that the record supported the trial court's ruling, the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Morris v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0176

Opinion Date: April 20, 2020
Judge: Bethel
Areas of Law: Constitutional Law, Criminal Law

Darius Morris was found guilty by jury of malice murder and other offenses in connection with the shooting death of Jameson Bush. Morris appealed, arguing he was denied the right to a timely appeal, that the trial court erred in restricting voir dire as to the religious beliefs and connections of potential jurors, that the trial court erred by giving a confusing jury charge regarding statements of co-conspirators, that the trial court erred by violating his right to a public trial by ordering that the courtroom doors be closed and locked during the court's charge to the jury, and that his trial counsel provided ineffective assistance by not objecting to the closure of the courtroom. Finding no error, the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Rickman v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0127
Opinion Date: April 20, 2020
Judge: Harold D. Melton
Areas of Law: Constitutional Law, Criminal Law

Victoria Rickman was convicted by jury of malice murder and a related firearm offense in connection with the shooting death of William Carter, Jr. Rickman and Carter had a tumultuous on-again, off-again relationship with a history of verbal and physical abuse, false accusations of sexual assault, empty threats to obtain temporary protective orders, and numerous calls to 911. In the days leading up to Carter's death, the pair was talking and meeting again despite a recent break-up. On one such 911 call, officers went to Rickman's residence responding to claims shots were fired. Rickman responded holding her small dog, hair wet, and in pajamas. She did not appear to be injured, and nothing in the home looked disturbed or out of place. Rickman told the officers, "he raped me again and I shot him." Officers found Carter laying face up on the bed naked with multiple gunshot wounds to his body. An autopsy revealed that Carter was shot ten times – four times in the chest, three times in the back, once on the arm, and twice in the head. Rickman's examining physician testified that he found no

injuries on Rickman consistent with her description of events, and no signs of trauma to her vaginal cavity. Rickman appealed her convictions, arguing she was denied effective assistance of counsel and that the trial court erred in admitting improper character evidence. Finding no reversible error, the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Robinson v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0265
Opinion Date: April 20, 2020
Judge: Peterson
Areas of Law: Constitutional Law, Criminal Law

Herbert Robinson appealed his convictions for malice murder, armed robbery, and possession of a firearm during the commission of a felony in connection with the death of Michael Moore. On appeal, he argued the trial court erred by allowing the State to use two firearms for demonstrative purposes during trial, and by allowing body-camera footage to be shown at trial. He also argued his trial counsel was ineffective for failing to object to a letter written by Robinson's cellmate being available to the jury for review during deliberations, and for failing to object to a visual aid used by the State during closing arguments. Because Robinson failed to show ineffective assistance of counsel or reversible error by the trial court, the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Santana v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0563
Opinion Date: April 20, 2020
Judge: Warren
Areas of Law: Constitutional Law, Criminal Law

Cuevas Carlos Santana was convicted by jury of malice murder and other

crimes in connection with the 2010 shooting deaths of Israel Espinoza Mendoza, Vincente Soto Chavez, and Renato Soto Valencia. On appeal, Santana argues that the evidence was insufficient to support his convictions, that the trial court erred by declining to grant Santana a new trial on the general grounds, and that trial counsel provided ineffective assistance. Finding no reversible error, the Georgia Supreme Court affirmed Santana's convictions.

Read Opinion Are you a lawyer? **Annotate this case**.

Sullivan v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0056
Opinion Date: April 20, 2020
Judge: Warren
Areas of Law: Constitutional Law, Criminal Law

A jury convicted Antonio Sullivan of malice murder and other crimes in connection with the shooting death of Wava Benton. On appeal, Sullivan contended his trial counsel was constitutionally ineffective by failing to present evidence at trial to corroborate Sullivan's testimony about prior difficulties between Sullivan and Benton, and by failing to procure expert testimony about Sullivan's mental health—specifically about post-traumatic stress disorder— to be presented to the jury. The Georgia Supreme Court determined Sullivan failed to establish that his trial counsel was deficient in either respect, and therefore affirmed his convictions.

Read Opinion Are you a lawyer? **Annotate this case**.

Turner v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0247
Opinion Date: April 20, 2020
Judge: Warren
Areas of Law: Constitutional Law, Criminal Law

Appellant Ronald Turner appeals from his conviction for malice murder stemming from the stabbing death of William King. The stabbing took place

outside an apartment at which Turner had driven in order to trade food for drugs. Turner testified in his own defense at trial and claimed that King hit him in the head with a beer bottle because Turner owed money to King from a prior drug transaction. Turner testified that he tried to get away from King, but that King chased him down and grabbed his jacket. According to Turner, King was getting ready to hit him again when Turner stabbed King in self-defense. Appealing his ultimate conviction, Turner contended he was denied the effective assistance of counsel in three respects. Seeing no reversible error after a review of the trial court record, the Georgia Supreme Court affirmed Turner's conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Valrie v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0380
Opinion Date: April 20, 2020
Judge: Keith R. Blackwell
Areas of Law: Constitutional Law, Criminal Law

Reuben Valrie was tried by jury and convicted of murder and other crimes in connection with the death of his infant daughter Aliyana. Valrie appealed, claiming that he was denied the effective assistance of counsel. Aliyana died as a result of closed head trauma, with a blunt-force abdominal injury as a secondary cause of death, which investigators determined was consistent with being shaken or dropped. At trial, Valrie presented the testimony of four expert witnesses who testified that Aliyana died of natural causes and that the injuries to her brain and abdomen were caused by events such as post-mortem CPR and the “rough” handling of her body by first responders. The jury rejected this defense and found Valrie guilty of murder and the other charges. Valrie contended that his trial lawyer should have raised a hearsay objection to the admission of recorded statements that his girlfriend (and Aliyana's mother) made to police investigators (as well as the testimony of one of those investigators about some of those statements). Alternatively, Valrie argued that his lawyer should have sought the redaction of certain portions of the recorded statements that impugned his character. The Georgia Supreme Court concluded Valrie failed to present evidence that his trial counsel was deficient, or that he was

prejudiced by any alleged failures. According, the Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Williams v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0241
Opinion Date: April 20, 2020
Judge: Keith R. Blackwell
Areas of Law: Constitutional Law, Criminal Law

Richard Williams, II, was tried by jury and convicted of murder in connection with the strangulation death of Cory Robinson. Williams and Robinson were involved in a sexual relationship and had been living together at an extended-stay hotel. Kelvin Spencer was a close friend of both Williams and Robinson. When Spencer met Williams at the hotel room, Williams looked angry and had scratches on his neck. Spencer saw Robinson lying on the floor in a “praying position.” Spencer did not believe Robinson was dead, and he helped Williams move clothes and other things to a U-Haul truck parked outside, in preparation for a move. Williams did not testify or present any evidence. Based on his lawyer’s opening and closing arguments, the defense theory was that Spencer killed Robinson because he was jealous of Williams’s relationship with Robinson. Williams’s sole claim on appeal was that he was denied the effective assistance of counsel when his trial lawyer failed to present as a defense that Williams accidentally killed Robinson during consensual erotic asphyxiation. He argued that his lawyer's discomfort with the topic of homosexual BDSM activity, and his own problems with the Georgia State Bar, precluded presentation of the "true" version of events, and that Williams acceded to the lawyer's defense strategy only "through ignorance and that he did not know that a defense based on consensual erotic asphyxiation was available." Finding no reversible error, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Idaho v. Burke

Court: Idaho Supreme Court - Criminal

Docket: 46841
Opinion Date: April 22, 2020
Judge: Moeller
Areas of Law: Constitutional Law, Criminal Law

Prior to sentencing, defendant James Burke was committed to the state mental hospital for 56 days to restore him to competency. After being evaluated and deemed competent to proceed to trial, Burke was returned to the county jail and later pleaded guilty pursuant to a plea agreement. At the conclusion of his sentencing hearing, Burke sought credit for the 56 days of time spent in court-ordered commitment. The district court denied the motion, concluding that commitment to a state mental hospital did not fall under the definition of 'incarceration' in Idaho Code section 18-309. After reviewing this issue carefully, the Idaho Supreme Court disagreed with the district court's "thorough and thoughtful analysis," holding that court-ordered commitment to state custody pursuant to Idaho Code sections 18-210 and 18-211 met the functional and legal definition of "incarceration" under Idaho Code section 18-309. "The extent of the liberty interests restricted by Burke's court-ordered commitment to State Hospital North are just too similar to imprisonment to conclude otherwise." Accordingly, the Court reversed the district court's order denying Burke's request for credit for time served and remanded the case for the district court to enter an order crediting him with the fifty-six days he spent committed to State Hospital North while the State restored his competency to face criminal charges.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Gibbs

Court: Iowa Supreme Court
Docket: 18-1298
Opinion Date: April 17, 2020
Judge: Edward M. Mansfield
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction of murder in the second degree, holding that Defendant's Fifth Amendment rights were invaded when the trial judge instructed the jury that Defendant was required to notify law enforcement of his use of deadly force, but the error was harmless. During trial, Defendant asserted the defense of justification in his

shooting of the victim. At issue on appeal was whether the district court abused its discretion by giving a jury instruction incorporating the terms of Iowa Code 704.2B. The instruction included a statement that a person using deadly force is required to notify law enforcement about his use of deadly force. Defendant argued before the Supreme Court that both section 704.2B and the jury instruction incorporating that section violated his Fifth Amendment rights. The Supreme Court affirmed, holding (1) instructing the jury that a homicide defendant is required to notify a law enforcement agency of his use of deadly force violates the defendant's Fifth Amendment rights; but (2) any error in this case was harmless beyond a reasonable doubt.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Harris
Court: Kansas Supreme Court
Docket: 117362
Opinion Date: April 17, 2020
Judge: Wilson
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court reversed the judgment of the court of appeals affirming Defendant's conviction of possession fo marijuana, holding that Defendant's waiver of jury trial was legally insufficient. On appeal, Defendant argued that he did not properly waive his right to a jury and asserted three other issues. The Supreme Court reversed the judgment of the court of appeals affirming Defendant's convictions without addressing the three remaining issues, holding that because the district court failed properly to apprise Defendant of his right to a jury trial and failed to ensure that Defendant understood the nature of the right he was giving up, Defendant's constitutional right to a jury trial was violated in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Paquin
Court: Maine Supreme Judicial Court
Citation: 2020 ME 53

Opinion Date: April 23, 2020
Judge: Andrew M. Mead
Areas of Law: Constitutional Law, Criminal Law

In this appeal from Defendant's conviction for eleven counts of gross sexual misconduct, the Supreme Judicial Court vacated the judgment of conviction on one count, vacated the dismissal of other counts and remanded for entry of a judgment of acquittal on those counts, and affirmed in all other respects, holding that Defendant's convictions on both Counts 5 and 30 violated his double jeopardy protections and that the court erred in allowing the State to dismiss Counts 27, 28, and 29 during trial without Defendant's consent. The indictment charged Defendant with fifteen counts (Counts 1-13, 30-31) of gross sexual misconduct against the victim and sixteen counts (Counts 14-29) of gross sexual misconduct against a second alleged victim. During trial, the court granted Defendant's motion for a judgment of acquittal on Counts 10-13, and the State dismissed Counts 27-29. Defendant was found guilty of Counts 1-9 and 30-31 and not guilty on the remaining counts. The court entered judgment in accordance with the verdict. The Supreme Judicial Court held that the trial court erred in failing to rule that the Double Jeopardy Clause barred convictions on both Counts 5 and 30 and allowing the State to dismiss Counts 27, 28, and 29 rather than entering a judgment of acquittal on those counts.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. McCarthy

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12750
Opinion Date: April 16, 2020
Judge: Gaziano
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Judicial Court affirmed the judgment of the district court denying Defendant's motions to suppress, holding that the limited use of automatic license plate readers (ALPRs) in this case did not implicate constitutional protections against unreasonable searches. While police were investigating Defendant on suspicion of drug distribution they used ALPRs on two bridges to track Defendant's movements. The police accessed historical data via ALPR technology and received real-time alerts, the last of

which led to Defendant's arrest. Defendant filed motions to suppress the ALPR data and the fruits of the arrest. The superior court denied the motions. The Supreme Judicial Court affirmed, holding that while the widespread use of ALPRs in the Commonwealth could implicate a defendant's constitutional protected expectation of privacy in the whole of his public movements, that interest was not invaded by the limited extent and use of the ALPR data in the instant case.

Read Opinion Are you a lawyer? **Annotate this case**.

Goldstein v. Secretary of the Commonwealth

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12931
Opinion Date: April 17, 2020
Judge: Ralph D. Gants
Areas of Law: Constitutional Law, Election Law

The Supreme Judicial Court granted Plaintiffs' emergency petition and allowed Plaintiff's application for declaratory relief to the extent that this Court declares, in light of emergency circumstances arising from the COVID-19 pandemic, that the minimum signature requirements in Mass. Gen. Laws ch. 53, 7 and 44 for candidates in the September 1, 2020 primary election are unconstitutional. Plaintiffs argued that, in the context of the current pandemic, the minimum signature requirements to be listed on the ballot for a party's nomination posed an unconstitutionally undue burden on Massachusetts would-be candidates' constitutional right to seek elective office. The Supreme Judicial Court agreed, holding (1) application of the signature requirements in the context of the current public health crisis imposes a severe burden a candidate's right to gain access to the September 1 primary ballot, triggering heightened scrutiny; and (2) in this time of pandemic, the justification for the current signature requirements cannot survive this scrutiny and are unconstitutional as applied to Plaintiffs. The Court fashioned equitable relief intended to substantially diminish that burden while respecting the legislative purpose for imposing minimum signature requirements.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Reek

Court: Minnesota Supreme Court
Docket: A19-0153
Opinion Date: April 22, 2020
Judge: G. Barry Anderson
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction for first-degree murder, holding that there was no error in the proceedings below. Specifically, the Supreme Court held (1) Appellant's right to a fair trial before an impartial tribunal was not violated when the district court stated that it might reconsider its prior Spreigl ruling if the defense presented certain witnesses; (2) the jury instructions on accomplice liability were plainly erroneous, but Appellant failed to establish that there was a reasonable likelihood that the error had a significant effect on the verdict; (3) the prosecutor did not commit misconduct in his closing arguments regarding the law of accomplice liability; (4) the district court did not abuse its discretion by granting the State's motion to admit evidence of appellant's past convictions for impeachment purposes, including by allowing the specific convictions to be disclosed to the jury; and (5) Appellant's pro se arguments were without merit.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Montoya

Court: Nebraska Supreme Court
Citation: 305 Neb. 581
Opinion Date: April 17, 2020
Judge: Freudenberg
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the judgment of the district court affirming Defendant's conviction and sentence for driving under the influence, holding that there was no error in the challenged rulings by the trial court. Specifically, the Supreme Court held that the district court did not err by (1) affirming the county court's order denying Defendant's motion to suppress fruits of the stop; (2) affirming the county court's order that denied

Defendant's motion to suppress the fruits of his arrest; (3) affirming the county court's order that denied Defendant's motion to suppress the results of the test of his breath alcohol content; (4) finding sufficient evidence to support the conviction; and (5) finding that Defendant's sentence was not excessive.

Read Opinion Are you a lawyer? **Annotate this case**.

Multnomah County v. Mehrwein

Court: Oregon Supreme Court
Docket: S066445
Opinion Date: April 23, 2020
Judge: Martha Lee Walters
Areas of Law: Constitutional Law, Election Law, Government & Administrative Law

In the November 2016 election, Multnomah County voters approved Measure 26-184, an amendment to the Multnomah County Home Rule Charter containing campaign finance provisions. Multnomah County then adopted new ordinances, Multnomah County Code (MCC) sections 5.200-203, mirroring and implementing those charter provisions. At issue before the Oregon Supreme Court was the validity of those ordinances under the free speech provisions of both the Oregon and United States Constitutions - Article I, section 8, and the First Amendment. The Court reached four conclusions: (1) the county's contribution limits did not, on their face, violate Article I, section 8, of the Oregon Constitution; (2) the case had to be remanded for factual findings and to consider, in the first instance, whether the contribution limits violated the First Amendment; (3) the county's expenditure limits were invalid under both constitutional provisions; and (4) the parties' dispute with respect to the disclosure provisions was moot.

Read Opinion Are you a lawyer? **Annotate this case**.

Pennsylvania v. Britton

Court: Supreme Court of Pennsylvania
Docket: 55 MAP 2018
Opinion Date: April 22, 2020
Judge: Max Baer

Areas of Law: Constitutional Law, Criminal Law

California law enforcement officers interviewed Appellant Stacy Britton in her California residence and, unbeknownst to her, recorded those interviews. Over Appellant's objection, Pennsylvania used those recordings as evidence to help convict Appellant of murder in Pennsylvania. The Pennsylvania Supreme Court granted allowance of appeal to examine whether the California law enforcement officers were acting as agents of the Pennsylvania State Police when they recorded the interviews with Appellant in her California home, and if so, whether Pennsylvania's constitutional and statutory protections were available to Appellant under those circumstances. The Court concluded the California law enforcement officers were not acting as agents of the Pennsylvania State Police when they interviewed Appellant, making analysis of whether any Pennsylvania-specific constitutional or statutory protections unwarranted. Because the Supreme Court concluded the Pennsylvania trial court reached the proper result in this matter, it affirmed that court's judgment.

Read Opinion Are you a lawyer? **Annotate this case**.

Pennsylvania v. Copenhaver

Court: Supreme Court of Pennsylvania
Docket: 48 MAP 2019
Opinion Date: April 22, 2020
Judge: Thomas G. Saylor
Areas of Law: Constitutional Law, Criminal Law

In August 2015, a deputy sheriff conducted a vehicle stop of Appellant Victor Copenhaver's pickup truck. Upon approaching the truck, the deputy noticed an odor of alcohol and marijuana emanating from the passenger compartment. After administering field sobriety tests, he arrested Appellant for suspected driving under the influence of alcohol and controlled substances ("DUI"). Appellant was ultimately charged with DUI and other offenses. Appellant challenged the deputy's authority to conduct a traffic stop and sought suppression of all evidence obtained during the encounter. Rather than presenting testimony at a suppression hearing, the parties stipulated that Appellant was driving the vehicle in question and that the deputy had training and qualifications equivalent to that of a police officer.

The parties also agreed that the vehicle stop occurred as a result of the deputy observing the tailgate to the pickup truck being in a down position, which caught the deputy's attention. The deputy further observed the registration on the pickup truck was expired, and additionally, the registration number was identified as belonging to a vehicle other than the one on which it was attached. The issue this case presented for the Pennsylvania Supreme Court's review was whether the deputy could lawfully conduct the traffic stop based on the expired registration sticker, on a theory that such a violation amounts to a breach of the peace. The Supreme Court concluded driving a vehicle with an expired registration did not entail a breach of the peace. It vacated the superior court's order insofar as it held that the expired registration was a breach of the peace, thus alone authorizing the deputy to stop Appellant's vehicle. Notably, in light of its holding, the Supreme Court found the superior court did not proceed to consider other relevant questions, such as whether the parties' factual stipulation should have been read as indicating that the officer's understanding that the registration sticker was associated with a different vehicle arose in the pre-stop timeframe – consistent with the Commonwealth's position throughout this litigation. "These issues should be resolved in the first instance by the intermediate court on remand."

Read Opinion Are you a lawyer? **Annotate this case**.

Pennsylvania v. Tedford

Court: Supreme Court of Pennsylvania
Docket: 773 CAP
Opinion Date: April 22, 2020
Judge: Donohue
Areas of Law: Constitutional Law, Criminal Law

Appellant Donald Tedford was convicted of first-degree murder and rape on February 6, 1987. He appealed the dismissal of his second petition for relief filed pursuant to the Post Conviction Relief Act ("PCRA"), on December 2, 2014, as amended by a counseled petition on May 5, 2015, and a supplemental petition filed on June 9, 2015. In connection with his initial filings, Tedford sought wholesale discovery of the prosecution's entire file, but the PCRA court concluded that the petition (as amended) was not timely filed. Tedford also appealed the PCRA court's order denying his

supplemental PCRA petition, in which he requested discovery, an evidentiary hearing, and/or a new trial based upon the admission of expert testimony presented at trial related to microscopic hair analysis. The PCRA court concluded that pursuant to PCRA Section 9545(b)(1)(ii), it had jurisdiction to consider the merits of Tedford's newly-discovered-facts claims, but ultimately it concluded Tedford had not asserted a meritorious claim in accordance with Section 9543(a)(2)(vi). Finding no reversible error in that analysis, the Pennsylvania Supreme Court affirmed dismissal of the petition for relief.

Read Opinion Are you a lawyer? **Annotate this case**.

Pennsylvania v. Trahey

Court: Supreme Court of Pennsylvania
Docket: 38 EAP 2018
Opinion Date: April 22, 2020
Judge: Wecht
Areas of Law: Constitutional Law, Criminal Law

The trial court granted Timothy Trahey's motion to suppress the results of a blood test that revealed his blood alcohol concentration ("BAC"), finding no justification for the investigating officers' failure to obtain a search warrant before conducting the test. On the Commonwealth's appeal, the Superior Court reversed, opining that the Commonwealth's evidence sufficiently established the existence of exigent circumstances, thus excusing the absence of a warrant. The Pennsylvania Supreme Court reversed, finding that while the exigency analysis is an objective one, "even disregarding the officers' subjective motivations, or their candid acknowledgment that they would have obtained a search warrant if they thought it necessary, there was no time-sensitive need to conduct a warrantless blood test under the circumstances of this case. Accordingly, the Superior Court's conclusion that the test was justified by exigent circumstances was drawn in error."

Read Opinion Are you a lawyer? **Annotate this case**.

In re Greg Abbott

Court: Supreme Court of Texas

Docket: 20-0291
Opinion Date: April 23, 2020
Judge: Per Curiam
Areas of Law: Constitutional Law, Criminal Law

The Supreme Court conditionally granted mandamus relief to the State seeking review of a temporary restraining order (TRO) blocking enforcement of Executive Order GA-13, which changes the rules applicable to judges' decisions regarding pre-trial bail, against judges, holding that the trial court lacked jurisdiction to order the judges' requested relief, even temporarily. GA-13 suspends certain statutes authorizing trial judges to release jail inmates with violent histories during the state of disaster due to the threat of the novel coronavirus. Plaintiffs alleged that GA-13 is unconstitutional and exceeds the governor's statutory emergency powers. Sixteen of the plaintiffs were Texas trial judges alleging that GA-13 improperly interferes with their judicial authority to make individualized bail decisions, and the other plaintiffs were public interest organizations and lawyer associations. The trial court issued a TRO blocking enforcement of GA-13 against judges. The Supreme Court conditionally granted mandamus relief, holding that the alleged threat of a criminal prosecution in this case did not give the judges standing to seek the invalidation of GA-13, and therefore, the trial court lacked jurisdiction to order their requested relief.

Read Opinion Are you a lawyer? **Annotate this case**.

Stahmann v. Texas

Court: Texas Court of Criminal Appeals
Docket: PD-0556-18
Opinion Date: April 22, 2020
Judge: Barbara Hervey
Areas of Law: Constitutional Law, Criminal Law

Appellant Karl Stahmann was involved in an automobile accident, after which he threw a bottle of promethazine, a controlled substance, over a nearby wire fence before law enforcement arrived. The bottle landed two to three feet past the fence in plain view. He was convicted of third-degree felony tampering with physical evidence and was sentenced to 10 years' confinement and fined $5,000. The judge suspended his sentence and placed him on community supervision for 10 years. Stahmann appealed,

arguing in part that the evidence was insufficient to prove that he destroyed, altered, or concealed the prescription bottle. The court of appeals agreed that the evidence was insufficient, but instead of rendering an acquittal, it reformed the judgment to show that Stahmann was convicted of the lesser-included offense of attempted tampering with physical evidence, a state-jail felony. After review of the evidence presented at trial, the Texas Court of Criminal Appeals concluded the evidence was indeed insufficient to prove that Appellant altered the prescription pill bottle when he threw it over the fence because the mere act of throwing the bottle did not change the bottle itself. "While a rational jury could have reasonably inferred that Stahmann intended to conceal the pill bottle when he threw it over the wire fence, the evidence shows that he failed to conceal it as he intended because the bottle landed short of the bush in plain view on top of some grass." The Court affirmed the trial court's judgment.

Read Opinion Are you a lawyer? **Annotate this case**.

Washington v. Escalante

Court: Washington Supreme Court
Docket: 97268-1
Opinion Date: April 23, 2020
Judge: Steven González
Areas of Law: Constitutional Law, Criminal Law

Alejandro Escalante was detained for hours in a secured area at a border crossing and, the State conceded, interrogated by federal agents without Miranda warnings. Statements he made during that interrogation were used by the State to convict him of drug possession. While a traveler briefly detained and questioned at the border was typically not "in custody" for Miranda purposes, "the government's power to detain and question people at the border without implicating Miranda has limits." Here, the Washington Supreme Court determined those limits were reached. "This border detention created the type of inherently coercive environment that demands Miranda warnings to ensure an individual's choice to speak is the product of free will." The Supreme Court held that Escalante was in custody when he was interrogated and reversed.

Read Opinion Are you a lawyer? **Annotate this case**.

Washington v. Haggard

Court: Washington Supreme Court
Docket: 97375-0
Opinion Date: April 23, 2020
Judge: Barbara Madsen
Areas of Law: Constitutional Law, Criminal Law

A class C felony "washes out" and is omitted from a defendant's offender score as long as he or she is not convicted of any crime within five years of the last date of release from confinement. David Haggard was convicted of a misdemeanor offense within this five-year period, which was dismissed pursuant to RCW 3.66.067. When Haggard later pleaded guilty to burglary and arson, the trial court included prior class C felonies in his criminal history, finding that the dismissed misdemeanor conviction interrupted the washout period for those offenses. Haggard contended on appeal this was error. The Washington Supreme Court determined that because a dismissed conviction constituted a "conviction" under the Sentencing Reform Act of 1981 (SRA), and misdemeanor dismissal and vacation were distinct processes, so Haggard's offender score was properly calculated.

Read Opinion Are you a lawyer? **Annotate this case**.

Morrisey v. West Virginia AFL-CIO

Court: Supreme Court of Appeals of West Virginia
Docket: 19-0298
Opinion Date: April 21, 2020
Judge: Jenkins
Areas of Law: Civil Rights, Constitutional Law, Labor & Employment Law

The Supreme Court reversed the rulings of the circuit court finding that the Workplace Freedom Act (the Act) infringes upon the rights to associate, as well as the liberty and property rights, of labor unions that are member organizations of the AFL-CIO (Labor Unions), holding that the Act does not violate constitutional rights at issue. In 2016, the Legislature enacted the Act, which prohibits collective bargaining agreements that require an employee to pay any dues, fees, assessments, or other similar charges as a condition of employment, or as a condition for the continuation of

employment, when the employee has chosen not to join a union. On remand, the circuit court ruled that the Act unconstitutionally fringes on the rights of the Labor Unions, who represent both private and government workers in West Virginia. The Supreme Court reversed, holding that the Act does not violate the West Virginia Constitution's protections of association, property, and liberty rights.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Taylor

Court: Supreme Court of Appeals of West Virginia
Docket: 18-0502
Opinion Date: April 21, 2020
Judge: Walker
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the judgment of the circuit court giving Petitioner credit for twelve days of time served toward the sentence he received for his felony conviction although Petitioner spent additional time in confinement for other charges that were dismissed in the universal plea agreement, holding that to grant Petitioner additional credit for time served would do little more than reward Petitioner for habitual criminal behavior. Petitioner was charged with several crimes and agreed to resolve the pending charges against him in a universal plea agreement. Under the terms of the agreement, Petitioner agreed to plea guilty to the charge of felony carrying a concealed firearm by a prohibited person. In exchange, the State agreed to drop the remaining charges. After he was sentenced, Petitioner argued that, in addition to the twelve days of credit for time served he was granted, he was constitutionally entitled to credit for time served while he was incarcerated for charges that were resolved in the universal plea agreement. The Supreme Court affirmed, holding that Petitioner's circumstances implicated neither double jeopardy nor equal protection of the law such that additional credit for time served was constitutionally mandated.

Read Opinion Are you a lawyer? **Annotate this case**.

About Justia Opinion Summaries

Justia Weekly Opinion Summaries is a free service, with 63 different newsletters, each covering a different practice area.

Justia also provides 68 daily jurisdictional newsletters, covering every federal appellate court and the highest courts of all US states.

All daily and weekly Justia newsletters are free. Subscribe or modify your newsletter subscription preferences at daily.justia.com.

You may freely redistribute this email in whole.

About Justia

Justia is an online platform that provides the community with open access to the law, legal information, and lawyers.

Contact Us | Privacy Policy

Unsubscribe From This Newsletter
or unsubscribe from all Justia newsletters immediately **here.**

Justia | 1380 Pear Ave #2B, Mountain View, CA 94043

From:	Criminal Law - Justia Weekly Opinion Summaries
To:	Hopkins, Tyler (POL)
Subject:	Latest 101 Cases This Week: Ramos v. Louisiana (U.S.), United States v. Diaz-Rivera (1st Cir.), United States v. Cotto (2d Cir.)
Date:	Friday, April 24, 2020 9:08:15 AM

If you are unable to see this message, click here to view it in a web browser.

Justia Weekly Opinion Summaries

Criminal Law
April 24, 2020

Table of Contents

Ramos v. Louisiana
Civil Rights, Constitutional Law, Criminal Law
US Supreme Court

United States v. Diaz-Rivera
Criminal Law

US Court of Appeals for the First Circuit

United States v. Cotto
Criminal Law
US Court of Appeals for the Second Circuit

United States v. Rosa
Criminal Law
US Court of Appeals for the Second Circuit

Fogle v. Sokol
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Third Circuit

James v. New Jersey State Police
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Third Circuit

Bazemore v. Best Buy
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Akande
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Chambers
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Ferebee
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Nance
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Johnson
Criminal Law
US Court of Appeals for the Fifth Circuit

United States v. McGinnis
Criminal Law
US Court of Appeals for the Fifth Circuit

Valentine v. Collier
Civil Rights, Constitutional Law, Criminal Law, Government & Administrative Law, Health Law
US Court of Appeals for the Fifth Circuit

United States v. Dowl
Criminal Law

US Court of Appeals for the Sixth Circuit

United States v. Fowler
Criminal Law
US Court of Appeals for the Sixth Circuit

United States v. Sumlin
Criminal Law
US Court of Appeals for the Sixth Circuit

United States v. Vance
Criminal Law, White Collar Crime
US Court of Appeals for the Sixth Circuit

Winburn v. Nagy
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Sixth Circuit

Lund v. City of Rockford
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

United States v. Perez
Criminal Law
US Court of Appeals for the Seventh Circuit

Jackson v. United States
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Bolman
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Boyd
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Gonzalez-Esparsa
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Sanchez-Velasco
Criminal Law, Immigration Law
US Court of Appeals for the Eighth Circuit

Anthony v. TRAX International Corp.
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Ninth Circuit

City of Almaty v. Khrapunov
Criminal Law, International Law, White Collar Crime

US Court of Appeals for the Ninth Circuit

United States v. Baldon
Criminal Law
US Court of Appeals for the Ninth Circuit

United States v. Costanzo
Criminal Law
US Court of Appeals for the Ninth Circuit

United States v. Manzanares
Constitutional Law, Criminal Law
US Court of Appeals for the Tenth Circuit

United States v. Delaney
Criminal Law
US Court of Appeals for the District of Columbia Circuit

Antenor v. Alaska, Department of Corrections
Civil Procedure, Criminal Law, Government & Administrative Law
Alaska Supreme Court

Berger v. Bryant
Criminal Law
Arkansas Supreme Court

Carroll v. State
Criminal Law
Arkansas Supreme Court

Cave v. State
Civil Rights, Constitutional Law, Criminal Law
Arkansas Supreme Court

Chatmon v. Kelley
Criminal Law
Arkansas Supreme Court

McClinton v. State
Criminal Law
Arkansas Supreme Court

Siegel v. State
Criminal Law
Arkansas Supreme Court

Thomas v. State
Civil Rights, Constitutional Law, Criminal Law
Arkansas Supreme Court

California v. Landowski
Constitutional Law, Criminal Law

California Courts of Appeal

California v. May
Constitutional Law, Criminal Law
California Courts of Appeal

California v. Perez
Constitutional Law, Criminal Law
California Courts of Appeal

In re S.R.
Criminal Law
California Courts of Appeal

People v. Bell
Criminal Law
California Courts of Appeal

People v. Drayton
Criminal Law
California Courts of Appeal

People v. Robinson
Criminal Law
California Courts of Appeal

People v. Torres
Criminal Law
California Courts of Appeal

Colorado v. Lujan
Constitutional Law, Criminal Law
Colorado Supreme Court

Archer v. State
Civil Rights, Constitutional Law, Criminal Law
Florida Supreme Court

Collins v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Heyward v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Howard v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Keller v. Georgia
Constitutional Law, Criminal Law

Supreme Court of Georgia

Mills v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Moore v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Morris v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Rickman v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Robinson v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Santana v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Sullivan v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Turner v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Valrie v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Williams v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

State v. Malave
Criminal Law
Supreme Court of Hawaii

State v. Malave
Criminal Law
Supreme Court of Hawaii

Idaho v. Burke
Constitutional Law, Criminal Law

Idaho Supreme Court - Criminal

State v. Gibbs
Civil Rights, Constitutional Law, Criminal Law
Iowa Supreme Court

State v. Broxton
Criminal Law
Kansas Supreme Court

State v. Corbin
Criminal Law
Kansas Supreme Court

State v. Frazier
Criminal Law
Kansas Supreme Court

State v. Harris
Civil Rights, Constitutional Law, Criminal Law
Kansas Supreme Court

State v. Uk
Criminal Law
Kansas Supreme Court

State v. Catruch
Criminal Law
Maine Supreme Judicial Court

State v. Paquin
Constitutional Law, Criminal Law
Maine Supreme Judicial Court

Watson v. State
Criminal Law
Maine Supreme Judicial Court

Commonwealth v. Mazza
Criminal Law
Massachusetts Supreme Judicial Court

Commonwealth v. McCarthy
Civil Rights, Constitutional Law, Criminal Law
Massachusetts Supreme Judicial Court

Garden v. Commonwealth
Criminal Law
Massachusetts Supreme Judicial Court

In re Mitchell
Criminal Law

Massachusetts Supreme Judicial Court

State v. Reek
Civil Rights, Constitutional Law, Criminal Law
Minnesota Supreme Court

State v. Woodard
Criminal Law
Minnesota Supreme Court

Huff v. Brown
Communications Law, Criminal Law
Nebraska Supreme Court

State v. Montoya
Civil Rights, Constitutional Law, Criminal Law
Nebraska Supreme Court

State v. Schroeder
Criminal Law
Nebraska Supreme Court

State ex rel. Kendrick v. Parker
Criminal Law
Supreme Court of Ohio

State ex rel. Nelson v. Russo
Criminal Law
Supreme Court of Ohio

State ex rel. Roberts v. Marsh
Criminal Law
Supreme Court of Ohio

State ex rel. Steiner v. Rinfret
Criminal Law
Supreme Court of Ohio

State v. Jeffries
Criminal Law
Supreme Court of Ohio

Pennsylvania v. Britton
Constitutional Law, Criminal Law
Supreme Court of Pennsylvania

Pennsylvania v. Copenhaver
Constitutional Law, Criminal Law
Supreme Court of Pennsylvania

Pennsylvania v. Tedford
Constitutional Law, Criminal Law

Supreme Court of Pennsylvania

Pennsylvania v. Trahey
Constitutional Law, Criminal Law
Supreme Court of Pennsylvania

In re Greg Abbott
Constitutional Law, Criminal Law
Supreme Court of Texas

Stahmann v. Texas
Constitutional Law, Criminal Law
Texas Court of Criminal Appeals

Blanke v. Board of Pardons & Parole
Criminal Law
Utah Supreme Court

Washington v. Escalante
Constitutional Law, Criminal Law
Washington Supreme Court

Washington v. Haggard
Constitutional Law, Criminal Law
Washington Supreme Court

State v. Taylor
Civil Rights, Constitutional Law, Criminal Law
Supreme Court of Appeals of West Virginia

State v. Harrison
Criminal Law
Wisconsin Supreme Court

COVID-19 Updates: Law & Legal Resources Related to Coronavirus

Click here to include Verdict article summaries with your newsletter(s).

Criminal Law Opinions

Ramos v. Louisiana

Court: US Supreme Court
Docket: 18-5924
Opinion Date: April 20, 2020
Judge: Neil M. Gorsuch
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

In 48 states and in federal court, a single juror's vote to acquit is enough to

prevent a conviction; Louisiana and Oregon punish people based on 10-to-2 verdicts. Ramos was convicted in a Louisiana court by a 10-to-2 jury verdict and was sentenced to life without parole. The Supreme Court reversed. The Sixth Amendment right to a jury trial, as incorporated against the states by the Fourteenth Amendment, requires a unanimous verdict to convict a defendant of a serious offense. Juror unanimity is a vital common law right. The Court rejected an "invitation" to "perform a cost-benefit analysis on the historic features of common law jury trials and to conclude that unanimity does not make the cut." In overturning its 1972 "Apodaca" decision, the Court stated that the reasoning, in that case, was "gravely mistaken" and "sits uneasily with 120 years of preceding case law." The fact that Louisiana and Oregon may need to retry defendants convicted of felonies by non-unanimous verdicts whose cases are still pending on direct appeal "will surely impose a cost, but new rules of criminal procedure usually do."

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Diaz-Rivera

Court: US Court of Appeals for the First Circuit
Docket: 18-1461
Opinion Date: April 20, 2020
Judge: Torruella
Areas of Law: Criminal Law

The First Circuit affirmed Defendant's upwardly variant sentence for one count of possession with intent to distribute cocaine and one count of using a firearm during and in relation to a drug-trafficking crime, holding that the sentence was neither procedurally nor substantively unreasonable. Pursuant to a plea agreement, Defendant pled guilty to drug-related crimes. After a sentencing hearing, the district court sentenced Defendant to an upwardly variant sentence of 180 months of imprisonment, thus declining to impose the government's requested sentence. On appeal, Defendant challenged both the procedural and substantive reasonableness of his sentence. The First Circuit affirmed, holding that the 180-month sentence was neither procedurally nor substantively unreasonable.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Cotto

Court: US Court of Appeals for the Second Circuit
Docket: 18-2970
Opinion Date: April 20, 2020
Judge: Leval
Areas of Law: Criminal Law

A conviction for retaliating against a witness in violation of 18 U.S.C. 1513 does not require that the Government prove that defendant had knowledge of the federal nature of the proceeding. The Second Circuit rejected defendant's arguments to the contrary and affirmed his conviction for retaliating against a witness. The court remanded for revision of the provision of the sentence relating to the substance abuse treatment condition of supervised release; instructed the district court to consider on remand whether the court's forthcoming order in United States v. Traficante, No. 18-1962 (2d Cir., submitted Oct. 25, 2019) requires modification of the risk notification provision of supervised release; and granted the parties leave to reinstate this appeal to permit review of the district court's decision on remand as to the risk notification provision.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Rosa

Court: US Court of Appeals for the Second Circuit
Docket: 17-2004
Opinion Date: April 17, 2020
Judge: Nardini
Areas of Law: Criminal Law

Where a district court offers no explanation for its sentence, and where neither the adopted presentence report nor the statement of reasons adequately demonstrates the court's reasoning, the court has committed plain error in violation of 18 U.S.C. 3553(c). The Second Circuit vacated defendant's sentence for conspiracy to commit wire fraud and aggravated identity theft. The court held that the district court failed to state its reasons for sentencing defendant as required under section 3553(c); the error is clear or obvious; and the error affected defendant's substantial rights. Accordingly, the court remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

Fogle v. Sokol

Court: US Court of Appeals for the Third Circuit
Docket: 19-1066
Opinion Date: April 21, 2020
Judge: Matey
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

In 1976, the body of 15-year-old “Kathy” was found near her Indiana County, Pennsylvania home. Kathy’s death involved a brutal assault, rape, and a gunshot to the head. Kathy's sisters, ages nine and 12, stated that she had gotten into a car with a man with blue eyes, black hair that came below his ears and curled at the ends, sideburns, heavy eyebrows, and a heavy mustache. Fogle had “straight reddish-blonde hair that dropped down his back and a matching, full beard that reached his waist.” After three years, Fogle became a suspect because a psychiatric patient described seeing Kathy get in a car with Fogle and his brother. The story was largely inconsistent with statements by Kathy’s sisters. Jailhouse informants were recruited and counseled by law enforcement with promises of leniency. The prosecutors “either knew about, encouraged, or permitted” this strategy. A jury found Fogle guilty of second-degree murder. In 2015, Fogle obtained DNA evidence excluding both himself and his brother as the source of semen collected from Kathy. His conviction was vacated. The Commonwealth declined to pursue new charges, describing the case as lacking “prosecutorial merit.” Fogle, having spent three decades in prison, sued the prosecutors and Indiana County under 42 U.S.C. 1983. The Third Circuit affirmed the denial of their motions to dismiss based on absolute immunity. Only truly prosecutorial functions, not investigative conduct, justify complete protection from suit. Fogle’s complaint alleges actions that fall outside the narrow doctrine of absolute immunity.

Read Opinion Are you a lawyer? **Annotate this case**.

James v. New Jersey State Police

Court: US Court of Appeals for the Third Circuit

Docket: 18-1432
Opinion Date: April 21, 2020
Judge: Porter
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Stephens called 911 and reported that Gibbons hit her and had a gun in his truck. The police responded. Stephens obtained a temporary restraining order, prohibiting Gibbons from possessing firearms and from returning to Stephens's house. The next day, Gibbons went to Stephens's house. Stephens was talking on the phone; the friend called the police. Gibbons left Stephens's house. Trooper Conza arrived. Stephens stated that Gibbons had waved a gun throughout their argument. Conza told Stephens to go to the police barracks and reported over the radio that Gibbons had brandished a firearm. Conza, with Troopers Bartelt and Korejko, visited the nearby home of Gibbons's mother, James. James stated that she did not know where Gibbons was and that he might be off his schizophrenia medication. While driving to the barracks, Stephens saw Gibbons walking alongside the road and called 911. The Troopers responded. Bartelt parked his car and, exiting, observed that Gibbons was pointing a gun at his own head. Bartelt drew his weapon, stood behind his car door, and twice told Gibbons to drop his weapon. Gibbons did not comply. Bartelt shot Gibbons twice within seconds of stopping his car. Gibbons died that night. In James' suit under 42 U.S.C. 1983, the Third Circuit held that Bartelt is entitled to qualified immunity because he did not violate Gibbons's clearly established rights. Bartelt's pre-standoff knowledge of Gibbons differs from that of officers involved in cited cases. Bartelt could reasonably conclude that Gibbons posed a threat to others.

Read Opinion Are you a lawyer? **Annotate this case**.

Bazemore v. Best Buy

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-2196
Opinion Date: April 21, 2020
Judge: Quattlebaum
Areas of Law: Criminal Law

Plaintiff filed suit against her employer, Best Buy, claiming that she was harassed because of her race and gender and subjected to a hostile work

environment in violation of Title VII of the Civil Rights Act of 1964. Plaintiff's complaint stemmed from an incident where a coworker made a racist and sexually charged joke to a small group of coworkers that included plaintiff. The Fourth Circuit affirmed the district court's motion to dismiss and held that, in the case of allegedly harassing comments by a co-worker, an employee must allege plausible facts that the employer knew, or should have known, about the harassment and failed to take action reasonably calculated to stop it. Because plaintiff failed to do this, the court affirmed the district court's judgment. In this case, the coworker's conduct was not imputable to Best Buy where Best Buy took steps that were not only reasonably calculated to end such behavior, but that it did in fact end it.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Akande

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-6833
Opinion Date: April 20, 2020
Judge: Diana Jane Gribbon Motz
Areas of Law: Criminal Law

After defendant moved under 28 U.S.C. 2255 to vacate his conviction based on the ineffective assistance of counsel, the district court denied the motion. The Fourth Circuit granted a certificate of appealability and reversed the district court's judgment. The court held that, given counsel's specific misadvice regarding defendant's rights to preserve his appellate rights, on which defendant understandably relied, the district court's general admonishments did not amount to the careful explanation that addresses the particular issue necessary to cure the error. In this case, the plea colloquy did not correct counsel's erroneous advice and the error prejudiced defendant. Accordingly, the court remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Chambers

Court: US Court of Appeals for the Fourth Circuit
Docket: 19-7104

Opinion Date: April 23, 2020
Judge: Floyd
Areas of Law: Criminal Law

After defendant was erroneously sentenced as a career offender, he moved to reduce his sentence to time served under the First Step Act. The district court denied defendant's motion to reduce his custodial sentence, though it granted the motion as to his supervised release term. The Fourth Circuit held that the First Step Act does not constrain courts from recognizing Guidelines errors. The court explained that First Step Act motions fall under 18 U.S.C. 3582(c)(1)(B), a distinct exception to finality, and that section 404(b) of the First Step Act expressly allows a court to impose a reduced sentence in order to give retroactive effect to sections 2 and 3 of the Fair Sentencing Act. Furthermore, 18 U.S.C. 3553(a) sentencing factors apply in the section 404(b) resentencing context, and the resentencing court has discretion within the section 404(b) framework to vary from the Guidelines and, in doing so, to consider movants' post-sentencing conduct. In this case, the district court seemingly believed that it could not vary from the Guidelines range to reflect post-sentencing information. Therefore, the court vacated the district court's sentencing order. Finally, the court held that any Guidelines error deemed retroactive, such as the error in this case, must be corrected in a First Step Act resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Ferebee

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-4266
Opinion Date: April 22, 2020
Judge: Traxler
Areas of Law: Criminal Law

The Fourth Circuit affirmed the denial of defendant's motion to suppress evidence recovered from a backpack, and the district court's conclusion that defendant abandoned the backpack and any legitimate expectation of privacy in its contents. The court rejected defendant's claim that the collective-knowledge doctrine has any bearing on the propriety of the district court's conclusion that defendant abandoned the backpack. The court also held that the district court is not precluded from finding abandonment in

cases where the defendant, as here, has physical possession of the property he has disavowed. In this case, the record supported the district court's conclusion that defendant clearly and unequivocally disavowed ownership of the backpack. Even if the district court erred by finding that defendant abandoned the backpack, reversal would not be required because the search of the backpack was a proper search incident to arrest for which no warrant was required under the facts of this case.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Nance

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-4585
Opinion Date: April 21, 2020
Judge: Pamela Harris
Areas of Law: Criminal Law

The Fourth Circuit affirmed defendant's above-Guidelines sentence imposed after he pleaded guilty to two federal drug- and firearm-related offenses. The court held that defendant's sentence was not procedurally unreasonable where the district court took into account defendant's extensive criminal history; his pattern of reoffending upon release; his disciplinary infractions in custody and inability to comply with the terms of his release; and the fact that the offenses of conviction occurred over the course of days, in which he was arrested once, released, and then arrested again just days later. The court also held that defendant's sentence was substantively reasonable where the district court conducted a thorough, individualized assessment of defendant and his offense conduct in light of the 18 U.S.C. 3553(a) factors, and did not abuse its discretion in formulating the sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Johnson

Court: US Court of Appeals for the Fifth Circuit
Docket: 17-60852
Opinion Date: April 21, 2020

Judge: Priscilla R. Owen
Areas of Law: Criminal Law

The Fifth Circuit vacated defendant's sentence imposed after he pleaded guilty to violating 18 U.S.C. 922(g) and 924(e) by knowingly possessing a firearm after he had been convicted of a misdemeanor crime of domestic violence. The court held that the district court committing plain error by violating Federal Rule of Criminal Procedure 32 when it relied on factual allegations in the confidential sentencing recommendation that were not in the presentence report and that were not disclosed by defendant. The court explained that the use of undisclosed facts to justify an above-guidelines sentence seriously affects the fairness, integrity, and public reputation of judicial proceedings. Therefore, the court remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. McGinnis

Court: US Court of Appeals for the Fifth Circuit
Docket: 19-10197
Opinion Date: April 21, 2020
Judge: Stuart Kyle Duncan
Areas of Law: Criminal Law

18 U.S.C. 922(g)(8), which prohibits individuals subject to certain domestic violence protective orders from possessing firearms or ammunition for any purpose, is facially constitutional under the Fifth Circuit's two-step NRA framework. Even assuming arguendo that the conduct at issue -- the keeping and possessing of firearms by individuals subject to domestic protective orders -- falls within the Second Amendment right, defendant's facial challenge fails. The court applied intermediate scrutiny and held that section 922(g)(8) is reasonably adapted to the government interest of reducing domestic gun abuse. The court also held that if the commonly understood definitions of terms in the protective order include acts involving "physical force," the protective order is sufficient to support a conviction under section 922(g)(8)(C)(ii). In this case, the jury plausibly found that the order satisfied the statute and the court declined to reverse defendant's conviction on this basis. However, the court remanded for the limited purpose of conforming defendant's written judgment to the district court's

oral pronouncement.

Read Opinion Are you a lawyer? **Annotate this case**.

Valentine v. Collier

Court: US Court of Appeals for the Fifth Circuit
Docket: 20-20207
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Criminal Law, Government & Administrative Law, Health Law

Plaintiffs filed suit alleging that TDCJ's adoption and implementation of measures guided by changing CDC recommendations in regards to the COVID-19 pandemic do not go far enough. Plaintiffs filed a class action alleging violations of the Eighth Amendment's prohibition against cruel and unusual punishment, and the Americans with Disabilities Act, seeking a preliminary injunction. The Fifth Circuit granted TDCJ's motion to stay the district court's preliminary injunction, which regulates the cleaning intervals for common areas, the types of bleach-based disinfectants the prison must use, the alcohol content of hand sanitizer that inmates must receive, mask requirements for inmates, and inmates' access to tissues (amongst many other things). The court held that TDCJ is likely to prevail on the merits of its appeal because: (1) after accounting for the protective measures TDCJ has taken, plaintiffs have not shown a "substantial risk of serious harm" that amounts to "cruel and unusual punishment"; and (2) the district court committed legal error in its application of Farmer v. Brennan, by treating inadequate measures as dispositive of defendants' mental state. In this case, even assuming that there is a substantial risk of serious harm, plaintiffs lack evidence of defendants' subjective deliberate indifference to that harm. The court also held that TDCJ has shown that it will be irreparably injured absent a stay, and that the balance of the harms and the public interest favor a stay. Finally, the court held that plaintiffs have not exhausted their administrative remedies as required in the Prison Litigation Reform Act (PLRA), and the district court's injunction goes well beyond the limits of what the PLRA would allow even if plaintiffs had properly exhausted their claims.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Dowl

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-2469
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

Dowl pleaded guilty to presenting false tax returns, 18 U.S.C. 286. He received a sentence of 30 months of imprisonment plus 24 months of supervised release. On supervised release, Dowl was charged with four new state crimes; failing to inform his probation officer that he had police contact; communicating with his co-defendant despite instructions to the contrary; failing to make payments on his restitution, fine, or special assessment; and failing to get a job. At a hearing, the court reviewed the evidence and allowed Dowl to tell his side of the story. The court deferred judgment on three of the four new state criminal law violations and dismissed the fourth and found Dowl gainfully employed. Dowl had failed to notify his probation officer about police contact, impermissibly communicated with his co-defendant, and did not pay his fines. After considering the 18 U.S.C. 3553(a) sentencing factors, the court returned Dowl to prison for 11 months, giving Dowl and his attorney the opportunity to raise any objections. Dowl had none. The Sixth Circuit affirmed, rejecting Dowl's argument that the court committed reversible error by not directly addressing him to solicit an allocution. The court employed the "plain error" standard because Dowl did not raise any objection during his revocation hearing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Fowler

Court: US Court of Appeals for the Sixth Circuit
Dockets: 19-3071, 19-3070
Opinion Date: April 21, 2020
Judge: Donald
Areas of Law: Criminal Law

In 2018, Fowler pled guilty to possession of child pornography and violations of the conditions of his supervised release from a previous conviction for the same. In addition to possessing child pornography, Fowler had failed drug testing, had threatened his parole officer, and had tried to harass his girlfriend to recant her testimony. The district court ordered Fowler to pay a $5,000 special assessment for possession of child pornography under the Justice for Victims of Trafficking Act, 18 U.S.C. 3014. The court also varied upward and sentenced Fowler to the maximum statutory penalty for violating the conditions of his supervised release, imposing a 120-month sentence for possessing child pornography and a consecutive 36-month sentence for violating the terms of his supervised release. The Sixth Circuit vacated as to the assessment and remanded for a determination of indigency. The district court committed plain error by failing to address Fowler's ability to pay; the parties did not contemplate the $5,000 special assessment as a part of the waiver provision in the plea agreement. The court affirmed the sentence. The district court did not consider an impermissible factor (whether Fowler had actually touched a child) and Fowler had no other challenge to the reasonableness of his sentence,

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Sumlin

Court: US Court of Appeals for the Sixth Circuit
Docket: 18-3819
Opinion Date: April 21, 2020
Judge: Bush
Areas of Law: Criminal Law

Sumlin was convicted of the distribution of drugs that caused the 2015 death of Carrie Dobbins, 21 U.S.C. 841(a)(1) and (b)(1)(C), which carries enhanced penalty provisions. The Sixth Circuit affirmed his convictions and his sentence to life in prison. The district court properly denied Sumlin's suppression motion, given that the affidavit established a sufficient nexus between his drug trafficking activity and residence that was searched. The court properly admitted testimony by the victim's sister, Kelly, who was Sumlin's former girlfriend and had purchased drugs from him. Kelly's testimony about Sumlin's drug-trafficking and that Sumlin was with Carrie on

the day of her overdose was intrinsic proof that was relevant for providing background information and contextualizing the government's case against Sumlin. Sufficient evidence supported the jury's verdict that Sumlin distributed the drugs that caused Carrie's death.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Vance

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-5160
Opinion Date: April 17, 2020
Judge: Bush
Areas of Law: Criminal Law, White Collar Crime

The Spriggs' bank account was established to receive social security checks. The Spriggs' great-grandson, Vance, filled out an application in Mr. Spriggs's name for a debit card to draw on the checking account. Mr. Spriggs had never used a debit card. The Spriggses did not authorize Vance to do so. Bank cameras photographed Vance using the card to withdraw cash. Vance also used the card for personal expenses. At another bank, Vance used Mr. Spriggs's social security number to establish an account and obtain a $15,000 cash advance. Vance made other, unsuccessful loan applications. Upon being notified by the banks about suspicious activities involving his identity, Mr. Spriggs filed a police report. The police arrested Vance. While searching Vance's car, the police located a large stash of personal and financial documents belonging to the Spriggses, including bank statements, tax return forms, property-tax bills, and a car title. The Sixth Circuit affirmed Vance's convictions for access-device fraud, 18 U.S.C. 1029(a)(5), and two counts of aggravated identity theft, 18 U.S.C. 1028A(a)(1), and his 65-month sentence. The court rejected arguments that the district court failed to make adequate findings of fact after the bench trial, improperly denied a motion for judgment of acquittal, and failed to correctly calculate the loss amount connected to Vance's charges under Sentencing Guidelines 2B1.1.

Read Opinion Are you a lawyer? **Annotate this case**.

Winburn v. Nagy

Court: US Court of Appeals for the Sixth Circuit
Dockets: 19-2399, 19-2398
Opinion Date: April 23, 2020
Judge: Jeffrey S. Sutton
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Winburn represented himself at his trial for armed robbery, home invasion, and conspiracy. Based on Winburn's disruptive behavior, the judge removed him from the courtroom and revoked Winburn's permission to represent himself, then granted a competency evaluation and a mistrial. While Winburn awaited his second trial, the judge permitted Winburn's stand-by attorney to withdraw because Winburn had sued her and enjoined Winburn from filing complaints or grievances against his new attorney, except to discharge her. Although represented by a new attorney, Winburn moved pro se to dismiss his charges on double jeopardy grounds. The trial judge denied the motion because Winburn's attorney had not filed it. Winburn filed a habeas petition under 28 U.S.C. 2241 challenging his retrial and another section 2241 petition challenging the injunction. The district judges denied both and declined to issue certificates of appealability. Winburn filed a notice of appeal for one petition and sought a certificate of appealability for the other. The Sixth Circuit held that state pretrial detainees proceeding under section 2241 may not appeal without certificates of appealability and granted Winburn a certificate on the injunction claim. A reasonable jurist could conclude that the unusual order was constitutionally infirm. The court denied relief with respect to double jeopardy. Winburn failed to exhaust his state-court remedies by a motion to dismiss.

Read Opinion Are you a lawyer? **Annotate this case**.

Lund v. City of Rockford

Court: US Court of Appeals for the Seventh Circuit
Docket: 19-1945
Opinion Date: April 20, 2020
Judge: ROVNER
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Lund, a reporter for the Rockford Scanner, heard, by police scanner, of multiple traffic stops in Midtown. He did not have a driver's license, so he

rode a motorized bicycle to Midtown to take photographs. He suspected a prostitution sting operation. An officer noticed Lund and radioed the team. Officers Welsh and Campbell knew of Lund's previous anti-police speech. They directed Lund to “move on.” Lund asked if he was breaking any laws. Campbell informed him that he was not, but that his continued presence would constitute obstruction of a police detail and result in arrest. Lund started his bicycle and called out, loudly, “goodbye officers.” Concerned that Lund might post pictures on social media while the sting operation was ongoing and create a danger for unarmed undercover officers, the officers followed Lund and arrested him for driving the wrong way on a one-way street, operating a vehicle without insurance, obstructing a police officer, felony aggravated driving on a revoked license, and operating a motor vehicle without a valid drivers’ license. News stories listed Lund’s name as an arrestee in the prostitution sting. The charges against Lund were dismissed. Lund sued the officers and the city under 42 U.S.C. 1983. The Seventh Circuit affirmed summary judgment for the defendants on First Amendment retaliation and malicious prosecution under Illinois law, citing the Supreme Court’s intervening "Nieves" (2019) holding, that, in most cases, probable cause to arrest defeats a claim of retaliatory arrest. There was probable cause to arrest Lund.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Perez

Court: US Court of Appeals for the Seventh Circuit
Docket: 18-3156
Opinion Date: April 23, 2020
Judge: KANNE
Areas of Law: Criminal Law

Beloit officers facilitated a recorded controlled buy of heroin from Perez, a suspected high-level drug dealer. Perez sold 98 grams of heroin to an informant. Based on that transaction alone, Perez pled guilty to distributing heroin. At Perez’s sentencing hearing, the judge expressed concern that the guidelines range of 33–41 months’ imprisonment did not reflect the full scope of his drug trafficking. The PSR described conduct that suggested that Perez was responsible for distributing large quantities of heroin, methamphetamine, and cocaine. The judge continued the hearing, directing

the government to file a memorandum, detailing which offense conduct it could support by a preponderance of the evidence. When the hearing reconvened, the government presented witness testimony that elaborated on conduct described in the PSR, including drug ledgers, Perez's post-arrest conversation with his girlfriend, large sums of cash, a money counter, cell phones, and Perez's passport. The judge calculated a higher guidelines range and imposed a 121-month sentence. The Seventh Circuit affirmed, rejecting an argument that the sentencing judge should have recused himself. Perez has not demonstrated that a reasonable observer would have questioned the judge's impartiality nor did he allege that the judge was biased based on events outside the proceedings. The judge's continuance was laudable, not prejudicial.

Read Opinion Are you a lawyer? **Annotate this case**.

Jackson v. United States

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1131
Opinion Date: April 20, 2020
Judge: Lavenski R. Smith
Areas of Law: Criminal Law

The Eighth Circuit affirmed the district court's denial of a 28 U.S.C. 2255 motion to vacate, set aside, or correct petitioner's sentence. The court held that the district court did not err in denying an evidentiary hearing as to petitioner's claim that counsel was constitutionally ineffective for failing to conduct adequate pretrial investigations. In this case, petitioner failed to identify any specific witnesses or evidence that counsel failed to uncover. Furthermore, petitioner failed to show that counsel's representation prejudiced his case. The court also held that the district court did not err in denying an evidentiary hearing as to petitioner's claim that his new counsel was ineffective for failing to subpoena witnesses, for convincing petitioner not to testify, for failing to object to or appeal the district court's answer to a jury question, and for failing to object to the district court's designation of petitioner as a career offender.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Bolman

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-2759
Opinion Date: April 21, 2020
Judge: Jane Louise Kelly
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's conviction for involuntary manslaughter after he struck and killed his nephew with his truck. The court held that the evidence was sufficient to support the conviction, because a reasonable jury could find defendant grossly negligent beyond a reasonable doubt. The court also held that the district court did not plainly err by failing to instruct the jury that actual knowledge is an essential element of the offense that is separate from gross negligence, because the instructions, viewed as a whole, accurately and adequately defined the essential elements of the offense.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Boyd

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-3528
Opinion Date: April 17, 2020
Judge: Kobes
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's sentence imposed after he pleaded guilty to being a felon in possession of a firearm. The court held that the facts underlying defendant's prior arrests were part of his history and characteristics under 18 U.S.C. 3553(a), and thus the district court could consider defendant's arrest records and the circumstances of those arrests. The court explained that the arrests were listed in the presentence report and gleaned from prior police reports. Furthermore, specific facts underlying the arrests may be considered for an upward departure and should be considered fair game for a variance where defendant did not object to them. The court also concluded that there is nothing here that suggested a corrected misstatement improperly influenced the district court's sentencing decision. Finally, the court held that the upward variance was not

unreasonable in consideration of defendant's previous assaults, coupled with the facts underlying his arrest in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Gonzalez-Esparsa

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1477
Opinion Date: April 22, 2020
Judge: Grasz
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's conviction for unlawful use of an identification document and misuse of a social security number. The court held that the evidence was sufficient to support defendant's convictions where a reasonable juror could conclude that defendant knew the permanent resident card bearing his name and photograph had been forged, counterfeited, falsely made, or unlawfully obtained when he used it to secure employment. Furthermore, a reasonable juror could conclude that defendant made the false representation regarding his purported social security number in order to deceive Midwest Concrete in order to obtain a job with the company.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Sanchez-Velasco

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-3568
Opinion Date: April 17, 2020
Judge: James B. Loken
Areas of Law: Criminal Law, Immigration Law

The Eighth Circuit affirmed the district court's denial of defendant's motion to suppress his responses to an ICE agent's two questions at the Treasurer's Office, because he was not in custody at the time of questioning. Although defendant was in custody at the ICE facility, the court held that an agent's questions were not custodial interrogation because the agent could not have known his questions were likely to elicit incriminating information regarding

the two criminal charges that were eventually brought against defendant. The court noted that the Attorney General's regulations carefully distinguish between the warrantless arrest of an alien for a criminal violation of the immigration laws, and what is called the "administrative arrest" of an alien who is reasonably believed to be illegally present in the United States. The court agreed with the district court that the agent's questioning was a request for routine information necessary for basic identification purposes that is not interrogation under Miranda, even if the information turns out to be incriminating.

Read Opinion Are you a lawyer? **Annotate this case**.

Anthony v. TRAX International Corp.

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-15662
Opinion Date: April 17, 2020
Judge: Kim McLane Wardlaw
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Ninth Circuit affirmed the district court's grant of summary judgment to TRAX in a disability discrimination action brought by plaintiff under Title I of the Americans with Disabilities Act (ADA). After TRAX terminated plaintiff from her position as a Technical Writer allegedly due to an inability or unwillingness to accommodate her disability, TRAX discovered during the course of litigation that plaintiff lacked the requisite bachelor's degree for her position. The panel held that, although McKennon v. Nashville Banner Publishing Co., 513 U.S. 352 (1995), held that after-acquired evidence cannot establish a superseding, non-discriminatory justification for an employer's challenged actions, after-acquired evidence remains available for other purposes, including to show that an individual is not qualified under the ADA. Because plaintiff did not satisfy one of the prerequisites for her position, she is not "otherwise qualified," and TRAX was not obligated to engage in the interactive process.

Read Opinion Are you a lawyer? **Annotate this case**.

City of Almaty v. Khrapunov

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-56451
Opinion Date: April 22, 2020
Judge: Marbley
Areas of Law: Criminal Law, International Law, White Collar Crime

The City of Almaty, in Kazakhstan, filed suit against defendant and his family under the Racketeer Influenced and Corrupt Organizations Act (RICO), alleging that they engaged in a scheme to defraud the city of millions of dollars. The City claimed that it was forced to spend money and resources in the United States to trace where its money was laundered. The district court dismissed the City's claim on the basis that it failed to state a domestic injury pursuant to the Supreme Court's recent decision in RJR Nabisco, Inc. v. European Community, 136 S. Ct. 2090 (2016). The Ninth Circuit held that the City failed to state any cognizable injury other than the foreign theft of its funds, and its voluntary expenditures were not proximately caused by defendants' acts of money laundering. In this case, the City's expenditure of funds to trace its allegedly stolen funds is a consequential damage of the initial theft suffered in Kazakhstan and is not causally connected to the predicate act of money laundering.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Baldon

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-10411
Opinion Date: April 21, 2020
Judge: Bennett
Areas of Law: Criminal Law

After defendant pleaded guilty to possession with intent to distribute a controlled substance, the district court sentenced him to 184 months in prison. The Ninth Circuit held that defendant's prior convictions for carjacking under section 215 of the California Penal Code are not categorical crimes of violence under USSG 4A1.1(e). Therefore, the district court incorrectly calculated defendant's criminal history by improperly including two points for his prior carjacking convictions. However, the panel held that the district court did not err in finding that defendant possessed a

firearm under USSG 2D1.1(b)(1). Accordingly, the panel affirmed in part, vacated in part, and remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Costanzo

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-10291
Opinion Date: April 17, 2020
Judge: Michael Daly Hawkins
Areas of Law: Criminal Law

The Ninth Circuit affirmed defendant's conviction of five counts of money laundering, holding that a reasonable trier of fact could have found beyond a reasonable doubt that the money laundering transactions, in which payment was made via bitcoin, affected interstate commerce in some way or to some degree. In this case, the transfer involved the use of an Internet or cellular network connected Personal Computer Device (PCD) to transfer bitcoin (together with the digital code necessary to unlock the bitcoin) to the digital wallet of another Internet or cellular network connected PCD.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Manzanares

Court: US Court of Appeals for the Tenth Circuit
Docket: 18-2010
Opinion Date: April 17, 2020
Judge: Mary Beck Briscoe
Areas of Law: Constitutional Law, Criminal Law

Defendant-Appellant Archie Manzanares appealed a district court's denial of his 28 U.S.C. 2255 motion challenging his sentence under the Armed Career Criminal Act (ACCA). Under the ACCA, an offense qualified as a violent felony by satisfying at least one of three definitions, which have come to be known as the Elements Clause, the Enumerated Clause, and the Residual Clause. Manzanares asserted that without the Residual Clause, his underlying New Mexico convictions (armed robbery, aggravated assault with a deadly weapon, and aggravated battery) no longer qualified

as violent felonies. The district court denied the motion, concluding that all three underlying convictions satisfied the Elements Clause. Manzanares appealed the classification of the armed robbery conviction as a violent felony to the Tenth Circuit, and sought to expand the certificate of appealability to allow him to appeal the decision regarding the aggravated assault with a deadly weapon and aggravated battery convictions. After review, the Tenth Circuit affirmed the district court's denial of Manzanares's 2255 motion, and denied his motion to expand the COA.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Delaney

Court: US Court of Appeals for the District of Columbia Circuit
Docket: 18-3093
Opinion Date: April 17, 2020
Judge: David S. Tatel
Areas of Law: Criminal Law

The DC Circuit vacated the district court's denial of defendant's motion to suppress evidence. The court held that officers violated the Fourth Amendment when they seized defendant because they lacked reasonable suspicion to justify the stop. In this case, a seizure occurred when the officers pulled into the parking lot, partially blocked defendant's vehicle, and activated their take-down light. The court held that any inference of suspicion that the officers drew from encountering defendant soon after hearing the nearby gunshots were undermined by the government's failure to identify specific and articulable facts supporting the officers' estimation of where the various shots came from. Accordingly, the court remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

Antenor v. Alaska, Department of Corrections

Court: Alaska Supreme Court
Docket: S-17005
Opinion Date: April 17, 2020
Judge: Carney

Areas of Law: Civil Procedure, Criminal Law, Government & Administrative Law

Several Alaska Department of Corrections inmates challenged the DOC's policy to charge for local telephone calls, arguing the rates they and call recipients had to pay for calls violated their constitutional right to rehabilitation, their statutory right to reasonable telephone access, and DOC's contractual obligations under a prior settlement and consent decree. In addition, one of the prisoners challenged DOC officers' decision to deny him access to a computer programming book he ordered from outside the prison. He contended that DOC placed a content-specific restriction on the educational materials and publications prisoners were allowed, violating the Alaska Constitution's free speech provisions as well as prisoners' right to reformation. Each of these challenges reached the Alaska Supreme Court after inmates exhausted the administrative process from prison. Inmates then appealed to the superior court, which denied relief. The Alaska Supreme Court determined the superior court record did not provide enough evidence for it to meaningfully determine the reasonableness of the rates charged inmates for local telephone calls; therefore the Court reversed denial of relief and remanded for further fact-finding by the trial court. The Court concluded that the facility's restrictions on programming-related books were rationally related to a legitimate interest, and because they did not infringe on the right to rehabilitation, it affirmed denial of a prisoner's motion to enforce his claimed right to a particular text about computer programming.

Read Opinion Are you a lawyer? **Annotate this case**.

Berger v. Bryant

Court: Arkansas Supreme Court
Citation: 2020 Ark. 357
Opinion Date: April 23, 2020
Judge: Rhonda K. Wood
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's petition to proceed in forma pauperis on a petition for writ of mandamus and a motion for declaratory judgment, holding that Appellant failed to state a colorable cause of action. In 1998, Appellant was convicted

of rape. In his petition for a writ of mandamus, Appellant asserted that he sought information pursuant to the Arkansas Freedom of Information Act regarding his rape conviction but received no response. The circuit court denied the petition. The Supreme Court affirmed, holding (1) even if Appellant had requested disclosable information, he would not be entitled to inspect it as an incarcerated person; and (2) Appellant did not demonstrate a legitimate claim given the facts presented and therefore failed to establish a colorable cause of action to support his request to proceed in forma pauperis.

Read Opinion Are you a lawyer? **Annotate this case**.

Carroll v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 360
Opinion Date: April 23, 2020
Judge: Wynne
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's motion for leave to file a petition for writ of error cram knobs, holding that the circuit court did not abuse its discretion in declining to issue the writ. Appellant pled guilty to rape and was sentenced as a habitual offender to 720 months' imprisonment. In his coram nobis petition, Appellant alleged several grounds for relief, including claims of actual innocence, an invalid arrest warrant, a coerced guilty plea, and prosecutorial misconduct. The circuit court denied the motion. The Supreme Court affirmed, holding that Appellant did not demonstrate that that the writ should issue and failed diligently to proceed on his claim for coram nobis relief.

Read Opinion Are you a lawyer? **Annotate this case**.

Cave v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 356
Opinion Date: April 23, 2020
Judge: Josephine L. Hart

Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's pro se petition for writ of habeas corpus, holding that the circuit court did not err in denying the petition. Appellant was found guilty of two counts of delivery of a controlled substance and one count of maintaining a drug premises. In his habeas petition, Appellant argued that he was actually innocent because his arrest and conviction was based on the false testimony of a witness who had a lengthy criminal history. Appellant further argued that the writ should issue because he was not afforded effective assistance of counsel. The circuit court denied the petition. The Supreme Court affirmed, holding (1) Appellant's claims regarding the witness's credibility do not constitute a valid assertion that he was being unlawfully detained; and (2) Appellant did not actually connect an allegation of ineffective assistance of counsel to his allegation that he was unlawfully detained.

Read Opinion Are you a lawyer? **Annotate this case**.

Chatmon v. Kelley

Court: Arkansas Supreme Court
Citation: 2020 Ark. 355
Opinion Date: April 23, 2020
Judge: Josephine L. Hart
Areas of Law: Criminal Law

The Supreme Court denied Appellant's appeal from the order of the circuit court denying his petition to proceed in forma pauperis on the grounds that Appellant failed to state a colorable cause of action in a petition for writ of habeas corpus, holding that the circuit court did not abuse its discretion by denying Appellant's in forma pauperis petition. In his habeas petition, Appellant alleged that the trial court lacked jurisdiction in his criminal case. Before this case was submitted to the Supreme Court, Appellant filed two motions, including a "Judicial Notice of a Void Judgment" and a "Notice to the Court." The Supreme Court denied the motions, holding that neither motion was cognizable under the Court's rules. The Court then affirmed the Supreme Court's denial of Appellant's in forma pauperis petition, holding that the circuit court correctly found that Appellant did not assert a colorable

cause of action.

Read Opinion Are you a lawyer? **Annotate this case**.

McClinton v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 353
Opinion Date: April 23, 2020
Judge: Karen R. Baker
Areas of Law: Criminal Law

The Supreme Court denied Petitioner's second petition requesting permission to proceed in the trial court with a petition for writ of error coram nobis, holding that Petitioner's proposed attack on the judgment had no merit. Petitioner was convicted of raping a mentally handicapped sixteen-year-old girl and was sentenced to life imprisonment. In his first petition for writ of error coram nobis Petitioner alleged a number of errors in the trial procedure. The first petition was denied. In his second coram nobis petition, Petitioner alleged violations of Brady v. Maryland, 373 U.S. 83 (1963). The Supreme Court denied the writ, holding that Petitioner failed to meet his burden of demonstrating a fundamental error of fact extrinsic to the record.

Read Opinion Are you a lawyer? **Annotate this case**.

Siegel v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 359
Opinion Date: April 23, 2020
Judge: Wynne
Areas of Law: Criminal Law

The Supreme Court dismissed Appellant's appeal from the circuit court's orders denying her motions to declare Ark. Code Ann. 5-62-106 (disposition of animal) and Ark. Code Ann. 5-62-111 (prevention of cruelty) unconstitutional and conditionally granting her motion for return of seized property, holding that there was no final, appealable order in this case. Appellant was convicted of thirty-one misdemeanor counts of cruelty to animals. The circuit court subsequently dismissed the charges on speedy-

trial grounds. The State appealed, and the Supreme Court dismissed the appeal on the grounds that it was not authorized. Appellant had filed motions seeking a declaration that sections 5-62-106 and -111 are unconstitutional and seeking the return of her seized property. The circuit court denied the constitutional claims and entered a conditional order granting Appellant's motion for return of seized property. Appellant appealed. The Supreme Court dismissed the appeal, holding that because the conditional order did not make specific findings as to the return of the property or as to damages and because it expressly left open the possibility of further proceedings, there was no final, appealable order in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

Thomas v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 354
Opinion Date: April 23, 2020
Judge: Josephine L. Hart
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Appellant's conviction of capital murder, holding that the evidence was sufficient to sustain the conviction and that the circuit court did not err in denying Appellant's motion to suppress tracking data generated by his cellphone. On appeal, Appellant argued that the trial court erred by denying his directed-verdict motion because the evidence supported the defense's theory of the case that he did not intend to shoot the victim. Further, Appellant argued that the court abused its discretion in denying his motion to suppress evidence obtained from the seizure of AT&T phone records. The Supreme Court disagreed, holding (1) the evidence was sufficient to support the capital murder conviction; and (2) the circuit court correctly denied the motion to suppress.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. Landowski

Court: California Courts of Appeal
Docket: C080210(Third Appellate District)

Opinion Date: April 23, 2020
Judge: Andrea Lynn Hoch
Areas of Law: Constitutional Law, Criminal Law

Defendant Michael Reyes, Jr., an active Norteno gang member (from the Broderick Boys subset), confronted a former Norteno gang member (from the Franklin Boys subset), "S.," about a physical altercation that occurred between S. and Reyes's stepfather over a debt. That earlier altercation had taken place in front of Reyes's autistic younger brother. Reyes pulled out a handgun and asked S. if he had a problem. S., who was riding his bicycle with his wife, "R.," when Reyes confronted him with the gun, stopped briefly, told Reyes to put the gun down if he wanted to fight, and then started to ride away. This angered Reyes, prompting him to fire six rounds at S. from behind. S. Was hit but survived. R. Was a short distance in front of S., but was not hit. Defendants Liberty Landowski and Lisa Humble were with Reyes at the time of the shooting and aided in his efforts to avoid being apprehended by law enforcement authorities. Reyes, Landowski, and Humble were tried together before the same jury. Reyes was convicted of one count of attempted murder (Count 1), two counts of assault with a semiautomatic firearm (Counts 2 and 4), one count of possession of a firearm by a convicted felon (Count 5), and one count of possession of ammunition by a convicted felon (Count 6). In addition to various firearm and other enhancements, the jury found Reyes committed the crimes for the benefit of, at the direction of, or in association with a criminal street gang with the specific intent to promote, further, or assist in criminal conduct by gang members. The jury convicted Landowski and Humble of being accessories to Reyes's criminal conduct (Count 9) and also found true gang enhancement allegations attached to that crime. Reyes challenged the sufficiency of the firearm evidence presented to support his conviction, and all defendants challenged the sufficiency of the evidence supporting their gang enhancements. The Court of Appeal determined Senate Bill 620 (2017-2018 Reg. Sess.) gave the trial court discretion to strike firearm enhancements in the interest of justice and applied retroactively; and Senate Bill 136 (2019-2020 Reg. Sess.) eliminated such enhancements, and also applied retroactively. To these issues, the Court remanded for the trial court's consideration. The Court affirmed the trial court in all other respects.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. May

Court: California Courts of Appeal
Docket: C084302(Third Appellate District)
Opinion Date: April 20, 2020
Judge: Ronald B. Robie
Areas of Law: Constitutional Law, Criminal Law

Defendant Raymond May was found guilty by jury of possessing an assault weapon and a machine gun based on his possession of a single AK-47 assault rifle while guarding a marijuana plantation. He was sentenced to probation, which included an electronic search condition. On appeal, defendant argued there was a lack of sufficient evidence corroborating his accomplice's testimony and demonstrating he knew of the firearm's illegal character. He further alleged the trial court erred in instructing the jury: that the accomplice instruction should have included language specifying that the accomplice testimony needed to prove more than defendant's mere presence or access to the firearm. Furthermore, defendant argued the electronic search condition imposed as part of his probation failed under the standards announced in California v. Lent, 15 Cal.3d 481 (1975). The Court of Appeal agreed defendant's electronic search condition should have been stricken, but otherwise affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. Perez

Court: California Courts of Appeal
Docket: E072260(Fourth Appellate District)
Opinion Date: April 20, 2020
Judge: Miller
Areas of Law: Constitutional Law, Criminal Law

In 2009, defendant-appellant Rudy Perez pled guilty to active gang participation under Penal Code section 186.22(a), and unlawful possession of a firearm under section 12025(b)(6). In 2010, defendant pled guilty to residential burglary under section 459, and active gang participation under section 186.22(a). In August of 2018, the State filed a new felony complaint, alleging one of the prior gang participation convictions as a strike prior. In

2018, defendant moved to vacate the two prior gang participation convictions based upon changes in the law that rendered them invalid. The trial court denied defendant's motion. In 2019, defendant asked for reconsideration, which was again denied. Thereafter, defendant filed a timely notice of appeal from the denial of his motion to vacate the convictions. The Court of Appeal found that defendant pled guilty to street terrorism under Penal Code section 186.22(a) in 2009 and 2010, and it was undisputed that while committing these offenses, defendant acted alone. However, subsequent to defendant's guilty pleas, in 2012, the California Supreme Court held that a defendant had to act in concert with a fellow gang member in order to be guilty of street terrorism. At that time, defendant could have filed a state habeas petition requesting relief, but failed to do so. "Defendants can lose remedies that are established by law when they fail to invoke such remedies in time." Section 1473.7 became effective in 2017. In defendant's motion filed in the trial court, defendant failed to state what new evidence was discovered, instead arguing that the trial court was allowed "to vacate a conviction where the defendant is innocent as a matter of law or where vacating the conviction is in the interest of justice, even though the defendant is no longer in custody or otherwise restrained by the conviction." The Court of Appeal concurred with the trial court's reason to deny relief, determining that "while the outcome in this case may be unfortunate for defendant, we are not here to rewrite legislation. The Legislature could amend section 1473.7 to address issues raised in this case. However, under the laws, as written, we must uphold the trial court's order."

Read Opinion Are you a lawyer? **Annotate this case**.

In re S.R.

Court: California Courts of Appeal
Docket: B300214(Second Appellate District)
Opinion Date: April 23, 2020
Judge: Bendix
Areas of Law: Criminal Law

Father appealed the juvenile court's dispositional ruling removing daughter from his custody, arguing that his mere possession of child pornography does not demonstrate that he poses a substantial risk of harm to his daughter. The Court of Appeal affirmed the order and held that there is

substantial evidence of risk of great harm to daughter—no matter how low the probability— that father will sexually abuse his daughter if he is provided unfettered access to her.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Bell

Court: California Courts of Appeal
Docket: B288528(Second Appellate District)
Opinion Date: April 23, 2020
Judge: Stratton
Areas of Law: Criminal Law

Defendant was convicted of one count of attempted robbery, one count of second degree murder, and one count of hit and run driving. The jury found not true the allegation that a principal was armed in the commission of the attempted robbery. The trial court found true the allegations that defendant had served four prior prison terms within the meaning of Penal Code section 667.5, subdivision (b). Defendant raised 13 claims of error on appeal. The Court of Appeal held that the section 667.5, subdivision (b) enhancement terms must be stricken and the matter remanded to the trial court for resentencing. The court also held that defendant forfeited some of his substantive claims and other lack merit. Finally, the court held that, if there is instructional error, the errors are harmless under any standard of review. Accordingly, the court affirmed the judgment of conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Drayton

Court: California Courts of Appeal
Docket: H046928(Sixth Appellate District)
Opinion Date: April 17, 2020
Judge: Danner
Areas of Law: Criminal Law

In 1991, the Wards and their teenage daughter awoke and discovered four men, including Drayton, inside their house. Two were armed. One told the daughter he was going to rape her and placed a firearm inside her vagina.

Drayton told the man not to do it. Drayton had a gun and held Mrs. Ward down during the robbery. Two others shot and killed Mr. Ward. Drayton and the others left without seeking help for the Wards. Drayton did not shoot Mr. Ward or threaten to rape the daughter. Drayton surrendered the next day. Drayton's sole prior conviction was a misdemeanor; he had no reported history of violence. Drayton was sentenced to 29 years to life imprisonment. In 2019, Drayton sought resentencing under Penal Code 1170.95, declaring that he "was not a major participant ... or did not act with reckless indifference to human life." Senate Bill 1437, effective January 1, 2019, restricted the circumstances under which a person can be liable for felony murder and enacted Penal Code 1170.95, which allows an individual, previously convicted of felony murder, to petition to have his murder conviction vacated and to be resentenced. The court of appeal directed the trial court to hold a hearing under section 1170.95(d) and to accept the assertions in the petition as true unless facts in the record conclusively refute them as a matter of law. If, accepting the petitioner's assertions as true, he meets section 1170.95(a)'s requirements for relief, the court must issue an order to show cause. In assessing the prima facie showing, the trial court should not weigh evidence or make credibility determinations.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Robinson

Court: California Courts of Appeal
Docket: B293746(Second Appellate District)
Opinion Date: April 20, 2020
Judge: Wiley
Areas of Law: Criminal Law

After defendant penetrated an unconscious woman with his fingers, he challenged evidentiary rulings and requests a presentence conduct credit. The Court of Appeal held that the trial court properly excluded cumulative evidence about past times the woman was intoxicated at the relevant bar, and any error in allowing a drug recognition expert to testify about whether the woman was incapacitated was harmless. However, the court held that the trial court undercalculated defendant's presentence custody credit because he was not convicted of a violent felony under Penal Code section 2933.1, which would otherwise limit those credits. Accordingly, the court

directed the trial court to award defendant 104 days of presentence custody credit and to amend the abstract of judgment, affirming in all other respects.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Torres

Court: California Courts of Appeal
Docket: B292551(Second Appellate District)
Opinion Date: April 20, 2020
Judge: Kenneth R. Yegan
Areas of Law: Criminal Law

Where, as here, the trial court factually finds that a self-represented defendant has engaged in an attempt to intimidate a witness, the constitutional right of self-representation can, in the exercise of the trial court's sound discretion, be revoked. The Court of Appeal affirmed defendant's conviction and sentence for two counts of battery on an ex-girlfriend. In this case, the trial court did not abuse its discretion in revoking defendant's pro se status after he asked his sister to contact the victim and have her say that she was coerced by the police detective to "press charges."

Read Opinion Are you a lawyer? **Annotate this case**.

Colorado v. Lujan

Court: Colorado Supreme Court
Citation: 2020 CO 26
Opinion Date: April 20, 2020
Judge: Brian D. Boatright
Areas of Law: Constitutional Law, Criminal Law

Abel Lujan was charged with first-degree murder for the death of his girlfriend after she was found beaten and strangled behind a friend’s house. At trial, two women testified for the State about Lujan’s prior violent behavior towards them. Prior to admitting this evidence, the trial court read a limiting instruction, telling the jury that it could only consider the evidence for the purposes of establishing Lujan’s motive, intent, or common plan. A copy of

this instruction was not given to the jury for deliberations; however, the jury did receive an instruction at the close of the evidence explaining that certain evidence could only be considered for the limited purposes for which it was admitted. While deliberating, the jury submitted a question seeking clarification about the limiting instruction. Over defense counsel's objection, the trial court cleared the courtroom of the public and parties, leaving only the judge, bailiff, and court reporter; the judge then brought in the jury and reread the limiting instruction that it had previously read twice in open court. The jury ultimately found Lujan guilty of second-degree murder. Lujan appealed, arguing that the court's actions when rereading the jury instruction constituted a courtroom closure that violated his Sixth Amendment right to a public trial. A division of the court of appeals agreed and reversed Lujan's conviction. The State argued on certiorari review that the Colorado Supreme Court adopt a triviality standard, under which a defendant's constitutional right to a public trial was not violated when the closure at issue was trivial. In so doing, the State argued that the brief courtroom closure here was trivial and therefore did not violate Lujan's public trial right. The Court concurred with the State, adopted the standard and reversed the appellate court's decision.

Read Opinion Are you a lawyer? **Annotate this case**.

Archer v. State

Court: Florida Supreme Court
Docket: SC19-841
Opinion Date: April 23, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the order of the circuit court denying Appellant's successive motion to vacate his sentence of death under Fla. R. Crim. P. 3.851, holding that the circuit court did not err in denying the Rule 3.851 motion. Appellant was convicted of first-degree murder, armed robbery, and grand theft. Appellant was sentenced to death for the murder. The Supreme Court affirmed the convictions but reversed Appellant's death sentence and remanded the case for a new penalty phase. After a new penalty phase, Appellant was again sentenced to death. In his successive Rule 3.851 motion, Appellant raised three claims. The circuit court denied

relief. The Supreme Court affirmed, holding that the circuit court (1) properly denied Appellant's claim that his death sentence violated the Sixth and Eighth Amendments in light of Hurst v. Florida, 136 S. Ct. 616 (2016), and Hurst v. State, 202 So. 3d 40 (Fla. 2016); (2) correctly denied Appellant's claim that his sentence violated the Eighth Amendment; and (3) did not err in denying Appellant's claim of newly discovered evidence.

Read Opinion Are you a lawyer? **Annotate this case**.

Collins v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0158
Opinion Date: April 20, 2020
Judge: David E. Nahmias
Areas of Law: Constitutional Law, Criminal Law

Appellant Tommy Collins was convicted of felony murder in connection with the stabbing death of 14-year-old Rueben Hand. Friends gathered to watch the Peach Drop on New Year's Eve 2010; a disagreement ensued and Hand was stabbed near the Five Points MARTS station shortly after midnight. Appellant's only argument on appeal was that the trial court plainly erred when it gave the jury the State's requested instruction on "revenge for a prior wrong." Seeing no error, "much less plain error," the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Heyward v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0399
Opinion Date: April 20, 2020
Judge: Peterson
Areas of Law: Constitutional Law, Criminal Law

Larmell Heyward was convicted by jury of malice murder and possession of a firearm during the commission of a felony in connection with the 2007 shooting death of Ramon Rogers. Heyward argued on appeal of those convictions that the trial court erred in denying his request to charge the jury

on voluntary manslaughter. After review, the Georgia Supreme Court determined the trial court's refusal to give the charge was harmless, since, in the Court's estimation, there was no realistic probability that the jury would have accepted the "slight" evidence of voluntary manslaughter in the light of the strong evidence of malice murder.

Read Opinion Are you a lawyer? **Annotate this case**.

Howard v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0819
Opinion Date: April 20, 2020
Judge: Keith R. Blackwell
Areas of Law: Constitutional Law, Criminal Law

Kenneth Howard was tried by jury and convicted of the murder of Emily Ann Smith Newbegin. Howard appealed, contending that the evidence was legally insufficient to sustain his conviction. Upon its review of the record and briefs, the Georgia Supreme Court found no merit in Howard's claim of error, and affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Keller v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0006
Opinion Date: April 20, 2020
Judge: Boggs
Areas of Law: Constitutional Law, Criminal Law

Randall Keller was convicted of felony murder and related crimes arising out of the beating death of his ex-wife's two-year-old son, William Powell. On appeal, Keller raised numerous claims of error, including ineffective assistance of counsel, the trial court's rulings on motions before and during trial, several evidentiary rulings, and alleged bias on the part of the trial judge. However, finding no reversible error, the Georgia Supreme Court affirmed Keller's convictions.

Read Opinion Are you a lawyer? **Annotate this case**.

Mills v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0364
Opinion Date: April 20, 2020
Judge: Ellington
Areas of Law: Constitutional Law, Criminal Law

Roger Mills was found guilty by jury of malice murder and aggravated assault in connection with the death of Masuto Garrett. Mills contended that the trial court erred when, during jury deliberations, it excused a holdout juror without sufficient inquiry or good cause. After review, the Georgia Supreme Court concurred with that contention, and reversed Mills's convictions. The Court also concluded the evidence presented at trial was legally sufficient to support the convictions, so the State could retry Mills if it chose.

Read Opinion Are you a lawyer? **Annotate this case**.

Moore v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0344
Opinion Date: April 20, 2020
Judge: David E. Nahmias
Areas of Law: Constitutional Law, Criminal Law

Appellant Carzell Moore, proceeding pro se, appealed a trial court's denial of his motion to set aside a September 2017 order denying his motion for an out-of-time appeal of his 2002 resentencing on his 1977 convictions for murder and rape. Moore contended the trial court abused its discretion by denying his motion to set aside because he was not given proper notice of the September 2017 order. Finding that the record supported the trial court's ruling, the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Morris v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0176
Opinion Date: April 20, 2020
Judge: Bethel
Areas of Law: Constitutional Law, Criminal Law

Darius Morris was found guilty by jury of malice murder and other offenses in connection with the shooting death of Jameson Bush. Morris appealed, arguing he was denied the right to a timely appeal, that the trial court erred in restricting voir dire as to the religious beliefs and connections of potential jurors, that the trial court erred by giving a confusing jury charge regarding statements of co-conspirators, that the trial court erred by violating his right to a public trial by ordering that the courtroom doors be closed and locked during the court's charge to the jury, and that his trial counsel provided ineffective assistance by not objecting to the closure of the courtroom. Finding no error, the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Rickman v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0127
Opinion Date: April 20, 2020
Judge: Harold D. Melton
Areas of Law: Constitutional Law, Criminal Law

Victoria Rickman was convicted by jury of malice murder and a related firearm offense in connection with the shooting death of William Carter, Jr. Rickman and Carter had a tumultuous on-again, off-again relationship with a history of verbal and physical abuse, false accusations of sexual assault, empty threats to obtain temporary protective orders, and numerous calls to 911. In the days leading up to Carter's death, the pair was talking and meeting again despite a recent break-up. On one such 911 call, officers went to Rickman's residence responding to claims shots were fired. Rickman responded holding her small dog, hair wet, and in pajamas. She did not appear to be injured, and nothing in the home looked disturbed or out of place. Rickman told the officers, "he raped me again and I shot him."

Officers found Carter laying face up on the bed naked with multiple gunshot wounds to his body. An autopsy revealed that Carter was shot ten times – four times in the chest, three times in the back, once on the arm, and twice in the head. Rickman's examining physician testified that he found no injuries on Rickman consistent with her description of events, and no signs of trauma to her vaginal cavity. Rickman appealed her convictions, arguing she was denied effective assistance of counsel and that the trial court erred in admitting improper character evidence. Finding no reversible error, the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Robinson v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0265
Opinion Date: April 20, 2020
Judge: Peterson
Areas of Law: Constitutional Law, Criminal Law

Herbert Robinson appealed his convictions for malice murder, armed robbery, and possession of a firearm during the commission of a felony in connection with the death of Michael Moore. On appeal, he argued the trial court erred by allowing the State to use two firearms for demonstrative purposes during trial, and by allowing body-camera footage to be shown at trial. He also argued his trial counsel was ineffective for failing to object to a letter written by Robinson's cellmate being available to the jury for review during deliberations, and for failing to object to a visual aid used by the State during closing arguments. Because Robinson failed to show ineffective assistance of counsel or reversible error by the trial court, the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Santana v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0563
Opinion Date: April 20, 2020

Judge: Warren
Areas of Law: Constitutional Law, Criminal Law

Cuevas Carlos Santana was convicted by jury of malice murder and other crimes in connection with the 2010 shooting deaths of Israel Espinoza Mendoza, Vincente Soto Chavez, and Renato Soto Valencia. On appeal, Santana argues that the evidence was insufficient to support his convictions, that the trial court erred by declining to grant Santana a new trial on the general grounds, and that trial counsel provided ineffective assistance. Finding no reversible error, the Georgia Supreme Court affirmed Santana's convictions.

Read Opinion Are you a lawyer? **Annotate this case**.

Sullivan v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0056
Opinion Date: April 20, 2020
Judge: Warren
Areas of Law: Constitutional Law, Criminal Law

A jury convicted Antonio Sullivan of malice murder and other crimes in connection with the shooting death of Wava Benton. On appeal, Sullivan contended his trial counsel was constitutionally ineffective by failing to present evidence at trial to corroborate Sullivan's testimony about prior difficulties between Sullivan and Benton, and by failing to procure expert testimony about Sullivan's mental health—specifically about post-traumatic stress disorder— to be presented to the jury. The Georgia Supreme Court determined Sullivan failed to establish that his trial counsel was deficient in either respect, and therefore affirmed his convictions.

Read Opinion Are you a lawyer? **Annotate this case**.

Turner v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0247
Opinion Date: April 20, 2020
Judge: Warren

Areas of Law: Constitutional Law, Criminal Law

Appellant Ronald Turner appeals from his conviction for malice murder stemming from the stabbing death of William King. The stabbing took place outside an apartment at which Turner had driven in order to trade food for drugs. Turner testified in his own defense at trial and claimed that King hit him in the head with a beer bottle because Turner owed money to King from a prior drug transaction. Turner testified that he tried to get away from King, but that King chased him down and grabbed his jacket. According to Turner, King was getting ready to hit him again when Turner stabbed King in self-defense. Appealing his ultimate conviction, Turner contended he was denied the effective assistance of counsel in three respects. Seeing no reversible error after a review of the trial court record, the Georgia Supreme Court affirmed Turner's conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Valrie v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0380
Opinion Date: April 20, 2020
Judge: Keith R. Blackwell
Areas of Law: Constitutional Law, Criminal Law

Reuben Valrie was tried by jury and convicted of murder and other crimes in connection with the death of his infant daughter Aliyana. Valrie appealed, claiming that he was denied the effective assistance of counsel. Aliyana died as a result of closed head trauma, with a blunt-force abdominal injury as a secondary cause of death, which investigators determined was consistent with being shaken or dropped. At trial, Valrie presented the testimony of four expert witnesses who testified that Aliyana died of natural causes and that the injuries to her brain and abdomen were caused by events such as post-mortem CPR and the “rough” handling of her body by first responders. The jury rejected this defense and found Valrie guilty of murder and the other charges. Valrie contended that his trial lawyer should have raised a hearsay objection to the admission of recorded statements that his girlfriend (and Aliyana's mother) made to police investigators (as well as the testimony of one of those investigators about some of those

statements). Alternatively, Valrie argued that his lawyer should have sought the redaction of certain portions of the recorded statements that impugned his character. The Georgia Supreme Court concluded Valrie failed to present evidence that his trial counsel was deficient, or that he was prejudiced by any alleged failures. According, the Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Williams v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0241
Opinion Date: April 20, 2020
Judge: Keith R. Blackwell
Areas of Law: Constitutional Law, Criminal Law

Richard Williams, II, was tried by jury and convicted of murder in connection with the strangulation death of Cory Robinson. Williams and Robinson were involved in a sexual relationship and had been living together at an extended-stay hotel. Kelvin Spencer was a close friend of both Williams and Robinson. When Spencer met Williams at the hotel room, Williams looked angry and had scratches on his neck. Spencer saw Robinson lying on the floor in a “praying position.” Spencer did not believe Robinson was dead, and he helped Williams move clothes and other things to a U-Haul truck parked outside, in preparation for a move. Williams did not testify or present any evidence. Based on his lawyer’s opening and closing arguments, the defense theory was that Spencer killed Robinson because he was jealous of Williams’s relationship with Robinson. Williams’s sole claim on appeal was that he was denied the effective assistance of counsel when his trial lawyer failed to present as a defense that Williams accidentally killed Robinson during consensual erotic asphyxiation. He argued that his lawyer's discomfort with the topic of homosexual BDSM activity, and his own problems with the Georgia State Bar, precluded presentation of the "true" version of events, and that Williams acceded to the lawyer's defense strategy only "through ignorance and that he did not know that a defense based on consensual erotic asphyxiation was available." Finding no reversible error, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Malave

Court: Supreme Court of Hawaii
Docket: SCWC-18-0000332
Opinion Date: April 20, 2020
Judge: Mark E. Recktenwald
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the intermediate court of appeals (ICA) affirming Defendant's conviction of sexual assault in the first degree on the complaining witness pursuant to Haw. Rev. Stat. 707-730(1)(b), holding that the ICA did not err in affirming the family court. Specifically, the Supreme Court held (1) the jury should have been instructed to determine jurisdictional facts, but the error was harmless beyond a reasonable doubt; and (2) the ICA did not err in finding that there was no rational basis in the record to support providing the jury instruction of the lesser included offense of sexual assault in the third degree.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Malave

Court: Supreme Court of Hawaii
Docket: SCWC-18-0000332
Opinion Date: April 22, 2020
Judge: Mark E. Recktenwald
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the intermediate court of appeals (ICA) affirming the judgment of the family court convicting Defendant on two counts of sexual assault in the first degree, holding that the ICA did not err in affirming the family court. At issue on appeal was the jurisdiction of the family court to try Defendant and the propriety of instructing the jury on a lesser included offense. The ICA affirmed, concluding that the family court had subject matter jurisdiction pursuant to Haw. Rev. Stat. 571-14(a)(1) and that there was no rational basis to support an instruction of the lesser included offense of sexual assault in the third degree. The Supreme Court affirmed, holding (1) although the jury should have been instructed to determine jurisdictional facts, the error was

harmless; and (2) the family court was not obligated to instruct the jury on the lesser included offense of sexual assault in the third degree.

Read Opinion Are you a lawyer? **Annotate this case**.

Idaho v. Burke

Court: Idaho Supreme Court - Criminal
Docket: 46841
Opinion Date: April 22, 2020
Judge: Moeller
Areas of Law: Constitutional Law, Criminal Law

Prior to sentencing, defendant James Burke was committed to the state mental hospital for 56 days to restore him to competency. After being evaluated and deemed competent to proceed to trial, Burke was returned to the county jail and later pleaded guilty pursuant to a plea agreement. At the conclusion of his sentencing hearing, Burke sought credit for the 56 days of time spent in court-ordered commitment. The district court denied the motion, concluding that commitment to a state mental hospital did not fall under the definition of 'incarceration' in Idaho Code section 18-309. After reviewing this issue carefully, the Idaho Supreme Court disagreed with the district court's "thorough and thoughtful analysis," holding that court-ordered commitment to state custody pursuant to Idaho Code sections 18-210 and 18-211 met the functional and legal definition of "incarceration" under Idaho Code section 18-309. "The extent of the liberty interests restricted by Burke's court-ordered commitment to State Hospital North are just too similar to imprisonment to conclude otherwise." Accordingly, the Court reversed the district court's order denying Burke's request for credit for time served and remanded the case for the district court to enter an order crediting him with the fifty-six days he spent committed to State Hospital North while the State restored his competency to face criminal charges.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Gibbs

Court: Iowa Supreme Court
Docket: 18-1298

Opinion Date: April 17, 2020
Judge: Edward M. Mansfield
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction of murder in the second degree, holding that Defendant's Fifth Amendment rights were invaded when the trial judge instructed the jury that Defendant was required to notify law enforcement of his use of deadly force, but the error was harmless. During trial, Defendant asserted the defense of justification in his shooting of the victim. At issue on appeal was whether the district court abused its discretion by giving a jury instruction incorporating the terms of Iowa Code 704.2B. The instruction included a statement that a person using deadly force is required to notify law enforcement about his use of deadly force. Defendant argued before the Supreme Court that both section 704.2B and the jury instruction incorporating that section violated his Fifth Amendment rights. The Supreme Court affirmed, holding (1) instructing the jury that a homicide defendant is required to notify a law enforcement agency of his use of deadly force violates the defendant's Fifth Amendment rights; but (2) any error in this case was harmless beyond a reasonable doubt.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Broxton

Court: Kansas Supreme Court
Docket: 114675
Opinion Date: April 17, 2020
Judge: Stegall
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's convictions for second-degree murder, burglary, and theft but reversed Defendant's sentences, holding that any error during the guilt phase was harmless but that the district court erred by scoring Defendant's prior Florida burglary conviction as a person felony instead of a nonperson felony. On appeal, the court of appeals concluded that a trial court may instruct the jury on felony murder even though the State only charged the defendant with premeditated first degree murder. The Supreme Court disagreed, holding (1) the court of appeals erred in concluding that a district court may elect to provide a felony-murder

instruction when that crime was not charged, and the district court properly found that the felony-murder instruction was not legally appropriate in this case; (2) the district court erred by excluding from evidence an exculpatory document from a Florida homicide investigation on the ground it was not relevant, but the error was harmless; and (3) the district court improperly scored Defendant's prior Florida burglary conviction as a person felony.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Corbin

Court: Kansas Supreme Court
Docket: 119665
Opinion Date: April 17, 2020
Judge: Dan Biles
Areas of Law: Criminal Law

The Supreme Court affirmed the ruling of the district court on remand resentencing Defendant to his original mandatory term of imprisonment after once again finding he was not a person with intellectual disability, holding that the district court did not abuse its discretion when it rejected Defendant's intellectual disability motion and imposed a mandatory term of imprisonment. Defendant pled no contest to first-degree premeditated murder. Before sentencing, Defendant filed a motion pursuant to Kan. Stat. Ann. 21-6622(b) asserting that he was a person with intellectual disability and was thus not subject to a mandatory minimum prison term. The district court denied the motion and sentenced Defendant to a hard twenty-five life sentence. While Defendant's appeal was pending, the Legislature amended Kan. Stat. Ann. 76-12b01(i), which provides new standards for deciding intellectual disability. The Supreme Court reversed and remanded for reconsideration of Defendant's motion using the new criteria. On remand, the district court reaffirmed its earlier ruling and again sentenced Defendant to a hard twenty-five life sentence. The Supreme Court affirmed, holding that the district court's ruling was reasonably based on the law and was supported by substantial competent evidence.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Frazier

Court: Kansas Supreme Court
Docket: 117456
Opinion Date: April 17, 2020
Judge: Wilson
Areas of Law: Criminal Law

The Supreme Court reversed the decision of the district court affirming the judgment of the district court denying Defendant's motion to withdraw plea of no contest to one count of possession of heroin with intent to distribute, holding that the district court's decision in finding no good cause for Defendant to withdraw his plea was based on errors of fact and law, which were grounds for finding abuse of discretion. On appeal, Defendant argued that the district court abused its discretion in denying his motion to withdraw his plea of no contest based on misleading or false statements contained in the plea agreement. The court of appeals affirmed the district court. The Supreme Court reversed, holding (1) there was enough uncertainty in this case to indicate that Defendant's plea agreement was not understandingly made; and (2) therefore, Defendant must be allowed to withdraw his plea.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Harris

Court: Kansas Supreme Court
Docket: 117362
Opinion Date: April 17, 2020
Judge: Wilson
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court reversed the judgment of the court of appeals affirming Defendant's conviction of possession fo marijuana, holding that Defendant's waiver of jury trial was legally insufficient. On appeal, Defendant argued that he did not properly waive his right to a jury and asserted three other issues. The Supreme Court reversed the judgment of the court of appeals affirming Defendant's convictions without addressing the three remaining issues, holding that because the district court failed properly to apprise Defendant of his right to a jury trial and failed to ensure that Defendant understood the nature of the right he was giving up, Defendant's constitutional right to a jury trial was violated in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Uk

Court: Kansas Supreme Court
Docket: 119712
Opinion Date: April 17, 2020
Judge: Wilson
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's conviction for first-degree premeditated murder, holding that the district court did not err in its challenged instructions to the jury. Specifically, the Supreme Court held (1) the district court did not err in refusing to give the jury Defendant's requested instruction on voluntary manslaughter as a lesser included offense of first-degree murder because the instruction was not factually appropriate; and (2) the district court did not commit clear error in issuing an unmodified version of Instruction No. 11, which contained the definition of "premeditation" and mirrored PIK Crim. 4th 54.150(d) because the instruction was legally appropriate.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Catruch

Court: Maine Supreme Judicial Court
Citation: 2020 ME 52
Opinion Date: April 23, 2020
Judge: Andrew M. Mead
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed the judgments of the trial court terminating Appellant's participation in the Co-Occurring Disorders and Veterans Court (Veterans Court), holding that the court did not err or abuse its discretion in terminating Appellant's participation in the Veterans Court. The Veterans Court is a criminal docket that provides judicial monitoring, specialized treatment, and other services for military veterans who have disorders often attributable to their military service. Appellant was charged

with leaving the scene of an accident and three other offenses. Appellant was admitted to the Veterans Court. Agreeing to sentencing outcomes in a plea agreement and entering into a bail contract, Appellant pleaded guilty to all charges against him. The court later terminated Appellant's participation in the Veterans Court, finding that Appellant had violated the conditions of his bail contract. The Supreme Judicial Court affirmed, holding (1) this matter was properly before the Court; and (2) given Appellant's failure to comply with the requirements for participation in the treatment court and his violations of the agreements, his termination from the Veterans Court was warranted.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Paquin

Court: Maine Supreme Judicial Court
Citation: 2020 ME 53
Opinion Date: April 23, 2020
Judge: Andrew M. Mead
Areas of Law: Constitutional Law, Criminal Law

In this appeal from Defendant's conviction for eleven counts of gross sexual misconduct, the Supreme Judicial Court vacated the judgment of conviction on one count, vacated the dismissal of other counts and remanded for entry of a judgment of acquittal on those counts, and affirmed in all other respects, holding that Defendant's convictions on both Counts 5 and 30 violated his double jeopardy protections and that the court erred in allowing the State to dismiss Counts 27, 28, and 29 during trial without Defendant's consent. The indictment charged Defendant with fifteen counts (Counts 1-13, 30-31) of gross sexual misconduct against the victim and sixteen counts (Counts 14-29) of gross sexual misconduct against a second alleged victim. During trial, the court granted Defendant's motion for a judgment of acquittal on Counts 10-13, and the State dismissed Counts 27-29. Defendant was found guilty of Counts 1-9 and 30-31 and not guilty on the remaining counts. The court entered judgment in accordance with the verdict. The Supreme Judicial Court held that the trial court erred in failing to rule that the Double Jeopardy Clause barred convictions on both Counts 5 and 30 and allowing the State to dismiss Counts 27, 28, and 29 rather than entering a judgment of acquittal on those counts.

Read Opinion Are you a lawyer? **Annotate this case**.

Watson v. State

Court: Maine Supreme Judicial Court
Citation: 2020 ME 51
Opinion Date: April 21, 2020
Judge: Joseph Jabar
Areas of Law: Criminal Law

The Supreme Judicial Court vacated the judgment of the unified criminal docket denying Appellant's petition for post-conviction review, holding that Appellant was deprived of the effective assistance of counsel when his trial attorney played a video of the ten-year-old victim's interview with police and that Appellant was adversely affected. Appellant was convicted of two counts of gross sexual assault, one count of unlawful sexual contact, and one count of visual sexual aggression against a child. The Supreme Court affirmed. Appellant later filed a petition for post-conviction review claiming that his trial attorney's representation was deficient because introducing the videotaped recording of the victim's entire interview with law enforcement was unnecessary to provide evidence supporting the victim's potential motive to fabricate the allegations. The post-conviction court denied denied the petition. The Supreme Court vacated the judgment below, holding that trial counsel's conduct was deficient and that counsel's actions rose to the level of comprising the reliability of Appellant's conviction and undermining confidence in it.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. Mazza

Court: Massachusetts Supreme Judicial Court
Docket: SJC-11363
Opinion Date: April 21, 2020
Judge: Budd
Areas of Law: Criminal Law

The Supreme Judicial Court reversed the order of the superior court denying Defendant's motion for a new trial and set aside the jury's verdicts

of first degree murder and robbery, holding that a recently discovered witness statement made to the police ago constituted newly discovered evidence that "would probably have been a real factor in the jury's deliberations." At issue was Defendant's sixth motion for a new trial, which was predicated on newly discovered evidence consisting of, among other things, a recently discovered statement made to the police in 1972. The superior court denied the motion. As to the police statement, the judge found that it did not constitute newly discovered evidence because Defendant failed to establish that defense counsel did not have possession of it at the time of trial. The Supreme Judicial Court reversed and remanded the case for a new trial, holding (1) Defendant sustained his burden of establishing that defense counsel did not have the 1972 police statement prior to or at trial, and therefore, the statement constituted newly discovered evidence; and (2) there was a substantial risk that the jury would have reached a different conclusion had the evidence been admitted at trial.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. McCarthy

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12750
Opinion Date: April 16, 2020
Judge: Gaziano
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Judicial Court affirmed the judgment of the district court denying Defendant's motions to suppress, holding that the limited use of automatic license plate readers (ALPRs) in this case did not implicate constitutional protections against unreasonable searches. While police were investigating Defendant on suspicion of drug distribution they used ALPRs on two bridges to track Defendant's movements. The police accessed historical data via ALPR technology and received real-time alerts, the last of which led to Defendant's arrest. Defendant filed motions to suppress the ALPR data and the fruits of the arrest. The superior court denied the motions. The Supreme Judicial Court affirmed, holding that while the widespread use of ALPRs in the Commonwealth could implicate a defendant's constitutional protected expectation of privacy in the whole of his public movements, that interest was not invaded by the limited extent

and use of the ALPR data in the instant case.

Read Opinion Are you a lawyer? **Annotate this case**.

Garden v. Commonwealth

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12821
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed the judgment of a single justice of the court denying Petitioner's petition for extraordinary relief under Mass. Gen. Laws ch. 211, 3 seeking an order vacating Petitioner's plea to aggravated rape and dismissing the underlying indictment, holding that the single justice did not err or abuse his discretion in denying relief. The issues raised by Petitioner had all been raised and adjudicated through the normal appellate process. Petitioner then filed a motion to withdraw his guilty plea. The motion was denied, and the Appeals Court affirmed. In this petition for extraordinary relief, Petitioner sought an order vacating his plea to aggravated rape and dismissing the underlying indictment. The single justice denied relief. The Supreme Judicial Court affirmed, holding that the superintendence power was not available as an additional layer of appellate review once all other avenues had been exhausted.

Read Opinion Are you a lawyer? **Annotate this case**.

In re Mitchell

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12910
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed the judgment of the county court denying, without a hearing, Petitioner's petition for relief under Mass. Gen. Laws ch. 211, 3, holding that the single justice did not err or abuse his discretion in denying relief. Defendant was convicted of several offenses.

The Appeals Court reversed the convictions and remanded the matter for a new trial. Thereafter, the Commonwealth filed a nolle prosequi as to all the charges. In his Mass. Gen. Laws ch. 211, 3 petition, Defendant alleged that no crime had been committed and that he was wrongfully prosecuted. The single justice denied relief. The Supreme Judicial Court affirmed, holding that Defendant did not demonstrate entitlement to the exercise of this Court's superintendence powers.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Reek

Court: Minnesota Supreme Court
Docket: A19-0153
Opinion Date: April 22, 2020
Judge: G. Barry Anderson
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction for first-degree murder, holding that there was no error in the proceedings below. Specifically, the Supreme Court held (1) Appellant's right to a fair trial before an impartial tribunal was not violated when the district court stated that it might reconsider its prior Spreigl ruling if the defense presented certain witnesses; (2) the jury instructions on accomplice liability were plainly erroneous, but Appellant failed to establish that there was a reasonable likelihood that the error had a significant effect on the verdict; (3) the prosecutor did not commit misconduct in his closing arguments regarding the law of accomplice liability; (4) the district court did not abuse its discretion by granting the State's motion to admit evidence of appellant's past convictions for impeachment purposes, including by allowing the specific convictions to be disclosed to the jury; and (5) Appellant's pro se arguments were without merit.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Woodard

Court: Minnesota Supreme Court
Docket: A18-1886

Opinion Date: April 22, 2020
Judge: Hudson
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the district court convicting Defendant of first-degree murder and sentencing him to life in prison without the possibility of release, holding that the district court did not err in denying Defendant's motion to present an alternative-perpetrator defense. Specifically, the Supreme Court held (1) the district court did not abuse its discretion in holding that Defendant's proffered evidence in support of his motion to present alternative-perpetrator evidence for lack of sufficient foundation; and (2) the district court committed an error that was plain in instructing the jury on the order in which to consider the charges against Defendant, but there was no reasonable likelihood that the instruction affected the jury's verdict and therefore did not affect Defendant's substantial rights.

Read Opinion Are you a lawyer? **Annotate this case**.

Huff v. Brown

Court: Nebraska Supreme Court
Citation: 305 Neb. 648
Opinion Date: April 23, 2020
Judge: Lindsey Miller-Lerman
Areas of Law: Communications Law, Criminal Law

The Supreme Court reversed the portion of the district court's order granting in part a writ of mandamus requiring Doug Brown, the sheriff of Furnas County, to provide records to Herchel Huff pursuant to the public records statutes, holding that the district court erred when it determined that Huff had shown that Brown had a clear duty to provide the requested records. Huff, an inmate, sought, among other documents, the criminal history records of jurors who had convicted hims. Furnas County sheriff Kurt Kapperman required a deposit of $750 before fulfilling the request. Huff subsequently filed a petition for writ of mandamus naming Kapperman as the defendant and seeking an order compelling Kapperman to release all requested documents. The court permitted Huff to substitute Brown, the current sheriff, in the caption of the case in place of Kapperman and granted in part mandamus. The Supreme Court reversed in part, holding that the

district court (1) did not err when it substituted Brown's name for Kapperman's; but (2) erred in issuing mandamus because Huff failed to demonstrate a prima facie case that he had been denied a request for public records that the sheriff had a clear duty to provide under Neb. Rev. Stat. 84-712.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Montoya

Court: Nebraska Supreme Court
Citation: 305 Neb. 581
Opinion Date: April 17, 2020
Judge: Freudenberg
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the judgment of the district court affirming Defendant's conviction and sentence for driving under the influence, holding that there was no error in the challenged rulings by the trial court. Specifically, the Supreme Court held that the district court did not err by (1) affirming the county court's order denying Defendant's motion to suppress fruits of the stop; (2) affirming the county court's order that denied Defendant's motion to suppress the fruits of his arrest; (3) affirming the county court's order that denied Defendant's motion to suppress the results of the test of his breath alcohol content; (4) finding sufficient evidence to support the conviction; and (5) finding that Defendant's sentence was not excessive.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Schroeder

Court: Nebraska Supreme Court
Citation: 305 Neb. 527
Opinion Date: April 17, 2020
Judge: Funke
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's sentence of death for first degree

murder, holding that there was no error in the sentence imposed by the sentencing panel. Specifically, the Supreme Court held that the sentencing panel did not err in (1) allowing the State to introduce evidence on the existence of mitigating circumstances; (2) acknowledging and weighing mitigating evidence from the presentence investigation report; (3) not requesting that documentation from the Department of Correctional Services regarding Defendant's time in custody for mitigation purposes be included in the presentence investigation report; (4) sentencing Defendant to death, where the Legislature has enacted safeguards to ensure fairness and accuracy in the resulting sentence; and (5) finding Defendant should be sentenced to death after balancing the aggravating evidence and mitigating evidence.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Kendrick v. Parker

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1509
Opinion Date: April 21, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals denying Appellant's request for a writ of prohibition and/or mandamus against Montgomery County Court of Common Pleas Judge E. Gerald Parker Jr., holding that the court of appeals correctly determined that Appellant's claim was barred by res judicata. Appellant sought a petition for writ of prohibition and/or mandamus against Judge Erik Blaine, the successor to the judge who sentenced Appellant, alleging that the sentencing court patently and unambiguously lacked jurisdiction to sentence him. Judge Parker, who had succeeded Judge Blaine, subsequently filed a motion for summary judgment. The court of appeals granted summary judgment for Judge Parker, concluding that Appellant failed to demonstrate that the sentencing court patently and unambiguously lacked jurisdiction or that he lacked an adequate remedy at law and that res judicata barred Appellant's claim. The Supreme Court affirmed, holding that Appellant's claim was barred by res judicata.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Nelson v. Russo

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1541
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals dismissing Appellant's petition for a writ of mandamus seeking to compel Cuyahoga County Court of Common Pleas Judge Nancy Margaret Russo to vacate the consecutive prison sentences imposed on Appellant in 1987, holding that Appellant had an adequate remedy at law and was barred from asserting additional claims of sentencing error he could have raised in his previous mandamus action. In 1987, Appellant was convicted of four counts of rape and one count of kidnapping. Appellant was sentenced to prison terms of fifteen to twenty-five years for each of the five counts, to be served consecutively. In 2019, Appellant sought a writ of mandamus to compel Judge Russo to vacate his consecutive sentences. The court of appeals dismissed the writ action, concluding that res judicata barred Appellant's claim and that his prior appeals were an adequate remedy at law to address the alleged defect in his consecutive sentences. The Supreme Court affirmed, holding that Appellant was not entitled to a writ of mandamus in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Roberts v. Marsh

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1540
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals dismissing Appellant's original action seeking a writ of procedendo and/or

mandamus to compel Hamilton County Court of Common Pleas Judge Melba Marsh to issue a corrected sentencing entry, holding that the court of appeals correctly dismissed the petition as moot. Appellant was convicted of murder with a repeat-violent-offender specification. Appellant later asked the trial court to correct his sentence, arguing that he had improperly been sentenced to postrelease control. On remand, Judge Marsh vacated the postrelease-control sentence. Appellant appealed that order. The court of appeals noted that the trial court had not set forth all the information required under Crim.R. 32(C) in a single document and dismissed the appeal for lack of a final, appealable order. Appellant then filed this original action seeking to compel Judge Marsh to issue a corrected sentencing entry that constitutes a final, appealable order. Judge Marsh issued a nunc pro tunc sentencing entry that constituted a final, appealable order. The court of appeals then dismissed the petition as moot. The Supreme Court affirmed, holding that because Judge Marsh performed the act Appellant requested, the court of appeals dismissed the petition as moot.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Steiner v. Rinfret

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1510
Opinion Date: April 21, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals dismissing Appellant's petition for a writ of mandamus against Holmes County Court of Common Pleas Judge Robert D. Rinfret, holding that the court of appeals correctly determined that Appellant had an adequate remedy in the ordinary course of the law. Appellant, who was serving consecutive prison terms for five convictions, filed a petition for a writ of mandamus arguing that Judge Rinfret improperly sentenced him to a prison term of nine years for his attempted rape conviction instead of the maximum term of eleven years. The court of appeals dismissed the petition, determining that Appellant had failed to file a mandatory affidavit of his prior civil actions and had an adequate remedy in the ordinary course of the law. The Supreme Court affirmed, holding that relief in mandamus was not

available because Petitioner had an adequate remedy in the ordinary course of the law.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Jeffries

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1539
Opinion Date: April 22, 2020
Judge: Donnelly
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals upholding Defendant's convictions of four counts related to two specific instances of sexual abuse of D.S., holding that the trial court and court of appeals correctly applied Ohio's rape-shield law and determined that evidence of D.S.'s prior nonconsensual sexual assault was inadmissible. On appeal, Defendant asserted that the trial court erred in prohibiting him from introducing evidence during trial that D.S. had previously been sexually assaulted by another person, arguing that the rape-shield law applies only to an accuser's prior consensual sexual activity. The lower court held that Ohio's rape-shield law addresses all sexual activity, not only consensual sexual activity. The court of appeals affirmed. The Supreme Court affirmed, holding (1) the plain meaning of the term "sexual activity" as used in the rape-shield law includes both consensual and nonconsensual sexual activity; and (2) therefore, all sexual activity is barred from admission into evidence by the rape-shield, absent certain exceptions listed in the law.

Read Opinion Are you a lawyer? **Annotate this case**.

Pennsylvania v. Britton

Court: Supreme Court of Pennsylvania
Docket: 55 MAP 2018
Opinion Date: April 22, 2020
Judge: Max Baer
Areas of Law: Constitutional Law, Criminal Law

California law enforcement officers interviewed Appellant Stacy Britton in

her California residence and, unbeknownst to her, recorded those interviews. Over Appellant's objection, Pennsylvania used those recordings as evidence to help convict Appellant of murder in Pennsylvania. The Pennsylvania Supreme Court granted allowance of appeal to examine whether the California law enforcement officers were acting as agents of the Pennsylvania State Police when they recorded the interviews with Appellant in her California home, and if so, whether Pennsylvania's constitutional and statutory protections were available to Appellant under those circumstances. The Court concluded the California law enforcement officers were not acting as agents of the Pennsylvania State Police when they interviewed Appellant, making analysis of whether any Pennsylvania-specific constitutional or statutory protections unwarranted. Because the Supreme Court concluded the Pennsylvania trial court reached the proper result in this matter, it affirmed that court's judgment.

Read Opinion Are you a lawyer? **Annotate this case**.

Pennsylvania v. Copenhaver

Court: Supreme Court of Pennsylvania
Docket: 48 MAP 2019
Opinion Date: April 22, 2020
Judge: Thomas G. Saylor
Areas of Law: Constitutional Law, Criminal Law

In August 2015, a deputy sheriff conducted a vehicle stop of Appellant Victor Copenhaver's pickup truck. Upon approaching the truck, the deputy noticed an odor of alcohol and marijuana emanating from the passenger compartment. After administering field sobriety tests, he arrested Appellant for suspected driving under the influence of alcohol and controlled substances ("DUI"). Appellant was ultimately charged with DUI and other offenses. Appellant challenged the deputy's authority to conduct a traffic stop and sought suppression of all evidence obtained during the encounter. Rather than presenting testimony at a suppression hearing, the parties stipulated that Appellant was driving the vehicle in question and that the deputy had training and qualifications equivalent to that of a police officer. The parties also agreed that the vehicle stop occurred as a result of the deputy observing the tailgate to the pickup truck being in a down position, which caught the deputy's attention. The deputy further observed the

registration on the pickup truck was expired, and additionally, the registration number was identified as belonging to a vehicle other than the one on which it was attached. The issue this case presented for the Pennsylvania Supreme Court's review was whether the deputy could lawfully conduct the traffic stop based on the expired registration sticker, on a theory that such a violation amounts to a breach of the peace. The Supreme Court concluded driving a vehicle with an expired registration did not entail a breach of the peace. It vacated the superior court's order insofar as it held that the expired registration was a breach of the peace, thus alone authorizing the deputy to stop Appellant's vehicle. Notably, in light of its holding, the Supreme Court found the superior court did not proceed to consider other relevant questions, such as whether the parties' factual stipulation should have been read as indicating that the officer's understanding that the registration sticker was associated with a different vehicle arose in the pre-stop timeframe – consistent with the Commonwealth's position throughout this litigation. "These issues should be resolved in the first instance by the intermediate court on remand."

Read Opinion Are you a lawyer? **Annotate this case**.

Pennsylvania v. Tedford

Court: Supreme Court of Pennsylvania
Docket: 773 CAP
Opinion Date: April 22, 2020
Judge: Donohue
Areas of Law: Constitutional Law, Criminal Law

Appellant Donald Tedford was convicted of first-degree murder and rape on February 6, 1987. He appealed the dismissal of his second petition for relief filed pursuant to the Post Conviction Relief Act ("PCRA"), on December 2, 2014, as amended by a counseled petition on May 5, 2015, and a supplemental petition filed on June 9, 2015. In connection with his initial filings, Tedford sought wholesale discovery of the prosecution's entire file, but the PCRA court concluded that the petition (as amended) was not timely filed. Tedford also appealed the PCRA court's order denying his supplemental PCRA petition, in which he requested discovery, an evidentiary hearing, and/or a new trial based upon the admission of expert testimony presented at trial related to microscopic hair analysis. The PCRA

court concluded that pursuant to PCRA Section 9545(b)(1)(ii), it had jurisdiction to consider the merits of Tedford's newly-discovered-facts claims, but ultimately it concluded Tedford had not asserted a meritorious claim in accordance with Section 9543(a)(2)(vi). Finding no reversible error in that analysis, the Pennsylvania Supreme Court affirmed dismissal of the petition for relief.

Read Opinion Are you a lawyer? **Annotate this case**.

Pennsylvania v. Trahey

Court: Supreme Court of Pennsylvania
Docket: 38 EAP 2018
Opinion Date: April 22, 2020
Judge: Wecht
Areas of Law: Constitutional Law, Criminal Law

The trial court granted Timothy Trahey's motion to suppress the results of a blood test that revealed his blood alcohol concentration ("BAC"), finding no justification for the investigating officers' failure to obtain a search warrant before conducting the test. On the Commonwealth's appeal, the Superior Court reversed, opining that the Commonwealth's evidence sufficiently established the existence of exigent circumstances, thus excusing the absence of a warrant. The Pennsylvania Supreme Court reversed, finding that while the exigency analysis is an objective one, "even disregarding the officers' subjective motivations, or their candid acknowledgment that they would have obtained a search warrant if they thought it necessary, there was no time-sensitive need to conduct a warrantless blood test under the circumstances of this case. Accordingly, the Superior Court's conclusion that the test was justified by exigent circumstances was drawn in error."

Read Opinion Are you a lawyer? **Annotate this case**.

In re Greg Abbott

Court: Supreme Court of Texas
Docket: 20-0291
Opinion Date: April 23, 2020
Judge: Per Curiam

Areas of Law: Constitutional Law, Criminal Law

The Supreme Court conditionally granted mandamus relief to the State seeking review of a temporary restraining order (TRO) blocking enforcement of Executive Order GA-13, which changes the rules applicable to judges' decisions regarding pre-trial bail, against judges, holding that the trial court lacked jurisdiction to order the judges' requested relief, even temporarily. GA-13 suspends certain statutes authorizing trial judges to release jail inmates with violent histories during the state of disaster due to the threat of the novel coronavirus. Plaintiffs alleged that GA-13 is unconstitutional and exceeds the governor's statutory emergency powers. Sixteen of the plaintiffs were Texas trial judges alleging that GA-13 improperly interferes with their judicial authority to make individualized bail decisions, and the other plaintiffs were public interest organizations and lawyer associations. The trial court issued a TRO blocking enforcement of GA-13 against judges. The Supreme Court conditionally granted mandamus relief, holding that the alleged threat of a criminal prosecution in this case did not give the judges standing to seek the invalidation of GA-13, and therefore, the trial court lacked jurisdiction to order their requested relief.

Read Opinion Are you a lawyer? **Annotate this case**.

Stahmann v. Texas

Court: Texas Court of Criminal Appeals
Docket: PD-0556-18
Opinion Date: April 22, 2020
Judge: Barbara Hervey
Areas of Law: Constitutional Law, Criminal Law

Appellant Karl Stahmann was involved in an automobile accident, after which he threw a bottle of promethazine, a controlled substance, over a nearby wire fence before law enforcement arrived. The bottle landed two to three feet past the fence in plain view. He was convicted of third-degree felony tampering with physical evidence and was sentenced to 10 years' confinement and fined $5,000. The judge suspended his sentence and placed him on community supervision for 10 years. Stahmann appealed, arguing in part that the evidence was insufficient to prove that he destroyed, altered, or concealed the prescription bottle. The court of appeals agreed

that the evidence was insufficient, but instead of rendering an acquittal, it reformed the judgment to show that Stahmann was convicted of the lesser-included offense of attempted tampering with physical evidence, a state-jail felony. After review of the evidence presented at trial, the Texas Court of Criminal Appeals concluded the evidence was indeed insufficient to prove that Appellant altered the prescription pill bottle when he threw it over the fence because the mere act of throwing the bottle did not change the bottle itself. "While a rational jury could have reasonably inferred that Stahmann intended to conceal the pill bottle when he threw it over the wire fence, the evidence shows that he failed to conceal it as he intended because the bottle landed short of the bush in plain view on top of some grass." The Court affirmed the trial court's judgment.

Read Opinion Are you a lawyer? **Annotate this case**.

Blanke v. Board of Pardons & Parole

Court: Utah Supreme Court
Citation: 2020 UT 16
Opinion Date: April 16, 2020
Judge: Himonas
Areas of Law: Criminal Law

The Supreme Court affirmed the decision of the court of appeals affirming the district court's denial of Appellant's petition for extraordinary relief, holding that, under the circumstances, the Utah Board of Pardons and Parole need not afford Appellant the due process protections explained in Neese v. Utah Board of Pardons and Parole, 416 P.3d 663 (2017), before it could determine that Appellant was a sex offender and condition his parole on sex offender treatment. Appellant was serving a prison sentence for his convictions of attempted child kidnapping and kidnapping. Because he was convicted of attempted child kidnapping Appellant was considered a sex offender under the sex offender registration statute. Further, Appellant admitted in his presentence report that he had sexual intercourse with a fifteen-year-old. Appellant filed a petition for extraordinary relief alleging that the Parole Board had violated his due process rights by conditioning his parole on completion of sex offender treatment even though he had not committed a sex offense. Summary judgment was granted for the Parole Board. The Supreme Court affirmed, holding that the Parole Board owed

Appellant no additional process before it considered unconnected sex offenses in its decision to require Appellant to undergo sex offender treatment.

Read Opinion Are you a lawyer? **Annotate this case**.

Washington v. Escalante

Court: Washington Supreme Court
Docket: 97268-1
Opinion Date: April 23, 2020
Judge: Steven González
Areas of Law: Constitutional Law, Criminal Law

Alejandro Escalante was detained for hours in a secured area at a border crossing and, the State conceded, interrogated by federal agents without Miranda warnings. Statements he made during that interrogation were used by the State to convict him of drug possession. While a traveler briefly detained and questioned at the border was typically not "in custody" for Miranda purposes, "the government's power to detain and question people at the border without implicating Miranda has limits." Here, the Washington Supreme Court determined those limits were reached. "This border detention created the type of inherently coercive environment that demands Miranda warnings to ensure an individual's choice to speak is the product of free will." The Supreme Court held that Escalante was in custody when he was interrogated and reversed.

Read Opinion Are you a lawyer? **Annotate this case**.

Washington v. Haggard

Court: Washington Supreme Court
Docket: 97375-0
Opinion Date: April 23, 2020
Judge: Barbara Madsen
Areas of Law: Constitutional Law, Criminal Law

A class C felony "washes out" and is omitted from a defendant's offender score as long as he or she is not convicted of any crime within five years of the last date of release from confinement. David Haggard was convicted of

a misdemeanor offense within this five-year period, which was dismissed pursuant to RCW 3.66.067. When Haggard later pleaded guilty to burglary and arson, the trial court included prior class C felonies in his criminal history, finding that the dismissed misdemeanor conviction interrupted the washout period for those offenses. Haggard contended on appeal this was error. The Washington Supreme Court determined that because a dismissed conviction constituted a "conviction" under the Sentencing Reform Act of 1981 (SRA), and misdemeanor dismissal and vacation were distinct processes, so Haggard's offender score was properly calculated.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Taylor

Court: Supreme Court of Appeals of West Virginia
Docket: 18-0502
Opinion Date: April 21, 2020
Judge: Walker
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the judgment of the circuit court giving Petitioner credit for twelve days of time served toward the sentence he received for his felony conviction although Petitioner spent additional time in confinement for other charges that were dismissed in the universal plea agreement, holding that to grant Petitioner additional credit for time served would do little more than reward Petitioner for habitual criminal behavior. Petitioner was charged with several crimes and agreed to resolve the pending charges against him in a universal plea agreement. Under the terms of the agreement, Petitioner agreed to plea guilty to the charge of felony carrying a concealed firearm by a prohibited person. In exchange, the State agreed to drop the remaining charges. After he was sentenced, Petitioner argued that, in addition to the twelve days of credit for time served he was granted, he was constitutionally entitled to credit for time served while he was incarcerated for charges that were resolved in the universal plea agreement. The Supreme Court affirmed, holding that Petitioner's circumstances implicated neither double jeopardy nor equal protection of the law such that additional credit for time served was constitutionally mandated.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Harrison

Court: Wisconsin Supreme Court
Dockets: 2017AP002441-CR, 2017AP002440-CR
Opinion Date: April 17, 2020
Judge: Patience D. Roggensack
Areas of Law: Criminal Law

The Supreme Court affirmed in part and reversed in part the decision of the court of appeals reversing an order of the circuit court that granted sentence credit to Defendant, holding that the court of appeals correctly found that Defendant was not entitled to sentence credit but erred by advancing the commencement of Defendant's terms of extended supervision for Defendant's 2007 and 2008 cases. Specifically, the Court held (1) Defendant was not entitled to sentence credit under Wis. Stat. 973.155(1)(a) because the days he spent in custody for which he sought sentence credit were not in connection with the courses of conduct for which those sentences were imposed; and (2) the court of appeals erred by advancing the commencement of Defendant's terms of extended supervision for his 2007 and 2008 cases to the date they would have begun but for Defendant's confinement for unrelated convictions that were later set aside, holding that whether to employ advancement is a public policy decision best left to the legislature.

Read Opinion Are you a lawyer? **Annotate this case**.

About Justia Opinion Summaries

Justia Weekly Opinion Summaries is a free service, with 63 different newsletters, each covering a different practice area.

Justia also provides 68 daily jurisdictional newsletters, covering every federal appellate court and the highest courts of all US states.

All daily and weekly Justia newsletters are free. Subscribe or modify your newsletter subscription preferences at daily.justia.com.

You may freely redistribute this email in whole.

About Justia

Justia is an online platform that provides the community with open access to the law, legal information, and lawyers.



Contact Us | Privacy Policy

Unsubscribe From This Newsletter

or unsubscribe from all Justia newsletters immediately **here.**



Justia | 1380 Pear Ave #2B, Mountain View, CA 94043

From: Criminal Law - Justia Weekly Opinion Summaries
To: Tyson, Christine E (POL)
Subject: Latest 101 Cases This Week: Ramos v. Louisiana (U.S.), United States v. Diaz-Rivera (1st Cir.), United States v. Cotto (2d Cir.)
Date: Friday, April 24, 2020 9:03:03 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

If you are unable to see this message, click here to view it in a web browser.

Justia Weekly Opinion Summaries

Criminal Law
April 24, 2020

Table of Contents

Ramos v. Louisiana
Civil Rights, Constitutional Law, Criminal Law
US Supreme Court

United States v. Diaz-Rivera
Criminal Law
US Court of Appeals for the First Circuit

United States v. Cotto
Criminal Law
US Court of Appeals for the Second Circuit

United States v. Rosa
Criminal Law
US Court of Appeals for the Second Circuit

Fogle v. Sokol
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Third Circuit

James v. New Jersey State Police
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Third Circuit

Bazemore v. Best Buy
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Akande
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Chambers
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Ferebee
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Nance
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Johnson
Criminal Law
US Court of Appeals for the Fifth Circuit

United States v. McGinnis
Criminal Law
US Court of Appeals for the Fifth Circuit

Valentine v. Collier
Civil Rights, Constitutional Law, Criminal Law, Government & Administrative Law, Health Law
US Court of Appeals for the Fifth Circuit

United States v. Dowl
Criminal Law
US Court of Appeals for the Sixth Circuit

United States v. Fowler
Criminal Law
US Court of Appeals for the Sixth Circuit

United States v. Sumlin
Criminal Law
US Court of Appeals for the Sixth Circuit

United States v. Vance
Criminal Law, White Collar Crime
US Court of Appeals for the Sixth Circuit

Winburn v. Nagy
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Sixth Circuit

Lund v. City of Rockford
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

United States v. Perez
Criminal Law
US Court of Appeals for the Seventh Circuit

Jackson v. United States
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Bolman
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Boyd
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Gonzalez-Esparsa
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Sanchez-Velasco
Criminal Law, Immigration Law
US Court of Appeals for the Eighth Circuit

Anthony v. TRAX International Corp.
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Ninth Circuit

City of Almaty v. Khrapunov
Criminal Law, International Law, White Collar Crime
US Court of Appeals for the Ninth Circuit

United States v. Baldon
Criminal Law
US Court of Appeals for the Ninth Circuit

United States v. Costanzo
Criminal Law
US Court of Appeals for the Ninth Circuit

United States v. Manzanares
Constitutional Law, Criminal Law
US Court of Appeals for the Tenth Circuit

United States v. Delaney
Criminal Law
US Court of Appeals for the District of Columbia Circuit

Antenor v. Alaska, Department of Corrections
Civil Procedure, Criminal Law, Government & Administrative Law
Alaska Supreme Court

Berger v. Bryant
Criminal Law
Arkansas Supreme Court

Carroll v. State
Criminal Law
Arkansas Supreme Court

Cave v. State
Civil Rights, Constitutional Law, Criminal Law
Arkansas Supreme Court

Chatmon v. Kelley
Criminal Law
Arkansas Supreme Court

McClinton v. State
Criminal Law
Arkansas Supreme Court

Siegel v. State
Criminal Law
Arkansas Supreme Court

Thomas v. State
Civil Rights, Constitutional Law, Criminal Law
Arkansas Supreme Court

California v. Landowski
Constitutional Law, Criminal Law
California Courts of Appeal

California v. May
Constitutional Law, Criminal Law
California Courts of Appeal

California v. Perez
Constitutional Law, Criminal Law
California Courts of Appeal

In re S.R.
Criminal Law
California Courts of Appeal

People v. Bell
Criminal Law
California Courts of Appeal

People v. Drayton
Criminal Law
California Courts of Appeal

People v. Robinson
Criminal Law
California Courts of Appeal

People v. Torres
Criminal Law
California Courts of Appeal

Colorado v. Lujan
Constitutional Law, Criminal Law
Colorado Supreme Court

Archer v. State
Civil Rights, Constitutional Law, Criminal Law
Florida Supreme Court

Collins v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Heyward v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Howard v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Keller v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Mills v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Moore v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Morris v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Rickman v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Robinson v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Santana v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Sullivan v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Turner v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Valrie v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Williams v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

State v. Malave
Criminal Law
Supreme Court of Hawaii

State v. Malave
Criminal Law
Supreme Court of Hawaii

Idaho v. Burke
Constitutional Law, Criminal Law
Idaho Supreme Court - Criminal

State v. Gibbs
Civil Rights, Constitutional Law, Criminal Law
Iowa Supreme Court

State v. Broxton
Criminal Law
Kansas Supreme Court

State v. Corbin
Criminal Law
Kansas Supreme Court

State v. Frazier
Criminal Law
Kansas Supreme Court

State v. Harris
Civil Rights, Constitutional Law, Criminal Law
Kansas Supreme Court

State v. Uk
Criminal Law
Kansas Supreme Court

State v. Catruch
Criminal Law
Maine Supreme Judicial Court

State v. Paquin
Constitutional Law, Criminal Law
Maine Supreme Judicial Court

Watson v. State
Criminal Law
Maine Supreme Judicial Court

Commonwealth v. Mazza
Criminal Law
Massachusetts Supreme Judicial Court

Commonwealth v. McCarthy
Civil Rights, Constitutional Law, Criminal Law
Massachusetts Supreme Judicial Court

Garden v. Commonwealth
Criminal Law
Massachusetts Supreme Judicial Court

In re Mitchell
Criminal Law
Massachusetts Supreme Judicial Court

State v. Reek
Civil Rights, Constitutional Law, Criminal Law
Minnesota Supreme Court

State v. Woodard
Criminal Law
Minnesota Supreme Court

Huff v. Brown
Communications Law, Criminal Law
Nebraska Supreme Court

State v. Montoya
Civil Rights, Constitutional Law, Criminal Law
Nebraska Supreme Court

State v. Schroeder
Criminal Law
Nebraska Supreme Court

State ex rel. Kendrick v. Parker
Criminal Law
Supreme Court of Ohio

State ex rel. Nelson v. Russo
Criminal Law
Supreme Court of Ohio

State ex rel. Roberts v. Marsh
Criminal Law
Supreme Court of Ohio

State ex rel. Steiner v. Rinfret
Criminal Law
Supreme Court of Ohio

State v. Jeffries
Criminal Law
Supreme Court of Ohio

Pennsylvania v. Britton
Constitutional Law, Criminal Law
Supreme Court of Pennsylvania

Pennsylvania v. Copenhaver
Constitutional Law, Criminal Law
Supreme Court of Pennsylvania

Pennsylvania v. Tedford
Constitutional Law, Criminal Law
Supreme Court of Pennsylvania

Pennsylvania v. Trahey
Constitutional Law, Criminal Law
Supreme Court of Pennsylvania

In re Greg Abbott
Constitutional Law, Criminal Law
Supreme Court of Texas

Stahmann v. Texas
Constitutional Law, Criminal Law
Texas Court of Criminal Appeals

Blanke v. Board of Pardons & Parole
Criminal Law
Utah Supreme Court

Washington v. Escalante
Constitutional Law, Criminal Law
Washington Supreme Court

Washington v. Haggard
Constitutional Law, Criminal Law
Washington Supreme Court

State v. Taylor
Civil Rights, Constitutional Law, Criminal Law
Supreme Court of Appeals of West Virginia

State v. Harrison
Criminal Law
Wisconsin Supreme Court

COVID-19 Updates: Law & Legal Resources Related to Coronavirus

Click here to remove Verdict from subsequent Justia newsletter(s).

New on Verdict

Legal Analysis and Commentary

Rethinking Retroactivity in Light of the Supreme Court's Jury Unanimity Requirement

MICHAEL C. DORF

verdict post



In light of the U.S. Supreme Court's decision Monday in *Ramos v. Louisiana*, in which it held that the federal Constitution forbids states from convicting defendants except by a unanimous jury, Cornell law professor Michael C. Dorf discusses the Court's jurisprudence on retroactivity. Dorf highlights some costs and benefits of retroactivity and argues that the Court's refusal to issue advisory opinions limits its ability to resolve retroactivity questions in a way that responds to all the relevant considerations.

Read More

Criminal Law Opinions

Ramos v. Louisiana

Court: US Supreme Court
Docket: 18-5924
Opinion Date: April 20, 2020
Judge: Neil M. Gorsuch
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

In 48 states and in federal court, a single juror's vote to acquit is enough to prevent a conviction; Louisiana and Oregon punish people based on 10-to-2 verdicts. Ramos was convicted in a Louisiana court by a 10-to-2 jury verdict and was sentenced to life without parole. The Supreme Court reversed. The Sixth Amendment right to a jury trial, as incorporated against the states by the Fourteenth Amendment, requires a unanimous verdict to convict a defendant of a serious offense. Juror unanimity is a vital common law right. The Court rejected an "invitation" to "perform a cost-benefit analysis on the historic features of common law jury trials and to conclude that unanimity does not make the cut." In overturning its 1972 "Apodaca" decision, the Court stated that the reasoning, in that case, was "gravely mistaken" and "sits uneasily with 120 years of preceding case law." The fact that Louisiana and Oregon may need to retry defendants convicted of felonies by non-unanimous verdicts whose cases are still pending on direct appeal "will surely impose a cost, but new rules of criminal procedure usually do."

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Diaz-Rivera

Court: US Court of Appeals for the First Circuit
Docket: 18-1461
Opinion Date: April 20, 2020
Judge: Torruella
Areas of Law: Criminal Law

The First Circuit affirmed Defendant's upwardly variant sentence for one count of possession with intent to distribute cocaine and one count of using a firearm during and in relation to a drug-trafficking crime, holding that the sentence was neither procedurally nor substantively unreasonable. Pursuant to a plea agreement, Defendant pled guilty to drug-related crimes. After a sentencing hearing, the district court sentenced Defendant to an upwardly variant sentence of 180 months of imprisonment, thus declining to

impose the government's requested sentence. On appeal, Defendant challenged both the procedural and substantive reasonableness of his sentence. The First Circuit affirmed, holding that the 180-month sentence was neither procedurally nor substantively unreasonable.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Cotto

Court: US Court of Appeals for the Second Circuit
Docket: 18-2970
Opinion Date: April 20, 2020
Judge: Leval
Areas of Law: Criminal Law

A conviction for retaliating against a witness in violation of 18 U.S.C. 1513 does not require that the Government prove that defendant had knowledge of the federal nature of the proceeding. The Second Circuit rejected defendant's arguments to the contrary and affirmed his conviction for retaliating against a witness. The court remanded for revision of the provision of the sentence relating to the substance abuse treatment condition of supervised release; instructed the district court to consider on remand whether the court's forthcoming order in United States v. Traficante, No. 18-1962 (2d Cir., submitted Oct. 25, 2019) requires modification of the risk notification provision of supervised release; and granted the parties leave to reinstate this appeal to permit review of the district court's decision on remand as to the risk notification provision.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Rosa

Court: US Court of Appeals for the Second Circuit
Docket: 17-2004
Opinion Date: April 17, 2020
Judge: Nardini
Areas of Law: Criminal Law

Where a district court offers no explanation for its sentence, and where neither the adopted presentence report nor the statement of reasons

adequately demonstrates the court's reasoning, the court has committed plain error in violation of 18 U.S.C. 3553(c). The Second Circuit vacated defendant's sentence for conspiracy to commit wire fraud and aggravated identity theft. The court held that the district court failed to state its reasons for sentencing defendant as required under section 3553(c); the error is clear or obvious; and the error affected defendant's substantial rights. Accordingly, the court remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

Fogle v. Sokol

Court: US Court of Appeals for the Third Circuit
Docket: 19-1066
Opinion Date: April 21, 2020
Judge: Matey
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

In 1976, the body of 15-year-old “Kathy” was found near her Indiana County, Pennsylvania home. Kathy’s death involved a brutal assault, rape, and a gunshot to the head. Kathy's sisters, ages nine and 12, stated that she had gotten into a car with a man with blue eyes, black hair that came below his ears and curled at the ends, sideburns, heavy eyebrows, and a heavy mustache. Fogle had “straight reddish-blonde hair that dropped down his back and a matching, full beard that reached his waist.” After three years, Fogle became a suspect because a psychiatric patient described seeing Kathy get in a car with Fogle and his brother. The story was largely inconsistent with statements by Kathy’s sisters. Jailhouse informants were recruited and counseled by law enforcement with promises of leniency. The prosecutors “either knew about, encouraged, or permitted” this strategy. A jury found Fogle guilty of second-degree murder. In 2015, Fogle obtained DNA evidence excluding both himself and his brother as the source of semen collected from Kathy. His conviction was vacated. The Commonwealth declined to pursue new charges, describing the case as lacking “prosecutorial merit.” Fogle, having spent three decades in prison, sued the prosecutors and Indiana County under 42 U.S.C. 1983. The Third Circuit affirmed the denial of their motions to dismiss based on absolute immunity. Only truly prosecutorial functions, not investigative conduct, justify complete protection from suit. Fogle’s complaint alleges actions that fall

outside the narrow doctrine of absolute immunity.

Read Opinion Are you a lawyer? **Annotate this case**.

James v. New Jersey State Police

Court: US Court of Appeals for the Third Circuit
Docket: 18-1432
Opinion Date: April 21, 2020
Judge: Porter
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Stephens called 911 and reported that Gibbons hit her and had a gun in his truck. The police responded. Stephens obtained a temporary restraining order, prohibiting Gibbons from possessing firearms and from returning to Stephens's house. The next day, Gibbons went to Stephens's house. Stephens was talking on the phone; the friend called the police. Gibbons left Stephens's house. Trooper Conza arrived. Stephens stated that Gibbons had waved a gun throughout their argument. Conza told Stephens to go to the police barracks and reported over the radio that Gibbons had brandished a firearm. Conza, with Troopers Bartelt and Korejko, visited the nearby home of Gibbons's mother, James. James stated that she did not know where Gibbons was and that he might be off his schizophrenia medication. While driving to the barracks, Stephens saw Gibbons walking alongside the road and called 911. The Troopers responded. Bartelt parked his car and, exiting, observed that Gibbons was pointing a gun at his own head. Bartelt drew his weapon, stood behind his car door, and twice told Gibbons to drop his weapon. Gibbons did not comply. Bartelt shot Gibbons twice within seconds of stopping his car. Gibbons died that night. In James' suit under 42 U.S.C. 1983, the Third Circuit held that Bartelt is entitled to qualified immunity because he did not violate Gibbons's clearly established rights. Bartelt's pre-standoff knowledge of Gibbons differs from that of officers involved in cited cases. Bartelt could reasonably conclude that Gibbons posed a threat to others.

Read Opinion Are you a lawyer? **Annotate this case**.

Bazemore v. Best Buy

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-2196
Opinion Date: April 21, 2020
Judge: Quattlebaum
Areas of Law: Criminal Law

Plaintiff filed suit against her employer, Best Buy, claiming that she was harassed because of her race and gender and subjected to a hostile work environment in violation of Title VII of the Civil Rights Act of 1964. Plaintiff's complaint stemmed from an incident where a coworker made a racist and sexually charged joke to a small group of coworkers that included plaintiff. The Fourth Circuit affirmed the district court's motion to dismiss and held that, in the case of allegedly harassing comments by a co-worker, an employee must allege plausible facts that the employer knew, or should have known, about the harassment and failed to take action reasonably calculated to stop it. Because plaintiff failed to do this, the court affirmed the district court's judgment. In this case, the coworker's conduct was not imputable to Best Buy where Best Buy took steps that were not only reasonably calculated to end such behavior, but that it did in fact end it.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Akande

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-6833
Opinion Date: April 20, 2020
Judge: Diana Jane Gribbon Motz
Areas of Law: Criminal Law

After defendant moved under 28 U.S.C. 2255 to vacate his conviction based on the ineffective assistance of counsel, the district court denied the motion. The Fourth Circuit granted a certificate of appealability and reversed the district court's judgment. The court held that, given counsel's specific misadvice regarding defendant's rights to preserve his appellate rights, on which defendant understandably relied, the district court's general admonishments did not amount to the careful explanation that addresses the particular issue necessary to cure the error. In this case, the plea colloquy did not correct counsel's erroneous advice and the error prejudiced defendant. Accordingly, the court remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Chambers

Court: US Court of Appeals for the Fourth Circuit
Docket: 19-7104
Opinion Date: April 23, 2020
Judge: Floyd
Areas of Law: Criminal Law

After defendant was erroneously sentenced as a career offender, he moved to reduce his sentence to time served under the First Step Act. The district court denied defendant's motion to reduce his custodial sentence, though it granted the motion as to his supervised release term. The Fourth Circuit held that the First Step Act does not constrain courts from recognizing Guidelines errors. The court explained that First Step Act motions fall under 18 U.S.C. 3582(c)(1)(B), a distinct exception to finality, and that section 404(b) of the First Step Act expressly allows a court to impose a reduced sentence in order to give retroactive effect to sections 2 and 3 of the Fair Sentencing Act. Furthermore, 18 U.S.C. 3553(a) sentencing factors apply in the section 404(b) resentencing context, and the resentencing court has discretion within the section 404(b) framework to vary from the Guidelines and, in doing so, to consider movants' post-sentencing conduct. In this case, the district court seemingly believed that it could not vary from the Guidelines range to reflect post-sentencing information. Therefore, the court vacated the district court's sentencing order. Finally, the court held that any Guidelines error deemed retroactive, such as the error in this case, must be corrected in a First Step Act resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Ferebee

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-4266
Opinion Date: April 22, 2020
Judge: Traxler
Areas of Law: Criminal Law

The Fourth Circuit affirmed the denial of defendant's motion to suppress evidence recovered from a backpack, and the district court's conclusion that defendant abandoned the backpack and any legitimate expectation of privacy in its contents. The court rejected defendant's claim that the collective-knowledge doctrine has any bearing on the propriety of the district court's conclusion that defendant abandoned the backpack. The court also held that the district court is not precluded from finding abandonment in cases where the defendant, as here, has physical possession of the property he has disavowed. In this case, the record supported the district court's conclusion that defendant clearly and unequivocally disavowed ownership of the backpack. Even if the district court erred by finding that defendant abandoned the backpack, reversal would not be required because the search of the backpack was a proper search incident to arrest for which no warrant was required under the facts of this case.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Nance

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-4585
Opinion Date: April 21, 2020
Judge: Pamela Harris
Areas of Law: Criminal Law

The Fourth Circuit affirmed defendant's above-Guidelines sentence imposed after he pleaded guilty to two federal drug- and firearm-related offenses. The court held that defendant's sentence was not procedurally unreasonable where the district court took into account defendant's extensive criminal history; his pattern of reoffending upon release; his disciplinary infractions in custody and inability to comply with the terms of his release; and the fact that the offenses of conviction occurred over the course of days, in which he was arrested once, released, and then arrested again just days later. The court also held that defendant's sentence was substantively reasonable where the district court conducted a thorough, individualized assessment of defendant and his offense conduct in light of the 18 U.S.C. 3553(a) factors, and did not abuse its discretion in formulating the sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Johnson

Court: US Court of Appeals for the Fifth Circuit
Docket: 17-60852
Opinion Date: April 21, 2020
Judge: Priscilla R. Owen
Areas of Law: Criminal Law

The Fifth Circuit vacated defendant's sentence imposed after he pleaded guilty to violating 18 U.S.C. 922(g) and 924(e) by knowingly possessing a firearm after he had been convicted of a misdemeanor crime of domestic violence. The court held that the district court committing plain error by violating Federal Rule of Criminal Procedure 32 when it relied on factual allegations in the confidential sentencing recommendation that were not in the presentence report and that were not disclosed by defendant. The court explained that the use of undisclosed facts to justify an above-guidelines sentence seriously affects the fairness, integrity, and public reputation of judicial proceedings. Therefore, the court remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. McGinnis

Court: US Court of Appeals for the Fifth Circuit
Docket: 19-10197
Opinion Date: April 21, 2020
Judge: Stuart Kyle Duncan
Areas of Law: Criminal Law

18 U.S.C. 922(g)(8), which prohibits individuals subject to certain domestic violence protective orders from possessing firearms or ammunition for any purpose, is facially constitutional under the Fifth Circuit's two-step NRA framework. Even assuming arguendo that the conduct at issue -- the keeping and possessing of firearms by individuals subject to domestic protective orders -- falls within the Second Amendment right, defendant's facial challenge fails. The court applied intermediate scrutiny and held that section 922(g)(8) is reasonably adapted to the government interest of

reducing domestic gun abuse. The court also held that if the commonly understood definitions of terms in the protective order include acts involving "physical force," the protective order is sufficient to support a conviction under section 922(g)(8)(C)(ii). In this case, the jury plausibly found that the order satisfied the statute and the court declined to reverse defendant's conviction on this basis. However, the court remanded for the limited purpose of conforming defendant's written judgment to the district court's oral pronouncement.

Read Opinion Are you a lawyer? **Annotate this case**.

Valentine v. Collier

Court: US Court of Appeals for the Fifth Circuit
Docket: 20-20207
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Criminal Law, Government & Administrative Law, Health Law

Plaintiffs filed suit alleging that TDCJ's adoption and implementation of measures guided by changing CDC recommendations in regards to the COVID-19 pandemic do not go far enough. Plaintiffs filed a class action alleging violations of the Eighth Amendment's prohibition against cruel and unusual punishment, and the Americans with Disabilities Act, seeking a preliminary injunction. The Fifth Circuit granted TDCJ's motion to stay the district court's preliminary injunction, which regulates the cleaning intervals for common areas, the types of bleach-based disinfectants the prison must use, the alcohol content of hand sanitizer that inmates must receive, mask requirements for inmates, and inmates' access to tissues (amongst many other things). The court held that TDCJ is likely to prevail on the merits of its appeal because: (1) after accounting for the protective measures TDCJ has taken, plaintiffs have not shown a "substantial risk of serious harm" that amounts to "cruel and unusual punishment"; and (2) the district court committed legal error in its application of Farmer v. Brennan, by treating inadequate measures as dispositive of defendants' mental state. In this case, even assuming that there is a substantial risk of serious harm, plaintiffs lack evidence of defendants' subjective deliberate indifference to that harm. The court also held that TDCJ has shown that it will be

irreparably injured absent a stay, and that the balance of the harms and the public interest favor a stay. Finally, the court held that plaintiffs have not exhausted their administrative remedies as required in the Prison Litigation Reform Act (PLRA), and the district court's injunction goes well beyond the limits of what the PLRA would allow even if plaintiffs had properly exhausted their claims.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Dowl

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-2469
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

Dowl pleaded guilty to presenting false tax returns, 18 U.S.C. 286. He received a sentence of 30 months of imprisonment plus 24 months of supervised release. On supervised release, Dowl was charged with four new state crimes; failing to inform his probation officer that he had police contact; communicating with his co-defendant despite instructions to the contrary; failing to make payments on his restitution, fine, or special assessment; and failing to get a job. At a hearing, the court reviewed the evidence and allowed Dowl to tell his side of the story. The court deferred judgment on three of the four new state criminal law violations and dismissed the fourth and found Dowl gainfully employed. Dowl had failed to notify his probation officer about police contact, impermissibly communicated with his co-defendant, and did not pay his fines. After considering the 18 U.S.C. 3553(a) sentencing factors, the court returned Dowl to prison for 11 months, giving Dowl and his attorney the opportunity to raise any objections. Dowl had none. The Sixth Circuit affirmed, rejecting Dowl’s argument that the court committed reversible error by not directly addressing him to solicit an allocution. The court employed the “plain error” standard because Dowl did not raise any objection during his revocation hearing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Fowler

Court: US Court of Appeals for the Sixth Circuit
Dockets: 19-3071, 19-3070
Opinion Date: April 21, 2020
Judge: Donald
Areas of Law: Criminal Law

In 2018, Fowler pled guilty to possession of child pornography and violations of the conditions of his supervised release from a previous conviction for the same. In addition to possessing child pornography, Fowler had failed drug testing, had threatened his parole officer, and had tried to harass his girlfriend to recant her testimony. The district court ordered Fowler to pay a $5,000 special assessment for possession of child pornography under the Justice for Victims of Trafficking Act, 18 U.S.C. 3014. The court also varied upward and sentenced Fowler to the maximum statutory penalty for violating the conditions of his supervised release, imposing a 120-month sentence for possessing child pornography and a consecutive 36-month sentence for violating the terms of his supervised release. The Sixth Circuit vacated as to the assessment and remanded for a determination of indigency. The district court committed plain error by failing to address Fowler's ability to pay; the parties did not contemplate the $5,000 special assessment as a part of the waiver provision in the plea agreement. The court affirmed the sentence. The district court did not consider an impermissible factor (whether Fowler had actually touched a child) and Fowler had no other challenge to the reasonableness of his sentence,

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Sumlin

Court: US Court of Appeals for the Sixth Circuit
Docket: 18-3819
Opinion Date: April 21, 2020
Judge: Bush
Areas of Law: Criminal Law

Sumlin was convicted of the distribution of drugs that caused the 2015 death of Carrie Dobbins, 21 U.S.C. 841(a)(1) and (b)(1)(C), which carries enhanced penalty provisions. The Sixth Circuit affirmed his convictions and

his sentence to life in prison. The district court properly denied Sumlin's suppression motion, given that the affidavit established a sufficient nexus between his drug trafficking activity and residence that was searched. The court properly admitted testimony by the victim's sister, Kelly, who was Sumlin's former girlfriend and had purchased drugs from him. Kelly's testimony about Sumlin's drug-trafficking and that Sumlin was with Carrie on the day of her overdose was intrinsic proof that was relevant for providing background information and contextualizing the government's case against Sumlin. Sufficient evidence supported the jury's verdict that Sumlin distributed the drugs that caused Carrie's death.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Vance

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-5160
Opinion Date: April 17, 2020
Judge: Bush
Areas of Law: Criminal Law, White Collar Crime

The Spriggs' bank account was established to receive social security checks. The Spriggs' great-grandson, Vance, filled out an application in Mr. Spriggs's name for a debit card to draw on the checking account. Mr. Spriggs had never used a debit card. The Spriggses did not authorize Vance to do so. Bank cameras photographed Vance using the card to withdraw cash. Vance also used the card for personal expenses. At another bank, Vance used Mr. Spriggs's social security number to establish an account and obtain a $15,000 cash advance. Vance made other, unsuccessful loan applications. Upon being notified by the banks about suspicious activities involving his identity, Mr. Spriggs filed a police report. The police arrested Vance. While searching Vance's car, the police located a large stash of personal and financial documents belonging to the Spriggses, including bank statements, tax return forms, property-tax bills, and a car title. The Sixth Circuit affirmed Vance's convictions for access-device fraud, 18 U.S.C. 1029(a)(5), and two counts of aggravated identity theft, 18 U.S.C. 1028A(a)(1), and his 65-month sentence. The court rejected arguments that the district court failed to make adequate findings of fact after the bench trial, improperly denied a motion for judgment of acquittal,

and failed to correctly calculate the loss amount connected to Vance's charges under Sentencing Guidelines 2B1.1.

Read Opinion Are you a lawyer? **Annotate this case**.

Winburn v. Nagy

Court: US Court of Appeals for the Sixth Circuit
Dockets: 19-2399, 19-2398
Opinion Date: April 23, 2020
Judge: Jeffrey S. Sutton
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Winburn represented himself at his trial for armed robbery, home invasion, and conspiracy. Based on Winburn's disruptive behavior, the judge removed him from the courtroom and revoked Winburn's permission to represent himself, then granted a competency evaluation and a mistrial. While Winburn awaited his second trial, the judge permitted Winburn's stand-by attorney to withdraw because Winburn had sued her and enjoined Winburn from filing complaints or grievances against his new attorney, except to discharge her. Although represented by a new attorney, Winburn moved pro se to dismiss his charges on double jeopardy grounds. The trial judge denied the motion because Winburn's attorney had not filed it. Winburn filed a habeas petition under 28 U.S.C. 2241 challenging his retrial and another section 2241 petition challenging the injunction. The district judges denied both and declined to issue certificates of appealability. Winburn filed a notice of appeal for one petition and sought a certificate of appealability for the other. The Sixth Circuit held that state pretrial detainees proceeding under section 2241 may not appeal without certificates of appealability and granted Winburn a certificate on the injunction claim. A reasonable jurist could conclude that the unusual order was constitutionally infirm. The court denied relief with respect to double jeopardy. Winburn failed to exhaust his state-court remedies by a motion to dismiss.

Read Opinion Are you a lawyer? **Annotate this case**.

Lund v. City of Rockford

Court: US Court of Appeals for the Seventh Circuit

Docket: 19-1945
Opinion Date: April 20, 2020
Judge: ROVNER
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Lund, a reporter for the Rockford Scanner, heard, by police scanner, of multiple traffic stops in Midtown. He did not have a driver's license, so he rode a motorized bicycle to Midtown to take photographs. He suspected a prostitution sting operation. An officer noticed Lund and radioed the team. Officers Welsh and Campbell knew of Lund's previous anti-police speech. They directed Lund to "move on." Lund asked if he was breaking any laws. Campbell informed him that he was not, but that his continued presence would constitute obstruction of a police detail and result in arrest. Lund started his bicycle and called out, loudly, "goodbye officers." Concerned that Lund might post pictures on social media while the sting operation was ongoing and create a danger for unarmed undercover officers, the officers followed Lund and arrested him for driving the wrong way on a one-way street, operating a vehicle without insurance, obstructing a police officer, felony aggravated driving on a revoked license, and operating a motor vehicle without a valid drivers' license. News stories listed Lund's name as an arrestee in the prostitution sting. The charges against Lund were dismissed. Lund sued the officers and the city under 42 U.S.C. 1983. The Seventh Circuit affirmed summary judgment for the defendants on First Amendment retaliation and malicious prosecution under Illinois law, citing the Supreme Court's intervening "Nieves" (2019) holding, that, in most cases, probable cause to arrest defeats a claim of retaliatory arrest. There was probable cause to arrest Lund.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Perez

Court: US Court of Appeals for the Seventh Circuit
Docket: 18-3156
Opinion Date: April 23, 2020
Judge: KANNE
Areas of Law: Criminal Law

Beloit officers facilitated a recorded controlled buy of heroin from Perez, a suspected high-level drug dealer. Perez sold 98 grams of heroin to an

informant. Based on that transaction alone, Perez pled guilty to distributing heroin. At Perez's sentencing hearing, the judge expressed concern that the guidelines range of 33–41 months' imprisonment did not reflect the full scope of his drug trafficking. The PSR described conduct that suggested that Perez was responsible for distributing large quantities of heroin, methamphetamine, and cocaine. The judge continued the hearing, directing the government to file a memorandum, detailing which offense conduct it could support by a preponderance of the evidence. When the hearing reconvened, the government presented witness testimony that elaborated on conduct described in the PSR, including drug ledgers, Perez's post-arrest conversation with his girlfriend, large sums of cash, a money counter, cell phones, and Perez's passport. The judge calculated a higher guidelines range and imposed a 121-month sentence. The Seventh Circuit affirmed, rejecting an argument that the sentencing judge should have recused himself. Perez has not demonstrated that a reasonable observer would have questioned the judge's impartiality nor did he allege that the judge was biased based on events outside the proceedings. The judge's continuance was laudable, not prejudicial.

Read Opinion Are you a lawyer? **Annotate this case**.

Jackson v. United States

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1131
Opinion Date: April 20, 2020
Judge: Lavenski R. Smith
Areas of Law: Criminal Law

The Eighth Circuit affirmed the district court's denial of a 28 U.S.C. 2255 motion to vacate, set aside, or correct petitioner's sentence. The court held that the district court did not err in denying an evidentiary hearing as to petitioner's claim that counsel was constitutionally ineffective for failing to conduct adequate pretrial investigations. In this case, petitioner failed to identify any specific witnesses or evidence that counsel failed to uncover. Furthermore, petitioner failed to show that counsel's representation prejudiced his case. The court also held that the district court did not err in denying an evidentiary hearing as to petitioner's claim that his new counsel was ineffective for failing to subpoena witnesses, for convincing petitioner

not to testify, for failing to object to or appeal the district court's answer to a jury question, and for failing to object to the district court's designation of petitioner as a career offender.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Bolman

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-2759
Opinion Date: April 21, 2020
Judge: Jane Louise Kelly
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's conviction for involuntary manslaughter after he struck and killed his nephew with his truck. The court held that the evidence was sufficient to support the conviction, because a reasonable jury could find defendant grossly negligent beyond a reasonable doubt. The court also held that the district court did not plainly err by failing to instruct the jury that actual knowledge is an essential element of the offense that is separate from gross negligence, because the instructions, viewed as a whole, accurately and adequately defined the essential elements of the offense.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Boyd

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-3528
Opinion Date: April 17, 2020
Judge: Kobes
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's sentence imposed after he pleaded guilty to being a felon in possession of a firearm. The court held that the facts underlying defendant's prior arrests were part of his history and characteristics under 18 U.S.C. 3553(a), and thus the district court could consider defendant's arrest records and the circumstances of those arrests. The court explained that the arrests were listed in the presentence report

and gleaned from prior police reports. Furthermore, specific facts underlying the arrests may be considered for an upward departure and should be considered fair game for a variance where defendant did not object to them. The court also concluded that there is nothing here that suggested a corrected misstatement improperly influenced the district court's sentencing decision. Finally, the court held that the upward variance was not unreasonable in consideration of defendant's previous assaults, coupled with the facts underlying his arrest in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Gonzalez-Esparsa

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1477
Opinion Date: April 22, 2020
Judge: Grasz
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's conviction for unlawful use of an identification document and misuse of a social security number. The court held that the evidence was sufficient to support defendant's convictions where a reasonable juror could conclude that defendant knew the permanent resident card bearing his name and photograph had been forged, counterfeited, falsely made, or unlawfully obtained when he used it to secure employment. Furthermore, a reasonable juror could conclude that defendant made the false representation regarding his purported social security number in order to deceive Midwest Concrete in order to obtain a job with the company.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Sanchez-Velasco

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-3568
Opinion Date: April 17, 2020
Judge: James B. Loken
Areas of Law: Criminal Law, Immigration Law

The Eighth Circuit affirmed the district court's denial of defendant's motion to suppress his responses to an ICE agent's two questions at the Treasurer's Office, because he was not in custody at the time of questioning. Although defendant was in custody at the ICE facility, the court held that an agent's questions were not custodial interrogation because the agent could not have known his questions were likely to elicit incriminating information regarding the two criminal charges that were eventually brought against defendant. The court noted that the Attorney General's regulations carefully distinguish between the warrantless arrest of an alien for a criminal violation of the immigration laws, and what is called the "administrative arrest" of an alien who is reasonably believed to be illegally present in the United States. The court agreed with the district court that the agent's questioning was a request for routine information necessary for basic identification purposes that is not interrogation under Miranda, even if the information turns out to be incriminating.

Read Opinion Are you a lawyer? **Annotate this case**.

Anthony v. TRAX International Corp.

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-15662
Opinion Date: April 17, 2020
Judge: Kim McLane Wardlaw
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Ninth Circuit affirmed the district court's grant of summary judgment to TRAX in a disability discrimination action brought by plaintiff under Title I of the Americans with Disabilities Act (ADA). After TRAX terminated plaintiff from her position as a Technical Writer allegedly due to an inability or unwillingness to accommodate her disability, TRAX discovered during the course of litigation that plaintiff lacked the requisite bachelor's degree for her position. The panel held that, although McKennon v. Nashville Banner Publishing Co., 513 U.S. 352 (1995), held that after-acquired evidence cannot establish a superseding, non-discriminatory justification for an employer's challenged actions, after-acquired evidence remains available for other purposes, including to show that an individual is not qualified under the ADA. Because plaintiff did not satisfy one of the prerequisites for her

position, she is not "otherwise qualified," and TRAX was not obligated to engage in the interactive process.

Read Opinion Are you a lawyer? **Annotate this case**.

City of Almaty v. Khrapunov

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-56451
Opinion Date: April 22, 2020
Judge: Marbley
Areas of Law: Criminal Law, International Law, White Collar Crime

The City of Almaty, in Kazakhstan, filed suit against defendant and his family under the Racketeer Influenced and Corrupt Organizations Act (RICO), alleging that they engaged in a scheme to defraud the city of millions of dollars. The City claimed that it was forced to spend money and resources in the United States to trace where its money was laundered. The district court dismissed the City's claim on the basis that it failed to state a domestic injury pursuant to the Supreme Court's recent decision in RJR Nabisco, Inc. v. European Community, 136 S. Ct. 2090 (2016). The Ninth Circuit held that the City failed to state any cognizable injury other than the foreign theft of its funds, and its voluntary expenditures were not proximately caused by defendants' acts of money laundering. In this case, the City's expenditure of funds to trace its allegedly stolen funds is a consequential damage of the initial theft suffered in Kazakhstan and is not causally connected to the predicate act of money laundering.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Baldon

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-10411
Opinion Date: April 21, 2020
Judge: Bennett
Areas of Law: Criminal Law

After defendant pleaded guilty to possession with intent to distribute a controlled substance, the district court sentenced him to 184 months in

prison. The Ninth Circuit held that defendant's prior convictions for carjacking under section 215 of the California Penal Code are not categorical crimes of violence under USSG 4A1.1(e). Therefore, the district court incorrectly calculated defendant's criminal history by improperly including two points for his prior carjacking convictions. However, the panel held that the district court did not err in finding that defendant possessed a firearm under USSG 2D1.1(b)(1). Accordingly, the panel affirmed in part, vacated in part, and remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Costanzo

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-10291
Opinion Date: April 17, 2020
Judge: Michael Daly Hawkins
Areas of Law: Criminal Law

The Ninth Circuit affirmed defendant's conviction of five counts of money laundering, holding that a reasonable trier of fact could have found beyond a reasonable doubt that the money laundering transactions, in which payment was made via bitcoin, affected interstate commerce in some way or to some degree. In this case, the transfer involved the use of an Internet or cellular network connected Personal Computer Device (PCD) to transfer bitcoin (together with the digital code necessary to unlock the bitcoin) to the digital wallet of another Internet or cellular network connected PCD.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Manzanares

Court: US Court of Appeals for the Tenth Circuit
Docket: 18-2010
Opinion Date: April 17, 2020
Judge: Mary Beck Briscoe
Areas of Law: Constitutional Law, Criminal Law

Defendant-Appellant Archie Manzanares appealed a district court's denial of his 28 U.S.C. 2255 motion challenging his sentence under the Armed

Career Criminal Act (ACCA). Under the ACCA, an offense qualified as a violent felony by satisfying at least one of three definitions, which have come to be known as the Elements Clause, the Enumerated Clause, and the Residual Clause. Manzanares asserted that without the Residual Clause, his underlying New Mexico convictions (armed robbery, aggravated assault with a deadly weapon, and aggravated battery) no longer qualified as violent felonies. The district court denied the motion, concluding that all three underlying convictions satisfied the Elements Clause. Manzanares appealed the classification of the armed robbery conviction as a violent felony to the Tenth Circuit, and sought to expand the certificate of appealability to allow him to appeal the decision regarding the aggravated assault with a deadly weapon and aggravated battery convictions. After review, the Tenth Circuit affirmed the district court's denial of Manzanares's 2255 motion, and denied his motion to expand the COA.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Delaney

Court: US Court of Appeals for the District of Columbia Circuit
Docket: 18-3093
Opinion Date: April 17, 2020
Judge: David S. Tatel
Areas of Law: Criminal Law

The DC Circuit vacated the district court's denial of defendant's motion to suppress evidence. The court held that officers violated the Fourth Amendment when they seized defendant because they lacked reasonable suspicion to justify the stop. In this case, a seizure occurred when the officers pulled into the parking lot, partially blocked defendant's vehicle, and activated their take-down light. The court held that any inference of suspicion that the officers drew from encountering defendant soon after hearing the nearby gunshots were undermined by the government's failure to identify specific and articulable facts supporting the officers' estimation of where the various shots came from. Accordingly, the court remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

Antenor v. Alaska, Department of Corrections

Court: Alaska Supreme Court
Docket: S-17005
Opinion Date: April 17, 2020
Judge: Carney
Areas of Law: Civil Procedure, Criminal Law, Government & Administrative Law

Several Alaska Department of Corrections inmates challenged the DOC's policy to charge for local telephone calls, arguing the rates they and call recipients had to pay for calls violated their constitutional right to rehabilitation, their statutory right to reasonable telephone access, and DOC's contractual obligations under a prior settlement and consent decree. In addition, one of the prisoners challenged DOC officers' decision to deny him access to a computer programming book he ordered from outside the prison. He contended that DOC placed a content-specific restriction on the educational materials and publications prisoners were allowed, violating the Alaska Constitution's free speech provisions as well as prisoners' right to reformation. Each of these challenges reached the Alaska Supreme Court after inmates exhausted the administrative process from prison. Inmates then appealed to the superior court, which denied relief. The Alaska Supreme Court determined the superior court record did not provide enough evidence for it to meaningfully determine the reasonableness of the rates charged inmates for local telephone calls; therefore the Court reversed denial of relief and remanded for further fact-finding by the trial court. The Court concluded that the facility's restrictions on programming-related books were rationally related to a legitimate interest, and because they did not infringe on the right to rehabilitation, it affirmed denial of a prisoner's motion to enforce his claimed right to a particular text about computer programming.

Read Opinion Are you a lawyer? **Annotate this case**.

Berger v. Bryant

Court: Arkansas Supreme Court
Citation: 2020 Ark. 357
Opinion Date: April 23, 2020
Judge: Rhonda K. Wood

Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's petition to proceed in forma pauperis on a petition for writ of mandamus and a motion for declaratory judgment, holding that Appellant failed to state a colorable cause of action. In 1998, Appellant was convicted of rape. In his petition for a writ of mandamus, Appellant asserted that he sought information pursuant to the Arkansas Freedom of Information Act regarding his rape conviction but received no response. The circuit court denied the petition. The Supreme Court affirmed, holding (1) even if Appellant had requested disclosable information, he would not be entitled to inspect it as an incarcerated person; and (2) Appellant did not demonstrate a legitimate claim given the facts presented and therefore failed to establish a colorable cause of action to support his request to proceed in forma pauperis.

Read Opinion Are you a lawyer? **Annotate this case**.

Carroll v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 360
Opinion Date: April 23, 2020
Judge: Wynne
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's motion for leave to file a petition for writ of error cram knobs, holding that the circuit court did not abuse its discretion in declining to issue the writ. Appellant pled guilty to rape and was sentenced as a habitual offender to 720 months' imprisonment. In his coram nobis petition, Appellant alleged several grounds for relief, including claims of actual innocence, an invalid arrest warrant, a coerced guilty plea, and prosecutorial misconduct. The circuit court denied the motion. The Supreme Court affirmed, holding that Appellant did not demonstrate that that the writ should issue and failed diligently to proceed on his claim for coram nobis relief.

Read Opinion Are you a lawyer? **Annotate this case**.

Cave v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 356
Opinion Date: April 23, 2020
Judge: Josephine L. Hart
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's pro se petition for writ of habeas corpus, holding that the circuit court did not err in denying the petition. Appellant was found guilty of two counts of delivery of a controlled substance and one count of maintaining a drug premises. In his habeas petition, Appellant argued that he was actually innocent because his arrest and conviction was based on the false testimony of a witness who had a lengthy criminal history. Appellant further argued that the writ should issue because he was not afforded effective assistance of counsel. The circuit court denied the petition. The Supreme Court affirmed, holding (1) Appellant's claims regarding the witness's credibility do not constitute a valid assertion that he was being unlawfully detained; and (2) Appellant did not actually connect an allegation of ineffective assistance of counsel to his allegation that he was unlawfully detained.

Read Opinion Are you a lawyer? **Annotate this case**.

Chatmon v. Kelley

Court: Arkansas Supreme Court
Citation: 2020 Ark. 355
Opinion Date: April 23, 2020
Judge: Josephine L. Hart
Areas of Law: Criminal Law

The Supreme Court denied Appellant's appeal from the order of the circuit court denying his petition to proceed in forma pauperis on the grounds that Appellant failed to state a colorable cause of action in a petition for writ of habeas corpus, holding that the circuit court did not abuse its discretion by denying Appellant's in forma pauperis petition. In his habeas petition, Appellant alleged that the trial court lacked jurisdiction in his criminal case. Before this case was submitted to the Supreme Court, Appellant filed two

motions, including a "Judicial Notice of a Void Judgment" and a "Notice to the Court." The Supreme Court denied the motions, holding that neither motion was cognizable under the Court's rules. The Court then affirmed the Supreme Court's denial of Appellant's in forma pauperis petition, holding that the circuit court correctly found that Appellant did not assert a colorable cause of action.

Read Opinion Are you a lawyer? **Annotate this case**.

McClinton v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 353
Opinion Date: April 23, 2020
Judge: Karen R. Baker
Areas of Law: Criminal Law

The Supreme Court denied Petitioner's second petition requesting permission to proceed in the trial court with a petition for writ of error coram nobis, holding that Petitioner's proposed attack on the judgment had no merit. Petitioner was convicted of raping a mentally handicapped sixteen-year-old girl and was sentenced to life imprisonment. In his first petition for writ of error coram nobis Petitioner alleged a number of errors in the trial procedure. The first petition was denied. In his second coram nobis petition, Petitioner alleged violations of Brady v. Maryland, 373 U.S. 83 (1963). The Supreme Court denied the writ, holding that Petitioner failed to meet his burden of demonstrating a fundamental error of fact extrinsic to the record.

Read Opinion Are you a lawyer? **Annotate this case**.

Siegel v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 359
Opinion Date: April 23, 2020
Judge: Wynne
Areas of Law: Criminal Law

The Supreme Court dismissed Appellant's appeal from the circuit court's orders denying her motions to declare Ark. Code Ann. 5-62-106 (disposition

of animal) and Ark. Code Ann. 5-62-111 (prevention of cruelty) unconstitutional and conditionally granting her motion for return of seized property, holding that there was no final, appealable order in this case. Appellant was convicted of thirty-one misdemeanor counts of cruelty to animals. The circuit court subsequently dismissed the charges on speedy-trial grounds. The State appealed, and the Supreme Court dismissed the appeal on the grounds that it was not authorized. Appellant had filed motions seeking a declaration that sections 5-62-106 and -111 are unconstitutional and seeking the return of her seized property. The circuit court denied the constitutional claims and entered a conditional order granting Appellant's motion for return of seized property. Appellant appealed. The Supreme Court dismissed the appeal, holding that because the conditional order did not make specific findings as to the return of the property or as to damages and because it expressly left open the possibility of further proceedings, there was no final, appealable order in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

Thomas v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 354
Opinion Date: April 23, 2020
Judge: Josephine L. Hart
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Appellant's conviction of capital murder, holding that the evidence was sufficient to sustain the conviction and that the circuit court did not err in denying Appellant's motion to suppress tracking data generated by his cellphone. On appeal, Appellant argued that the trial court erred by denying his directed-verdict motion because the evidence supported the defense's theory of the case that he did not intend to shoot the victim. Further, Appellant argued that the court abused its discretion in denying his motion to suppress evidence obtained from the seizure of AT&T phone records. The Supreme Court disagreed, holding (1) the evidence was sufficient to support the capital murder conviction; and (2) the circuit court correctly denied the motion to suppress.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. Landowski

Court: California Courts of Appeal
Docket: C080210(Third Appellate District)
Opinion Date: April 23, 2020
Judge: Andrea Lynn Hoch
Areas of Law: Constitutional Law, Criminal Law

Defendant Michael Reyes, Jr., an active Norteno gang member (from the Broderick Boys subset), confronted a former Norteno gang member (from the Franklin Boys subset), "S.," about a physical altercation that occurred between S. and Reyes's stepfather over a debt. That earlier altercation had taken place in front of Reyes's autistic younger brother. Reyes pulled out a handgun and asked S. if he had a problem. S., who was riding his bicycle with his wife, "R.," when Reyes confronted him with the gun, stopped briefly, told Reyes to put the gun down if he wanted to fight, and then started to ride away. This angered Reyes, prompting him to fire six rounds at S. from behind. S. Was hit but survived. R. Was a short distance in front of S., but was not hit. Defendants Liberty Landowski and Lisa Humble were with Reyes at the time of the shooting and aided in his efforts to avoid being apprehended by law enforcement authorities. Reyes, Landowski, and Humble were tried together before the same jury. Reyes was convicted of one count of attempted murder (Count 1), two counts of assault with a semiautomatic firearm (Counts 2 and 4), one count of possession of a firearm by a convicted felon (Count 5), and one count of possession of ammunition by a convicted felon (Count 6). In addition to various firearm and other enhancements, the jury found Reyes committed the crimes for the benefit of, at the direction of, or in association with a criminal street gang with the specific intent to promote, further, or assist in criminal conduct by gang members. The jury convicted Landowski and Humble of being accessories to Reyes's criminal conduct (Count 9) and also found true gang enhancement allegations attached to that crime. Reyes challenged the sufficiency of the firearm evidence presented to support his conviction, and all defendants challenged the sufficiency of the evidence supporting their gang enhancements. The Court of Appeal determined Senate Bill 620 (2017-2018 Reg. Sess.) gave the trial court discretion to strike firearm enhancements in the interest of justice and applied retroactively; and Senate Bill 136 (2019-2020 Reg. Sess.) eliminated such enhancements,

and also applied retroactively. To these issues, the Court remanded for the trial court's consideration. The Court affirmed the trial court in all other respects.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. May

Court: California Courts of Appeal
Docket: C084302(Third Appellate District)
Opinion Date: April 20, 2020
Judge: Ronald B. Robie
Areas of Law: Constitutional Law, Criminal Law

Defendant Raymond May was found guilty by jury of possessing an assault weapon and a machine gun based on his possession of a single AK-47 assault rifle while guarding a marijuana plantation. He was sentenced to probation, which included an electronic search condition. On appeal, defendant argued there was a lack of sufficient evidence corroborating his accomplice's testimony and demonstrating he knew of the firearm's illegal character. He further alleged the trial court erred in instructing the jury: that the accomplice instruction should have included language specifying that the accomplice testimony needed to prove more than defendant's mere presence or access to the firearm. Furthermore, defendant argued the electronic search condition imposed as part of his probation failed under the standards announced in California v. Lent, 15 Cal.3d 481 (1975). The Court of Appeal agreed defendant's electronic search condition should have been stricken, but otherwise affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. Perez

Court: California Courts of Appeal
Docket: E072260(Fourth Appellate District)
Opinion Date: April 20, 2020
Judge: Miller
Areas of Law: Constitutional Law, Criminal Law

In 2009, defendant-appellant Rudy Perez pled guilty to active gang

participation under Penal Code section 186.22(a), and unlawful possession of a firearm under section 12025(b)(6). In 2010, defendant pled guilty to residential burglary under section 459, and active gang participation under section 186.22(a). In August of 2018, the State filed a new felony complaint, alleging one of the prior gang participation convictions as a strike prior. In 2018, defendant moved to vacate the two prior gang participation convictions based upon changes in the law that rendered them invalid. The trial court denied defendant's motion. In 2019, defendant asked for reconsideration, which was again denied. Thereafter, defendant filed a timely notice of appeal from the denial of his motion to vacate the convictions. The Court of Appeal found that defendant pled guilty to street terrorism under Penal Code section 186.22(a) in 2009 and 2010, and it was undisputed that while committing these offenses, defendant acted alone. However, subsequent to defendant's guilty pleas, in 2012, the California Supreme Court held that a defendant had to act in concert with a fellow gang member in order to be guilty of street terrorism. At that time, defendant could have filed a state habeas petition requesting relief, but failed to do so. "Defendants can lose remedies that are established by law when they fail to invoke such remedies in time." Section 1473.7 became effective in 2017. In defendant's motion filed in the trial court, defendant failed to state what new evidence was discovered, instead arguing that the trial court was allowed "to vacate a conviction where the defendant is innocent as a matter of law or where vacating the conviction is in the interest of justice, even though the defendant is no longer in custody or otherwise restrained by the conviction." The Court of Appeal concurred with the trial court's reason to deny relief, determining that "while the outcome in this case may be unfortunate for defendant, we are not here to rewrite legislation. The Legislature could amend section 1473.7 to address issues raised in this case. However, under the laws, as written, we must uphold the trial court's order."

Read Opinion Are you a lawyer? **Annotate this case**.

In re S.R.

Court: California Courts of Appeal
Docket: B300214(Second Appellate District)
Opinion Date: April 23, 2020
Judge: Bendix

Areas of Law: Criminal Law

Father appealed the juvenile court's dispositional ruling removing daughter from his custody, arguing that his mere possession of child pornography does not demonstrate that he poses a substantial risk of harm to his daughter. The Court of Appeal affirmed the order and held that there is substantial evidence of risk of great harm to daughter—no matter how low the probability— that father will sexually abuse his daughter if he is provided unfettered access to her.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Bell

Court: California Courts of Appeal
Docket: B288528(Second Appellate District)
Opinion Date: April 23, 2020
Judge: Stratton
Areas of Law: Criminal Law

Defendant was convicted of one count of attempted robbery, one count of second degree murder, and one count of hit and run driving. The jury found not true the allegation that a principal was armed in the commission of the attempted robbery. The trial court found true the allegations that defendant had served four prior prison terms within the meaning of Penal Code section 667.5, subdivision (b). Defendant raised 13 claims of error on appeal. The Court of Appeal held that the section 667.5, subdivision (b) enhancement terms must be stricken and the matter remanded to the trial court for resentencing. The court also held that defendant forfeited some of his substantive claims and other lack merit. Finally, the court held that, if there is instructional error, the errors are harmless under any standard of review. Accordingly, the court affirmed the judgment of conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Drayton

Court: California Courts of Appeal
Docket: H046928(Sixth Appellate District)

Opinion Date: April 17, 2020
Judge: Danner
Areas of Law: Criminal Law

In 1991, the Wards and their teenage daughter awoke and discovered four men, including Drayton, inside their house. Two were armed. One told the daughter he was going to rape her and placed a firearm inside her vagina. Drayton told the man not to do it. Drayton had a gun and held Mrs. Ward down during the robbery. Two others shot and killed Mr. Ward. Drayton and the others left without seeking help for the Wards. Drayton did not shoot Mr. Ward or threaten to rape the daughter. Drayton surrendered the next day. Drayton's sole prior conviction was a misdemeanor; he had no reported history of violence. Drayton was sentenced to 29 years to life imprisonment. In 2019, Drayton sought resentencing under Penal Code 1170.95, declaring that he "was not a major participant ... or did not act with reckless indifference to human life." Senate Bill 1437, effective January 1, 2019, restricted the circumstances under which a person can be liable for felony murder and enacted Penal Code 1170.95, which allows an individual, previously convicted of felony murder, to petition to have his murder conviction vacated and to be resentenced. The court of appeal directed the trial court to hold a hearing under section 1170.95(d) and to accept the assertions in the petition as true unless facts in the record conclusively refute them as a matter of law. If, accepting the petitioner's assertions as true, he meets section 1170.95(a)'s requirements for relief, the court must issue an order to show cause. In assessing the prima facie showing, the trial court should not weigh evidence or make credibility determinations.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Robinson

Court: California Courts of Appeal
Docket: B293746(Second Appellate District)
Opinion Date: April 20, 2020
Judge: Wiley
Areas of Law: Criminal Law

After defendant penetrated an unconscious woman with his fingers, he challenged evidentiary rulings and requests a presentence conduct credit. The Court of Appeal held that the trial court properly excluded cumulative

evidence about past times the woman was intoxicated at the relevant bar, and any error in allowing a drug recognition expert to testify about whether the woman was incapacitated was harmless. However, the court held that the trial court undercalculated defendant's presentence custody credit because he was not convicted of a violent felony under Penal Code section 2933.1, which would otherwise limit those credits. Accordingly, the court directed the trial court to award defendant 104 days of presentence custody credit and to amend the abstract of judgment, affirming in all other respects.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Torres

Court: California Courts of Appeal
Docket: B292551(Second Appellate District)
Opinion Date: April 20, 2020
Judge: Kenneth R. Yegan
Areas of Law: Criminal Law

Where, as here, the trial court factually finds that a self-represented defendant has engaged in an attempt to intimidate a witness, the constitutional right of self-representation can, in the exercise of the trial court's sound discretion, be revoked. The Court of Appeal affirmed defendant's conviction and sentence for two counts of battery on an ex-girlfriend. In this case, the trial court did not abuse its discretion in revoking defendant's pro se status after he asked his sister to contact the victim and have her say that she was coerced by the police detective to "press charges."

Read Opinion Are you a lawyer? **Annotate this case**.

Colorado v. Lujan

Court: Colorado Supreme Court
Citation: 2020 CO 26
Opinion Date: April 20, 2020
Judge: Brian D. Boatright
Areas of Law: Constitutional Law, Criminal Law

Abel Lujan was charged with first-degree murder for the death of his girlfriend after she was found beaten and strangled behind a friend's house. At trial, two women testified for the State about Lujan's prior violent behavior towards them. Prior to admitting this evidence, the trial court read a limiting instruction, telling the jury that it could only consider the evidence for the purposes of establishing Lujan's motive, intent, or common plan. A copy of this instruction was not given to the jury for deliberations; however, the jury did receive an instruction at the close of the evidence explaining that certain evidence could only be considered for the limited purposes for which it was admitted. While deliberating, the jury submitted a question seeking clarification about the limiting instruction. Over defense counsel's objection, the trial court cleared the courtroom of the public and parties, leaving only the judge, bailiff, and court reporter; the judge then brought in the jury and reread the limiting instruction that it had previously read twice in open court. The jury ultimately found Lujan guilty of second-degree murder. Lujan appealed, arguing that the court's actions when rereading the jury instruction constituted a courtroom closure that violated his Sixth Amendment right to a public trial. A division of the court of appeals agreed and reversed Lujan's conviction. The State argued on certiorari review that the Colorado Supreme Court adopt a triviality standard, under which a defendant's constitutional right to a public trial was not violated when the closure at issue was trivial. In so doing, the State argued that the brief courtroom closure here was trivial and therefore did not violate Lujan's public trial right. The Court concurred with the State, adopted the standard and reversed the appellate court's decision.

Read Opinion Are you a lawyer? **Annotate this case**.

Archer v. State

Court: Florida Supreme Court
Docket: SC19-841
Opinion Date: April 23, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the order of the circuit court denying Appellant's successive motion to vacate his sentence of death under Fla. R. Crim. P. 3.851, holding that the circuit court did not err in denying the Rule

3.851 motion. Appellant was convicted of first-degree murder, armed robbery, and grand theft. Appellant was sentenced to death for the murder. The Supreme Court affirmed the convictions but reversed Appellant's death sentence and remanded the case for a new penalty phase. After a new penalty phase, Appellant was again sentenced to death. In his successive Rule 3.851 motion, Appellant raised three claims. The circuit court denied relief. The Supreme Court affirmed, holding that the circuit court (1) properly denied Appellant's claim that his death sentence violated the Sixth and Eighth Amendments in light of Hurst v. Florida, 136 S. Ct. 616 (2016), and Hurst v. State, 202 So. 3d 40 (Fla. 2016); (2) correctly denied Appellant's claim that his sentence violated the Eighth Amendment; and (3) did not err in denying Appellant's claim of newly discovered evidence.

Read Opinion Are you a lawyer? **Annotate this case**.

Collins v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0158
Opinion Date: April 20, 2020
Judge: David E. Nahmias
Areas of Law: Constitutional Law, Criminal Law

Appellant Tommy Collins was convicted of felony murder in connection with the stabbing death of 14-year-old Rueben Hand. Friends gathered to watch the Peach Drop on New Year's Eve 2010; a disagreement ensued and Hand was stabbed near the Five Points MARTS station shortly after midnight. Appellant's only argument on appeal was that the trial court plainly erred when it gave the jury the State's requested instruction on "revenge for a prior wrong." Seeing no error, "much less plain error," the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Heyward v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0399
Opinion Date: April 20, 2020

Judge: Peterson
Areas of Law: Constitutional Law, Criminal Law

Larmell Heyward was convicted by jury of malice murder and possession of a firearm during the commission of a felony in connection with the 2007 shooting death of Ramon Rogers. Heyward argued on appeal of those convictions that the trial court erred in denying his request to charge the jury on voluntary manslaughter. After review, the Georgia Supreme Court determined the trial court's refusal to give the charge was harmless, since, in the Court's estimation, there was no realistic probability that the jury would have accepted the "slight" evidence of voluntary manslaughter in the light of the strong evidence of malice murder.

Read Opinion Are you a lawyer? **Annotate this case**.

Howard v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0819
Opinion Date: April 20, 2020
Judge: Keith R. Blackwell
Areas of Law: Constitutional Law, Criminal Law

Kenneth Howard was tried by jury and convicted of the murder of Emily Ann Smith Newbegin. Howard appealed, contending that the evidence was legally insufficient to sustain his conviction. Upon its review of the record and briefs, the Georgia Supreme Court found no merit in Howard's claim of error, and affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Keller v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0006
Opinion Date: April 20, 2020
Judge: Boggs
Areas of Law: Constitutional Law, Criminal Law

Randall Keller was convicted of felony murder and related crimes arising out

of the beating death of his ex-wife's two-year-old son, William Powell. On appeal, Keller raised numerous claims of error, including ineffective assistance of counsel, the trial court's rulings on motions before and during trial, several evidentiary rulings, and alleged bias on the part of the trial judge. However, finding no reversible error, the Georgia Supreme Court affirmed Keller's convictions.

Read Opinion Are you a lawyer? **Annotate this case**.

Mills v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0364
Opinion Date: April 20, 2020
Judge: Ellington
Areas of Law: Constitutional Law, Criminal Law

Roger Mills was found guilty by jury of malice murder and aggravated assault in connection with the death of Masuto Garrett. Mills contended that the trial court erred when, during jury deliberations, it excused a holdout juror without sufficient inquiry or good cause. After review, the Georgia Supreme Court concurred with that contention, and reversed Mills's convictions. The Court also concluded the evidence presented at trial was legally sufficient to support the convictions, so the State could retry Mills if it chose.

Read Opinion Are you a lawyer? **Annotate this case**.

Moore v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0344
Opinion Date: April 20, 2020
Judge: David E. Nahmias
Areas of Law: Constitutional Law, Criminal Law

Appellant Carzell Moore, proceeding pro se, appealed a trial court's denial of his motion to set aside a September 2017 order denying his motion for an out-of-time appeal of his 2002 resentencing on his 1977 convictions for murder and rape. Moore contended the trial court abused its discretion by

denying his motion to set aside because he was not given proper notice of the September 2017 order. Finding that the record supported the trial court's ruling, the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Morris v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0176
Opinion Date: April 20, 2020
Judge: Bethel
Areas of Law: Constitutional Law, Criminal Law

Darius Morris was found guilty by jury of malice murder and other offenses in connection with the shooting death of Jameson Bush. Morris appealed, arguing he was denied the right to a timely appeal, that the trial court erred in restricting voir dire as to the religious beliefs and connections of potential jurors, that the trial court erred by giving a confusing jury charge regarding statements of co-conspirators, that the trial court erred by violating his right to a public trial by ordering that the courtroom doors be closed and locked during the court's charge to the jury, and that his trial counsel provided ineffective assistance by not objecting to the closure of the courtroom. Finding no error, the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Rickman v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0127
Opinion Date: April 20, 2020
Judge: Harold D. Melton
Areas of Law: Constitutional Law, Criminal Law

Victoria Rickman was convicted by jury of malice murder and a related firearm offense in connection with the shooting death of William Carter, Jr. Rickman and Carter had a tumultuous on-again, off-again relationship with a history of verbal and physical abuse, false accusations of sexual assault, empty threats to obtain temporary protective orders, and numerous calls to

911. In the days leading up to Carter's death, the pair was talking and meeting again despite a recent break-up. On one such 911 call, officers went to Rickman's residence responding to claims shots were fired. Rickman responded holding her small dog, hair wet, and in pajamas. She did not appear to be injured, and nothing in the home looked disturbed or out of place. Rickman told the officers, "he raped me again and I shot him." Officers found Carter laying face up on the bed naked with multiple gunshot wounds to his body. An autopsy revealed that Carter was shot ten times – four times in the chest, three times in the back, once on the arm, and twice in the head. Rickman's examining physician testified that he found no injuries on Rickman consistent with her description of events, and no signs of trauma to her vaginal cavity. Rickman appealed her convictions, arguing she was denied effective assistance of counsel and that the trial court erred in admitting improper character evidence. Finding no reversible error, the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Robinson v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0265
Opinion Date: April 20, 2020
Judge: Peterson
Areas of Law: Constitutional Law, Criminal Law

Herbert Robinson appealed his convictions for malice murder, armed robbery, and possession of a firearm during the commission of a felony in connection with the death of Michael Moore. On appeal, he argued the trial court erred by allowing the State to use two firearms for demonstrative purposes during trial, and by allowing body-camera footage to be shown at trial. He also argued his trial counsel was ineffective for failing to object to a letter written by Robinson's cellmate being available to the jury for review during deliberations, and for failing to object to a visual aid used by the State during closing arguments. Because Robinson failed to show ineffective assistance of counsel or reversible error by the trial court, the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Santana v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0563
Opinion Date: April 20, 2020
Judge: Warren
Areas of Law: Constitutional Law, Criminal Law

Cuevas Carlos Santana was convicted by jury of malice murder and other crimes in connection with the 2010 shooting deaths of Israel Espinoza Mendoza, Vincente Soto Chavez, and Renato Soto Valencia. On appeal, Santana argues that the evidence was insufficient to support his convictions, that the trial court erred by declining to grant Santana a new trial on the general grounds, and that trial counsel provided ineffective assistance. Finding no reversible error, the Georgia Supreme Court affirmed Santana's convictions.

Read Opinion Are you a lawyer? **Annotate this case**.

Sullivan v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0056
Opinion Date: April 20, 2020
Judge: Warren
Areas of Law: Constitutional Law, Criminal Law

A jury convicted Antonio Sullivan of malice murder and other crimes in connection with the shooting death of Wava Benton. On appeal, Sullivan contended his trial counsel was constitutionally ineffective by failing to present evidence at trial to corroborate Sullivan's testimony about prior difficulties between Sullivan and Benton, and by failing to procure expert testimony about Sullivan's mental health—specifically about post-traumatic stress disorder— to be presented to the jury. The Georgia Supreme Court determined Sullivan failed to establish that his trial counsel was deficient in either respect, and therefore affirmed his convictions.

Read Opinion Are you a lawyer? **Annotate this case**.

Turner v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0247
Opinion Date: April 20, 2020
Judge: Warren
Areas of Law: Constitutional Law, Criminal Law

Appellant Ronald Turner appeals from his conviction for malice murder stemming from the stabbing death of William King. The stabbing took place outside an apartment at which Turner had driven in order to trade food for drugs. Turner testified in his own defense at trial and claimed that King hit him in the head with a beer bottle because Turner owed money to King from a prior drug transaction. Turner testified that he tried to get away from King, but that King chased him down and grabbed his jacket. According to Turner, King was getting ready to hit him again when Turner stabbed King in self-defense. Appealing his ultimate conviction, Turner contended he was denied the effective assistance of counsel in three respects. Seeing no reversible error after a review of the trial court record, the Georgia Supreme Court affirmed Turner's conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Valrie v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0380
Opinion Date: April 20, 2020
Judge: Keith R. Blackwell
Areas of Law: Constitutional Law, Criminal Law

Reuben Valrie was tried by jury and convicted of murder and other crimes in connection with the death of his infant daughter Aliyana. Valrie appealed, claiming that he was denied the effective assistance of counsel. Aliyana died as a result of closed head trauma, with a blunt-force abdominal injury as a secondary cause of death, which investigators determined was consistent with being shaken or dropped. At trial, Valrie presented the testimony of four expert witnesses who testified that Aliyana died of natural causes and that the injuries to her brain and abdomen were caused by

events such as post-mortem CPR and the “rough” handling of her body by first responders. The jury rejected this defense and found Valrie guilty of murder and the other charges. Valrie contended that his trial lawyer should have raised a hearsay objection to the admission of recorded statements that his girlfriend (and Aliyana's mother) made to police investigators (as well as the testimony of one of those investigators about some of those statements). Alternatively, Valrie argued that his lawyer should have sought the redaction of certain portions of the recorded statements that impugned his character. The Georgia Supreme Court concluded Valrie failed to present evidence that his trial counsel was deficient, or that he was prejudiced by any alleged failures. According, the Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Williams v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0241
Opinion Date: April 20, 2020
Judge: Keith R. Blackwell
Areas of Law: Constitutional Law, Criminal Law

Richard Williams, II, was tried by jury and convicted of murder in connection with the strangulation death of Cory Robinson. Williams and Robinson were involved in a sexual relationship and had been living together at an extended-stay hotel. Kelvin Spencer was a close friend of both Williams and Robinson. When Spencer met Williams at the hotel room, Williams looked angry and had scratches on his neck. Spencer saw Robinson lying on the floor in a “praying position.” Spencer did not believe Robinson was dead, and he helped Williams move clothes and other things to a U-Haul truck parked outside, in preparation for a move. Williams did not testify or present any evidence. Based on his lawyer’s opening and closing arguments, the defense theory was that Spencer killed Robinson because he was jealous of Williams’s relationship with Robinson. Williams’s sole claim on appeal was that he was denied the effective assistance of counsel when his trial lawyer failed to present as a defense that Williams accidentally killed Robinson during consensual erotic asphyxiation. He argued that his lawyer's discomfort with the topic of homosexual BDSM activity, and his own problems with the Georgia State Bar, precluded presentation of the "true"

version of events, and that Williams acceded to the lawyer's defense strategy only "through ignorance and that he did not know that a defense based on consensual erotic asphyxiation was available." Finding no reversible error, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Malave

Court: Supreme Court of Hawaii
Docket: SCWC-18-0000332
Opinion Date: April 20, 2020
Judge: Mark E. Recktenwald
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the intermediate court of appeals (ICA) affirming Defendant's conviction of sexual assault in the first degree on the complaining witness pursuant to Haw. Rev. Stat. 707-730(1)(b), holding that the ICA did not err in affirming the family court. Specifically, the Supreme Court held (1) the jury should have been instructed to determine jurisdictional facts, but the error was harmless beyond a reasonable doubt; and (2) the ICA did not err in finding that there was no rational basis in the record to support providing the jury instruction of the lesser included offense of sexual assault in the third degree.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Malave

Court: Supreme Court of Hawaii
Docket: SCWC-18-0000332
Opinion Date: April 22, 2020
Judge: Mark E. Recktenwald
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the intermediate court of appeals (ICA) affirming the judgment of the family court convicting Defendant on two counts of sexual assault in the first degree, holding that the ICA did not err in affirming the family court. At issue on appeal was the jurisdiction of the family court to try Defendant and the propriety of

instructing the jury on a lesser included offense. The ICA affirmed, concluding that the family court had subject matter jurisdiction pursuant to Haw. Rev. Stat. 571-14(a)(1) and that there was no rational basis to support an instruction of the lesser included offense of sexual assault in the third degree. The Supreme Court affirmed, holding (1) although the jury should have been instructed to determine jurisdictional facts, the error was harmless; and (2) the family court was not obligated to instruct the jury on the lesser included offense of sexual assault in the third degree.

Read Opinion Are you a lawyer? **Annotate this case**.

Idaho v. Burke

Court: Idaho Supreme Court - Criminal
Docket: 46841
Opinion Date: April 22, 2020
Judge: Moeller
Areas of Law: Constitutional Law, Criminal Law

Prior to sentencing, defendant James Burke was committed to the state mental hospital for 56 days to restore him to competency. After being evaluated and deemed competent to proceed to trial, Burke was returned to the county jail and later pleaded guilty pursuant to a plea agreement. At the conclusion of his sentencing hearing, Burke sought credit for the 56 days of time spent in court-ordered commitment. The district court denied the motion, concluding that commitment to a state mental hospital did not fall under the definition of 'incarceration' in Idaho Code section 18-309. After reviewing this issue carefully, the Idaho Supreme Court disagreed with the district court's "thorough and thoughtful analysis," holding that court-ordered commitment to state custody pursuant to Idaho Code sections 18-210 and 18-211 met the functional and legal definition of "incarceration" under Idaho Code section 18-309. "The extent of the liberty interests restricted by Burke's court-ordered commitment to State Hospital North are just too similar to imprisonment to conclude otherwise." Accordingly, the Court reversed the district court's order denying Burke's request for credit for time served and remanded the case for the district court to enter an order crediting him with the fifty-six days he spent committed to State Hospital North while the State restored his competency to face criminal charges.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Gibbs

Court: Iowa Supreme Court
Docket: 18-1298
Opinion Date: April 17, 2020
Judge: Edward M. Mansfield
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction of murder in the second degree, holding that Defendant's Fifth Amendment rights were invaded when the trial judge instructed the jury that Defendant was required to notify law enforcement of his use of deadly force, but the error was harmless. During trial, Defendant asserted the defense of justification in his shooting of the victim. At issue on appeal was whether the district court abused its discretion by giving a jury instruction incorporating the terms of Iowa Code 704.2B. The instruction included a statement that a person using deadly force is required to notify law enforcement about his use of deadly force. Defendant argued before the Supreme Court that both section 704.2B and the jury instruction incorporating that section violated his Fifth Amendment rights. The Supreme Court affirmed, holding (1) instructing the jury that a homicide defendant is required to notify a law enforcement agency of his use of deadly force violates the defendant's Fifth Amendment rights; but (2) any error in this case was harmless beyond a reasonable doubt.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Broxton

Court: Kansas Supreme Court
Docket: 114675
Opinion Date: April 17, 2020
Judge: Stegall
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's convictions for second-degree murder, burglary, and theft but reversed Defendant's sentences, holding

that any error during the guilt phase was harmless but that the district court erred by scoring Defendant's prior Florida burglary conviction as a person felony instead of a nonperson felony. On appeal, the court of appeals concluded that a trial court may instruct the jury on felony murder even though the State only charged the defendant with premeditated first degree murder. The Supreme Court disagreed, holding (1) the court of appeals erred in concluding that a district court may elect to provide a felony-murder instruction when that crime was not charged, and the district court properly found that the felony-murder instruction was not legally appropriate in this case; (2) the district court erred by excluding from evidence an exculpatory document from a Florida homicide investigation on the ground it was not relevant, but the error was harmless; and (3) the district court improperly scored Defendant's prior Florida burglary conviction as a person felony.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Corbin

Court: Kansas Supreme Court
Docket: 119665
Opinion Date: April 17, 2020
Judge: Dan Biles
Areas of Law: Criminal Law

The Supreme Court affirmed the ruling of the district court on remand resentencing Defendant to his original mandatory term of imprisonment after once again finding he was not a person with intellectual disability, holding that the district court did not abuse its discretion when it rejected Defendant's intellectual disability motion and imposed a mandatory term of imprisonment. Defendant pled no contest to first-degree premeditated murder. Before sentencing, Defendant filed a motion pursuant to Kan. Stat. Ann. 21-6622(b) asserting that he was a person with intellectual disability and was thus not subject to a mandatory minimum prison term. The district court denied the motion and sentenced Defendant to a hard twenty-five life sentence. While Defendant's appeal was pending, the Legislature amended Kan. Stat. Ann. 76-12b01(i), which provides new standards for deciding intellectual disability. The Supreme Court reversed and remanded for reconsideration of Defendant's motion using the new criteria. On remand, the district court reaffirmed its earlier ruling and again sentenced Defendant

to a hard twenty-five life sentence. The Supreme Court affirmed, holding that the district court's ruling was reasonably based on the law and was supported by substantial competent evidence.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Frazier

Court: Kansas Supreme Court
Docket: 117456
Opinion Date: April 17, 2020
Judge: Wilson
Areas of Law: Criminal Law

The Supreme Court reversed the decision of the district court affirming the judgment of the district court denying Defendant's motion to withdraw plea of no contest to one count of possession of heroin with intent to distribute, holding that the district court's decision in finding no good cause for Defendant to withdraw his plea was based on errors of fact and law, which were grounds for finding abuse of discretion. On appeal, Defendant argued that the district court abused its discretion in denying his motion to withdraw his plea of no contest based on misleading or false statements contained in the plea agreement. The court of appeals affirmed the district court. The Supreme Court reversed, holding (1) there was enough uncertainty in this case to indicate that Defendant's plea agreement was not understandingly made; and (2) therefore, Defendant must be allowed to withdraw his plea.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Harris

Court: Kansas Supreme Court
Docket: 117362
Opinion Date: April 17, 2020
Judge: Wilson
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court reversed the judgment of the court of appeals affirming Defendant's conviction of possession fo marijuana, holding that Defendant's waiver of jury trial was legally insufficient. On appeal, Defendant argued that

he did not properly waive his right to a jury and asserted three other issues. The Supreme Court reversed the judgment of the court of appeals affirming Defendant's convictions without addressing the three remaining issues, holding that because the district court failed properly to apprise Defendant of his right to a jury trial and failed to ensure that Defendant understood the nature of the right he was giving up, Defendant's constitutional right to a jury trial was violated in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Uk

Court: Kansas Supreme Court
Docket: 119712
Opinion Date: April 17, 2020
Judge: Wilson
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's conviction for first-degree premeditated murder, holding that the district court did not err in its challenged instructions to the jury. Specifically, the Supreme Court held (1) the district court did not err in refusing to give the jury Defendant's requested instruction on voluntary manslaughter as a lesser included offense of first-degree murder because the instruction was not factually appropriate; and (2) the district court did not commit clear error in issuing an unmodified version of Instruction No. 11, which contained the definition of "premeditation" and mirrored PIK Crim. 4th 54.150(d) because the instruction was legally appropriate.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Catruch

Court: Maine Supreme Judicial Court
Citation: 2020 ME 52
Opinion Date: April 23, 2020
Judge: Andrew M. Mead
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed the judgments of the trial court

terminating Appellant's participation in the Co-Occurring Disorders and Veterans Court (Veterans Court), holding that the court did not err or abuse its discretion in terminating Appellant's participation in the Veterans Court. The Veterans Court is a criminal docket that provides judicial monitoring, specialized treatment, and other services for military veterans who have disorders often attributable to their military service. Appellant was charged with leaving the scene of an accident and three other offenses. Appellant was admitted to the Veterans Court. Agreeing to sentencing outcomes in a plea agreement and entering into a bail contract, Appellant pleaded guilty to all charges against him. The court later terminated Appellant's participation in the Veterans Court, finding that Appellant had violated the conditions of his bail contract. The Supreme Judicial Court affirmed, holding (1) this matter was properly before the Court; and (2) given Appellant's failure to comply with the requirements for participation in the treatment court and his violations of the agreements, his termination from the Veterans Court was warranted.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Paquin

Court: Maine Supreme Judicial Court
Citation: 2020 ME 53
Opinion Date: April 23, 2020
Judge: Andrew M. Mead
Areas of Law: Constitutional Law, Criminal Law

In this appeal from Defendant's conviction for eleven counts of gross sexual misconduct, the Supreme Judicial Court vacated the judgment of conviction on one count, vacated the dismissal of other counts and remanded for entry of a judgment of acquittal on those counts, and affirmed in all other respects, holding that Defendant's convictions on both Counts 5 and 30 violated his double jeopardy protections and that the court erred in allowing the State to dismiss Counts 27, 28, and 29 during trial without Defendant's consent. The indictment charged Defendant with fifteen counts (Counts 1-13, 30-31) of gross sexual misconduct against the victim and sixteen counts (Counts 14-29) of gross sexual misconduct against a second alleged victim. During trial, the court granted Defendant's motion for a judgment of acquittal on Counts 10-13, and the State dismissed Counts 27-29. Defendant was

found guilty of Counts 1-9 and 30-31 and not guilty on the remaining counts. The court entered judgment in accordance with the verdict. The Supreme Judicial Court held that the trial court erred in failing to rule that the Double Jeopardy Clause barred convictions on both Counts 5 and 30 and allowing the State to dismiss Counts 27, 28, and 29 rather than entering a judgment of acquittal on those counts.

Read Opinion Are you a lawyer? **Annotate this case**.

Watson v. State

Court: Maine Supreme Judicial Court
Citation: 2020 ME 51
Opinion Date: April 21, 2020
Judge: Joseph Jabar
Areas of Law: Criminal Law

The Supreme Judicial Court vacated the judgment of the unified criminal docket denying Appellant's petition for post-conviction review, holding that Appellant was deprived of the effective assistance of counsel when his trial attorney played a video of the ten-year-old victim's interview with police and that Appellant was adversely affected. Appellant was convicted of two counts of gross sexual assault, one count of unlawful sexual contact, and one count of visual sexual aggression against a child. The Supreme Court affirmed. Appellant later filed a petition for post-conviction review claiming that his trial attorney's representation was deficient because introducing the videotaped recording of the victim's entire interview with law enforcement was unnecessary to provide evidence supporting the victim's potential motive to fabricate the allegations. The post-conviction court denied denied the petition. The Supreme Court vacated the judgment below, holding that trial counsel's conduct was deficient and that counsel's actions rose to the level of comprising the reliability of Appellant's conviction and undermining confidence in it.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. Mazza

Court: Massachusetts Supreme Judicial Court

Docket: SJC-11363
Opinion Date: April 21, 2020
Judge: Budd
Areas of Law: Criminal Law

The Supreme Judicial Court reversed the order of the superior court denying Defendant's motion for a new trial and set aside the jury's verdicts of first degree murder and robbery, holding that a recently discovered witness statement made to the police ago constituted newly discovered evidence that "would probably have been a real factor in the jury's deliberations." At issue was Defendant's sixth motion for a new trial, which was predicated on newly discovered evidence consisting of, among other things, a recently discovered statement made to the police in 1972. The superior court denied the motion. As to the police statement, the judge found that it did not constitute newly discovered evidence because Defendant failed to establish that defense counsel did not have possession of it at the time of trial. The Supreme Judicial Court reversed and remanded the case for a new trial, holding (1) Defendant sustained his burden of establishing that defense counsel did not have the 1972 police statement prior to or at trial, and therefore, the statement constituted newly discovered evidence; and (2) there was a substantial risk that the jury would have reached a different conclusion had the evidence been admitted at trial.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. McCarthy

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12750
Opinion Date: April 16, 2020
Judge: Gaziano
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Judicial Court affirmed the judgment of the district court denying Defendant's motions to suppress, holding that the limited use of automatic license plate readers (ALPRs) in this case did not implicate constitutional protections against unreasonable searches. While police were investigating Defendant on suspicion of drug distribution they used ALPRs on two bridges to track Defendant's movements. The police accessed historical data via ALPR technology and received real-time alerts, the last of

which led to Defendant's arrest. Defendant filed motions to suppress the ALPR data and the fruits of the arrest. The superior court denied the motions. The Supreme Judicial Court affirmed, holding that while the widespread use of ALPRs in the Commonwealth could implicate a defendant's constitutional protected expectation of privacy in the whole of his public movements, that interest was not invaded by the limited extent and use of the ALPR data in the instant case.

Read Opinion Are you a lawyer? **Annotate this case**.

Garden v. Commonwealth

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12821
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed the judgment of a single justice of the court denying Petitioner's petition for extraordinary relief under Mass. Gen. Laws ch. 211, 3 seeking an order vacating Petitioner's plea to aggravated rape and dismissing the underlying indictment, holding that the single justice did not err or abuse his discretion in denying relief. The issues raised by Petitioner had all been raised and adjudicated through the normal appellate process. Petitioner then filed a motion to withdraw his guilty plea. The motion was denied, and the Appeals Court affirmed. In this petition for extraordinary relief, Petitioner sought an order vacating his plea to aggravated rape and dismissing the underlying indictment. The single justice denied relief. The Supreme Judicial Court affirmed, holding that the superintendence power was not available as an additional layer of appellate review once all other avenues had been exhausted.

Read Opinion Are you a lawyer? **Annotate this case**.

In re Mitchell

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12910
Opinion Date: April 22, 2020

Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed the judgment of the county court denying, without a hearing, Petitioner's petition for relief under Mass. Gen. Laws ch. 211, 3, holding that the single justice did not err or abuse his discretion in denying relief. Defendant was convicted of several offenses. The Appeals Court reversed the convictions and remanded the matter for a new trial. Thereafter, the Commonwealth filed a nolle prosequi as to all the charges. In his Mass. Gen. Laws ch. 211, 3 petition, Defendant alleged that no crime had been committed and that he was wrongfully prosecuted. The single justice denied relief. The Supreme Judicial Court affirmed, holding that Defendant did not demonstrate entitlement to the exercise of this Court's superintendence powers.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Reek

Court: Minnesota Supreme Court
Docket: A19-0153
Opinion Date: April 22, 2020
Judge: G. Barry Anderson
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction for first-degree murder, holding that there was no error in the proceedings below. Specifically, the Supreme Court held (1) Appellant's right to a fair trial before an impartial tribunal was not violated when the district court stated that it might reconsider its prior Spreigl ruling if the defense presented certain witnesses; (2) the jury instructions on accomplice liability were plainly erroneous, but Appellant failed to establish that there was a reasonable likelihood that the error had a significant effect on the verdict; (3) the prosecutor did not commit misconduct in his closing arguments regarding the law of accomplice liability; (4) the district court did not abuse its discretion by granting the State’s motion to admit evidence of appellant’s past convictions for impeachment purposes, including by allowing the specific convictions to be disclosed to the jury; and (5) Appellant’s pro se arguments were without merit.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Woodard

Court: Minnesota Supreme Court
Docket: A18-1886
Opinion Date: April 22, 2020
Judge: Hudson
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the district court convicting Defendant of first-degree murder and sentencing him to life in prison without the possibility of release, holding that the district court did not err in denying Defendant's motion to present an alternative-perpetrator defense. Specifically, the Supreme Court held (1) the district court did not abuse its discretion in holding that Defendant's proffered evidence in support of his motion to present alternative-perpetrator evidence for lack of sufficient foundation; and (2) the district court committed an error that was plain in instructing the jury on the order in which to consider the charges against Defendant, but there was no reasonable likelihood that the instruction affected the jury's verdict and therefore did not affect Defendant's substantial rights.

Read Opinion Are you a lawyer? **Annotate this case**.

Huff v. Brown

Court: Nebraska Supreme Court
Citation: 305 Neb. 648
Opinion Date: April 23, 2020
Judge: Lindsey Miller-Lerman
Areas of Law: Communications Law, Criminal Law

The Supreme Court reversed the portion of the district court's order granting in part a writ of mandamus requiring Doug Brown, the sheriff of Furnas County, to provide records to Herchel Huff pursuant to the public records statutes, holding that the district court erred when it determined that Huff had shown that Brown had a clear duty to provide the requested records. Huff, an inmate, sought, among other documents, the criminal history

records of jurors who had convicted hims. Furnas County sheriff Kurt Kapperman required a deposit of $750 before fulfilling the request. Huff subsequently filed a petition for writ of mandamus naming Kapperman as the defendant and seeking an order compelling Kapperman to release all requested documents. The court permitted Huff to substitute Brown, the current sheriff, in the caption of the case in place of Kapperman and granted in part mandamus. The Supreme Court reversed in part, holding that the district court (1) did not err when it substituted Brown's name for Kapperman's; but (2) erred in issuing mandamus because Huff failed to demonstrate a prima facie case that he had been denied a request for public records that the sheriff had a clear duty to provide under Neb. Rev. Stat. 84-712.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Montoya

Court: Nebraska Supreme Court
Citation: 305 Neb. 581
Opinion Date: April 17, 2020
Judge: Freudenberg
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the judgment of the district court affirming Defendant's conviction and sentence for driving under the influence, holding that there was no error in the challenged rulings by the trial court. Specifically, the Supreme Court held that the district court did not err by (1) affirming the county court's order denying Defendant's motion to suppress fruits of the stop; (2) affirming the county court's order that denied Defendant's motion to suppress the fruits of his arrest; (3) affirming the county court's order that denied Defendant's motion to suppress the results of the test of his breath alcohol content; (4) finding sufficient evidence to support the conviction; and (5) finding that Defendant's sentence was not excessive.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Schroeder

Court: Nebraska Supreme Court
Citation: 305 Neb. 527
Opinion Date: April 17, 2020
Judge: Funke
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's sentence of death for first degree murder, holding that there was no error in the sentence imposed by the sentencing panel. Specifically, the Supreme Court held that the sentencing panel did not err in (1) allowing the State to introduce evidence on the existence of mitigating circumstances; (2) acknowledging and weighing mitigating evidence from the presentence investigation report; (3) not requesting that documentation from the Department of Correctional Services regarding Defendant's time in custody for mitigation purposes be included in the presentence investigation report; (4) sentencing Defendant to death, where the Legislature has enacted safeguards to ensure fairness and accuracy in the resulting sentence; and (5) finding Defendant should be sentenced to death after balancing the aggravating evidence and mitigating evidence.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Kendrick v. Parker

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1509
Opinion Date: April 21, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals denying Appellant's request for a writ of prohibition and/or mandamus against Montgomery County Court of Common Pleas Judge E. Gerald Parker Jr., holding that the court of appeals correctly determined that Appellant's claim was barred by res judicata. Appellant sought a petition for writ of prohibition and/or mandamus against Judge Erik Blaine, the successor to the judge who sentenced Appellant, alleging that the sentencing court patently and unambiguously lacked jurisdiction to sentence him. Judge Parker, who had succeeded Judge Blaine, subsequently filed a motion for summary judgment. The court of appeals granted summary judgment for Judge

Parker, concluding that Appellant failed to demonstrate that the sentencing court patently and unambiguously lacked jurisdiction or that he lacked an adequate remedy at law and that res judicata barred Appellant's claim. The Supreme Court affirmed, holding that Appellant's claim was barred by res judicata.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Nelson v. Russo

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1541
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals dismissing Appellant's petition for a writ of mandamus seeking to compel Cuyahoga County Court of Common Pleas Judge Nancy Margaret Russo to vacate the consecutive prison sentences imposed on Appellant in 1987, holding that Appellant had an adequate remedy at law and was barred from asserting additional claims of sentencing error he could have raised in his previous mandamus action. In 1987, Appellant was convicted of four counts of rape and one count of kidnapping. Appellant was sentenced to prison terms of fifteen to twenty-five years for each of the five counts, to be served consecutively. In 2019, Appellant sought a writ of mandamus to compel Judge Russo to vacate his consecutive sentences. The court of appeals dismissed the writ action, concluding that res judicata barred Appellant's claim and that his prior appeals were an adequate remedy at law to address the alleged defect in his consecutive sentences. The Supreme Court affirmed, holding that Appellant was not entitled to a writ of mandamus in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Roberts v. Marsh

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1540

Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals dismissing Appellant's original action seeking a writ of procedendo and/or mandamus to compel Hamilton County Court of Common Pleas Judge Melba Marsh to issue a corrected sentencing entry, holding that the court of appeals correctly dismissed the petition as moot. Appellant was convicted of murder with a repeat-violent-offender specification. Appellant later asked the trial court to correct his sentence, arguing that he had improperly been sentenced to postrelease control. On remand, Judge Marsh vacated the postrelease-control sentence. Appellant appealed that order. The court of appeals noted that the trial court had not set forth all the information required under Crim.R. 32(C) in a single document and dismissed the appeal for lack of a final, appealable order. Appellant then filed this original action seeking to compel Judge Marsh to issue a corrected sentencing entry that constitutes a final, appealable order. Judge Marsh issued a nunc pro tunc sentencing entry that constituted a final, appealable order. The court of appeals then dismissed the petition as moot. The Supreme Court affirmed, holding that because Judge Marsh performed the act Appellant requested, the court of appeals dismissed the petition as moot.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Steiner v. Rinfret

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1510
Opinion Date: April 21, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals dismissing Appellant's petition for a writ of mandamus against Holmes County Court of Common Pleas Judge Robert D. Rinfret, holding that the court of appeals correctly determined that Appellant had an adequate remedy in the ordinary course of the law. Appellant, who was serving consecutive prison terms for five convictions, filed a petition for a writ of mandamus arguing that Judge Rinfret improperly sentenced him to a prison

term of nine years for his attempted rape conviction instead of the maximum term of eleven years. The court of appeals dismissed the petition, determining that Appellant had failed to file a mandatory affidavit of his prior civil actions and had an adequate remedy in the ordinary course of the law. The Supreme Court affirmed, holding that relief in mandamus was not available because Petitioner had an adequate remedy in the ordinary course of the law.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Jeffries

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1539
Opinion Date: April 22, 2020
Judge: Donnelly
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals upholding Defendant's convictions of four counts related to two specific instances of sexual abuse of D.S., holding that the trial court and court of appeals correctly applied Ohio's rape-shield law and determined that evidence of D.S.'s prior nonconsensual sexual assault was inadmissible. On appeal, Defendant asserted that the trial court erred in prohibiting him from introducing evidence during trial that D.S. had previously been sexually assaulted by another person, arguing that the rape-shield law applies only to an accuser's prior consensual sexual activity. The lower court held that Ohio's rape-shield law addresses all sexual activity, not only consensual sexual activity. The court of appeals affirmed. The Supreme Court affirmed, holding (1) the plain meaning of the term "sexual activity" as used in the rape-shield law includes both consensual and nonconsensual sexual activity; and (2) therefore, all sexual activity is barred from admission into evidence by the rape-shield, absent certain exceptions listed in the law.

Read Opinion Are you a lawyer? **Annotate this case**.

Pennsylvania v. Britton

Court: Supreme Court of Pennsylvania

Docket: 55 MAP 2018
Opinion Date: April 22, 2020
Judge: Max Baer
Areas of Law: Constitutional Law, Criminal Law

California law enforcement officers interviewed Appellant Stacy Britton in her California residence and, unbeknownst to her, recorded those interviews. Over Appellant's objection, Pennsylvania used those recordings as evidence to help convict Appellant of murder in Pennsylvania. The Pennsylvania Supreme Court granted allowance of appeal to examine whether the California law enforcement officers were acting as agents of the Pennsylvania State Police when they recorded the interviews with Appellant in her California home, and if so, whether Pennsylvania's constitutional and statutory protections were available to Appellant under those circumstances. The Court concluded the California law enforcement officers were not acting as agents of the Pennsylvania State Police when they interviewed Appellant, making analysis of whether any Pennsylvania-specific constitutional or statutory protections unwarranted. Because the Supreme Court concluded the Pennsylvania trial court reached the proper result in this matter, it affirmed that court's judgment.

Read Opinion Are you a lawyer? **Annotate this case**.

Pennsylvania v. Copenhaver

Court: Supreme Court of Pennsylvania
Docket: 48 MAP 2019
Opinion Date: April 22, 2020
Judge: Thomas G. Saylor
Areas of Law: Constitutional Law, Criminal Law

In August 2015, a deputy sheriff conducted a vehicle stop of Appellant Victor Copenhaver's pickup truck. Upon approaching the truck, the deputy noticed an odor of alcohol and marijuana emanating from the passenger compartment. After administering field sobriety tests, he arrested Appellant for suspected driving under the influence of alcohol and controlled substances ("DUI"). Appellant was ultimately charged with DUI and other offenses. Appellant challenged the deputy's authority to conduct a traffic stop and sought suppression of all evidence obtained during the encounter. Rather than presenting testimony at a suppression hearing, the parties

stipulated that Appellant was driving the vehicle in question and that the deputy had training and qualifications equivalent to that of a police officer. The parties also agreed that the vehicle stop occurred as a result of the deputy observing the tailgate to the pickup truck being in a down position, which caught the deputy's attention. The deputy further observed the registration on the pickup truck was expired, and additionally, the registration number was identified as belonging to a vehicle other than the one on which it was attached. The issue this case presented for the Pennsylvania Supreme Court's review was whether the deputy could lawfully conduct the traffic stop based on the expired registration sticker, on a theory that such a violation amounts to a breach of the peace. The Supreme Court concluded driving a vehicle with an expired registration did not entail a breach of the peace. It vacated the superior court's order insofar as it held that the expired registration was a breach of the peace, thus alone authorizing the deputy to stop Appellant's vehicle. Notably, in light of its holding, the Supreme Court found the superior court did not proceed to consider other relevant questions, such as whether the parties' factual stipulation should have been read as indicating that the officer's understanding that the registration sticker was associated with a different vehicle arose in the pre-stop timeframe – consistent with the Commonwealth's position throughout this litigation. "These issues should be resolved in the first instance by the intermediate court on remand."

Read Opinion Are you a lawyer? **Annotate this case**.

Pennsylvania v. Tedford

Court: Supreme Court of Pennsylvania
Docket: 773 CAP
Opinion Date: April 22, 2020
Judge: Donohue
Areas of Law: Constitutional Law, Criminal Law

Appellant Donald Tedford was convicted of first-degree murder and rape on February 6, 1987. He appealed the dismissal of his second petition for relief filed pursuant to the Post Conviction Relief Act ("PCRA"), on December 2, 2014, as amended by a counseled petition on May 5, 2015, and a supplemental petition filed on June 9, 2015. In connection with his initial filings, Tedford sought wholesale discovery of the prosecution's entire file,

but the PCRA court concluded that the petition (as amended) was not timely filed. Tedford also appealed the PCRA court's order denying his supplemental PCRA petition, in which he requested discovery, an evidentiary hearing, and/or a new trial based upon the admission of expert testimony presented at trial related to microscopic hair analysis. The PCRA court concluded that pursuant to PCRA Section 9545(b)(1)(ii), it had jurisdiction to consider the merits of Tedford's newly-discovered-facts claims, but ultimately it concluded Tedford had not asserted a meritorious claim in accordance with Section 9543(a)(2)(vi). Finding no reversible error in that analysis, the Pennsylvania Supreme Court affirmed dismissal of the petition for relief.

Read Opinion Are you a lawyer? **Annotate this case**.

Pennsylvania v. Trahey

Court: Supreme Court of Pennsylvania
Docket: 38 EAP 2018
Opinion Date: April 22, 2020
Judge: Wecht
Areas of Law: Constitutional Law, Criminal Law

The trial court granted Timothy Trahey's motion to suppress the results of a blood test that revealed his blood alcohol concentration ("BAC"), finding no justification for the investigating officers' failure to obtain a search warrant before conducting the test. On the Commonwealth's appeal, the Superior Court reversed, opining that the Commonwealth's evidence sufficiently established the existence of exigent circumstances, thus excusing the absence of a warrant. The Pennsylvania Supreme Court reversed, finding that while the exigency analysis is an objective one, "even disregarding the officers' subjective motivations, or their candid acknowledgment that they would have obtained a search warrant if they thought it necessary, there was no time-sensitive need to conduct a warrantless blood test under the circumstances of this case. Accordingly, the Superior Court's conclusion that the test was justified by exigent circumstances was drawn in error."

Read Opinion Are you a lawyer? **Annotate this case**.

In re Greg Abbott

Court: Supreme Court of Texas
Docket: 20-0291
Opinion Date: April 23, 2020
Judge: Per Curiam
Areas of Law: Constitutional Law, Criminal Law

The Supreme Court conditionally granted mandamus relief to the State seeking review of a temporary restraining order (TRO) blocking enforcement of Executive Order GA-13, which changes the rules applicable to judges' decisions regarding pre-trial bail, against judges, holding that the trial court lacked jurisdiction to order the judges' requested relief, even temporarily. GA-13 suspends certain statutes authorizing trial judges to release jail inmates with violent histories during the state of disaster due to the threat of the novel coronavirus. Plaintiffs alleged that GA-13 is unconstitutional and exceeds the governor's statutory emergency powers. Sixteen of the plaintiffs were Texas trial judges alleging that GA-13 improperly interferes with their judicial authority to make individualized bail decisions, and the other plaintiffs were public interest organizations and lawyer associations. The trial court issued a TRO blocking enforcement of GA-13 against judges. The Supreme Court conditionally granted mandamus relief, holding that the alleged threat of a criminal prosecution in this case did not give the judges standing to seek the invalidation of GA-13, and therefore, the trial court lacked jurisdiction to order their requested relief.

Read Opinion Are you a lawyer? **Annotate this case**.

Stahmann v. Texas

Court: Texas Court of Criminal Appeals
Docket: PD-0556-18
Opinion Date: April 22, 2020
Judge: Barbara Hervey
Areas of Law: Constitutional Law, Criminal Law

Appellant Karl Stahmann was involved in an automobile accident, after which he threw a bottle of promethazine, a controlled substance, over a nearby wire fence before law enforcement arrived. The bottle landed two to three feet past the fence in plain view. He was convicted of third-degree

felony tampering with physical evidence and was sentenced to 10 years' confinement and fined $5,000. The judge suspended his sentence and placed him on community supervision for 10 years. Stahmann appealed, arguing in part that the evidence was insufficient to prove that he destroyed, altered, or concealed the prescription bottle. The court of appeals agreed that the evidence was insufficient, but instead of rendering an acquittal, it reformed the judgment to show that Stahmann was convicted of the lesser-included offense of attempted tampering with physical evidence, a state-jail felony. After review of the evidence presented at trial, the Texas Court of Criminal Appeals concluded the evidence was indeed insufficient to prove that Appellant altered the prescription pill bottle when he threw it over the fence because the mere act of throwing the bottle did not change the bottle itself. "While a rational jury could have reasonably inferred that Stahmann intended to conceal the pill bottle when he threw it over the wire fence, the evidence shows that he failed to conceal it as he intended because the bottle landed short of the bush in plain view on top of some grass." The Court affirmed the trial court's judgment.

Read Opinion Are you a lawyer? **Annotate this case**.

Blanke v. Board of Pardons & Parole

Court: Utah Supreme Court
Citation: 2020 UT 16
Opinion Date: April 16, 2020
Judge: Himonas
Areas of Law: Criminal Law

The Supreme Court affirmed the decision of the court of appeals affirming the district court's denial of Appellant's petition for extraordinary relief, holding that, under the circumstances, the Utah Board of Pardons and Parole need not afford Appellant the due process protections explained in Neese v. Utah Board of Pardons and Parole, 416 P.3d 663 (2017), before it could determine that Appellant was a sex offender and condition his parole on sex offender treatment. Appellant was serving a prison sentence for his convictions of attempted child kidnapping and kidnapping. Because he was convicted of attempted child kidnapping Appellant was considered a sex offender under the sex offender registration statute. Further, Appellant admitted in his presentence report that he had sexual intercourse with a

fifteen-year-old. Appellant filed a petition for extraordinary relief alleging that the Parole Board had violated his due process rights by conditioning his parole on completion of sex offender treatment even though he had not committed a sex offense. Summary judgment was granted for the Parole Board. The Supreme Court affirmed, holding that the Parole Board owed Appellant no additional process before it considered unconnected sex offenses in its decision to require Appellant to undergo sex offender treatment.

Read Opinion Are you a lawyer? **Annotate this case**.

Washington v. Escalante

Court: Washington Supreme Court
Docket: 97268-1
Opinion Date: April 23, 2020
Judge: Steven González
Areas of Law: Constitutional Law, Criminal Law

Alejandro Escalante was detained for hours in a secured area at a border crossing and, the State conceded, interrogated by federal agents without Miranda warnings. Statements he made during that interrogation were used by the State to convict him of drug possession. While a traveler briefly detained and questioned at the border was typically not "in custody" for Miranda purposes, "the government's power to detain and question people at the border without implicating Miranda has limits." Here, the Washington Supreme Court determined those limits were reached. "This border detention created the type of inherently coercive environment that demands Miranda warnings to ensure an individual's choice to speak is the product of free will." The Supreme Court held that Escalante was in custody when he was interrogated and reversed.

Read Opinion Are you a lawyer? **Annotate this case**.

Washington v. Haggard

Court: Washington Supreme Court
Docket: 97375-0
Opinion Date: April 23, 2020

Judge: Barbara Madsen
Areas of Law: Constitutional Law, Criminal Law

A class C felony "washes out" and is omitted from a defendant's offender score as long as he or she is not convicted of any crime within five years of the last date of release from confinement. David Haggard was convicted of a misdemeanor offense within this five-year period, which was dismissed pursuant to RCW 3.66.067. When Haggard later pleaded guilty to burglary and arson, the trial court included prior class C felonies in his criminal history, finding that the dismissed misdemeanor conviction interrupted the washout period for those offenses. Haggard contended on appeal this was error. The Washington Supreme Court determined that because a dismissed conviction constituted a "conviction" under the Sentencing Reform Act of 1981 (SRA), and misdemeanor dismissal and vacation were distinct processes, so Haggard's offender score was properly calculated.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Taylor

Court: Supreme Court of Appeals of West Virginia
Docket: 18-0502
Opinion Date: April 21, 2020
Judge: Walker
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the judgment of the circuit court giving Petitioner credit for twelve days of time served toward the sentence he received for his felony conviction although Petitioner spent additional time in confinement for other charges that were dismissed in the universal plea agreement, holding that to grant Petitioner additional credit for time served would do little more than reward Petitioner for habitual criminal behavior. Petitioner was charged with several crimes and agreed to resolve the pending charges against him in a universal plea agreement. Under the terms of the agreement, Petitioner agreed to plea guilty to the charge of felony carrying a concealed firearm by a prohibited person. In exchange, the State agreed to drop the remaining charges. After he was sentenced, Petitioner argued that, in addition to the twelve days of credit for time served he was granted, he was constitutionally entitled to credit for time served

while he was incarcerated for charges that were resolved in the universal plea agreement. The Supreme Court affirmed, holding that Petitioner's circumstances implicated neither double jeopardy nor equal protection of the law such that additional credit for time served was constitutionally mandated.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Harrison

Court: Wisconsin Supreme Court
Dockets: 2017AP002441-CR, 2017AP002440-CR
Opinion Date: April 17, 2020
Judge: Patience D. Roggensack
Areas of Law: Criminal Law

The Supreme Court affirmed in part and reversed in part the decision of the court of appeals reversing an order of the circuit court that granted sentence credit to Defendant, holding that the court of appeals correctly found that Defendant was not entitled to sentence credit but erred by advancing the commencement of Defendant's terms of extended supervision for Defendant's 2007 and 2008 cases. Specifically, the Court held (1) Defendant was not entitled to sentence credit under Wis. Stat. 973.155(1)(a) because the days he spent in custody for which he sought sentence credit were not in connection with the courses of conduct for which those sentences were imposed; and (2) the court of appeals erred by advancing the commencement of Defendant's terms of extended supervision for his 2007 and 2008 cases to the date they would have begun but for Defendant's confinement for unrelated convictions that were later set aside, holding that whether to employ advancement is a public policy decision best left to the legislature.

Read Opinion Are you a lawyer? **Annotate this case**.

About Justia Opinion Summaries

Justia Weekly Opinion Summaries is a free service, with 63 different

newsletters, each covering a different practice area.

Justia also provides 68 daily jurisdictional newsletters, covering every federal appellate court and the highest courts of all US states.

All daily and weekly Justia newsletters are free. Subscribe or modify your newsletter subscription preferences at daily.justia.com.

You may freely redistribute this email in whole.

About Justia

Justia is an online platform that provides the community with open access to the law, legal information, and lawyers.



Contact Us | Privacy Policy

Unsubscribe From This Newsletter
or unsubscribe from all Justia newsletters immediately **here.**



Justia | 1380 Pear Ave #2B, Mountain View, CA 94043

From: Criminal Law - Justia Weekly Opinion Summaries
To: Sullivan, Kristen (POL)
Subject: Latest 101 Cases This Week: Ramos v. Louisiana (U.S.), United States v. Diaz-Rivera (1st Cir.), United States v. Cotto (2d Cir.)
Date: Friday, April 24, 2020 9:02:18 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

If you are unable to see this message, click here to view it in a web browser.

Justia Weekly Opinion Summaries

Criminal Law
April 24, 2020

Table of Contents

Ramos v. Louisiana
Civil Rights, Constitutional Law, Criminal Law
US Supreme Court

United States v. Diaz-Rivera
Criminal Law
US Court of Appeals for the First Circuit

United States v. Cotto
Criminal Law
US Court of Appeals for the Second Circuit

United States v. Rosa
Criminal Law
US Court of Appeals for the Second Circuit

Fogle v. Sokol
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Third Circuit

James v. New Jersey State Police
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Third Circuit

Bazemore v. Best Buy
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Akande
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Chambers
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Ferebee
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Nance
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Johnson
Criminal Law
US Court of Appeals for the Fifth Circuit

United States v. McGinnis
Criminal Law
US Court of Appeals for the Fifth Circuit

Valentine v. Collier
Civil Rights, Constitutional Law, Criminal Law, Government & Administrative Law, Health Law
US Court of Appeals for the Fifth Circuit

United States v. Dowl
Criminal Law
US Court of Appeals for the Sixth Circuit

United States v. Fowler
Criminal Law
US Court of Appeals for the Sixth Circuit

United States v. Sumlin
Criminal Law
US Court of Appeals for the Sixth Circuit

United States v. Vance
Criminal Law, White Collar Crime
US Court of Appeals for the Sixth Circuit

Winburn v. Nagy
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Sixth Circuit

Lund v. City of Rockford
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

United States v. Perez
Criminal Law
US Court of Appeals for the Seventh Circuit

Jackson v. United States
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Bolman
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Boyd
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Gonzalez-Esparsa
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Sanchez-Velasco
Criminal Law, Immigration Law
US Court of Appeals for the Eighth Circuit

Anthony v. TRAX International Corp.
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Ninth Circuit

City of Almaty v. Khrapunov
Criminal Law, International Law, White Collar Crime
US Court of Appeals for the Ninth Circuit

United States v. Baldon
Criminal Law
US Court of Appeals for the Ninth Circuit

United States v. Costanzo
Criminal Law
US Court of Appeals for the Ninth Circuit

United States v. Manzanares
Constitutional Law, Criminal Law
US Court of Appeals for the Tenth Circuit

United States v. Delaney
Criminal Law
US Court of Appeals for the District of Columbia Circuit

Antenor v. Alaska, Department of Corrections
Civil Procedure, Criminal Law, Government & Administrative Law
Alaska Supreme Court

Berger v. Bryant
Criminal Law
Arkansas Supreme Court

Carroll v. State
Criminal Law
Arkansas Supreme Court

Cave v. State
Civil Rights, Constitutional Law, Criminal Law
Arkansas Supreme Court

Chatmon v. Kelley
Criminal Law
Arkansas Supreme Court

McClinton v. State
Criminal Law
Arkansas Supreme Court

Siegel v. State
Criminal Law
Arkansas Supreme Court

Thomas v. State
Civil Rights, Constitutional Law, Criminal Law
Arkansas Supreme Court

California v. Landowski
Constitutional Law, Criminal Law
California Courts of Appeal

California v. May
Constitutional Law, Criminal Law
California Courts of Appeal

California v. Perez
Constitutional Law, Criminal Law
California Courts of Appeal

In re S.R.
Criminal Law
California Courts of Appeal

People v. Bell
Criminal Law
California Courts of Appeal

People v. Drayton
Criminal Law
California Courts of Appeal

People v. Robinson
Criminal Law
California Courts of Appeal

People v. Torres
Criminal Law
California Courts of Appeal

Colorado v. Lujan
Constitutional Law, Criminal Law
Colorado Supreme Court

Archer v. State
Civil Rights, Constitutional Law, Criminal Law
Florida Supreme Court

Collins v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Heyward v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Howard v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Keller v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Mills v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Moore v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Morris v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Rickman v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Robinson v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Santana v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Sullivan v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Turner v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Valrie v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Williams v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

State v. Malave
Criminal Law
Supreme Court of Hawaii

State v. Malave
Criminal Law
Supreme Court of Hawaii

Idaho v. Burke
Constitutional Law, Criminal Law
Idaho Supreme Court - Criminal

State v. Gibbs
Civil Rights, Constitutional Law, Criminal Law
Iowa Supreme Court

State v. Broxton
Criminal Law
Kansas Supreme Court

State v. Corbin
Criminal Law
Kansas Supreme Court

State v. Frazier
Criminal Law
Kansas Supreme Court

State v. Harris
Civil Rights, Constitutional Law, Criminal Law
Kansas Supreme Court

State v. Uk
Criminal Law
Kansas Supreme Court

State v. Catruch
Criminal Law
Maine Supreme Judicial Court

State v. Paquin
Constitutional Law, Criminal Law
Maine Supreme Judicial Court

Watson v. State
Criminal Law
Maine Supreme Judicial Court

Commonwealth v. Mazza
Criminal Law
Massachusetts Supreme Judicial Court

Commonwealth v. McCarthy
Civil Rights, Constitutional Law, Criminal Law
Massachusetts Supreme Judicial Court

Garden v. Commonwealth
Criminal Law
Massachusetts Supreme Judicial Court

In re Mitchell
Criminal Law
Massachusetts Supreme Judicial Court

State v. Reek
Civil Rights, Constitutional Law, Criminal Law
Minnesota Supreme Court

State v. Woodard
Criminal Law
Minnesota Supreme Court

Huff v. Brown
Communications Law, Criminal Law
Nebraska Supreme Court

State v. Montoya
Civil Rights, Constitutional Law, Criminal Law
Nebraska Supreme Court

State v. Schroeder
Criminal Law
Nebraska Supreme Court

State ex rel. Kendrick v. Parker
Criminal Law
Supreme Court of Ohio

State ex rel. Nelson v. Russo
Criminal Law
Supreme Court of Ohio

State ex rel. Roberts v. Marsh
Criminal Law
Supreme Court of Ohio

State ex rel. Steiner v. Rinfret
Criminal Law
Supreme Court of Ohio

State v. Jeffries
Criminal Law
Supreme Court of Ohio

Pennsylvania v. Britton
Constitutional Law, Criminal Law
Supreme Court of Pennsylvania

Pennsylvania v. Copenhaver
Constitutional Law, Criminal Law
Supreme Court of Pennsylvania

Pennsylvania v. Tedford
Constitutional Law, Criminal Law
Supreme Court of Pennsylvania

Pennsylvania v. Trahey
Constitutional Law, Criminal Law
Supreme Court of Pennsylvania

In re Greg Abbott
Constitutional Law, Criminal Law
Supreme Court of Texas

Stahmann v. Texas
Constitutional Law, Criminal Law
Texas Court of Criminal Appeals

Blanke v. Board of Pardons & Parole
Criminal Law
Utah Supreme Court

Washington v. Escalante
Constitutional Law, Criminal Law
Washington Supreme Court

Washington v. Haggard
Constitutional Law, Criminal Law
Washington Supreme Court

State v. Taylor
Civil Rights, Constitutional Law, Criminal Law
Supreme Court of Appeals of West Virginia

State v. Harrison
Criminal Law
Wisconsin Supreme Court

COVID-19 Updates: Law & Legal Resources Related to Coronavirus

Click here to remove Verdict from subsequent Justia newsletter(s).

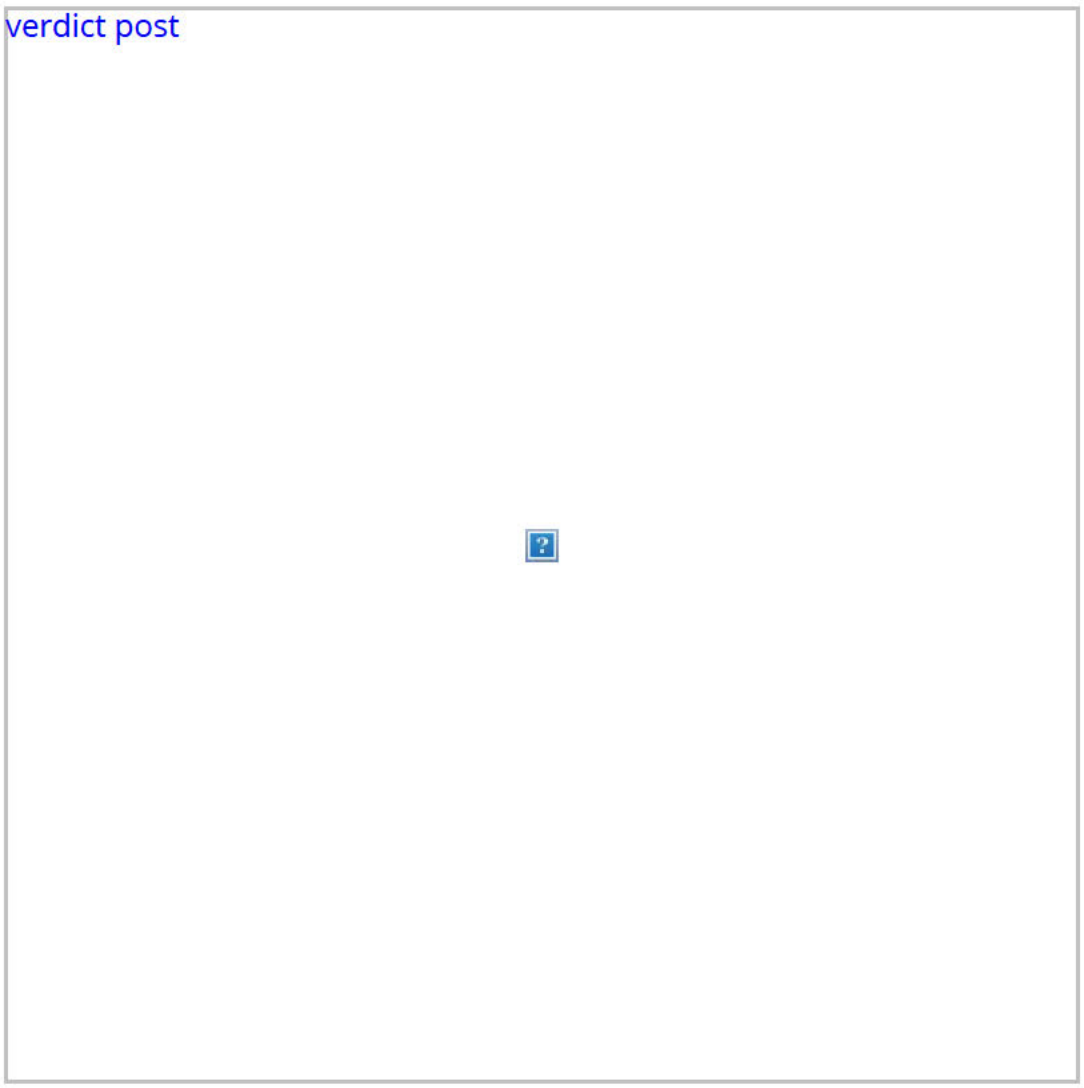
New on Verdict

Legal Analysis and Commentary

Rethinking Retroactivity in Light of the Supreme Court's Jury Unanimity Requirement

MICHAEL C. DORF

verdict post



In light of the U.S. Supreme Court's decision Monday in *Ramos v. Louisiana*, in which it held that the federal Constitution forbids states from convicting defendants except by a unanimous jury, Cornell law professor Michael C. Dorf discusses the Court's jurisprudence on retroactivity. Dorf highlights some costs and benefits of retroactivity and argues that the Court's refusal to issue advisory opinions limits its ability to resolve retroactivity questions in a way that responds to all the relevant considerations.

Read More

Criminal Law Opinions

Ramos v. Louisiana

Court: US Supreme Court
Docket: 18-5924
Opinion Date: April 20, 2020
Judge: Neil M. Gorsuch
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

In 48 states and in federal court, a single juror's vote to acquit is enough to prevent a conviction; Louisiana and Oregon punish people based on 10-to-2 verdicts. Ramos was convicted in a Louisiana court by a 10-to-2 jury verdict and was sentenced to life without parole. The Supreme Court reversed. The Sixth Amendment right to a jury trial, as incorporated against the states by the Fourteenth Amendment, requires a unanimous verdict to convict a defendant of a serious offense. Juror unanimity is a vital common law right. The Court rejected an "invitation" to "perform a cost-benefit analysis on the historic features of common law jury trials and to conclude that unanimity does not make the cut." In overturning its 1972 "Apodaca" decision, the Court stated that the reasoning, in that case, was "gravely mistaken" and "sits uneasily with 120 years of preceding case law." The fact that Louisiana and Oregon may need to retry defendants convicted of felonies by non-unanimous verdicts whose cases are still pending on direct appeal "will surely impose a cost, but new rules of criminal procedure usually do."

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Diaz-Rivera

Court: US Court of Appeals for the First Circuit
Docket: 18-1461
Opinion Date: April 20, 2020
Judge: Torruella
Areas of Law: Criminal Law

The First Circuit affirmed Defendant's upwardly variant sentence for one count of possession with intent to distribute cocaine and one count of using a firearm during and in relation to a drug-trafficking crime, holding that the sentence was neither procedurally nor substantively unreasonable. Pursuant to a plea agreement, Defendant pled guilty to drug-related crimes. After a sentencing hearing, the district court sentenced Defendant to an upwardly variant sentence of 180 months of imprisonment, thus declining to

impose the government's requested sentence. On appeal, Defendant challenged both the procedural and substantive reasonableness of his sentence. The First Circuit affirmed, holding that the 180-month sentence was neither procedurally nor substantively unreasonable.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Cotto

Court: US Court of Appeals for the Second Circuit
Docket: 18-2970
Opinion Date: April 20, 2020
Judge: Leval
Areas of Law: Criminal Law

A conviction for retaliating against a witness in violation of 18 U.S.C. 1513 does not require that the Government prove that defendant had knowledge of the federal nature of the proceeding. The Second Circuit rejected defendant's arguments to the contrary and affirmed his conviction for retaliating against a witness. The court remanded for revision of the provision of the sentence relating to the substance abuse treatment condition of supervised release; instructed the district court to consider on remand whether the court's forthcoming order in United States v. Traficante, No. 18-1962 (2d Cir., submitted Oct. 25, 2019) requires modification of the risk notification provision of supervised release; and granted the parties leave to reinstate this appeal to permit review of the district court's decision on remand as to the risk notification provision.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Rosa

Court: US Court of Appeals for the Second Circuit
Docket: 17-2004
Opinion Date: April 17, 2020
Judge: Nardini
Areas of Law: Criminal Law

Where a district court offers no explanation for its sentence, and where neither the adopted presentence report nor the statement of reasons

adequately demonstrates the court's reasoning, the court has committed plain error in violation of 18 U.S.C. 3553(c). The Second Circuit vacated defendant's sentence for conspiracy to commit wire fraud and aggravated identity theft. The court held that the district court failed to state its reasons for sentencing defendant as required under section 3553(c); the error is clear or obvious; and the error affected defendant's substantial rights. Accordingly, the court remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

Fogle v. Sokol

Court: US Court of Appeals for the Third Circuit
Docket: 19-1066
Opinion Date: April 21, 2020
Judge: Matey
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

In 1976, the body of 15-year-old “Kathy” was found near her Indiana County, Pennsylvania home. Kathy’s death involved a brutal assault, rape, and a gunshot to the head. Kathy's sisters, ages nine and 12, stated that she had gotten into a car with a man with blue eyes, black hair that came below his ears and curled at the ends, sideburns, heavy eyebrows, and a heavy mustache. Fogle had “straight reddish-blonde hair that dropped down his back and a matching, full beard that reached his waist.” After three years, Fogle became a suspect because a psychiatric patient described seeing Kathy get in a car with Fogle and his brother. The story was largely inconsistent with statements by Kathy’s sisters. Jailhouse informants were recruited and counseled by law enforcement with promises of leniency. The prosecutors “either knew about, encouraged, or permitted” this strategy. A jury found Fogle guilty of second-degree murder. In 2015, Fogle obtained DNA evidence excluding both himself and his brother as the source of semen collected from Kathy. His conviction was vacated. The Commonwealth declined to pursue new charges, describing the case as lacking “prosecutorial merit.” Fogle, having spent three decades in prison, sued the prosecutors and Indiana County under 42 U.S.C. 1983. The Third Circuit affirmed the denial of their motions to dismiss based on absolute immunity. Only truly prosecutorial functions, not investigative conduct, justify complete protection from suit. Fogle’s complaint alleges actions that fall

outside the narrow doctrine of absolute immunity.

Read Opinion Are you a lawyer? **Annotate this case**.

James v. New Jersey State Police

Court: US Court of Appeals for the Third Circuit
Docket: 18-1432
Opinion Date: April 21, 2020
Judge: Porter
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Stephens called 911 and reported that Gibbons hit her and had a gun in his truck. The police responded. Stephens obtained a temporary restraining order, prohibiting Gibbons from possessing firearms and from returning to Stephens's house. The next day, Gibbons went to Stephens's house. Stephens was talking on the phone; the friend called the police. Gibbons left Stephens's house. Trooper Conza arrived. Stephens stated that Gibbons had waved a gun throughout their argument. Conza told Stephens to go to the police barracks and reported over the radio that Gibbons had brandished a firearm. Conza, with Troopers Bartelt and Korejko, visited the nearby home of Gibbons's mother, James. James stated that she did not know where Gibbons was and that he might be off his schizophrenia medication. While driving to the barracks, Stephens saw Gibbons walking alongside the road and called 911. The Troopers responded. Bartelt parked his car and, exiting, observed that Gibbons was pointing a gun at his own head. Bartelt drew his weapon, stood behind his car door, and twice told Gibbons to drop his weapon. Gibbons did not comply. Bartelt shot Gibbons twice within seconds of stopping his car. Gibbons died that night. In James' suit under 42 U.S.C. 1983, the Third Circuit held that Bartelt is entitled to qualified immunity because he did not violate Gibbons's clearly established rights. Bartelt's pre-standoff knowledge of Gibbons differs from that of officers involved in cited cases. Bartelt could reasonably conclude that Gibbons posed a threat to others.

Read Opinion Are you a lawyer? **Annotate this case**.

Bazemore v. Best Buy

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-2196
Opinion Date: April 21, 2020
Judge: Quattlebaum
Areas of Law: Criminal Law

Plaintiff filed suit against her employer, Best Buy, claiming that she was harassed because of her race and gender and subjected to a hostile work environment in violation of Title VII of the Civil Rights Act of 1964. Plaintiff's complaint stemmed from an incident where a coworker made a racist and sexually charged joke to a small group of coworkers that included plaintiff. The Fourth Circuit affirmed the district court's motion to dismiss and held that, in the case of allegedly harassing comments by a co-worker, an employee must allege plausible facts that the employer knew, or should have known, about the harassment and failed to take action reasonably calculated to stop it. Because plaintiff failed to do this, the court affirmed the district court's judgment. In this case, the coworker's conduct was not imputable to Best Buy where Best Buy took steps that were not only reasonably calculated to end such behavior, but that it did in fact end it.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Akande

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-6833
Opinion Date: April 20, 2020
Judge: Diana Jane Gribbon Motz
Areas of Law: Criminal Law

After defendant moved under 28 U.S.C. 2255 to vacate his conviction based on the ineffective assistance of counsel, the district court denied the motion. The Fourth Circuit granted a certificate of appealability and reversed the district court's judgment. The court held that, given counsel's specific misadvice regarding defendant's rights to preserve his appellate rights, on which defendant understandably relied, the district court's general admonishments did not amount to the careful explanation that addresses the particular issue necessary to cure the error. In this case, the plea colloquy did not correct counsel's erroneous advice and the error prejudiced defendant. Accordingly, the court remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Chambers

Court: US Court of Appeals for the Fourth Circuit
Docket: 19-7104
Opinion Date: April 23, 2020
Judge: Floyd
Areas of Law: Criminal Law

After defendant was erroneously sentenced as a career offender, he moved to reduce his sentence to time served under the First Step Act. The district court denied defendant's motion to reduce his custodial sentence, though it granted the motion as to his supervised release term. The Fourth Circuit held that the First Step Act does not constrain courts from recognizing Guidelines errors. The court explained that First Step Act motions fall under 18 U.S.C. 3582(c)(1)(B), a distinct exception to finality, and that section 404(b) of the First Step Act expressly allows a court to impose a reduced sentence in order to give retroactive effect to sections 2 and 3 of the Fair Sentencing Act. Furthermore, 18 U.S.C. 3553(a) sentencing factors apply in the section 404(b) resentencing context, and the resentencing court has discretion within the section 404(b) framework to vary from the Guidelines and, in doing so, to consider movants' post-sentencing conduct. In this case, the district court seemingly believed that it could not vary from the Guidelines range to reflect post-sentencing information. Therefore, the court vacated the district court's sentencing order. Finally, the court held that any Guidelines error deemed retroactive, such as the error in this case, must be corrected in a First Step Act resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Ferebee

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-4266
Opinion Date: April 22, 2020
Judge: Traxler
Areas of Law: Criminal Law

The Fourth Circuit affirmed the denial of defendant's motion to suppress evidence recovered from a backpack, and the district court's conclusion that defendant abandoned the backpack and any legitimate expectation of privacy in its contents. The court rejected defendant's claim that the collective-knowledge doctrine has any bearing on the propriety of the district court's conclusion that defendant abandoned the backpack. The court also held that the district court is not precluded from finding abandonment in cases where the defendant, as here, has physical possession of the property he has disavowed. In this case, the record supported the district court's conclusion that defendant clearly and unequivocally disavowed ownership of the backpack. Even if the district court erred by finding that defendant abandoned the backpack, reversal would not be required because the search of the backpack was a proper search incident to arrest for which no warrant was required under the facts of this case.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Nance

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-4585
Opinion Date: April 21, 2020
Judge: Pamela Harris
Areas of Law: Criminal Law

The Fourth Circuit affirmed defendant's above-Guidelines sentence imposed after he pleaded guilty to two federal drug- and firearm-related offenses. The court held that defendant's sentence was not procedurally unreasonable where the district court took into account defendant's extensive criminal history; his pattern of reoffending upon release; his disciplinary infractions in custody and inability to comply with the terms of his release; and the fact that the offenses of conviction occurred over the course of days, in which he was arrested once, released, and then arrested again just days later. The court also held that defendant's sentence was substantively reasonable where the district court conducted a thorough, individualized assessment of defendant and his offense conduct in light of the 18 U.S.C. 3553(a) factors, and did not abuse its discretion in formulating the sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Johnson

Court: US Court of Appeals for the Fifth Circuit
Docket: 17-60852
Opinion Date: April 21, 2020
Judge: Priscilla R. Owen
Areas of Law: Criminal Law

The Fifth Circuit vacated defendant's sentence imposed after he pleaded guilty to violating 18 U.S.C. 922(g) and 924(e) by knowingly possessing a firearm after he had been convicted of a misdemeanor crime of domestic violence. The court held that the district court committing plain error by violating Federal Rule of Criminal Procedure 32 when it relied on factual allegations in the confidential sentencing recommendation that were not in the presentence report and that were not disclosed by defendant. The court explained that the use of undisclosed facts to justify an above-guidelines sentence seriously affects the fairness, integrity, and public reputation of judicial proceedings. Therefore, the court remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. McGinnis

Court: US Court of Appeals for the Fifth Circuit
Docket: 19-10197
Opinion Date: April 21, 2020
Judge: Stuart Kyle Duncan
Areas of Law: Criminal Law

18 U.S.C. 922(g)(8), which prohibits individuals subject to certain domestic violence protective orders from possessing firearms or ammunition for any purpose, is facially constitutional under the Fifth Circuit's two-step NRA framework. Even assuming arguendo that the conduct at issue -- the keeping and possessing of firearms by individuals subject to domestic protective orders -- falls within the Second Amendment right, defendant's facial challenge fails. The court applied intermediate scrutiny and held that section 922(g)(8) is reasonably adapted to the government interest of

reducing domestic gun abuse. The court also held that if the commonly understood definitions of terms in the protective order include acts involving "physical force," the protective order is sufficient to support a conviction under section 922(g)(8)(C)(ii). In this case, the jury plausibly found that the order satisfied the statute and the court declined to reverse defendant's conviction on this basis. However, the court remanded for the limited purpose of conforming defendant's written judgment to the district court's oral pronouncement.

Read Opinion Are you a lawyer? **Annotate this case**.

Valentine v. Collier

Court: US Court of Appeals for the Fifth Circuit
Docket: 20-20207
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Criminal Law, Government & Administrative Law, Health Law

Plaintiffs filed suit alleging that TDCJ's adoption and implementation of measures guided by changing CDC recommendations in regards to the COVID-19 pandemic do not go far enough. Plaintiffs filed a class action alleging violations of the Eighth Amendment's prohibition against cruel and unusual punishment, and the Americans with Disabilities Act, seeking a preliminary injunction. The Fifth Circuit granted TDCJ's motion to stay the district court's preliminary injunction, which regulates the cleaning intervals for common areas, the types of bleach-based disinfectants the prison must use, the alcohol content of hand sanitizer that inmates must receive, mask requirements for inmates, and inmates' access to tissues (amongst many other things). The court held that TDCJ is likely to prevail on the merits of its appeal because: (1) after accounting for the protective measures TDCJ has taken, plaintiffs have not shown a "substantial risk of serious harm" that amounts to "cruel and unusual punishment"; and (2) the district court committed legal error in its application of Farmer v. Brennan, by treating inadequate measures as dispositive of defendants' mental state. In this case, even assuming that there is a substantial risk of serious harm, plaintiffs lack evidence of defendants' subjective deliberate indifference to that harm. The court also held that TDCJ has shown that it will be

irreparably injured absent a stay, and that the balance of the harms and the public interest favor a stay. Finally, the court held that plaintiffs have not exhausted their administrative remedies as required in the Prison Litigation Reform Act (PLRA), and the district court's injunction goes well beyond the limits of what the PLRA would allow even if plaintiffs had properly exhausted their claims.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Dowl

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-2469
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

Dowl pleaded guilty to presenting false tax returns, 18 U.S.C. 286. He received a sentence of 30 months of imprisonment plus 24 months of supervised release. On supervised release, Dowl was charged with four new state crimes; failing to inform his probation officer that he had police contact; communicating with his co-defendant despite instructions to the contrary; failing to make payments on his restitution, fine, or special assessment; and failing to get a job. At a hearing, the court reviewed the evidence and allowed Dowl to tell his side of the story. The court deferred judgment on three of the four new state criminal law violations and dismissed the fourth and found Dowl gainfully employed. Dowl had failed to notify his probation officer about police contact, impermissibly communicated with his co-defendant, and did not pay his fines. After considering the 18 U.S.C. 3553(a) sentencing factors, the court returned Dowl to prison for 11 months, giving Dowl and his attorney the opportunity to raise any objections. Dowl had none. The Sixth Circuit affirmed, rejecting Dowl’s argument that the court committed reversible error by not directly addressing him to solicit an allocution. The court employed the “plain error” standard because Dowl did not raise any objection during his revocation hearing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Fowler

Court: US Court of Appeals for the Sixth Circuit
Dockets: 19-3071, 19-3070
Opinion Date: April 21, 2020
Judge: Donald
Areas of Law: Criminal Law

In 2018, Fowler pled guilty to possession of child pornography and violations of the conditions of his supervised release from a previous conviction for the same. In addition to possessing child pornography, Fowler had failed drug testing, had threatened his parole officer, and had tried to harass his girlfriend to recant her testimony. The district court ordered Fowler to pay a $5,000 special assessment for possession of child pornography under the Justice for Victims of Trafficking Act, 18 U.S.C. 3014. The court also varied upward and sentenced Fowler to the maximum statutory penalty for violating the conditions of his supervised release, imposing a 120-month sentence for possessing child pornography and a consecutive 36-month sentence for violating the terms of his supervised release. The Sixth Circuit vacated as to the assessment and remanded for a determination of indigency. The district court committed plain error by failing to address Fowler's ability to pay; the parties did not contemplate the $5,000 special assessment as a part of the waiver provision in the plea agreement. The court affirmed the sentence. The district court did not consider an impermissible factor (whether Fowler had actually touched a child) and Fowler had no other challenge to the reasonableness of his sentence,

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Sumlin

Court: US Court of Appeals for the Sixth Circuit
Docket: 18-3819
Opinion Date: April 21, 2020
Judge: Bush
Areas of Law: Criminal Law

Sumlin was convicted of the distribution of drugs that caused the 2015 death of Carrie Dobbins, 21 U.S.C. 841(a)(1) and (b)(1)(C), which carries enhanced penalty provisions. The Sixth Circuit affirmed his convictions and

his sentence to life in prison. The district court properly denied Sumlin's suppression motion, given that the affidavit established a sufficient nexus between his drug trafficking activity and residence that was searched. The court properly admitted testimony by the victim's sister, Kelly, who was Sumlin's former girlfriend and had purchased drugs from him. Kelly's testimony about Sumlin's drug-trafficking and that Sumlin was with Carrie on the day of her overdose was intrinsic proof that was relevant for providing background information and contextualizing the government's case against Sumlin. Sufficient evidence supported the jury's verdict that Sumlin distributed the drugs that caused Carrie's death.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Vance

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-5160
Opinion Date: April 17, 2020
Judge: Bush
Areas of Law: Criminal Law, White Collar Crime

The Spriggs' bank account was established to receive social security checks. The Spriggs' great-grandson, Vance, filled out an application in Mr. Spriggs's name for a debit card to draw on the checking account. Mr. Spriggs had never used a debit card. The Spriggses did not authorize Vance to do so. Bank cameras photographed Vance using the card to withdraw cash. Vance also used the card for personal expenses. At another bank, Vance used Mr. Spriggs's social security number to establish an account and obtain a $15,000 cash advance. Vance made other, unsuccessful loan applications. Upon being notified by the banks about suspicious activities involving his identity, Mr. Spriggs filed a police report. The police arrested Vance. While searching Vance's car, the police located a large stash of personal and financial documents belonging to the Spriggses, including bank statements, tax return forms, property-tax bills, and a car title. The Sixth Circuit affirmed Vance's convictions for access-device fraud, 18 U.S.C. 1029(a)(5), and two counts of aggravated identity theft, 18 U.S.C. 1028A(a)(1), and his 65-month sentence. The court rejected arguments that the district court failed to make adequate findings of fact after the bench trial, improperly denied a motion for judgment of acquittal,

and failed to correctly calculate the loss amount connected to Vance's charges under Sentencing Guidelines 2B1.1.

Read Opinion Are you a lawyer? **Annotate this case**.

Winburn v. Nagy

Court: US Court of Appeals for the Sixth Circuit
Dockets: 19-2399, 19-2398
Opinion Date: April 23, 2020
Judge: Jeffrey S. Sutton
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Winburn represented himself at his trial for armed robbery, home invasion, and conspiracy. Based on Winburn's disruptive behavior, the judge removed him from the courtroom and revoked Winburn's permission to represent himself, then granted a competency evaluation and a mistrial. While Winburn awaited his second trial, the judge permitted Winburn's stand-by attorney to withdraw because Winburn had sued her and enjoined Winburn from filing complaints or grievances against his new attorney, except to discharge her. Although represented by a new attorney, Winburn moved pro se to dismiss his charges on double jeopardy grounds. The trial judge denied the motion because Winburn's attorney had not filed it. Winburn filed a habeas petition under 28 U.S.C. 2241 challenging his retrial and another section 2241 petition challenging the injunction. The district judges denied both and declined to issue certificates of appealability. Winburn filed a notice of appeal for one petition and sought a certificate of appealability for the other. The Sixth Circuit held that state pretrial detainees proceeding under section 2241 may not appeal without certificates of appealability and granted Winburn a certificate on the injunction claim. A reasonable jurist could conclude that the unusual order was constitutionally infirm. The court denied relief with respect to double jeopardy. Winburn failed to exhaust his state-court remedies by a motion to dismiss.

Read Opinion Are you a lawyer? **Annotate this case**.

Lund v. City of Rockford

Court: US Court of Appeals for the Seventh Circuit

Docket: 19-1945
Opinion Date: April 20, 2020
Judge: ROVNER
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Lund, a reporter for the Rockford Scanner, heard, by police scanner, of multiple traffic stops in Midtown. He did not have a driver's license, so he rode a motorized bicycle to Midtown to take photographs. He suspected a prostitution sting operation. An officer noticed Lund and radioed the team. Officers Welsh and Campbell knew of Lund's previous anti-police speech. They directed Lund to "move on." Lund asked if he was breaking any laws. Campbell informed him that he was not, but that his continued presence would constitute obstruction of a police detail and result in arrest. Lund started his bicycle and called out, loudly, "goodbye officers." Concerned that Lund might post pictures on social media while the sting operation was ongoing and create a danger for unarmed undercover officers, the officers followed Lund and arrested him for driving the wrong way on a one-way street, operating a vehicle without insurance, obstructing a police officer, felony aggravated driving on a revoked license, and operating a motor vehicle without a valid drivers' license. News stories listed Lund's name as an arrestee in the prostitution sting. The charges against Lund were dismissed. Lund sued the officers and the city under 42 U.S.C. 1983. The Seventh Circuit affirmed summary judgment for the defendants on First Amendment retaliation and malicious prosecution under Illinois law, citing the Supreme Court's intervening "Nieves" (2019) holding, that, in most cases, probable cause to arrest defeats a claim of retaliatory arrest. There was probable cause to arrest Lund.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Perez

Court: US Court of Appeals for the Seventh Circuit
Docket: 18-3156
Opinion Date: April 23, 2020
Judge: KANNE
Areas of Law: Criminal Law

Beloit officers facilitated a recorded controlled buy of heroin from Perez, a suspected high-level drug dealer. Perez sold 98 grams of heroin to an

informant. Based on that transaction alone, Perez pled guilty to distributing heroin. At Perez's sentencing hearing, the judge expressed concern that the guidelines range of 33–41 months' imprisonment did not reflect the full scope of his drug trafficking. The PSR described conduct that suggested that Perez was responsible for distributing large quantities of heroin, methamphetamine, and cocaine. The judge continued the hearing, directing the government to file a memorandum, detailing which offense conduct it could support by a preponderance of the evidence. When the hearing reconvened, the government presented witness testimony that elaborated on conduct described in the PSR, including drug ledgers, Perez's post-arrest conversation with his girlfriend, large sums of cash, a money counter, cell phones, and Perez's passport. The judge calculated a higher guidelines range and imposed a 121-month sentence. The Seventh Circuit affirmed, rejecting an argument that the sentencing judge should have recused himself. Perez has not demonstrated that a reasonable observer would have questioned the judge's impartiality nor did he allege that the judge was biased based on events outside the proceedings. The judge's continuance was laudable, not prejudicial.

Read Opinion Are you a lawyer? **Annotate this case**.

Jackson v. United States

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1131
Opinion Date: April 20, 2020
Judge: Lavenski R. Smith
Areas of Law: Criminal Law

The Eighth Circuit affirmed the district court's denial of a 28 U.S.C. 2255 motion to vacate, set aside, or correct petitioner's sentence. The court held that the district court did not err in denying an evidentiary hearing as to petitioner's claim that counsel was constitutionally ineffective for failing to conduct adequate pretrial investigations. In this case, petitioner failed to identify any specific witnesses or evidence that counsel failed to uncover. Furthermore, petitioner failed to show that counsel's representation prejudiced his case. The court also held that the district court did not err in denying an evidentiary hearing as to petitioner's claim that his new counsel was ineffective for failing to subpoena witnesses, for convincing petitioner

not to testify, for failing to object to or appeal the district court's answer to a jury question, and for failing to object to the district court's designation of petitioner as a career offender.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Bolman

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-2759
Opinion Date: April 21, 2020
Judge: Jane Louise Kelly
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's conviction for involuntary manslaughter after he struck and killed his nephew with his truck. The court held that the evidence was sufficient to support the conviction, because a reasonable jury could find defendant grossly negligent beyond a reasonable doubt. The court also held that the district court did not plainly err by failing to instruct the jury that actual knowledge is an essential element of the offense that is separate from gross negligence, because the instructions, viewed as a whole, accurately and adequately defined the essential elements of the offense.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Boyd

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-3528
Opinion Date: April 17, 2020
Judge: Kobes
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's sentence imposed after he pleaded guilty to being a felon in possession of a firearm. The court held that the facts underlying defendant's prior arrests were part of his history and characteristics under 18 U.S.C. 3553(a), and thus the district court could consider defendant's arrest records and the circumstances of those arrests. The court explained that the arrests were listed in the presentence report

and gleaned from prior police reports. Furthermore, specific facts underlying the arrests may be considered for an upward departure and should be considered fair game for a variance where defendant did not object to them. The court also concluded that there is nothing here that suggested a corrected misstatement improperly influenced the district court's sentencing decision. Finally, the court held that the upward variance was not unreasonable in consideration of defendant's previous assaults, coupled with the facts underlying his arrest in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Gonzalez-Esparsa

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1477
Opinion Date: April 22, 2020
Judge: Grasz
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's conviction for unlawful use of an identification document and misuse of a social security number. The court held that the evidence was sufficient to support defendant's convictions where a reasonable juror could conclude that defendant knew the permanent resident card bearing his name and photograph had been forged, counterfeited, falsely made, or unlawfully obtained when he used it to secure employment. Furthermore, a reasonable juror could conclude that defendant made the false representation regarding his purported social security number in order to deceive Midwest Concrete in order to obtain a job with the company.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Sanchez-Velasco

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-3568
Opinion Date: April 17, 2020
Judge: James B. Loken
Areas of Law: Criminal Law, Immigration Law

The Eighth Circuit affirmed the district court's denial of defendant's motion to suppress his responses to an ICE agent's two questions at the Treasurer's Office, because he was not in custody at the time of questioning. Although defendant was in custody at the ICE facility, the court held that an agent's questions were not custodial interrogation because the agent could not have known his questions were likely to elicit incriminating information regarding the two criminal charges that were eventually brought against defendant. The court noted that the Attorney General's regulations carefully distinguish between the warrantless arrest of an alien for a criminal violation of the immigration laws, and what is called the "administrative arrest" of an alien who is reasonably believed to be illegally present in the United States. The court agreed with the district court that the agent's questioning was a request for routine information necessary for basic identification purposes that is not interrogation under Miranda, even if the information turns out to be incriminating.

Read Opinion Are you a lawyer? **Annotate this case**.

Anthony v. TRAX International Corp.

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-15662
Opinion Date: April 17, 2020
Judge: Kim McLane Wardlaw
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Ninth Circuit affirmed the district court's grant of summary judgment to TRAX in a disability discrimination action brought by plaintiff under Title I of the Americans with Disabilities Act (ADA). After TRAX terminated plaintiff from her position as a Technical Writer allegedly due to an inability or unwillingness to accommodate her disability, TRAX discovered during the course of litigation that plaintiff lacked the requisite bachelor's degree for her position. The panel held that, although McKennon v. Nashville Banner Publishing Co., 513 U.S. 352 (1995), held that after-acquired evidence cannot establish a superseding, non-discriminatory justification for an employer's challenged actions, after-acquired evidence remains available for other purposes, including to show that an individual is not qualified under the ADA. Because plaintiff did not satisfy one of the prerequisites for her

position, she is not "otherwise qualified," and TRAX was not obligated to engage in the interactive process.

Read Opinion Are you a lawyer? **Annotate this case**.

City of Almaty v. Khrapunov

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-56451
Opinion Date: April 22, 2020
Judge: Marbley
Areas of Law: Criminal Law, International Law, White Collar Crime

The City of Almaty, in Kazakhstan, filed suit against defendant and his family under the Racketeer Influenced and Corrupt Organizations Act (RICO), alleging that they engaged in a scheme to defraud the city of millions of dollars. The City claimed that it was forced to spend money and resources in the United States to trace where its money was laundered. The district court dismissed the City's claim on the basis that it failed to state a domestic injury pursuant to the Supreme Court's recent decision in RJR Nabisco, Inc. v. European Community, 136 S. Ct. 2090 (2016). The Ninth Circuit held that the City failed to state any cognizable injury other than the foreign theft of its funds, and its voluntary expenditures were not proximately caused by defendants' acts of money laundering. In this case, the City's expenditure of funds to trace its allegedly stolen funds is a consequential damage of the initial theft suffered in Kazakhstan and is not causally connected to the predicate act of money laundering.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Baldon

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-10411
Opinion Date: April 21, 2020
Judge: Bennett
Areas of Law: Criminal Law

After defendant pleaded guilty to possession with intent to distribute a controlled substance, the district court sentenced him to 184 months in

prison. The Ninth Circuit held that defendant's prior convictions for carjacking under section 215 of the California Penal Code are not categorical crimes of violence under USSG 4A1.1(e). Therefore, the district court incorrectly calculated defendant's criminal history by improperly including two points for his prior carjacking convictions. However, the panel held that the district court did not err in finding that defendant possessed a firearm under USSG 2D1.1(b)(1). Accordingly, the panel affirmed in part, vacated in part, and remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Costanzo

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-10291
Opinion Date: April 17, 2020
Judge: Michael Daly Hawkins
Areas of Law: Criminal Law

The Ninth Circuit affirmed defendant's conviction of five counts of money laundering, holding that a reasonable trier of fact could have found beyond a reasonable doubt that the money laundering transactions, in which payment was made via bitcoin, affected interstate commerce in some way or to some degree. In this case, the transfer involved the use of an Internet or cellular network connected Personal Computer Device (PCD) to transfer bitcoin (together with the digital code necessary to unlock the bitcoin) to the digital wallet of another Internet or cellular network connected PCD.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Manzanares

Court: US Court of Appeals for the Tenth Circuit
Docket: 18-2010
Opinion Date: April 17, 2020
Judge: Mary Beck Briscoe
Areas of Law: Constitutional Law, Criminal Law

Defendant-Appellant Archie Manzanares appealed a district court's denial of his 28 U.S.C. 2255 motion challenging his sentence under the Armed

Career Criminal Act (ACCA). Under the ACCA, an offense qualified as a violent felony by satisfying at least one of three definitions, which have come to be known as the Elements Clause, the Enumerated Clause, and the Residual Clause. Manzanares asserted that without the Residual Clause, his underlying New Mexico convictions (armed robbery, aggravated assault with a deadly weapon, and aggravated battery) no longer qualified as violent felonies. The district court denied the motion, concluding that all three underlying convictions satisfied the Elements Clause. Manzanares appealed the classification of the armed robbery conviction as a violent felony to the Tenth Circuit, and sought to expand the certificate of appealability to allow him to appeal the decision regarding the aggravated assault with a deadly weapon and aggravated battery convictions. After review, the Tenth Circuit affirmed the district court's denial of Manzanares's 2255 motion, and denied his motion to expand the COA.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Delaney

Court: US Court of Appeals for the District of Columbia Circuit
Docket: 18-3093
Opinion Date: April 17, 2020
Judge: David S. Tatel
Areas of Law: Criminal Law

The DC Circuit vacated the district court's denial of defendant's motion to suppress evidence. The court held that officers violated the Fourth Amendment when they seized defendant because they lacked reasonable suspicion to justify the stop. In this case, a seizure occurred when the officers pulled into the parking lot, partially blocked defendant's vehicle, and activated their take-down light. The court held that any inference of suspicion that the officers drew from encountering defendant soon after hearing the nearby gunshots were undermined by the government's failure to identify specific and articulable facts supporting the officers' estimation of where the various shots came from. Accordingly, the court remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

Antenor v. Alaska, Department of Corrections

Court: Alaska Supreme Court
Docket: S-17005
Opinion Date: April 17, 2020
Judge: Carney
Areas of Law: Civil Procedure, Criminal Law, Government & Administrative Law

Several Alaska Department of Corrections inmates challenged the DOC's policy to charge for local telephone calls, arguing the rates they and call recipients had to pay for calls violated their constitutional right to rehabilitation, their statutory right to reasonable telephone access, and DOC's contractual obligations under a prior settlement and consent decree. In addition, one of the prisoners challenged DOC officers' decision to deny him access to a computer programming book he ordered from outside the prison. He contended that DOC placed a content-specific restriction on the educational materials and publications prisoners were allowed, violating the Alaska Constitution's free speech provisions as well as prisoners' right to reformation. Each of these challenges reached the Alaska Supreme Court after inmates exhausted the administrative process from prison. Inmates then appealed to the superior court, which denied relief. The Alaska Supreme Court determined the superior court record did not provide enough evidence for it to meaningfully determine the reasonableness of the rates charged inmates for local telephone calls; therefore the Court reversed denial of relief and remanded for further fact-finding by the trial court. The Court concluded that the facility's restrictions on programming-related books were rationally related to a legitimate interest, and because they did not infringe on the right to rehabilitation, it affirmed denial of a prisoner's motion to enforce his claimed right to a particular text about computer programming.

Read Opinion Are you a lawyer? **Annotate this case**.

Berger v. Bryant

Court: Arkansas Supreme Court
Citation: 2020 Ark. 357
Opinion Date: April 23, 2020
Judge: Rhonda K. Wood

Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's petition to proceed in forma pauperis on a petition for writ of mandamus and a motion for declaratory judgment, holding that Appellant failed to state a colorable cause of action. In 1998, Appellant was convicted of rape. In his petition for a writ of mandamus, Appellant asserted that he sought information pursuant to the Arkansas Freedom of Information Act regarding his rape conviction but received no response. The circuit court denied the petition. The Supreme Court affirmed, holding (1) even if Appellant had requested disclosable information, he would not be entitled to inspect it as an incarcerated person; and (2) Appellant did not demonstrate a legitimate claim given the facts presented and therefore failed to establish a colorable cause of action to support his request to proceed in forma pauperis.

Read Opinion Are you a lawyer? **Annotate this case**.

Carroll v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 360
Opinion Date: April 23, 2020
Judge: Wynne
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's motion for leave to file a petition for writ of error cram knobs, holding that the circuit court did not abuse its discretion in declining to issue the writ. Appellant pled guilty to rape and was sentenced as a habitual offender to 720 months' imprisonment. In his coram nobis petition, Appellant alleged several grounds for relief, including claims of actual innocence, an invalid arrest warrant, a coerced guilty plea, and prosecutorial misconduct. The circuit court denied the motion. The Supreme Court affirmed, holding that Appellant did not demonstrate that that the writ should issue and failed diligently to proceed on his claim for coram nobis relief.

Read Opinion Are you a lawyer? **Annotate this case**.

Cave v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 356
Opinion Date: April 23, 2020
Judge: Josephine L. Hart
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's pro se petition for writ of habeas corpus, holding that the circuit court did not err in denying the petition. Appellant was found guilty of two counts of delivery of a controlled substance and one count of maintaining a drug premises. In his habeas petition, Appellant argued that he was actually innocent because his arrest and conviction was based on the false testimony of a witness who had a lengthy criminal history. Appellant further argued that the writ should issue because he was not afforded effective assistance of counsel. The circuit court denied the petition. The Supreme Court affirmed, holding (1) Appellant's claims regarding the witness's credibility do not constitute a valid assertion that he was being unlawfully detained; and (2) Appellant did not actually connect an allegation of ineffective assistance of counsel to his allegation that he was unlawfully detained.

Read Opinion Are you a lawyer? **Annotate this case**.

Chatmon v. Kelley

Court: Arkansas Supreme Court
Citation: 2020 Ark. 355
Opinion Date: April 23, 2020
Judge: Josephine L. Hart
Areas of Law: Criminal Law

The Supreme Court denied Appellant's appeal from the order of the circuit court denying his petition to proceed in forma pauperis on the grounds that Appellant failed to state a colorable cause of action in a petition for writ of habeas corpus, holding that the circuit court did not abuse its discretion by denying Appellant's in forma pauperis petition. In his habeas petition, Appellant alleged that the trial court lacked jurisdiction in his criminal case. Before this case was submitted to the Supreme Court, Appellant filed two

motions, including a "Judicial Notice of a Void Judgment" and a "Notice to the Court." The Supreme Court denied the motions, holding that neither motion was cognizable under the Court's rules. The Court then affirmed the Supreme Court's denial of Appellant's in forma pauperis petition, holding that the circuit court correctly found that Appellant did not assert a colorable cause of action.

Read Opinion Are you a lawyer? **Annotate this case**.

McClinton v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 353
Opinion Date: April 23, 2020
Judge: Karen R. Baker
Areas of Law: Criminal Law

The Supreme Court denied Petitioner's second petition requesting permission to proceed in the trial court with a petition for writ of error coram nobis, holding that Petitioner's proposed attack on the judgment had no merit. Petitioner was convicted of raping a mentally handicapped sixteen-year-old girl and was sentenced to life imprisonment. In his first petition for writ of error coram nobis Petitioner alleged a number of errors in the trial procedure. The first petition was denied. In his second coram nobis petition, Petitioner alleged violations of Brady v. Maryland, 373 U.S. 83 (1963). The Supreme Court denied the writ, holding that Petitioner failed to meet his burden of demonstrating a fundamental error of fact extrinsic to the record.

Read Opinion Are you a lawyer? **Annotate this case**.

Siegel v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 359
Opinion Date: April 23, 2020
Judge: Wynne
Areas of Law: Criminal Law

The Supreme Court dismissed Appellant's appeal from the circuit court's orders denying her motions to declare Ark. Code Ann. 5-62-106 (disposition

of animal) and Ark. Code Ann. 5-62-111 (prevention of cruelty) unconstitutional and conditionally granting her motion for return of seized property, holding that there was no final, appealable order in this case. Appellant was convicted of thirty-one misdemeanor counts of cruelty to animals. The circuit court subsequently dismissed the charges on speedy-trial grounds. The State appealed, and the Supreme Court dismissed the appeal on the grounds that it was not authorized. Appellant had filed motions seeking a declaration that sections 5-62-106 and -111 are unconstitutional and seeking the return of her seized property. The circuit court denied the constitutional claims and entered a conditional order granting Appellant's motion for return of seized property. Appellant appealed. The Supreme Court dismissed the appeal, holding that because the conditional order did not make specific findings as to the return of the property or as to damages and because it expressly left open the possibility of further proceedings, there was no final, appealable order in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

Thomas v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 354
Opinion Date: April 23, 2020
Judge: Josephine L. Hart
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Appellant's conviction of capital murder, holding that the evidence was sufficient to sustain the conviction and that the circuit court did not err in denying Appellant's motion to suppress tracking data generated by his cellphone. On appeal, Appellant argued that the trial court erred by denying his directed-verdict motion because the evidence supported the defense's theory of the case that he did not intend to shoot the victim. Further, Appellant argued that the court abused its discretion in denying his motion to suppress evidence obtained from the seizure of AT&T phone records. The Supreme Court disagreed, holding (1) the evidence was sufficient to support the capital murder conviction; and (2) the circuit court correctly denied the motion to suppress.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. Landowski

Court: California Courts of Appeal
Docket: C080210(Third Appellate District)
Opinion Date: April 23, 2020
Judge: Andrea Lynn Hoch
Areas of Law: Constitutional Law, Criminal Law

Defendant Michael Reyes, Jr., an active Norteno gang member (from the Broderick Boys subset), confronted a former Norteno gang member (from the Franklin Boys subset), "S.," about a physical altercation that occurred between S. and Reyes's stepfather over a debt. That earlier altercation had taken place in front of Reyes's autistic younger brother. Reyes pulled out a handgun and asked S. if he had a problem. S., who was riding his bicycle with his wife, "R.," when Reyes confronted him with the gun, stopped briefly, told Reyes to put the gun down if he wanted to fight, and then started to ride away. This angered Reyes, prompting him to fire six rounds at S. from behind. S. Was hit but survived. R. Was a short distance in front of S., but was not hit. Defendants Liberty Landowski and Lisa Humble were with Reyes at the time of the shooting and aided in his efforts to avoid being apprehended by law enforcement authorities. Reyes, Landowski, and Humble were tried together before the same jury. Reyes was convicted of one count of attempted murder (Count 1), two counts of assault with a semiautomatic firearm (Counts 2 and 4), one count of possession of a firearm by a convicted felon (Count 5), and one count of possession of ammunition by a convicted felon (Count 6). In addition to various firearm and other enhancements, the jury found Reyes committed the crimes for the benefit of, at the direction of, or in association with a criminal street gang with the specific intent to promote, further, or assist in criminal conduct by gang members. The jury convicted Landowski and Humble of being accessories to Reyes's criminal conduct (Count 9) and also found true gang enhancement allegations attached to that crime. Reyes challenged the sufficiency of the firearm evidence presented to support his conviction, and all defendants challenged the sufficiency of the evidence supporting their gang enhancements. The Court of Appeal determined Senate Bill 620 (2017-2018 Reg. Sess.) gave the trial court discretion to strike firearm enhancements in the interest of justice and applied retroactively; and Senate Bill 136 (2019-2020 Reg. Sess.) eliminated such enhancements,

and also applied retroactively. To these issues, the Court remanded for the trial court's consideration. The Court affirmed the trial court in all other respects.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. May

Court: California Courts of Appeal
Docket: C084302(Third Appellate District)
Opinion Date: April 20, 2020
Judge: Ronald B. Robie
Areas of Law: Constitutional Law, Criminal Law

Defendant Raymond May was found guilty by jury of possessing an assault weapon and a machine gun based on his possession of a single AK-47 assault rifle while guarding a marijuana plantation. He was sentenced to probation, which included an electronic search condition. On appeal, defendant argued there was a lack of sufficient evidence corroborating his accomplice's testimony and demonstrating he knew of the firearm's illegal character. He further alleged the trial court erred in instructing the jury: that the accomplice instruction should have included language specifying that the accomplice testimony needed to prove more than defendant's mere presence or access to the firearm. Furthermore, defendant argued the electronic search condition imposed as part of his probation failed under the standards announced in California v. Lent, 15 Cal.3d 481 (1975). The Court of Appeal agreed defendant's electronic search condition should have been stricken, but otherwise affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. Perez

Court: California Courts of Appeal
Docket: E072260(Fourth Appellate District)
Opinion Date: April 20, 2020
Judge: Miller
Areas of Law: Constitutional Law, Criminal Law

In 2009, defendant-appellant Rudy Perez pled guilty to active gang

participation under Penal Code section 186.22(a), and unlawful possession of a firearm under section 12025(b)(6). In 2010, defendant pled guilty to residential burglary under section 459, and active gang participation under section 186.22(a). In August of 2018, the State filed a new felony complaint, alleging one of the prior gang participation convictions as a strike prior. In 2018, defendant moved to vacate the two prior gang participation convictions based upon changes in the law that rendered them invalid. The trial court denied defendant's motion. In 2019, defendant asked for reconsideration, which was again denied. Thereafter, defendant filed a timely notice of appeal from the denial of his motion to vacate the convictions. The Court of Appeal found that defendant pled guilty to street terrorism under Penal Code section 186.22(a) in 2009 and 2010, and it was undisputed that while committing these offenses, defendant acted alone. However, subsequent to defendant's guilty pleas, in 2012, the California Supreme Court held that a defendant had to act in concert with a fellow gang member in order to be guilty of street terrorism. At that time, defendant could have filed a state habeas petition requesting relief, but failed to do so. "Defendants can lose remedies that are established by law when they fail to invoke such remedies in time." Section 1473.7 became effective in 2017. In defendant's motion filed in the trial court, defendant failed to state what new evidence was discovered, instead arguing that the trial court was allowed "to vacate a conviction where the defendant is innocent as a matter of law or where vacating the conviction is in the interest of justice, even though the defendant is no longer in custody or otherwise restrained by the conviction." The Court of Appeal concurred with the trial court's reason to deny relief, determining that "while the outcome in this case may be unfortunate for defendant, we are not here to rewrite legislation. The Legislature could amend section 1473.7 to address issues raised in this case. However, under the laws, as written, we must uphold the trial court's order."

Read Opinion Are you a lawyer? **Annotate this case**.

In re S.R.

Court: California Courts of Appeal
Docket: B300214(Second Appellate District)
Opinion Date: April 23, 2020
Judge: Bendix

Areas of Law: Criminal Law

Father appealed the juvenile court's dispositional ruling removing daughter from his custody, arguing that his mere possession of child pornography does not demonstrate that he poses a substantial risk of harm to his daughter. The Court of Appeal affirmed the order and held that there is substantial evidence of risk of great harm to daughter—no matter how low the probability— that father will sexually abuse his daughter if he is provided unfettered access to her.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Bell

Court: California Courts of Appeal
Docket: B288528(Second Appellate District)
Opinion Date: April 23, 2020
Judge: Stratton
Areas of Law: Criminal Law

Defendant was convicted of one count of attempted robbery, one count of second degree murder, and one count of hit and run driving. The jury found not true the allegation that a principal was armed in the commission of the attempted robbery. The trial court found true the allegations that defendant had served four prior prison terms within the meaning of Penal Code section 667.5, subdivision (b). Defendant raised 13 claims of error on appeal. The Court of Appeal held that the section 667.5, subdivision (b) enhancement terms must be stricken and the matter remanded to the trial court for resentencing. The court also held that defendant forfeited some of his substantive claims and other lack merit. Finally, the court held that, if there is instructional error, the errors are harmless under any standard of review. Accordingly, the court affirmed the judgment of conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Drayton

Court: California Courts of Appeal
Docket: H046928(Sixth Appellate District)

Opinion Date: April 17, 2020
Judge: Danner
Areas of Law: Criminal Law

In 1991, the Wards and their teenage daughter awoke and discovered four men, including Drayton, inside their house. Two were armed. One told the daughter he was going to rape her and placed a firearm inside her vagina. Drayton told the man not to do it. Drayton had a gun and held Mrs. Ward down during the robbery. Two others shot and killed Mr. Ward. Drayton and the others left without seeking help for the Wards. Drayton did not shoot Mr. Ward or threaten to rape the daughter. Drayton surrendered the next day. Drayton's sole prior conviction was a misdemeanor; he had no reported history of violence. Drayton was sentenced to 29 years to life imprisonment. In 2019, Drayton sought resentencing under Penal Code 1170.95, declaring that he "was not a major participant ... or did not act with reckless indifference to human life." Senate Bill 1437, effective January 1, 2019, restricted the circumstances under which a person can be liable for felony murder and enacted Penal Code 1170.95, which allows an individual, previously convicted of felony murder, to petition to have his murder conviction vacated and to be resentenced. The court of appeal directed the trial court to hold a hearing under section 1170.95(d) and to accept the assertions in the petition as true unless facts in the record conclusively refute them as a matter of law. If, accepting the petitioner's assertions as true, he meets section 1170.95(a)'s requirements for relief, the court must issue an order to show cause. In assessing the prima facie showing, the trial court should not weigh evidence or make credibility determinations.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Robinson

Court: California Courts of Appeal
Docket: B293746(Second Appellate District)
Opinion Date: April 20, 2020
Judge: Wiley
Areas of Law: Criminal Law

After defendant penetrated an unconscious woman with his fingers, he challenged evidentiary rulings and requests a presentence conduct credit. The Court of Appeal held that the trial court properly excluded cumulative

evidence about past times the woman was intoxicated at the relevant bar, and any error in allowing a drug recognition expert to testify about whether the woman was incapacitated was harmless. However, the court held that the trial court undercalculated defendant's presentence custody credit because he was not convicted of a violent felony under Penal Code section 2933.1, which would otherwise limit those credits. Accordingly, the court directed the trial court to award defendant 104 days of presentence custody credit and to amend the abstract of judgment, affirming in all other respects.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Torres

Court: California Courts of Appeal
Docket: B292551(Second Appellate District)
Opinion Date: April 20, 2020
Judge: Kenneth R. Yegan
Areas of Law: Criminal Law

Where, as here, the trial court factually finds that a self-represented defendant has engaged in an attempt to intimidate a witness, the constitutional right of self-representation can, in the exercise of the trial court's sound discretion, be revoked. The Court of Appeal affirmed defendant's conviction and sentence for two counts of battery on an ex-girlfriend. In this case, the trial court did not abuse its discretion in revoking defendant's pro se status after he asked his sister to contact the victim and have her say that she was coerced by the police detective to "press charges."

Read Opinion Are you a lawyer? **Annotate this case**.

Colorado v. Lujan

Court: Colorado Supreme Court
Citation: 2020 CO 26
Opinion Date: April 20, 2020
Judge: Brian D. Boatright
Areas of Law: Constitutional Law, Criminal Law

Abel Lujan was charged with first-degree murder for the death of his girlfriend after she was found beaten and strangled behind a friend's house. At trial, two women testified for the State about Lujan's prior violent behavior towards them. Prior to admitting this evidence, the trial court read a limiting instruction, telling the jury that it could only consider the evidence for the purposes of establishing Lujan's motive, intent, or common plan. A copy of this instruction was not given to the jury for deliberations; however, the jury did receive an instruction at the close of the evidence explaining that certain evidence could only be considered for the limited purposes for which it was admitted. While deliberating, the jury submitted a question seeking clarification about the limiting instruction. Over defense counsel's objection, the trial court cleared the courtroom of the public and parties, leaving only the judge, bailiff, and court reporter; the judge then brought in the jury and reread the limiting instruction that it had previously read twice in open court. The jury ultimately found Lujan guilty of second-degree murder. Lujan appealed, arguing that the court's actions when rereading the jury instruction constituted a courtroom closure that violated his Sixth Amendment right to a public trial. A division of the court of appeals agreed and reversed Lujan's conviction. The State argued on certiorari review that the Colorado Supreme Court adopt a triviality standard, under which a defendant's constitutional right to a public trial was not violated when the closure at issue was trivial. In so doing, the State argued that the brief courtroom closure here was trivial and therefore did not violate Lujan's public trial right. The Court concurred with the State, adopted the standard and reversed the appellate court's decision.

Read Opinion Are you a lawyer? **Annotate this case**.

Archer v. State

Court: Florida Supreme Court
Docket: SC19-841
Opinion Date: April 23, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the order of the circuit court denying Appellant's successive motion to vacate his sentence of death under Fla. R. Crim. P. 3.851, holding that the circuit court did not err in denying the Rule

3.851 motion. Appellant was convicted of first-degree murder, armed robbery, and grand theft. Appellant was sentenced to death for the murder. The Supreme Court affirmed the convictions but reversed Appellant's death sentence and remanded the case for a new penalty phase. After a new penalty phase, Appellant was again sentenced to death. In his successive Rule 3.851 motion, Appellant raised three claims. The circuit court denied relief. The Supreme Court affirmed, holding that the circuit court (1) properly denied Appellant's claim that his death sentence violated the Sixth and Eighth Amendments in light of Hurst v. Florida, 136 S. Ct. 616 (2016), and Hurst v. State, 202 So. 3d 40 (Fla. 2016); (2) correctly denied Appellant's claim that his sentence violated the Eighth Amendment; and (3) did not err in denying Appellant's claim of newly discovered evidence.

Read Opinion Are you a lawyer? **Annotate this case**.

Collins v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0158
Opinion Date: April 20, 2020
Judge: David E. Nahmias
Areas of Law: Constitutional Law, Criminal Law

Appellant Tommy Collins was convicted of felony murder in connection with the stabbing death of 14-year-old Rueben Hand. Friends gathered to watch the Peach Drop on New Year's Eve 2010; a disagreement ensued and Hand was stabbed near the Five Points MARTS station shortly after midnight. Appellant's only argument on appeal was that the trial court plainly erred when it gave the jury the State's requested instruction on "revenge for a prior wrong." Seeing no error, "much less plain error," the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Heyward v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0399
Opinion Date: April 20, 2020

Judge: Peterson
Areas of Law: Constitutional Law, Criminal Law

Larmell Heyward was convicted by jury of malice murder and possession of a firearm during the commission of a felony in connection with the 2007 shooting death of Ramon Rogers. Heyward argued on appeal of those convictions that the trial court erred in denying his request to charge the jury on voluntary manslaughter. After review, the Georgia Supreme Court determined the trial court's refusal to give the charge was harmless, since, in the Court's estimation, there was no realistic probability that the jury would have accepted the "slight" evidence of voluntary manslaughter in the light of the strong evidence of malice murder.

Read Opinion Are you a lawyer? **Annotate this case**.

Howard v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0819
Opinion Date: April 20, 2020
Judge: Keith R. Blackwell
Areas of Law: Constitutional Law, Criminal Law

Kenneth Howard was tried by jury and convicted of the murder of Emily Ann Smith Newbegin. Howard appealed, contending that the evidence was legally insufficient to sustain his conviction. Upon its review of the record and briefs, the Georgia Supreme Court found no merit in Howard's claim of error, and affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Keller v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0006
Opinion Date: April 20, 2020
Judge: Boggs
Areas of Law: Constitutional Law, Criminal Law

Randall Keller was convicted of felony murder and related crimes arising out

of the beating death of his ex-wife's two-year-old son, William Powell. On appeal, Keller raised numerous claims of error, including ineffective assistance of counsel, the trial court's rulings on motions before and during trial, several evidentiary rulings, and alleged bias on the part of the trial judge. However, finding no reversible error, the Georgia Supreme Court affirmed Keller's convictions.

Read Opinion Are you a lawyer? **Annotate this case**.

Mills v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0364
Opinion Date: April 20, 2020
Judge: Ellington
Areas of Law: Constitutional Law, Criminal Law

Roger Mills was found guilty by jury of malice murder and aggravated assault in connection with the death of Masuto Garrett. Mills contended that the trial court erred when, during jury deliberations, it excused a holdout juror without sufficient inquiry or good cause. After review, the Georgia Supreme Court concurred with that contention, and reversed Mills's convictions. The Court also concluded the evidence presented at trial was legally sufficient to support the convictions, so the State could retry Mills if it chose.

Read Opinion Are you a lawyer? **Annotate this case**.

Moore v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0344
Opinion Date: April 20, 2020
Judge: David E. Nahmias
Areas of Law: Constitutional Law, Criminal Law

Appellant Carzell Moore, proceeding pro se, appealed a trial court's denial of his motion to set aside a September 2017 order denying his motion for an out-of-time appeal of his 2002 resentencing on his 1977 convictions for murder and rape. Moore contended the trial court abused its discretion by

denying his motion to set aside because he was not given proper notice of the September 2017 order. Finding that the record supported the trial court's ruling, the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Morris v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0176
Opinion Date: April 20, 2020
Judge: Bethel
Areas of Law: Constitutional Law, Criminal Law

Darius Morris was found guilty by jury of malice murder and other offenses in connection with the shooting death of Jameson Bush. Morris appealed, arguing he was denied the right to a timely appeal, that the trial court erred in restricting voir dire as to the religious beliefs and connections of potential jurors, that the trial court erred by giving a confusing jury charge regarding statements of co-conspirators, that the trial court erred by violating his right to a public trial by ordering that the courtroom doors be closed and locked during the court's charge to the jury, and that his trial counsel provided ineffective assistance by not objecting to the closure of the courtroom. Finding no error, the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Rickman v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0127
Opinion Date: April 20, 2020
Judge: Harold D. Melton
Areas of Law: Constitutional Law, Criminal Law

Victoria Rickman was convicted by jury of malice murder and a related firearm offense in connection with the shooting death of William Carter, Jr. Rickman and Carter had a tumultuous on-again, off-again relationship with a history of verbal and physical abuse, false accusations of sexual assault, empty threats to obtain temporary protective orders, and numerous calls to

911. In the days leading up to Carter's death, the pair was talking and meeting again despite a recent break-up. On one such 911 call, officers went to Rickman's residence responding to claims shots were fired. Rickman responded holding her small dog, hair wet, and in pajamas. She did not appear to be injured, and nothing in the home looked disturbed or out of place. Rickman told the officers, "he raped me again and I shot him." Officers found Carter laying face up on the bed naked with multiple gunshot wounds to his body. An autopsy revealed that Carter was shot ten times – four times in the chest, three times in the back, once on the arm, and twice in the head. Rickman's examining physician testified that he found no injuries on Rickman consistent with her description of events, and no signs of trauma to her vaginal cavity. Rickman appealed her convictions, arguing she was denied effective assistance of counsel and that the trial court erred in admitting improper character evidence. Finding no reversible error, the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Robinson v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0265
Opinion Date: April 20, 2020
Judge: Peterson
Areas of Law: Constitutional Law, Criminal Law

Herbert Robinson appealed his convictions for malice murder, armed robbery, and possession of a firearm during the commission of a felony in connection with the death of Michael Moore. On appeal, he argued the trial court erred by allowing the State to use two firearms for demonstrative purposes during trial, and by allowing body-camera footage to be shown at trial. He also argued his trial counsel was ineffective for failing to object to a letter written by Robinson's cellmate being available to the jury for review during deliberations, and for failing to object to a visual aid used by the State during closing arguments. Because Robinson failed to show ineffective assistance of counsel or reversible error by the trial court, the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Santana v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0563
Opinion Date: April 20, 2020
Judge: Warren
Areas of Law: Constitutional Law, Criminal Law

Cuevas Carlos Santana was convicted by jury of malice murder and other crimes in connection with the 2010 shooting deaths of Israel Espinoza Mendoza, Vincente Soto Chavez, and Renato Soto Valencia. On appeal, Santana argues that the evidence was insufficient to support his convictions, that the trial court erred by declining to grant Santana a new trial on the general grounds, and that trial counsel provided ineffective assistance. Finding no reversible error, the Georgia Supreme Court affirmed Santana's convictions.

Read Opinion Are you a lawyer? **Annotate this case**.

Sullivan v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0056
Opinion Date: April 20, 2020
Judge: Warren
Areas of Law: Constitutional Law, Criminal Law

A jury convicted Antonio Sullivan of malice murder and other crimes in connection with the shooting death of Wava Benton. On appeal, Sullivan contended his trial counsel was constitutionally ineffective by failing to present evidence at trial to corroborate Sullivan's testimony about prior difficulties between Sullivan and Benton, and by failing to procure expert testimony about Sullivan's mental health—specifically about post-traumatic stress disorder— to be presented to the jury. The Georgia Supreme Court determined Sullivan failed to establish that his trial counsel was deficient in either respect, and therefore affirmed his convictions.

Read Opinion Are you a lawyer? **Annotate this case**.

Turner v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0247
Opinion Date: April 20, 2020
Judge: Warren
Areas of Law: Constitutional Law, Criminal Law

Appellant Ronald Turner appeals from his conviction for malice murder stemming from the stabbing death of William King. The stabbing took place outside an apartment at which Turner had driven in order to trade food for drugs. Turner testified in his own defense at trial and claimed that King hit him in the head with a beer bottle because Turner owed money to King from a prior drug transaction. Turner testified that he tried to get away from King, but that King chased him down and grabbed his jacket. According to Turner, King was getting ready to hit him again when Turner stabbed King in self-defense. Appealing his ultimate conviction, Turner contended he was denied the effective assistance of counsel in three respects. Seeing no reversible error after a review of the trial court record, the Georgia Supreme Court affirmed Turner's conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Valrie v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0380
Opinion Date: April 20, 2020
Judge: Keith R. Blackwell
Areas of Law: Constitutional Law, Criminal Law

Reuben Valrie was tried by jury and convicted of murder and other crimes in connection with the death of his infant daughter Aliyana. Valrie appealed, claiming that he was denied the effective assistance of counsel. Aliyana died as a result of closed head trauma, with a blunt-force abdominal injury as a secondary cause of death, which investigators determined was consistent with being shaken or dropped. At trial, Valrie presented the testimony of four expert witnesses who testified that Aliyana died of natural causes and that the injuries to her brain and abdomen were caused by

events such as post-mortem CPR and the “rough” handling of her body by first responders. The jury rejected this defense and found Valrie guilty of murder and the other charges. Valrie contended that his trial lawyer should have raised a hearsay objection to the admission of recorded statements that his girlfriend (and Aliyana's mother) made to police investigators (as well as the testimony of one of those investigators about some of those statements). Alternatively, Valrie argued that his lawyer should have sought the redaction of certain portions of the recorded statements that impugned his character. The Georgia Supreme Court concluded Valrie failed to present evidence that his trial counsel was deficient, or that he was prejudiced by any alleged failures. According, the Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Williams v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0241
Opinion Date: April 20, 2020
Judge: Keith R. Blackwell
Areas of Law: Constitutional Law, Criminal Law

Richard Williams, II, was tried by jury and convicted of murder in connection with the strangulation death of Cory Robinson. Williams and Robinson were involved in a sexual relationship and had been living together at an extended-stay hotel. Kelvin Spencer was a close friend of both Williams and Robinson. When Spencer met Williams at the hotel room, Williams looked angry and had scratches on his neck. Spencer saw Robinson lying on the floor in a “praying position.” Spencer did not believe Robinson was dead, and he helped Williams move clothes and other things to a U-Haul truck parked outside, in preparation for a move. Williams did not testify or present any evidence. Based on his lawyer’s opening and closing arguments, the defense theory was that Spencer killed Robinson because he was jealous of Williams’s relationship with Robinson. Williams’s sole claim on appeal was that he was denied the effective assistance of counsel when his trial lawyer failed to present as a defense that Williams accidentally killed Robinson during consensual erotic asphyxiation. He argued that his lawyer's discomfort with the topic of homosexual BDSM activity, and his own problems with the Georgia State Bar, precluded presentation of the "true"

version of events, and that Williams acceded to the lawyer's defense strategy only "through ignorance and that he did not know that a defense based on consensual erotic asphyxiation was available." Finding no reversible error, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Malave

Court: Supreme Court of Hawaii
Docket: SCWC-18-0000332
Opinion Date: April 20, 2020
Judge: Mark E. Recktenwald
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the intermediate court of appeals (ICA) affirming Defendant's conviction of sexual assault in the first degree on the complaining witness pursuant to Haw. Rev. Stat. 707-730(1)(b), holding that the ICA did not err in affirming the family court. Specifically, the Supreme Court held (1) the jury should have been instructed to determine jurisdictional facts, but the error was harmless beyond a reasonable doubt; and (2) the ICA did not err in finding that there was no rational basis in the record to support providing the jury instruction of the lesser included offense of sexual assault in the third degree.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Malave

Court: Supreme Court of Hawaii
Docket: SCWC-18-0000332
Opinion Date: April 22, 2020
Judge: Mark E. Recktenwald
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the intermediate court of appeals (ICA) affirming the judgment of the family court convicting Defendant on two counts of sexual assault in the first degree, holding that the ICA did not err in affirming the family court. At issue on appeal was the jurisdiction of the family court to try Defendant and the propriety of

instructing the jury on a lesser included offense. The ICA affirmed, concluding that the family court had subject matter jurisdiction pursuant to Haw. Rev. Stat. 571-14(a)(1) and that there was no rational basis to support an instruction of the lesser included offense of sexual assault in the third degree. The Supreme Court affirmed, holding (1) although the jury should have been instructed to determine jurisdictional facts, the error was harmless; and (2) the family court was not obligated to instruct the jury on the lesser included offense of sexual assault in the third degree.

Read Opinion Are you a lawyer? **Annotate this case**.

Idaho v. Burke

Court: Idaho Supreme Court - Criminal
Docket: 46841
Opinion Date: April 22, 2020
Judge: Moeller
Areas of Law: Constitutional Law, Criminal Law

Prior to sentencing, defendant James Burke was committed to the state mental hospital for 56 days to restore him to competency. After being evaluated and deemed competent to proceed to trial, Burke was returned to the county jail and later pleaded guilty pursuant to a plea agreement. At the conclusion of his sentencing hearing, Burke sought credit for the 56 days of time spent in court-ordered commitment. The district court denied the motion, concluding that commitment to a state mental hospital did not fall under the definition of 'incarceration' in Idaho Code section 18-309. After reviewing this issue carefully, the Idaho Supreme Court disagreed with the district court's "thorough and thoughtful analysis," holding that court-ordered commitment to state custody pursuant to Idaho Code sections 18-210 and 18-211 met the functional and legal definition of "incarceration" under Idaho Code section 18-309. "The extent of the liberty interests restricted by Burke's court-ordered commitment to State Hospital North are just too similar to imprisonment to conclude otherwise." Accordingly, the Court reversed the district court's order denying Burke's request for credit for time served and remanded the case for the district court to enter an order crediting him with the fifty-six days he spent committed to State Hospital North while the State restored his competency to face criminal charges.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Gibbs

Court: Iowa Supreme Court
Docket: 18-1298
Opinion Date: April 17, 2020
Judge: Edward M. Mansfield
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction of murder in the second degree, holding that Defendant's Fifth Amendment rights were invaded when the trial judge instructed the jury that Defendant was required to notify law enforcement of his use of deadly force, but the error was harmless. During trial, Defendant asserted the defense of justification in his shooting of the victim. At issue on appeal was whether the district court abused its discretion by giving a jury instruction incorporating the terms of Iowa Code 704.2B. The instruction included a statement that a person using deadly force is required to notify law enforcement about his use of deadly force. Defendant argued before the Supreme Court that both section 704.2B and the jury instruction incorporating that section violated his Fifth Amendment rights. The Supreme Court affirmed, holding (1) instructing the jury that a homicide defendant is required to notify a law enforcement agency of his use of deadly force violates the defendant's Fifth Amendment rights; but (2) any error in this case was harmless beyond a reasonable doubt.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Broxton

Court: Kansas Supreme Court
Docket: 114675
Opinion Date: April 17, 2020
Judge: Stegall
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's convictions for second-degree murder, burglary, and theft but reversed Defendant's sentences, holding

that any error during the guilt phase was harmless but that the district court erred by scoring Defendant's prior Florida burglary conviction as a person felony instead of a nonperson felony. On appeal, the court of appeals concluded that a trial court may instruct the jury on felony murder even though the State only charged the defendant with premeditated first degree murder. The Supreme Court disagreed, holding (1) the court of appeals erred in concluding that a district court may elect to provide a felony-murder instruction when that crime was not charged, and the district court properly found that the felony-murder instruction was not legally appropriate in this case; (2) the district court erred by excluding from evidence an exculpatory document from a Florida homicide investigation on the ground it was not relevant, but the error was harmless; and (3) the district court improperly scored Defendant's prior Florida burglary conviction as a person felony.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Corbin

Court: Kansas Supreme Court
Docket: 119665
Opinion Date: April 17, 2020
Judge: Dan Biles
Areas of Law: Criminal Law

The Supreme Court affirmed the ruling of the district court on remand resentencing Defendant to his original mandatory term of imprisonment after once again finding he was not a person with intellectual disability, holding that the district court did not abuse its discretion when it rejected Defendant's intellectual disability motion and imposed a mandatory term of imprisonment. Defendant pled no contest to first-degree premeditated murder. Before sentencing, Defendant filed a motion pursuant to Kan. Stat. Ann. 21-6622(b) asserting that he was a person with intellectual disability and was thus not subject to a mandatory minimum prison term. The district court denied the motion and sentenced Defendant to a hard twenty-five life sentence. While Defendant's appeal was pending, the Legislature amended Kan. Stat. Ann. 76-12b01(i), which provides new standards for deciding intellectual disability. The Supreme Court reversed and remanded for reconsideration of Defendant's motion using the new criteria. On remand, the district court reaffirmed its earlier ruling and again sentenced Defendant

to a hard twenty-five life sentence. The Supreme Court affirmed, holding that the district court's ruling was reasonably based on the law and was supported by substantial competent evidence.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Frazier

Court: Kansas Supreme Court
Docket: 117456
Opinion Date: April 17, 2020
Judge: Wilson
Areas of Law: Criminal Law

The Supreme Court reversed the decision of the district court affirming the judgment of the district court denying Defendant's motion to withdraw plea of no contest to one count of possession of heroin with intent to distribute, holding that the district court's decision in finding no good cause for Defendant to withdraw his plea was based on errors of fact and law, which were grounds for finding abuse of discretion. On appeal, Defendant argued that the district court abused its discretion in denying his motion to withdraw his plea of no contest based on misleading or false statements contained in the plea agreement. The court of appeals affirmed the district court. The Supreme Court reversed, holding (1) there was enough uncertainty in this case to indicate that Defendant's plea agreement was not understandingly made; and (2) therefore, Defendant must be allowed to withdraw his plea.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Harris

Court: Kansas Supreme Court
Docket: 117362
Opinion Date: April 17, 2020
Judge: Wilson
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court reversed the judgment of the court of appeals affirming Defendant's conviction of possession fo marijuana, holding that Defendant's waiver of jury trial was legally insufficient. On appeal, Defendant argued that

he did not properly waive his right to a jury and asserted three other issues. The Supreme Court reversed the judgment of the court of appeals affirming Defendant's convictions without addressing the three remaining issues, holding that because the district court failed properly to apprise Defendant of his right to a jury trial and failed to ensure that Defendant understood the nature of the right he was giving up, Defendant's constitutional right to a jury trial was violated in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Uk

Court: Kansas Supreme Court
Docket: 119712
Opinion Date: April 17, 2020
Judge: Wilson
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's conviction for first-degree premeditated murder, holding that the district court did not err in its challenged instructions to the jury. Specifically, the Supreme Court held (1) the district court did not err in refusing to give the jury Defendant's requested instruction on voluntary manslaughter as a lesser included offense of first-degree murder because the instruction was not factually appropriate; and (2) the district court did not commit clear error in issuing an unmodified version of Instruction No. 11, which contained the definition of "premeditation" and mirrored PIK Crim. 4th 54.150(d) because the instruction was legally appropriate.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Catruch

Court: Maine Supreme Judicial Court
Citation: 2020 ME 52
Opinion Date: April 23, 2020
Judge: Andrew M. Mead
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed the judgments of the trial court

terminating Appellant's participation in the Co-Occurring Disorders and Veterans Court (Veterans Court), holding that the court did not err or abuse its discretion in terminating Appellant's participation in the Veterans Court. The Veterans Court is a criminal docket that provides judicial monitoring, specialized treatment, and other services for military veterans who have disorders often attributable to their military service. Appellant was charged with leaving the scene of an accident and three other offenses. Appellant was admitted to the Veterans Court. Agreeing to sentencing outcomes in a plea agreement and entering into a bail contract, Appellant pleaded guilty to all charges against him. The court later terminated Appellant's participation in the Veterans Court, finding that Appellant had violated the conditions of his bail contract. The Supreme Judicial Court affirmed, holding (1) this matter was properly before the Court; and (2) given Appellant's failure to comply with the requirements for participation in the treatment court and his violations of the agreements, his termination from the Veterans Court was warranted.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Paquin

Court: Maine Supreme Judicial Court
Citation: 2020 ME 53
Opinion Date: April 23, 2020
Judge: Andrew M. Mead
Areas of Law: Constitutional Law, Criminal Law

In this appeal from Defendant's conviction for eleven counts of gross sexual misconduct, the Supreme Judicial Court vacated the judgment of conviction on one count, vacated the dismissal of other counts and remanded for entry of a judgment of acquittal on those counts, and affirmed in all other respects, holding that Defendant's convictions on both Counts 5 and 30 violated his double jeopardy protections and that the court erred in allowing the State to dismiss Counts 27, 28, and 29 during trial without Defendant's consent. The indictment charged Defendant with fifteen counts (Counts 1-13, 30-31) of gross sexual misconduct against the victim and sixteen counts (Counts 14-29) of gross sexual misconduct against a second alleged victim. During trial, the court granted Defendant's motion for a judgment of acquittal on Counts 10-13, and the State dismissed Counts 27-29. Defendant was

found guilty of Counts 1-9 and 30-31 and not guilty on the remaining counts. The court entered judgment in accordance with the verdict. The Supreme Judicial Court held that the trial court erred in failing to rule that the Double Jeopardy Clause barred convictions on both Counts 5 and 30 and allowing the State to dismiss Counts 27, 28, and 29 rather than entering a judgment of acquittal on those counts.

Read Opinion Are you a lawyer? **Annotate this case**.

Watson v. State

Court: Maine Supreme Judicial Court
Citation: 2020 ME 51
Opinion Date: April 21, 2020
Judge: Joseph Jabar
Areas of Law: Criminal Law

The Supreme Judicial Court vacated the judgment of the unified criminal docket denying Appellant's petition for post-conviction review, holding that Appellant was deprived of the effective assistance of counsel when his trial attorney played a video of the ten-year-old victim's interview with police and that Appellant was adversely affected. Appellant was convicted of two counts of gross sexual assault, one count of unlawful sexual contact, and one count of visual sexual aggression against a child. The Supreme Court affirmed. Appellant later filed a petition for post-conviction review claiming that his trial attorney's representation was deficient because introducing the videotaped recording of the victim's entire interview with law enforcement was unnecessary to provide evidence supporting the victim's potential motive to fabricate the allegations. The post-conviction court denied denied the petition. The Supreme Court vacated the judgment below, holding that trial counsel's conduct was deficient and that counsel's actions rose to the level of comprising the reliability of Appellant's conviction and undermining confidence in it.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. Mazza

Court: Massachusetts Supreme Judicial Court

Docket: SJC-11363
Opinion Date: April 21, 2020
Judge: Budd
Areas of Law: Criminal Law

The Supreme Judicial Court reversed the order of the superior court denying Defendant's motion for a new trial and set aside the jury's verdicts of first degree murder and robbery, holding that a recently discovered witness statement made to the police ago constituted newly discovered evidence that "would probably have been a real factor in the jury's deliberations." At issue was Defendant's sixth motion for a new trial, which was predicated on newly discovered evidence consisting of, among other things, a recently discovered statement made to the police in 1972. The superior court denied the motion. As to the police statement, the judge found that it did not constitute newly discovered evidence because Defendant failed to establish that defense counsel did not have possession of it at the time of trial. The Supreme Judicial Court reversed and remanded the case for a new trial, holding (1) Defendant sustained his burden of establishing that defense counsel did not have the 1972 police statement prior to or at trial, and therefore, the statement constituted newly discovered evidence; and (2) there was a substantial risk that the jury would have reached a different conclusion had the evidence been admitted at trial.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. McCarthy

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12750
Opinion Date: April 16, 2020
Judge: Gaziano
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Judicial Court affirmed the judgment of the district court denying Defendant's motions to suppress, holding that the limited use of automatic license plate readers (ALPRs) in this case did not implicate constitutional protections against unreasonable searches. While police were investigating Defendant on suspicion of drug distribution they used ALPRs on two bridges to track Defendant's movements. The police accessed historical data via ALPR technology and received real-time alerts, the last of

which led to Defendant's arrest. Defendant filed motions to suppress the ALPR data and the fruits of the arrest. The superior court denied the motions. The Supreme Judicial Court affirmed, holding that while the widespread use of ALPRs in the Commonwealth could implicate a defendant's constitutional protected expectation of privacy in the whole of his public movements, that interest was not invaded by the limited extent and use of the ALPR data in the instant case.

Read Opinion Are you a lawyer? **Annotate this case**.

Garden v. Commonwealth

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12821
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed the judgment of a single justice of the court denying Petitioner's petition for extraordinary relief under Mass. Gen. Laws ch. 211, 3 seeking an order vacating Petitioner's plea to aggravated rape and dismissing the underlying indictment, holding that the single justice did not err or abuse his discretion in denying relief. The issues raised by Petitioner had all been raised and adjudicated through the normal appellate process. Petitioner then filed a motion to withdraw his guilty plea. The motion was denied, and the Appeals Court affirmed. In this petition for extraordinary relief, Petitioner sought an order vacating his plea to aggravated rape and dismissing the underlying indictment. The single justice denied relief. The Supreme Judicial Court affirmed, holding that the superintendence power was not available as an additional layer of appellate review once all other avenues had been exhausted.

Read Opinion Are you a lawyer? **Annotate this case**.

In re Mitchell

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12910
Opinion Date: April 22, 2020

Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed the judgment of the county court denying, without a hearing, Petitioner's petition for relief under Mass. Gen. Laws ch. 211, 3, holding that the single justice did not err or abuse his discretion in denying relief. Defendant was convicted of several offenses. The Appeals Court reversed the convictions and remanded the matter for a new trial. Thereafter, the Commonwealth filed a nolle prosequi as to all the charges. In his Mass. Gen. Laws ch. 211, 3 petition, Defendant alleged that no crime had been committed and that he was wrongfully prosecuted. The single justice denied relief. The Supreme Judicial Court affirmed, holding that Defendant did not demonstrate entitlement to the exercise of this Court's superintendence powers.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Reek

Court: Minnesota Supreme Court
Docket: A19-0153
Opinion Date: April 22, 2020
Judge: G. Barry Anderson
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction for first-degree murder, holding that there was no error in the proceedings below. Specifically, the Supreme Court held (1) Appellant's right to a fair trial before an impartial tribunal was not violated when the district court stated that it might reconsider its prior Spreigl ruling if the defense presented certain witnesses; (2) the jury instructions on accomplice liability were plainly erroneous, but Appellant failed to establish that there was a reasonable likelihood that the error had a significant effect on the verdict; (3) the prosecutor did not commit misconduct in his closing arguments regarding the law of accomplice liability; (4) the district court did not abuse its discretion by granting the State’s motion to admit evidence of appellant’s past convictions for impeachment purposes, including by allowing the specific convictions to be disclosed to the jury; and (5) Appellant’s pro se arguments were without merit.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Woodard

Court: Minnesota Supreme Court
Docket: A18-1886
Opinion Date: April 22, 2020
Judge: Hudson
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the district court convicting Defendant of first-degree murder and sentencing him to life in prison without the possibility of release, holding that the district court did not err in denying Defendant's motion to present an alternative-perpetrator defense. Specifically, the Supreme Court held (1) the district court did not abuse its discretion in holding that Defendant's proffered evidence in support of his motion to present alternative-perpetrator evidence for lack of sufficient foundation; and (2) the district court committed an error that was plain in instructing the jury on the order in which to consider the charges against Defendant, but there was no reasonable likelihood that the instruction affected the jury's verdict and therefore did not affect Defendant's substantial rights.

Read Opinion Are you a lawyer? **Annotate this case**.

Huff v. Brown

Court: Nebraska Supreme Court
Citation: 305 Neb. 648
Opinion Date: April 23, 2020
Judge: Lindsey Miller-Lerman
Areas of Law: Communications Law, Criminal Law

The Supreme Court reversed the portion of the district court's order granting in part a writ of mandamus requiring Doug Brown, the sheriff of Furnas County, to provide records to Herchel Huff pursuant to the public records statutes, holding that the district court erred when it determined that Huff had shown that Brown had a clear duty to provide the requested records. Huff, an inmate, sought, among other documents, the criminal history

records of jurors who had convicted hims. Furnas County sheriff Kurt Kapperman required a deposit of $750 before fulfilling the request. Huff subsequently filed a petition for writ of mandamus naming Kapperman as the defendant and seeking an order compelling Kapperman to release all requested documents. The court permitted Huff to substitute Brown, the current sheriff, in the caption of the case in place of Kapperman and granted in part mandamus. The Supreme Court reversed in part, holding that the district court (1) did not err when it substituted Brown's name for Kapperman's; but (2) erred in issuing mandamus because Huff failed to demonstrate a prima facie case that he had been denied a request for public records that the sheriff had a clear duty to provide under Neb. Rev. Stat. 84-712.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Montoya

Court: Nebraska Supreme Court
Citation: 305 Neb. 581
Opinion Date: April 17, 2020
Judge: Freudenberg
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the judgment of the district court affirming Defendant's conviction and sentence for driving under the influence, holding that there was no error in the challenged rulings by the trial court. Specifically, the Supreme Court held that the district court did not err by (1) affirming the county court's order denying Defendant's motion to suppress fruits of the stop; (2) affirming the county court's order that denied Defendant's motion to suppress the fruits of his arrest; (3) affirming the county court's order that denied Defendant's motion to suppress the results of the test of his breath alcohol content; (4) finding sufficient evidence to support the conviction; and (5) finding that Defendant's sentence was not excessive.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Schroeder

Court: Nebraska Supreme Court
Citation: 305 Neb. 527
Opinion Date: April 17, 2020
Judge: Funke
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's sentence of death for first degree murder, holding that there was no error in the sentence imposed by the sentencing panel. Specifically, the Supreme Court held that the sentencing panel did not err in (1) allowing the State to introduce evidence on the existence of mitigating circumstances; (2) acknowledging and weighing mitigating evidence from the presentence investigation report; (3) not requesting that documentation from the Department of Correctional Services regarding Defendant's time in custody for mitigation purposes be included in the presentence investigation report; (4) sentencing Defendant to death, where the Legislature has enacted safeguards to ensure fairness and accuracy in the resulting sentence; and (5) finding Defendant should be sentenced to death after balancing the aggravating evidence and mitigating evidence.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Kendrick v. Parker

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1509
Opinion Date: April 21, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals denying Appellant's request for a writ of prohibition and/or mandamus against Montgomery County Court of Common Pleas Judge E. Gerald Parker Jr., holding that the court of appeals correctly determined that Appellant's claim was barred by res judicata. Appellant sought a petition for writ of prohibition and/or mandamus against Judge Erik Blaine, the successor to the judge who sentenced Appellant, alleging that the sentencing court patently and unambiguously lacked jurisdiction to sentence him. Judge Parker, who had succeeded Judge Blaine, subsequently filed a motion for summary judgment. The court of appeals granted summary judgment for Judge

Parker, concluding that Appellant failed to demonstrate that the sentencing court patently and unambiguously lacked jurisdiction or that he lacked an adequate remedy at law and that res judicata barred Appellant's claim. The Supreme Court affirmed, holding that Appellant's claim was barred by res judicata.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Nelson v. Russo

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1541
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals dismissing Appellant's petition for a writ of mandamus seeking to compel Cuyahoga County Court of Common Pleas Judge Nancy Margaret Russo to vacate the consecutive prison sentences imposed on Appellant in 1987, holding that Appellant had an adequate remedy at law and was barred from asserting additional claims of sentencing error he could have raised in his previous mandamus action. In 1987, Appellant was convicted of four counts of rape and one count of kidnapping. Appellant was sentenced to prison terms of fifteen to twenty-five years for each of the five counts, to be served consecutively. In 2019, Appellant sought a writ of mandamus to compel Judge Russo to vacate his consecutive sentences. The court of appeals dismissed the writ action, concluding that res judicata barred Appellant's claim and that his prior appeals were an adequate remedy at law to address the alleged defect in his consecutive sentences. The Supreme Court affirmed, holding that Appellant was not entitled to a writ of mandamus in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Roberts v. Marsh

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1540

Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals dismissing Appellant's original action seeking a writ of procedendo and/or mandamus to compel Hamilton County Court of Common Pleas Judge Melba Marsh to issue a corrected sentencing entry, holding that the court of appeals correctly dismissed the petition as moot. Appellant was convicted of murder with a repeat-violent-offender specification. Appellant later asked the trial court to correct his sentence, arguing that he had improperly been sentenced to postrelease control. On remand, Judge Marsh vacated the postrelease-control sentence. Appellant appealed that order. The court of appeals noted that the trial court had not set forth all the information required under Crim.R. 32(C) in a single document and dismissed the appeal for lack of a final, appealable order. Appellant then filed this original action seeking to compel Judge Marsh to issue a corrected sentencing entry that constitutes a final, appealable order. Judge Marsh issued a nunc pro tunc sentencing entry that constituted a final, appealable order. The court of appeals then dismissed the petition as moot. The Supreme Court affirmed, holding that because Judge Marsh performed the act Appellant requested, the court of appeals dismissed the petition as moot.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Steiner v. Rinfret

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1510
Opinion Date: April 21, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals dismissing Appellant's petition for a writ of mandamus against Holmes County Court of Common Pleas Judge Robert D. Rinfret, holding that the court of appeals correctly determined that Appellant had an adequate remedy in the ordinary course of the law. Appellant, who was serving consecutive prison terms for five convictions, filed a petition for a writ of mandamus arguing that Judge Rinfret improperly sentenced him to a prison

term of nine years for his attempted rape conviction instead of the maximum term of eleven years. The court of appeals dismissed the petition, determining that Appellant had failed to file a mandatory affidavit of his prior civil actions and had an adequate remedy in the ordinary course of the law. The Supreme Court affirmed, holding that relief in mandamus was not available because Petitioner had an adequate remedy in the ordinary course of the law.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Jeffries

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1539
Opinion Date: April 22, 2020
Judge: Donnelly
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals upholding Defendant's convictions of four counts related to two specific instances of sexual abuse of D.S., holding that the trial court and court of appeals correctly applied Ohio's rape-shield law and determined that evidence of D.S.'s prior nonconsensual sexual assault was inadmissible. On appeal, Defendant asserted that the trial court erred in prohibiting him from introducing evidence during trial that D.S. had previously been sexually assaulted by another person, arguing that the rape-shield law applies only to an accuser's prior consensual sexual activity. The lower court held that Ohio's rape-shield law addresses all sexual activity, not only consensual sexual activity. The court of appeals affirmed. The Supreme Court affirmed, holding (1) the plain meaning of the term "sexual activity" as used in the rape-shield law includes both consensual and nonconsensual sexual activity; and (2) therefore, all sexual activity is barred from admission into evidence by the rape-shield, absent certain exceptions listed in the law.

Read Opinion Are you a lawyer? **Annotate this case**.

Pennsylvania v. Britton

Court: Supreme Court of Pennsylvania

Docket: 55 MAP 2018
Opinion Date: April 22, 2020
Judge: Max Baer
Areas of Law: Constitutional Law, Criminal Law

California law enforcement officers interviewed Appellant Stacy Britton in her California residence and, unbeknownst to her, recorded those interviews. Over Appellant's objection, Pennsylvania used those recordings as evidence to help convict Appellant of murder in Pennsylvania. The Pennsylvania Supreme Court granted allowance of appeal to examine whether the California law enforcement officers were acting as agents of the Pennsylvania State Police when they recorded the interviews with Appellant in her California home, and if so, whether Pennsylvania's constitutional and statutory protections were available to Appellant under those circumstances. The Court concluded the California law enforcement officers were not acting as agents of the Pennsylvania State Police when they interviewed Appellant, making analysis of whether any Pennsylvania-specific constitutional or statutory protections unwarranted. Because the Supreme Court concluded the Pennsylvania trial court reached the proper result in this matter, it affirmed that court's judgment.

Read Opinion Are you a lawyer? **Annotate this case**.

Pennsylvania v. Copenhaver

Court: Supreme Court of Pennsylvania
Docket: 48 MAP 2019
Opinion Date: April 22, 2020
Judge: Thomas G. Saylor
Areas of Law: Constitutional Law, Criminal Law

In August 2015, a deputy sheriff conducted a vehicle stop of Appellant Victor Copenhaver's pickup truck. Upon approaching the truck, the deputy noticed an odor of alcohol and marijuana emanating from the passenger compartment. After administering field sobriety tests, he arrested Appellant for suspected driving under the influence of alcohol and controlled substances ("DUI"). Appellant was ultimately charged with DUI and other offenses. Appellant challenged the deputy's authority to conduct a traffic stop and sought suppression of all evidence obtained during the encounter. Rather than presenting testimony at a suppression hearing, the parties

stipulated that Appellant was driving the vehicle in question and that the deputy had training and qualifications equivalent to that of a police officer. The parties also agreed that the vehicle stop occurred as a result of the deputy observing the tailgate to the pickup truck being in a down position, which caught the deputy's attention. The deputy further observed the registration on the pickup truck was expired, and additionally, the registration number was identified as belonging to a vehicle other than the one on which it was attached. The issue this case presented for the Pennsylvania Supreme Court's review was whether the deputy could lawfully conduct the traffic stop based on the expired registration sticker, on a theory that such a violation amounts to a breach of the peace. The Supreme Court concluded driving a vehicle with an expired registration did not entail a breach of the peace. It vacated the superior court's order insofar as it held that the expired registration was a breach of the peace, thus alone authorizing the deputy to stop Appellant's vehicle. Notably, in light of its holding, the Supreme Court found the superior court did not proceed to consider other relevant questions, such as whether the parties' factual stipulation should have been read as indicating that the officer's understanding that the registration sticker was associated with a different vehicle arose in the pre-stop timeframe – consistent with the Commonwealth's position throughout this litigation. "These issues should be resolved in the first instance by the intermediate court on remand."

Read Opinion Are you a lawyer? **Annotate this case**.

Pennsylvania v. Tedford

Court: Supreme Court of Pennsylvania
Docket: 773 CAP
Opinion Date: April 22, 2020
Judge: Donohue
Areas of Law: Constitutional Law, Criminal Law

Appellant Donald Tedford was convicted of first-degree murder and rape on February 6, 1987. He appealed the dismissal of his second petition for relief filed pursuant to the Post Conviction Relief Act ("PCRA"), on December 2, 2014, as amended by a counseled petition on May 5, 2015, and a supplemental petition filed on June 9, 2015. In connection with his initial filings, Tedford sought wholesale discovery of the prosecution's entire file,

but the PCRA court concluded that the petition (as amended) was not timely filed. Tedford also appealed the PCRA court's order denying his supplemental PCRA petition, in which he requested discovery, an evidentiary hearing, and/or a new trial based upon the admission of expert testimony presented at trial related to microscopic hair analysis. The PCRA court concluded that pursuant to PCRA Section 9545(b)(1)(ii), it had jurisdiction to consider the merits of Tedford's newly-discovered-facts claims, but ultimately it concluded Tedford had not asserted a meritorious claim in accordance with Section 9543(a)(2)(vi). Finding no reversible error in that analysis, the Pennsylvania Supreme Court affirmed dismissal of the petition for relief.

Read Opinion Are you a lawyer? **Annotate this case**.

Pennsylvania v. Trahey

Court: Supreme Court of Pennsylvania
Docket: 38 EAP 2018
Opinion Date: April 22, 2020
Judge: Wecht
Areas of Law: Constitutional Law, Criminal Law

The trial court granted Timothy Trahey's motion to suppress the results of a blood test that revealed his blood alcohol concentration ("BAC"), finding no justification for the investigating officers' failure to obtain a search warrant before conducting the test. On the Commonwealth's appeal, the Superior Court reversed, opining that the Commonwealth's evidence sufficiently established the existence of exigent circumstances, thus excusing the absence of a warrant. The Pennsylvania Supreme Court reversed, finding that while the exigency analysis is an objective one, "even disregarding the officers' subjective motivations, or their candid acknowledgment that they would have obtained a search warrant if they thought it necessary, there was no time-sensitive need to conduct a warrantless blood test under the circumstances of this case. Accordingly, the Superior Court's conclusion that the test was justified by exigent circumstances was drawn in error."

Read Opinion Are you a lawyer? **Annotate this case**.

In re Greg Abbott

Court: Supreme Court of Texas
Docket: 20-0291
Opinion Date: April 23, 2020
Judge: Per Curiam
Areas of Law: Constitutional Law, Criminal Law

The Supreme Court conditionally granted mandamus relief to the State seeking review of a temporary restraining order (TRO) blocking enforcement of Executive Order GA-13, which changes the rules applicable to judges' decisions regarding pre-trial bail, against judges, holding that the trial court lacked jurisdiction to order the judges' requested relief, even temporarily. GA-13 suspends certain statutes authorizing trial judges to release jail inmates with violent histories during the state of disaster due to the threat of the novel coronavirus. Plaintiffs alleged that GA-13 is unconstitutional and exceeds the governor's statutory emergency powers. Sixteen of the plaintiffs were Texas trial judges alleging that GA-13 improperly interferes with their judicial authority to make individualized bail decisions, and the other plaintiffs were public interest organizations and lawyer associations. The trial court issued a TRO blocking enforcement of GA-13 against judges. The Supreme Court conditionally granted mandamus relief, holding that the alleged threat of a criminal prosecution in this case did not give the judges standing to seek the invalidation of GA-13, and therefore, the trial court lacked jurisdiction to order their requested relief.

Read Opinion Are you a lawyer? **Annotate this case**.

Stahmann v. Texas

Court: Texas Court of Criminal Appeals
Docket: PD-0556-18
Opinion Date: April 22, 2020
Judge: Barbara Hervey
Areas of Law: Constitutional Law, Criminal Law

Appellant Karl Stahmann was involved in an automobile accident, after which he threw a bottle of promethazine, a controlled substance, over a nearby wire fence before law enforcement arrived. The bottle landed two to three feet past the fence in plain view. He was convicted of third-degree

felony tampering with physical evidence and was sentenced to 10 years' confinement and fined $5,000. The judge suspended his sentence and placed him on community supervision for 10 years. Stahmann appealed, arguing in part that the evidence was insufficient to prove that he destroyed, altered, or concealed the prescription bottle. The court of appeals agreed that the evidence was insufficient, but instead of rendering an acquittal, it reformed the judgment to show that Stahmann was convicted of the lesser-included offense of attempted tampering with physical evidence, a state-jail felony. After review of the evidence presented at trial, the Texas Court of Criminal Appeals concluded the evidence was indeed insufficient to prove that Appellant altered the prescription pill bottle when he threw it over the fence because the mere act of throwing the bottle did not change the bottle itself. "While a rational jury could have reasonably inferred that Stahmann intended to conceal the pill bottle when he threw it over the wire fence, the evidence shows that he failed to conceal it as he intended because the bottle landed short of the bush in plain view on top of some grass." The Court affirmed the trial court's judgment.

Read Opinion Are you a lawyer? **Annotate this case**.

Blanke v. Board of Pardons & Parole

Court: Utah Supreme Court
Citation: 2020 UT 16
Opinion Date: April 16, 2020
Judge: Himonas
Areas of Law: Criminal Law

The Supreme Court affirmed the decision of the court of appeals affirming the district court's denial of Appellant's petition for extraordinary relief, holding that, under the circumstances, the Utah Board of Pardons and Parole need not afford Appellant the due process protections explained in Neese v. Utah Board of Pardons and Parole, 416 P.3d 663 (2017), before it could determine that Appellant was a sex offender and condition his parole on sex offender treatment. Appellant was serving a prison sentence for his convictions of attempted child kidnapping and kidnapping. Because he was convicted of attempted child kidnapping Appellant was considered a sex offender under the sex offender registration statute. Further, Appellant admitted in his presentence report that he had sexual intercourse with a

fifteen-year-old. Appellant filed a petition for extraordinary relief alleging that the Parole Board had violated his due process rights by conditioning his parole on completion of sex offender treatment even though he had not committed a sex offense. Summary judgment was granted for the Parole Board. The Supreme Court affirmed, holding that the Parole Board owed Appellant no additional process before it considered unconnected sex offenses in its decision to require Appellant to undergo sex offender treatment.

Read Opinion Are you a lawyer? **Annotate this case**.

Washington v. Escalante

Court: Washington Supreme Court
Docket: 97268-1
Opinion Date: April 23, 2020
Judge: Steven González
Areas of Law: Constitutional Law, Criminal Law

Alejandro Escalante was detained for hours in a secured area at a border crossing and, the State conceded, interrogated by federal agents without Miranda warnings. Statements he made during that interrogation were used by the State to convict him of drug possession. While a traveler briefly detained and questioned at the border was typically not "in custody" for Miranda purposes, "the government's power to detain and question people at the border without implicating Miranda has limits." Here, the Washington Supreme Court determined those limits were reached. "This border detention created the type of inherently coercive environment that demands Miranda warnings to ensure an individual's choice to speak is the product of free will." The Supreme Court held that Escalante was in custody when he was interrogated and reversed.

Read Opinion Are you a lawyer? **Annotate this case**.

Washington v. Haggard

Court: Washington Supreme Court
Docket: 97375-0
Opinion Date: April 23, 2020

Judge: Barbara Madsen
Areas of Law: Constitutional Law, Criminal Law

A class C felony "washes out" and is omitted from a defendant's offender score as long as he or she is not convicted of any crime within five years of the last date of release from confinement. David Haggard was convicted of a misdemeanor offense within this five-year period, which was dismissed pursuant to RCW 3.66.067. When Haggard later pleaded guilty to burglary and arson, the trial court included prior class C felonies in his criminal history, finding that the dismissed misdemeanor conviction interrupted the washout period for those offenses. Haggard contended on appeal this was error. The Washington Supreme Court determined that because a dismissed conviction constituted a "conviction" under the Sentencing Reform Act of 1981 (SRA), and misdemeanor dismissal and vacation were distinct processes, so Haggard's offender score was properly calculated.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Taylor

Court: Supreme Court of Appeals of West Virginia
Docket: 18-0502
Opinion Date: April 21, 2020
Judge: Walker
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the judgment of the circuit court giving Petitioner credit for twelve days of time served toward the sentence he received for his felony conviction although Petitioner spent additional time in confinement for other charges that were dismissed in the universal plea agreement, holding that to grant Petitioner additional credit for time served would do little more than reward Petitioner for habitual criminal behavior. Petitioner was charged with several crimes and agreed to resolve the pending charges against him in a universal plea agreement. Under the terms of the agreement, Petitioner agreed to plea guilty to the charge of felony carrying a concealed firearm by a prohibited person. In exchange, the State agreed to drop the remaining charges. After he was sentenced, Petitioner argued that, in addition to the twelve days of credit for time served he was granted, he was constitutionally entitled to credit for time served

while he was incarcerated for charges that were resolved in the universal plea agreement. The Supreme Court affirmed, holding that Petitioner's circumstances implicated neither double jeopardy nor equal protection of the law such that additional credit for time served was constitutionally mandated.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Harrison

Court: Wisconsin Supreme Court
Dockets: 2017AP002441-CR, 2017AP002440-CR
Opinion Date: April 17, 2020
Judge: Patience D. Roggensack
Areas of Law: Criminal Law

The Supreme Court affirmed in part and reversed in part the decision of the court of appeals reversing an order of the circuit court that granted sentence credit to Defendant, holding that the court of appeals correctly found that Defendant was not entitled to sentence credit but erred by advancing the commencement of Defendant's terms of extended supervision for Defendant's 2007 and 2008 cases. Specifically, the Court held (1) Defendant was not entitled to sentence credit under Wis. Stat. 973.155(1)(a) because the days he spent in custody for which he sought sentence credit were not in connection with the courses of conduct for which those sentences were imposed; and (2) the court of appeals erred by advancing the commencement of Defendant's terms of extended supervision for his 2007 and 2008 cases to the date they would have begun but for Defendant's confinement for unrelated convictions that were later set aside, holding that whether to employ advancement is a public policy decision best left to the legislature.

Read Opinion Are you a lawyer? **Annotate this case**.

About Justia Opinion Summaries

Justia Weekly Opinion Summaries is a free service, with 63 different

newsletters, each covering a different practice area.

Justia also provides 68 daily jurisdictional newsletters, covering every federal appellate court and the highest courts of all US states.

All daily and weekly Justia newsletters are free. Subscribe or modify your newsletter subscription preferences at daily.justia.com.

You may freely redistribute this email in whole.

About Justia

Justia is an online platform that provides the community with open access to the law, legal information, and lawyers.

Contact Us | Privacy Policy

Unsubscribe From This Newsletter
or unsubscribe from all Justia newsletters immediately **here.**

Justia | 1380 Pear Ave #2B, Mountain View, CA 94043

From: Criminal Law - Justia Weekly Opinion Summaries
To: Grassia, Michael (POL)
Subject: Latest 101 Cases This Week: Ramos v. Louisiana (U.S.), United States v. Diaz-Rivera (1st Cir.), United States v. Cotto (2d Cir.)
Date: Friday, April 24, 2020 9:02:06 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

If you are unable to see this message, click here to view it in a web browser.

Justia Weekly Opinion Summaries

Criminal Law
April 24, 2020

Table of Contents

Ramos v. Louisiana
Civil Rights, Constitutional Law, Criminal Law
US Supreme Court

United States v. Diaz-Rivera
Criminal Law
US Court of Appeals for the First Circuit

United States v. Cotto
Criminal Law
US Court of Appeals for the Second Circuit

United States v. Rosa
Criminal Law
US Court of Appeals for the Second Circuit

Fogle v. Sokol
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Third Circuit

James v. New Jersey State Police
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Third Circuit

Bazemore v. Best Buy
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Akande
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Chambers
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Ferebee
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Nance
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Johnson
Criminal Law
US Court of Appeals for the Fifth Circuit

United States v. McGinnis
Criminal Law
US Court of Appeals for the Fifth Circuit

Valentine v. Collier
Civil Rights, Constitutional Law, Criminal Law, Government & Administrative Law, Health Law
US Court of Appeals for the Fifth Circuit

United States v. Dowl
Criminal Law
US Court of Appeals for the Sixth Circuit

United States v. Fowler
Criminal Law
US Court of Appeals for the Sixth Circuit

United States v. Sumlin
Criminal Law
US Court of Appeals for the Sixth Circuit

United States v. Vance
Criminal Law, White Collar Crime
US Court of Appeals for the Sixth Circuit

Winburn v. Nagy
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Sixth Circuit

Lund v. City of Rockford
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

United States v. Perez
Criminal Law
US Court of Appeals for the Seventh Circuit

Jackson v. United States
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Bolman
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Boyd
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Gonzalez-Esparsa
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Sanchez-Velasco
Criminal Law, Immigration Law
US Court of Appeals for the Eighth Circuit

Anthony v. TRAX International Corp.
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Ninth Circuit

City of Almaty v. Khrapunov
Criminal Law, International Law, White Collar Crime
US Court of Appeals for the Ninth Circuit

United States v. Baldon
Criminal Law
US Court of Appeals for the Ninth Circuit

United States v. Costanzo
Criminal Law
US Court of Appeals for the Ninth Circuit

United States v. Manzanares
Constitutional Law, Criminal Law
US Court of Appeals for the Tenth Circuit

United States v. Delaney
Criminal Law
US Court of Appeals for the District of Columbia Circuit

Antenor v. Alaska, Department of Corrections
Civil Procedure, Criminal Law, Government & Administrative Law
Alaska Supreme Court

Berger v. Bryant
Criminal Law
Arkansas Supreme Court

Carroll v. State
Criminal Law
Arkansas Supreme Court

Cave v. State
Civil Rights, Constitutional Law, Criminal Law
Arkansas Supreme Court

Chatmon v. Kelley
Criminal Law
Arkansas Supreme Court

McClinton v. State
Criminal Law
Arkansas Supreme Court

Siegel v. State
Criminal Law
Arkansas Supreme Court

Thomas v. State
Civil Rights, Constitutional Law, Criminal Law
Arkansas Supreme Court

California v. Landowski
Constitutional Law, Criminal Law
California Courts of Appeal

California v. May
Constitutional Law, Criminal Law
California Courts of Appeal

California v. Perez
Constitutional Law, Criminal Law
California Courts of Appeal

In re S.R.
Criminal Law
California Courts of Appeal

People v. Bell
Criminal Law
California Courts of Appeal

People v. Drayton
Criminal Law
California Courts of Appeal

People v. Robinson
Criminal Law
California Courts of Appeal

People v. Torres
Criminal Law
California Courts of Appeal

Colorado v. Lujan
Constitutional Law, Criminal Law
Colorado Supreme Court

Archer v. State
Civil Rights, Constitutional Law, Criminal Law
Florida Supreme Court

Collins v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Heyward v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Howard v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Keller v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Mills v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Moore v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Morris v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Rickman v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Robinson v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Santana v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Sullivan v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Turner v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Valrie v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Williams v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

State v. Malave
Criminal Law
Supreme Court of Hawaii

State v. Malave
Criminal Law
Supreme Court of Hawaii

Idaho v. Burke
Constitutional Law, Criminal Law
Idaho Supreme Court - Criminal

State v. Gibbs
Civil Rights, Constitutional Law, Criminal Law
Iowa Supreme Court

State v. Broxton
Criminal Law
Kansas Supreme Court

State v. Corbin
Criminal Law
Kansas Supreme Court

State v. Frazier
Criminal Law
Kansas Supreme Court

State v. Harris
Civil Rights, Constitutional Law, Criminal Law
Kansas Supreme Court

State v. Uk
Criminal Law
Kansas Supreme Court

State v. Catruch
Criminal Law
Maine Supreme Judicial Court

State v. Paquin
Constitutional Law, Criminal Law
Maine Supreme Judicial Court

Watson v. State
Criminal Law
Maine Supreme Judicial Court

Commonwealth v. Mazza
Criminal Law
Massachusetts Supreme Judicial Court

Commonwealth v. McCarthy
Civil Rights, Constitutional Law, Criminal Law
Massachusetts Supreme Judicial Court

Garden v. Commonwealth
Criminal Law
Massachusetts Supreme Judicial Court

In re Mitchell
Criminal Law
Massachusetts Supreme Judicial Court

State v. Reek
Civil Rights, Constitutional Law, Criminal Law
Minnesota Supreme Court

State v. Woodard
Criminal Law
Minnesota Supreme Court

Huff v. Brown
Communications Law, Criminal Law
Nebraska Supreme Court

State v. Montoya
Civil Rights, Constitutional Law, Criminal Law
Nebraska Supreme Court

State v. Schroeder
Criminal Law
Nebraska Supreme Court

State ex rel. Kendrick v. Parker
Criminal Law
Supreme Court of Ohio

State ex rel. Nelson v. Russo
Criminal Law
Supreme Court of Ohio

State ex rel. Roberts v. Marsh
Criminal Law
Supreme Court of Ohio

State ex rel. Steiner v. Rinfret
Criminal Law
Supreme Court of Ohio

State v. Jeffries
Criminal Law
Supreme Court of Ohio

Pennsylvania v. Britton
Constitutional Law, Criminal Law
Supreme Court of Pennsylvania

Pennsylvania v. Copenhaver
Constitutional Law, Criminal Law
Supreme Court of Pennsylvania

Pennsylvania v. Tedford
Constitutional Law, Criminal Law
Supreme Court of Pennsylvania

Pennsylvania v. Trahey
Constitutional Law, Criminal Law
Supreme Court of Pennsylvania

In re Greg Abbott
Constitutional Law, Criminal Law
Supreme Court of Texas

Stahmann v. Texas
Constitutional Law, Criminal Law
Texas Court of Criminal Appeals

Blanke v. Board of Pardons & Parole
Criminal Law
Utah Supreme Court

Washington v. Escalante
Constitutional Law, Criminal Law
Washington Supreme Court

Washington v. Haggard
Constitutional Law, Criminal Law
Washington Supreme Court

State v. Taylor
Civil Rights, Constitutional Law, Criminal Law
Supreme Court of Appeals of West Virginia

State v. Harrison
Criminal Law
Wisconsin Supreme Court

COVID-19 Updates: Law & Legal Resources Related to Coronavirus

Click here to remove Verdict from subsequent Justia newsletter(s).

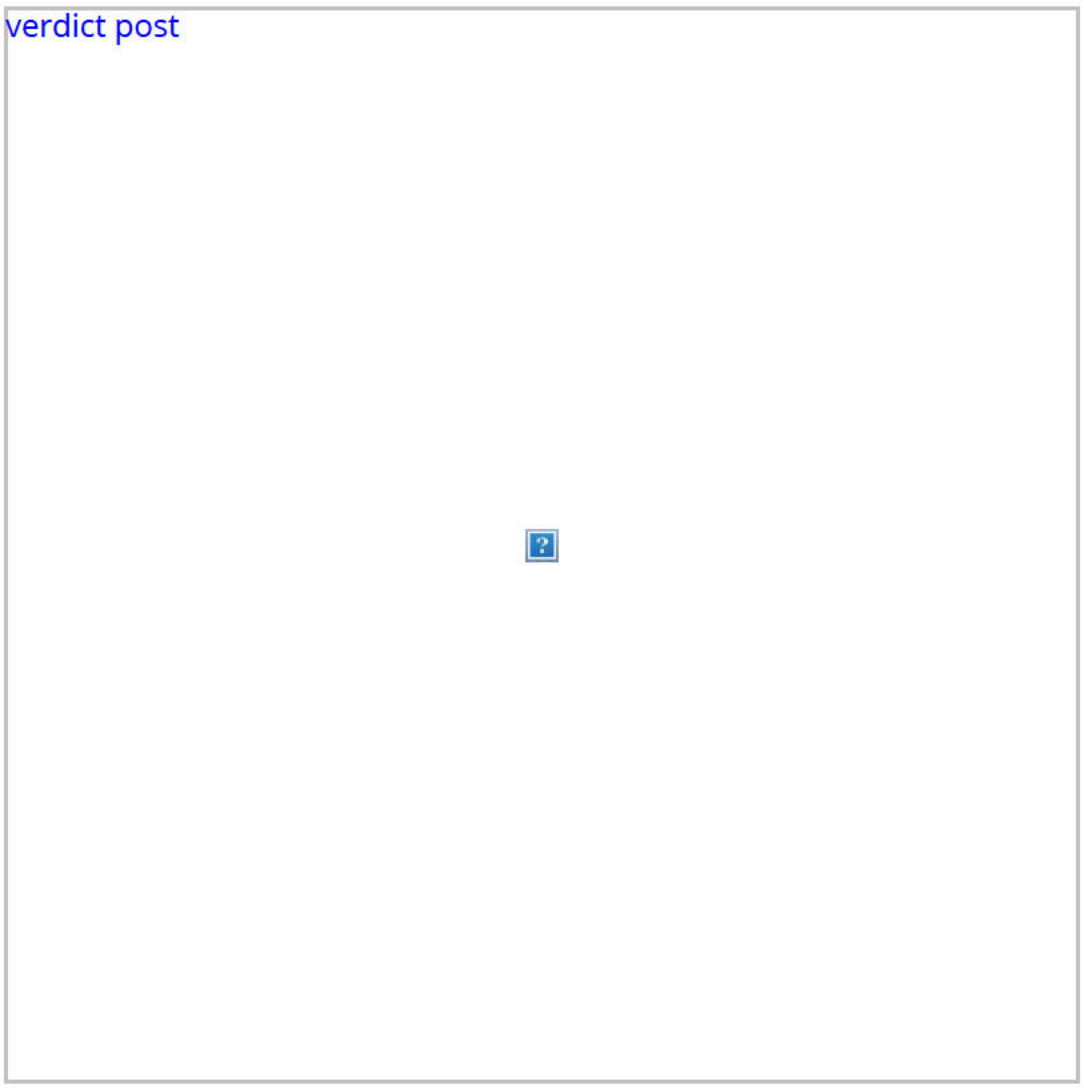
New on Verdict

Legal Analysis and Commentary

Rethinking Retroactivity in Light of the Supreme Court's Jury Unanimity Requirement

MICHAEL C. DORF

verdict post



In light of the U.S. Supreme Court's decision Monday in *Ramos v. Louisiana*, in which it held that the federal Constitution forbids states from convicting defendants except by a unanimous jury, Cornell law professor Michael C. Dorf discusses the Court's jurisprudence on retroactivity. Dorf highlights some costs and benefits of retroactivity and argues that the Court's refusal to issue advisory opinions limits its ability to resolve retroactivity questions in a way that responds to all the relevant considerations.

Read More

Criminal Law Opinions

Ramos v. Louisiana

Court: US Supreme Court
Docket: 18-5924
Opinion Date: April 20, 2020
Judge: Neil M. Gorsuch
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

In 48 states and in federal court, a single juror's vote to acquit is enough to prevent a conviction; Louisiana and Oregon punish people based on 10-to-2 verdicts. Ramos was convicted in a Louisiana court by a 10-to-2 jury verdict and was sentenced to life without parole. The Supreme Court reversed. The Sixth Amendment right to a jury trial, as incorporated against the states by the Fourteenth Amendment, requires a unanimous verdict to convict a defendant of a serious offense. Juror unanimity is a vital common law right. The Court rejected an "invitation" to "perform a cost-benefit analysis on the historic features of common law jury trials and to conclude that unanimity does not make the cut." In overturning its 1972 "Apodaca" decision, the Court stated that the reasoning, in that case, was "gravely mistaken" and "sits uneasily with 120 years of preceding case law." The fact that Louisiana and Oregon may need to retry defendants convicted of felonies by non-unanimous verdicts whose cases are still pending on direct appeal "will surely impose a cost, but new rules of criminal procedure usually do."

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Diaz-Rivera

Court: US Court of Appeals for the First Circuit
Docket: 18-1461
Opinion Date: April 20, 2020
Judge: Torruella
Areas of Law: Criminal Law

The First Circuit affirmed Defendant's upwardly variant sentence for one count of possession with intent to distribute cocaine and one count of using a firearm during and in relation to a drug-trafficking crime, holding that the sentence was neither procedurally nor substantively unreasonable. Pursuant to a plea agreement, Defendant pled guilty to drug-related crimes. After a sentencing hearing, the district court sentenced Defendant to an upwardly variant sentence of 180 months of imprisonment, thus declining to

impose the government's requested sentence. On appeal, Defendant challenged both the procedural and substantive reasonableness of his sentence. The First Circuit affirmed, holding that the 180-month sentence was neither procedurally nor substantively unreasonable.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Cotto

Court: US Court of Appeals for the Second Circuit
Docket: 18-2970
Opinion Date: April 20, 2020
Judge: Leval
Areas of Law: Criminal Law

A conviction for retaliating against a witness in violation of 18 U.S.C. 1513 does not require that the Government prove that defendant had knowledge of the federal nature of the proceeding. The Second Circuit rejected defendant's arguments to the contrary and affirmed his conviction for retaliating against a witness. The court remanded for revision of the provision of the sentence relating to the substance abuse treatment condition of supervised release; instructed the district court to consider on remand whether the court's forthcoming order in United States v. Traficante, No. 18-1962 (2d Cir., submitted Oct. 25, 2019) requires modification of the risk notification provision of supervised release; and granted the parties leave to reinstate this appeal to permit review of the district court's decision on remand as to the risk notification provision.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Rosa

Court: US Court of Appeals for the Second Circuit
Docket: 17-2004
Opinion Date: April 17, 2020
Judge: Nardini
Areas of Law: Criminal Law

Where a district court offers no explanation for its sentence, and where neither the adopted presentence report nor the statement of reasons

adequately demonstrates the court's reasoning, the court has committed plain error in violation of 18 U.S.C. 3553(c). The Second Circuit vacated defendant's sentence for conspiracy to commit wire fraud and aggravated identity theft. The court held that the district court failed to state its reasons for sentencing defendant as required under section 3553(c); the error is clear or obvious; and the error affected defendant's substantial rights. Accordingly, the court remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

Fogle v. Sokol

Court: US Court of Appeals for the Third Circuit
Docket: 19-1066
Opinion Date: April 21, 2020
Judge: Matey
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

In 1976, the body of 15-year-old “Kathy” was found near her Indiana County, Pennsylvania home. Kathy’s death involved a brutal assault, rape, and a gunshot to the head. Kathy's sisters, ages nine and 12, stated that she had gotten into a car with a man with blue eyes, black hair that came below his ears and curled at the ends, sideburns, heavy eyebrows, and a heavy mustache. Fogle had “straight reddish-blonde hair that dropped down his back and a matching, full beard that reached his waist.” After three years, Fogle became a suspect because a psychiatric patient described seeing Kathy get in a car with Fogle and his brother. The story was largely inconsistent with statements by Kathy’s sisters. Jailhouse informants were recruited and counseled by law enforcement with promises of leniency. The prosecutors “either knew about, encouraged, or permitted” this strategy. A jury found Fogle guilty of second-degree murder. In 2015, Fogle obtained DNA evidence excluding both himself and his brother as the source of semen collected from Kathy. His conviction was vacated. The Commonwealth declined to pursue new charges, describing the case as lacking “prosecutorial merit.” Fogle, having spent three decades in prison, sued the prosecutors and Indiana County under 42 U.S.C. 1983. The Third Circuit affirmed the denial of their motions to dismiss based on absolute immunity. Only truly prosecutorial functions, not investigative conduct, justify complete protection from suit. Fogle’s complaint alleges actions that fall

outside the narrow doctrine of absolute immunity.

Read Opinion Are you a lawyer? **Annotate this case**.

James v. New Jersey State Police

Court: US Court of Appeals for the Third Circuit
Docket: 18-1432
Opinion Date: April 21, 2020
Judge: Porter
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Stephens called 911 and reported that Gibbons hit her and had a gun in his truck. The police responded. Stephens obtained a temporary restraining order, prohibiting Gibbons from possessing firearms and from returning to Stephens's house. The next day, Gibbons went to Stephens's house. Stephens was talking on the phone; the friend called the police. Gibbons left Stephens's house. Trooper Conza arrived. Stephens stated that Gibbons had waved a gun throughout their argument. Conza told Stephens to go to the police barracks and reported over the radio that Gibbons had brandished a firearm. Conza, with Troopers Bartelt and Korejko, visited the nearby home of Gibbons's mother, James. James stated that she did not know where Gibbons was and that he might be off his schizophrenia medication. While driving to the barracks, Stephens saw Gibbons walking alongside the road and called 911. The Troopers responded. Bartelt parked his car and, exiting, observed that Gibbons was pointing a gun at his own head. Bartelt drew his weapon, stood behind his car door, and twice told Gibbons to drop his weapon. Gibbons did not comply. Bartelt shot Gibbons twice within seconds of stopping his car. Gibbons died that night. In James' suit under 42 U.S.C. 1983, the Third Circuit held that Bartelt is entitled to qualified immunity because he did not violate Gibbons's clearly established rights. Bartelt's pre-standoff knowledge of Gibbons differs from that of officers involved in cited cases. Bartelt could reasonably conclude that Gibbons posed a threat to others.

Read Opinion Are you a lawyer? **Annotate this case**.

Bazemore v. Best Buy

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-2196
Opinion Date: April 21, 2020
Judge: Quattlebaum
Areas of Law: Criminal Law

Plaintiff filed suit against her employer, Best Buy, claiming that she was harassed because of her race and gender and subjected to a hostile work environment in violation of Title VII of the Civil Rights Act of 1964. Plaintiff's complaint stemmed from an incident where a coworker made a racist and sexually charged joke to a small group of coworkers that included plaintiff. The Fourth Circuit affirmed the district court's motion to dismiss and held that, in the case of allegedly harassing comments by a co-worker, an employee must allege plausible facts that the employer knew, or should have known, about the harassment and failed to take action reasonably calculated to stop it. Because plaintiff failed to do this, the court affirmed the district court's judgment. In this case, the coworker's conduct was not imputable to Best Buy where Best Buy took steps that were not only reasonably calculated to end such behavior, but that it did in fact end it.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Akande

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-6833
Opinion Date: April 20, 2020
Judge: Diana Jane Gribbon Motz
Areas of Law: Criminal Law

After defendant moved under 28 U.S.C. 2255 to vacate his conviction based on the ineffective assistance of counsel, the district court denied the motion. The Fourth Circuit granted a certificate of appealability and reversed the district court's judgment. The court held that, given counsel's specific misadvice regarding defendant's rights to preserve his appellate rights, on which defendant understandably relied, the district court's general admonishments did not amount to the careful explanation that addresses the particular issue necessary to cure the error. In this case, the plea colloquy did not correct counsel's erroneous advice and the error prejudiced defendant. Accordingly, the court remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Chambers

Court: US Court of Appeals for the Fourth Circuit
Docket: 19-7104
Opinion Date: April 23, 2020
Judge: Floyd
Areas of Law: Criminal Law

After defendant was erroneously sentenced as a career offender, he moved to reduce his sentence to time served under the First Step Act. The district court denied defendant's motion to reduce his custodial sentence, though it granted the motion as to his supervised release term. The Fourth Circuit held that the First Step Act does not constrain courts from recognizing Guidelines errors. The court explained that First Step Act motions fall under 18 U.S.C. 3582(c)(1)(B), a distinct exception to finality, and that section 404(b) of the First Step Act expressly allows a court to impose a reduced sentence in order to give retroactive effect to sections 2 and 3 of the Fair Sentencing Act. Furthermore, 18 U.S.C. 3553(a) sentencing factors apply in the section 404(b) resentencing context, and the resentencing court has discretion within the section 404(b) framework to vary from the Guidelines and, in doing so, to consider movants' post-sentencing conduct. In this case, the district court seemingly believed that it could not vary from the Guidelines range to reflect post-sentencing information. Therefore, the court vacated the district court's sentencing order. Finally, the court held that any Guidelines error deemed retroactive, such as the error in this case, must be corrected in a First Step Act resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Ferebee

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-4266
Opinion Date: April 22, 2020
Judge: Traxler
Areas of Law: Criminal Law

The Fourth Circuit affirmed the denial of defendant's motion to suppress evidence recovered from a backpack, and the district court's conclusion that defendant abandoned the backpack and any legitimate expectation of privacy in its contents. The court rejected defendant's claim that the collective-knowledge doctrine has any bearing on the propriety of the district court's conclusion that defendant abandoned the backpack. The court also held that the district court is not precluded from finding abandonment in cases where the defendant, as here, has physical possession of the property he has disavowed. In this case, the record supported the district court's conclusion that defendant clearly and unequivocally disavowed ownership of the backpack. Even if the district court erred by finding that defendant abandoned the backpack, reversal would not be required because the search of the backpack was a proper search incident to arrest for which no warrant was required under the facts of this case.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Nance

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-4585
Opinion Date: April 21, 2020
Judge: Pamela Harris
Areas of Law: Criminal Law

The Fourth Circuit affirmed defendant's above-Guidelines sentence imposed after he pleaded guilty to two federal drug- and firearm-related offenses. The court held that defendant's sentence was not procedurally unreasonable where the district court took into account defendant's extensive criminal history; his pattern of reoffending upon release; his disciplinary infractions in custody and inability to comply with the terms of his release; and the fact that the offenses of conviction occurred over the course of days, in which he was arrested once, released, and then arrested again just days later. The court also held that defendant's sentence was substantively reasonable where the district court conducted a thorough, individualized assessment of defendant and his offense conduct in light of the 18 U.S.C. 3553(a) factors, and did not abuse its discretion in formulating the sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Johnson

Court: US Court of Appeals for the Fifth Circuit
Docket: 17-60852
Opinion Date: April 21, 2020
Judge: Priscilla R. Owen
Areas of Law: Criminal Law

The Fifth Circuit vacated defendant's sentence imposed after he pleaded guilty to violating 18 U.S.C. 922(g) and 924(e) by knowingly possessing a firearm after he had been convicted of a misdemeanor crime of domestic violence. The court held that the district court committing plain error by violating Federal Rule of Criminal Procedure 32 when it relied on factual allegations in the confidential sentencing recommendation that were not in the presentence report and that were not disclosed by defendant. The court explained that the use of undisclosed facts to justify an above-guidelines sentence seriously affects the fairness, integrity, and public reputation of judicial proceedings. Therefore, the court remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. McGinnis

Court: US Court of Appeals for the Fifth Circuit
Docket: 19-10197
Opinion Date: April 21, 2020
Judge: Stuart Kyle Duncan
Areas of Law: Criminal Law

18 U.S.C. 922(g)(8), which prohibits individuals subject to certain domestic violence protective orders from possessing firearms or ammunition for any purpose, is facially constitutional under the Fifth Circuit's two-step NRA framework. Even assuming arguendo that the conduct at issue -- the keeping and possessing of firearms by individuals subject to domestic protective orders -- falls within the Second Amendment right, defendant's facial challenge fails. The court applied intermediate scrutiny and held that section 922(g)(8) is reasonably adapted to the government interest of

reducing domestic gun abuse. The court also held that if the commonly understood definitions of terms in the protective order include acts involving "physical force," the protective order is sufficient to support a conviction under section 922(g)(8)(C)(ii). In this case, the jury plausibly found that the order satisfied the statute and the court declined to reverse defendant's conviction on this basis. However, the court remanded for the limited purpose of conforming defendant's written judgment to the district court's oral pronouncement.

Read Opinion Are you a lawyer? **Annotate this case**.

Valentine v. Collier

Court: US Court of Appeals for the Fifth Circuit
Docket: 20-20207
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Criminal Law, Government & Administrative Law, Health Law

Plaintiffs filed suit alleging that TDCJ's adoption and implementation of measures guided by changing CDC recommendations in regards to the COVID-19 pandemic do not go far enough. Plaintiffs filed a class action alleging violations of the Eighth Amendment's prohibition against cruel and unusual punishment, and the Americans with Disabilities Act, seeking a preliminary injunction. The Fifth Circuit granted TDCJ's motion to stay the district court's preliminary injunction, which regulates the cleaning intervals for common areas, the types of bleach-based disinfectants the prison must use, the alcohol content of hand sanitizer that inmates must receive, mask requirements for inmates, and inmates' access to tissues (amongst many other things). The court held that TDCJ is likely to prevail on the merits of its appeal because: (1) after accounting for the protective measures TDCJ has taken, plaintiffs have not shown a "substantial risk of serious harm" that amounts to "cruel and unusual punishment"; and (2) the district court committed legal error in its application of Farmer v. Brennan, by treating inadequate measures as dispositive of defendants' mental state. In this case, even assuming that there is a substantial risk of serious harm, plaintiffs lack evidence of defendants' subjective deliberate indifference to that harm. The court also held that TDCJ has shown that it will be

irreparably injured absent a stay, and that the balance of the harms and the public interest favor a stay. Finally, the court held that plaintiffs have not exhausted their administrative remedies as required in the Prison Litigation Reform Act (PLRA), and the district court's injunction goes well beyond the limits of what the PLRA would allow even if plaintiffs had properly exhausted their claims.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Dowl

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-2469
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

Dowl pleaded guilty to presenting false tax returns, 18 U.S.C. 286. He received a sentence of 30 months of imprisonment plus 24 months of supervised release. On supervised release, Dowl was charged with four new state crimes; failing to inform his probation officer that he had police contact; communicating with his co-defendant despite instructions to the contrary; failing to make payments on his restitution, fine, or special assessment; and failing to get a job. At a hearing, the court reviewed the evidence and allowed Dowl to tell his side of the story. The court deferred judgment on three of the four new state criminal law violations and dismissed the fourth and found Dowl gainfully employed. Dowl had failed to notify his probation officer about police contact, impermissibly communicated with his co-defendant, and did not pay his fines. After considering the 18 U.S.C. 3553(a) sentencing factors, the court returned Dowl to prison for 11 months, giving Dowl and his attorney the opportunity to raise any objections. Dowl had none. The Sixth Circuit affirmed, rejecting Dowl’s argument that the court committed reversible error by not directly addressing him to solicit an allocution. The court employed the “plain error” standard because Dowl did not raise any objection during his revocation hearing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Fowler

Court: US Court of Appeals for the Sixth Circuit
Dockets: 19-3071, 19-3070
Opinion Date: April 21, 2020
Judge: Donald
Areas of Law: Criminal Law

In 2018, Fowler pled guilty to possession of child pornography and violations of the conditions of his supervised release from a previous conviction for the same. In addition to possessing child pornography, Fowler had failed drug testing, had threatened his parole officer, and had tried to harass his girlfriend to recant her testimony. The district court ordered Fowler to pay a $5,000 special assessment for possession of child pornography under the Justice for Victims of Trafficking Act, 18 U.S.C. 3014. The court also varied upward and sentenced Fowler to the maximum statutory penalty for violating the conditions of his supervised release, imposing a 120-month sentence for possessing child pornography and a consecutive 36-month sentence for violating the terms of his supervised release. The Sixth Circuit vacated as to the assessment and remanded for a determination of indigency. The district court committed plain error by failing to address Fowler's ability to pay; the parties did not contemplate the $5,000 special assessment as a part of the waiver provision in the plea agreement. The court affirmed the sentence. The district court did not consider an impermissible factor (whether Fowler had actually touched a child) and Fowler had no other challenge to the reasonableness of his sentence,

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Sumlin

Court: US Court of Appeals for the Sixth Circuit
Docket: 18-3819
Opinion Date: April 21, 2020
Judge: Bush
Areas of Law: Criminal Law

Sumlin was convicted of the distribution of drugs that caused the 2015 death of Carrie Dobbins, 21 U.S.C. 841(a)(1) and (b)(1)(C), which carries enhanced penalty provisions. The Sixth Circuit affirmed his convictions and

his sentence to life in prison. The district court properly denied Sumlin's suppression motion, given that the affidavit established a sufficient nexus between his drug trafficking activity and residence that was searched. The court properly admitted testimony by the victim's sister, Kelly, who was Sumlin's former girlfriend and had purchased drugs from him. Kelly's testimony about Sumlin's drug-trafficking and that Sumlin was with Carrie on the day of her overdose was intrinsic proof that was relevant for providing background information and contextualizing the government's case against Sumlin. Sufficient evidence supported the jury's verdict that Sumlin distributed the drugs that caused Carrie's death.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Vance

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-5160
Opinion Date: April 17, 2020
Judge: Bush
Areas of Law: Criminal Law, White Collar Crime

The Spriggs' bank account was established to receive social security checks. The Spriggs' great-grandson, Vance, filled out an application in Mr. Spriggs's name for a debit card to draw on the checking account. Mr. Spriggs had never used a debit card. The Spriggses did not authorize Vance to do so. Bank cameras photographed Vance using the card to withdraw cash. Vance also used the card for personal expenses. At another bank, Vance used Mr. Spriggs's social security number to establish an account and obtain a $15,000 cash advance. Vance made other, unsuccessful loan applications. Upon being notified by the banks about suspicious activities involving his identity, Mr. Spriggs filed a police report. The police arrested Vance. While searching Vance's car, the police located a large stash of personal and financial documents belonging to the Spriggses, including bank statements, tax return forms, property-tax bills, and a car title. The Sixth Circuit affirmed Vance's convictions for access-device fraud, 18 U.S.C. 1029(a)(5), and two counts of aggravated identity theft, 18 U.S.C. 1028A(a)(1), and his 65-month sentence. The court rejected arguments that the district court failed to make adequate findings of fact after the bench trial, improperly denied a motion for judgment of acquittal,

and failed to correctly calculate the loss amount connected to Vance's charges under Sentencing Guidelines 2B1.1.

Read Opinion Are you a lawyer? **Annotate this case**.

Winburn v. Nagy

Court: US Court of Appeals for the Sixth Circuit
Dockets: 19-2399, 19-2398
Opinion Date: April 23, 2020
Judge: Jeffrey S. Sutton
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Winburn represented himself at his trial for armed robbery, home invasion, and conspiracy. Based on Winburn's disruptive behavior, the judge removed him from the courtroom and revoked Winburn's permission to represent himself, then granted a competency evaluation and a mistrial. While Winburn awaited his second trial, the judge permitted Winburn's stand-by attorney to withdraw because Winburn had sued her and enjoined Winburn from filing complaints or grievances against his new attorney, except to discharge her. Although represented by a new attorney, Winburn moved pro se to dismiss his charges on double jeopardy grounds. The trial judge denied the motion because Winburn's attorney had not filed it. Winburn filed a habeas petition under 28 U.S.C. 2241 challenging his retrial and another section 2241 petition challenging the injunction. The district judges denied both and declined to issue certificates of appealability. Winburn filed a notice of appeal for one petition and sought a certificate of appealability for the other. The Sixth Circuit held that state pretrial detainees proceeding under section 2241 may not appeal without certificates of appealability and granted Winburn a certificate on the injunction claim. A reasonable jurist could conclude that the unusual order was constitutionally infirm. The court denied relief with respect to double jeopardy. Winburn failed to exhaust his state-court remedies by a motion to dismiss.

Read Opinion Are you a lawyer? **Annotate this case**.

Lund v. City of Rockford

Court: US Court of Appeals for the Seventh Circuit

Docket: 19-1945
Opinion Date: April 20, 2020
Judge: ROVNER
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Lund, a reporter for the Rockford Scanner, heard, by police scanner, of multiple traffic stops in Midtown. He did not have a driver's license, so he rode a motorized bicycle to Midtown to take photographs. He suspected a prostitution sting operation. An officer noticed Lund and radioed the team. Officers Welsh and Campbell knew of Lund's previous anti-police speech. They directed Lund to "move on." Lund asked if he was breaking any laws. Campbell informed him that he was not, but that his continued presence would constitute obstruction of a police detail and result in arrest. Lund started his bicycle and called out, loudly, "goodbye officers." Concerned that Lund might post pictures on social media while the sting operation was ongoing and create a danger for unarmed undercover officers, the officers followed Lund and arrested him for driving the wrong way on a one-way street, operating a vehicle without insurance, obstructing a police officer, felony aggravated driving on a revoked license, and operating a motor vehicle without a valid drivers' license. News stories listed Lund's name as an arrestee in the prostitution sting. The charges against Lund were dismissed. Lund sued the officers and the city under 42 U.S.C. 1983. The Seventh Circuit affirmed summary judgment for the defendants on First Amendment retaliation and malicious prosecution under Illinois law, citing the Supreme Court's intervening "Nieves" (2019) holding, that, in most cases, probable cause to arrest defeats a claim of retaliatory arrest. There was probable cause to arrest Lund.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Perez

Court: US Court of Appeals for the Seventh Circuit
Docket: 18-3156
Opinion Date: April 23, 2020
Judge: KANNE
Areas of Law: Criminal Law

Beloit officers facilitated a recorded controlled buy of heroin from Perez, a suspected high-level drug dealer. Perez sold 98 grams of heroin to an

informant. Based on that transaction alone, Perez pled guilty to distributing heroin. At Perez's sentencing hearing, the judge expressed concern that the guidelines range of 33–41 months' imprisonment did not reflect the full scope of his drug trafficking. The PSR described conduct that suggested that Perez was responsible for distributing large quantities of heroin, methamphetamine, and cocaine. The judge continued the hearing, directing the government to file a memorandum, detailing which offense conduct it could support by a preponderance of the evidence. When the hearing reconvened, the government presented witness testimony that elaborated on conduct described in the PSR, including drug ledgers, Perez's post-arrest conversation with his girlfriend, large sums of cash, a money counter, cell phones, and Perez's passport. The judge calculated a higher guidelines range and imposed a 121-month sentence. The Seventh Circuit affirmed, rejecting an argument that the sentencing judge should have recused himself. Perez has not demonstrated that a reasonable observer would have questioned the judge's impartiality nor did he allege that the judge was biased based on events outside the proceedings. The judge's continuance was laudable, not prejudicial.

Read Opinion Are you a lawyer? **Annotate this case**.

Jackson v. United States

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1131
Opinion Date: April 20, 2020
Judge: Lavenski R. Smith
Areas of Law: Criminal Law

The Eighth Circuit affirmed the district court's denial of a 28 U.S.C. 2255 motion to vacate, set aside, or correct petitioner's sentence. The court held that the district court did not err in denying an evidentiary hearing as to petitioner's claim that counsel was constitutionally ineffective for failing to conduct adequate pretrial investigations. In this case, petitioner failed to identify any specific witnesses or evidence that counsel failed to uncover. Furthermore, petitioner failed to show that counsel's representation prejudiced his case. The court also held that the district court did not err in denying an evidentiary hearing as to petitioner's claim that his new counsel was ineffective for failing to subpoena witnesses, for convincing petitioner

not to testify, for failing to object to or appeal the district court's answer to a jury question, and for failing to object to the district court's designation of petitioner as a career offender.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Bolman

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-2759
Opinion Date: April 21, 2020
Judge: Jane Louise Kelly
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's conviction for involuntary manslaughter after he struck and killed his nephew with his truck. The court held that the evidence was sufficient to support the conviction, because a reasonable jury could find defendant grossly negligent beyond a reasonable doubt. The court also held that the district court did not plainly err by failing to instruct the jury that actual knowledge is an essential element of the offense that is separate from gross negligence, because the instructions, viewed as a whole, accurately and adequately defined the essential elements of the offense.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Boyd

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-3528
Opinion Date: April 17, 2020
Judge: Kobes
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's sentence imposed after he pleaded guilty to being a felon in possession of a firearm. The court held that the facts underlying defendant's prior arrests were part of his history and characteristics under 18 U.S.C. 3553(a), and thus the district court could consider defendant's arrest records and the circumstances of those arrests. The court explained that the arrests were listed in the presentence report

and gleaned from prior police reports. Furthermore, specific facts underlying the arrests may be considered for an upward departure and should be considered fair game for a variance where defendant did not object to them. The court also concluded that there is nothing here that suggested a corrected misstatement improperly influenced the district court's sentencing decision. Finally, the court held that the upward variance was not unreasonable in consideration of defendant's previous assaults, coupled with the facts underlying his arrest in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Gonzalez-Esparsa

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1477
Opinion Date: April 22, 2020
Judge: Grasz
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's conviction for unlawful use of an identification document and misuse of a social security number. The court held that the evidence was sufficient to support defendant's convictions where a reasonable juror could conclude that defendant knew the permanent resident card bearing his name and photograph had been forged, counterfeited, falsely made, or unlawfully obtained when he used it to secure employment. Furthermore, a reasonable juror could conclude that defendant made the false representation regarding his purported social security number in order to deceive Midwest Concrete in order to obtain a job with the company.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Sanchez-Velasco

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-3568
Opinion Date: April 17, 2020
Judge: James B. Loken
Areas of Law: Criminal Law, Immigration Law

The Eighth Circuit affirmed the district court's denial of defendant's motion to suppress his responses to an ICE agent's two questions at the Treasurer's Office, because he was not in custody at the time of questioning. Although defendant was in custody at the ICE facility, the court held that an agent's questions were not custodial interrogation because the agent could not have known his questions were likely to elicit incriminating information regarding the two criminal charges that were eventually brought against defendant. The court noted that the Attorney General's regulations carefully distinguish between the warrantless arrest of an alien for a criminal violation of the immigration laws, and what is called the "administrative arrest" of an alien who is reasonably believed to be illegally present in the United States. The court agreed with the district court that the agent's questioning was a request for routine information necessary for basic identification purposes that is not interrogation under Miranda, even if the information turns out to be incriminating.

Read Opinion Are you a lawyer? **Annotate this case**.

Anthony v. TRAX International Corp.

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-15662
Opinion Date: April 17, 2020
Judge: Kim McLane Wardlaw
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Ninth Circuit affirmed the district court's grant of summary judgment to TRAX in a disability discrimination action brought by plaintiff under Title I of the Americans with Disabilities Act (ADA). After TRAX terminated plaintiff from her position as a Technical Writer allegedly due to an inability or unwillingness to accommodate her disability, TRAX discovered during the course of litigation that plaintiff lacked the requisite bachelor's degree for her position. The panel held that, although McKennon v. Nashville Banner Publishing Co., 513 U.S. 352 (1995), held that after-acquired evidence cannot establish a superseding, non-discriminatory justification for an employer's challenged actions, after-acquired evidence remains available for other purposes, including to show that an individual is not qualified under the ADA. Because plaintiff did not satisfy one of the prerequisites for her

position, she is not "otherwise qualified," and TRAX was not obligated to engage in the interactive process.

Read Opinion Are you a lawyer? **Annotate this case**.

City of Almaty v. Khrapunov

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-56451
Opinion Date: April 22, 2020
Judge: Marbley
Areas of Law: Criminal Law, International Law, White Collar Crime

The City of Almaty, in Kazakhstan, filed suit against defendant and his family under the Racketeer Influenced and Corrupt Organizations Act (RICO), alleging that they engaged in a scheme to defraud the city of millions of dollars. The City claimed that it was forced to spend money and resources in the United States to trace where its money was laundered. The district court dismissed the City's claim on the basis that it failed to state a domestic injury pursuant to the Supreme Court's recent decision in RJR Nabisco, Inc. v. European Community, 136 S. Ct. 2090 (2016). The Ninth Circuit held that the City failed to state any cognizable injury other than the foreign theft of its funds, and its voluntary expenditures were not proximately caused by defendants' acts of money laundering. In this case, the City's expenditure of funds to trace its allegedly stolen funds is a consequential damage of the initial theft suffered in Kazakhstan and is not causally connected to the predicate act of money laundering.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Baldon

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-10411
Opinion Date: April 21, 2020
Judge: Bennett
Areas of Law: Criminal Law

After defendant pleaded guilty to possession with intent to distribute a controlled substance, the district court sentenced him to 184 months in

prison. The Ninth Circuit held that defendant's prior convictions for carjacking under section 215 of the California Penal Code are not categorical crimes of violence under USSG 4A1.1(e). Therefore, the district court incorrectly calculated defendant's criminal history by improperly including two points for his prior carjacking convictions. However, the panel held that the district court did not err in finding that defendant possessed a firearm under USSG 2D1.1(b)(1). Accordingly, the panel affirmed in part, vacated in part, and remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Costanzo

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-10291
Opinion Date: April 17, 2020
Judge: Michael Daly Hawkins
Areas of Law: Criminal Law

The Ninth Circuit affirmed defendant's conviction of five counts of money laundering, holding that a reasonable trier of fact could have found beyond a reasonable doubt that the money laundering transactions, in which payment was made via bitcoin, affected interstate commerce in some way or to some degree. In this case, the transfer involved the use of an Internet or cellular network connected Personal Computer Device (PCD) to transfer bitcoin (together with the digital code necessary to unlock the bitcoin) to the digital wallet of another Internet or cellular network connected PCD.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Manzanares

Court: US Court of Appeals for the Tenth Circuit
Docket: 18-2010
Opinion Date: April 17, 2020
Judge: Mary Beck Briscoe
Areas of Law: Constitutional Law, Criminal Law

Defendant-Appellant Archie Manzanares appealed a district court's denial of his 28 U.S.C. 2255 motion challenging his sentence under the Armed

Career Criminal Act (ACCA). Under the ACCA, an offense qualified as a violent felony by satisfying at least one of three definitions, which have come to be known as the Elements Clause, the Enumerated Clause, and the Residual Clause. Manzanares asserted that without the Residual Clause, his underlying New Mexico convictions (armed robbery, aggravated assault with a deadly weapon, and aggravated battery) no longer qualified as violent felonies. The district court denied the motion, concluding that all three underlying convictions satisfied the Elements Clause. Manzanares appealed the classification of the armed robbery conviction as a violent felony to the Tenth Circuit, and sought to expand the certificate of appealability to allow him to appeal the decision regarding the aggravated assault with a deadly weapon and aggravated battery convictions. After review, the Tenth Circuit affirmed the district court's denial of Manzanares's 2255 motion, and denied his motion to expand the COA.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Delaney

Court: US Court of Appeals for the District of Columbia Circuit
Docket: 18-3093
Opinion Date: April 17, 2020
Judge: David S. Tatel
Areas of Law: Criminal Law

The DC Circuit vacated the district court's denial of defendant's motion to suppress evidence. The court held that officers violated the Fourth Amendment when they seized defendant because they lacked reasonable suspicion to justify the stop. In this case, a seizure occurred when the officers pulled into the parking lot, partially blocked defendant's vehicle, and activated their take-down light. The court held that any inference of suspicion that the officers drew from encountering defendant soon after hearing the nearby gunshots were undermined by the government's failure to identify specific and articulable facts supporting the officers' estimation of where the various shots came from. Accordingly, the court remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

Antenor v. Alaska, Department of Corrections

Court: Alaska Supreme Court
Docket: S-17005
Opinion Date: April 17, 2020
Judge: Carney
Areas of Law: Civil Procedure, Criminal Law, Government & Administrative Law

Several Alaska Department of Corrections inmates challenged the DOC's policy to charge for local telephone calls, arguing the rates they and call recipients had to pay for calls violated their constitutional right to rehabilitation, their statutory right to reasonable telephone access, and DOC's contractual obligations under a prior settlement and consent decree. In addition, one of the prisoners challenged DOC officers' decision to deny him access to a computer programming book he ordered from outside the prison. He contended that DOC placed a content-specific restriction on the educational materials and publications prisoners were allowed, violating the Alaska Constitution's free speech provisions as well as prisoners' right to reformation. Each of these challenges reached the Alaska Supreme Court after inmates exhausted the administrative process from prison. Inmates then appealed to the superior court, which denied relief. The Alaska Supreme Court determined the superior court record did not provide enough evidence for it to meaningfully determine the reasonableness of the rates charged inmates for local telephone calls; therefore the Court reversed denial of relief and remanded for further fact-finding by the trial court. The Court concluded that the facility's restrictions on programming-related books were rationally related to a legitimate interest, and because they did not infringe on the right to rehabilitation, it affirmed denial of a prisoner's motion to enforce his claimed right to a particular text about computer programming.

Read Opinion Are you a lawyer? **Annotate this case**.

Berger v. Bryant

Court: Arkansas Supreme Court
Citation: 2020 Ark. 357
Opinion Date: April 23, 2020
Judge: Rhonda K. Wood

Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's petition to proceed in forma pauperis on a petition for writ of mandamus and a motion for declaratory judgment, holding that Appellant failed to state a colorable cause of action. In 1998, Appellant was convicted of rape. In his petition for a writ of mandamus, Appellant asserted that he sought information pursuant to the Arkansas Freedom of Information Act regarding his rape conviction but received no response. The circuit court denied the petition. The Supreme Court affirmed, holding (1) even if Appellant had requested disclosable information, he would not be entitled to inspect it as an incarcerated person; and (2) Appellant did not demonstrate a legitimate claim given the facts presented and therefore failed to establish a colorable cause of action to support his request to proceed in forma pauperis.

Read Opinion Are you a lawyer? **Annotate this case**.

Carroll v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 360
Opinion Date: April 23, 2020
Judge: Wynne
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's motion for leave to file a petition for writ of error cram knobs, holding that the circuit court did not abuse its discretion in declining to issue the writ. Appellant pled guilty to rape and was sentenced as a habitual offender to 720 months' imprisonment. In his coram nobis petition, Appellant alleged several grounds for relief, including claims of actual innocence, an invalid arrest warrant, a coerced guilty plea, and prosecutorial misconduct. The circuit court denied the motion. The Supreme Court affirmed, holding that Appellant did not demonstrate that that the writ should issue and failed diligently to proceed on his claim for coram nobis relief.

Read Opinion Are you a lawyer? **Annotate this case**.

Cave v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 356
Opinion Date: April 23, 2020
Judge: Josephine L. Hart
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's pro se petition for writ of habeas corpus, holding that the circuit court did not err in denying the petition. Appellant was found guilty of two counts of delivery of a controlled substance and one count of maintaining a drug premises. In his habeas petition, Appellant argued that he was actually innocent because his arrest and conviction was based on the false testimony of a witness who had a lengthy criminal history. Appellant further argued that the writ should issue because he was not afforded effective assistance of counsel. The circuit court denied the petition. The Supreme Court affirmed, holding (1) Appellant's claims regarding the witness's credibility do not constitute a valid assertion that he was being unlawfully detained; and (2) Appellant did not actually connect an allegation of ineffective assistance of counsel to his allegation that he was unlawfully detained.

Read Opinion Are you a lawyer? **Annotate this case**.

Chatmon v. Kelley

Court: Arkansas Supreme Court
Citation: 2020 Ark. 355
Opinion Date: April 23, 2020
Judge: Josephine L. Hart
Areas of Law: Criminal Law

The Supreme Court denied Appellant's appeal from the order of the circuit court denying his petition to proceed in forma pauperis on the grounds that Appellant failed to state a colorable cause of action in a petition for writ of habeas corpus, holding that the circuit court did not abuse its discretion by denying Appellant's in forma pauperis petition. In his habeas petition, Appellant alleged that the trial court lacked jurisdiction in his criminal case. Before this case was submitted to the Supreme Court, Appellant filed two

motions, including a "Judicial Notice of a Void Judgment" and a "Notice to the Court." The Supreme Court denied the motions, holding that neither motion was cognizable under the Court's rules. The Court then affirmed the Supreme Court's denial of Appellant's in forma pauperis petition, holding that the circuit court correctly found that Appellant did not assert a colorable cause of action.

Read Opinion Are you a lawyer? **Annotate this case**.

McClinton v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 353
Opinion Date: April 23, 2020
Judge: Karen R. Baker
Areas of Law: Criminal Law

The Supreme Court denied Petitioner's second petition requesting permission to proceed in the trial court with a petition for writ of error coram nobis, holding that Petitioner's proposed attack on the judgment had no merit. Petitioner was convicted of raping a mentally handicapped sixteen-year-old girl and was sentenced to life imprisonment. In his first petition for writ of error coram nobis Petitioner alleged a number of errors in the trial procedure. The first petition was denied. In his second coram nobis petition, Petitioner alleged violations of Brady v. Maryland, 373 U.S. 83 (1963). The Supreme Court denied the writ, holding that Petitioner failed to meet his burden of demonstrating a fundamental error of fact extrinsic to the record.

Read Opinion Are you a lawyer? **Annotate this case**.

Siegel v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 359
Opinion Date: April 23, 2020
Judge: Wynne
Areas of Law: Criminal Law

The Supreme Court dismissed Appellant's appeal from the circuit court's orders denying her motions to declare Ark. Code Ann. 5-62-106 (disposition

of animal) and Ark. Code Ann. 5-62-111 (prevention of cruelty) unconstitutional and conditionally granting her motion for return of seized property, holding that there was no final, appealable order in this case. Appellant was convicted of thirty-one misdemeanor counts of cruelty to animals. The circuit court subsequently dismissed the charges on speedy-trial grounds. The State appealed, and the Supreme Court dismissed the appeal on the grounds that it was not authorized. Appellant had filed motions seeking a declaration that sections 5-62-106 and -111 are unconstitutional and seeking the return of her seized property. The circuit court denied the constitutional claims and entered a conditional order granting Appellant's motion for return of seized property. Appellant appealed. The Supreme Court dismissed the appeal, holding that because the conditional order did not make specific findings as to the return of the property or as to damages and because it expressly left open the possibility of further proceedings, there was no final, appealable order in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

Thomas v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 354
Opinion Date: April 23, 2020
Judge: Josephine L. Hart
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Appellant's conviction of capital murder, holding that the evidence was sufficient to sustain the conviction and that the circuit court did not err in denying Appellant's motion to suppress tracking data generated by his cellphone. On appeal, Appellant argued that the trial court erred by denying his directed-verdict motion because the evidence supported the defense's theory of the case that he did not intend to shoot the victim. Further, Appellant argued that the court abused its discretion in denying his motion to suppress evidence obtained from the seizure of AT&T phone records. The Supreme Court disagreed, holding (1) the evidence was sufficient to support the capital murder conviction; and (2) the circuit court correctly denied the motion to suppress.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. Landowski

Court: California Courts of Appeal
Docket: C080210(Third Appellate District)
Opinion Date: April 23, 2020
Judge: Andrea Lynn Hoch
Areas of Law: Constitutional Law, Criminal Law

Defendant Michael Reyes, Jr., an active Norteno gang member (from the Broderick Boys subset), confronted a former Norteno gang member (from the Franklin Boys subset), "S.," about a physical altercation that occurred between S. and Reyes's stepfather over a debt. That earlier altercation had taken place in front of Reyes's autistic younger brother. Reyes pulled out a handgun and asked S. if he had a problem. S., who was riding his bicycle with his wife, "R.," when Reyes confronted him with the gun, stopped briefly, told Reyes to put the gun down if he wanted to fight, and then started to ride away. This angered Reyes, prompting him to fire six rounds at S. from behind. S. Was hit but survived. R. Was a short distance in front of S., but was not hit. Defendants Liberty Landowski and Lisa Humble were with Reyes at the time of the shooting and aided in his efforts to avoid being apprehended by law enforcement authorities. Reyes, Landowski, and Humble were tried together before the same jury. Reyes was convicted of one count of attempted murder (Count 1), two counts of assault with a semiautomatic firearm (Counts 2 and 4), one count of possession of a firearm by a convicted felon (Count 5), and one count of possession of ammunition by a convicted felon (Count 6). In addition to various firearm and other enhancements, the jury found Reyes committed the crimes for the benefit of, at the direction of, or in association with a criminal street gang with the specific intent to promote, further, or assist in criminal conduct by gang members. The jury convicted Landowski and Humble of being accessories to Reyes's criminal conduct (Count 9) and also found true gang enhancement allegations attached to that crime. Reyes challenged the sufficiency of the firearm evidence presented to support his conviction, and all defendants challenged the sufficiency of the evidence supporting their gang enhancements. The Court of Appeal determined Senate Bill 620 (2017-2018 Reg. Sess.) gave the trial court discretion to strike firearm enhancements in the interest of justice and applied retroactively; and Senate Bill 136 (2019-2020 Reg. Sess.) eliminated such enhancements,

and also applied retroactively. To these issues, the Court remanded for the trial court's consideration. The Court affirmed the trial court in all other respects.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. May

Court: California Courts of Appeal
Docket: C084302(Third Appellate District)
Opinion Date: April 20, 2020
Judge: Ronald B. Robie
Areas of Law: Constitutional Law, Criminal Law

Defendant Raymond May was found guilty by jury of possessing an assault weapon and a machine gun based on his possession of a single AK-47 assault rifle while guarding a marijuana plantation. He was sentenced to probation, which included an electronic search condition. On appeal, defendant argued there was a lack of sufficient evidence corroborating his accomplice's testimony and demonstrating he knew of the firearm's illegal character. He further alleged the trial court erred in instructing the jury: that the accomplice instruction should have included language specifying that the accomplice testimony needed to prove more than defendant's mere presence or access to the firearm. Furthermore, defendant argued the electronic search condition imposed as part of his probation failed under the standards announced in California v. Lent, 15 Cal.3d 481 (1975). The Court of Appeal agreed defendant's electronic search condition should have been stricken, but otherwise affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. Perez

Court: California Courts of Appeal
Docket: E072260(Fourth Appellate District)
Opinion Date: April 20, 2020
Judge: Miller
Areas of Law: Constitutional Law, Criminal Law

In 2009, defendant-appellant Rudy Perez pled guilty to active gang

participation under Penal Code section 186.22(a), and unlawful possession of a firearm under section 12025(b)(6). In 2010, defendant pled guilty to residential burglary under section 459, and active gang participation under section 186.22(a). In August of 2018, the State filed a new felony complaint, alleging one of the prior gang participation convictions as a strike prior. In 2018, defendant moved to vacate the two prior gang participation convictions based upon changes in the law that rendered them invalid. The trial court denied defendant's motion. In 2019, defendant asked for reconsideration, which was again denied. Thereafter, defendant filed a timely notice of appeal from the denial of his motion to vacate the convictions. The Court of Appeal found that defendant pled guilty to street terrorism under Penal Code section 186.22(a) in 2009 and 2010, and it was undisputed that while committing these offenses, defendant acted alone. However, subsequent to defendant's guilty pleas, in 2012, the California Supreme Court held that a defendant had to act in concert with a fellow gang member in order to be guilty of street terrorism. At that time, defendant could have filed a state habeas petition requesting relief, but failed to do so. "Defendants can lose remedies that are established by law when they fail to invoke such remedies in time." Section 1473.7 became effective in 2017. In defendant's motion filed in the trial court, defendant failed to state what new evidence was discovered, instead arguing that the trial court was allowed "to vacate a conviction where the defendant is innocent as a matter of law or where vacating the conviction is in the interest of justice, even though the defendant is no longer in custody or otherwise restrained by the conviction." The Court of Appeal concurred with the trial court's reason to deny relief, determining that "while the outcome in this case may be unfortunate for defendant, we are not here to rewrite legislation. The Legislature could amend section 1473.7 to address issues raised in this case. However, under the laws, as written, we must uphold the trial court's order."

Read Opinion Are you a lawyer? **Annotate this case**.

In re S.R.

Court: California Courts of Appeal
Docket: B300214(Second Appellate District)
Opinion Date: April 23, 2020
Judge: Bendix

Areas of Law: Criminal Law

Father appealed the juvenile court's dispositional ruling removing daughter from his custody, arguing that his mere possession of child pornography does not demonstrate that he poses a substantial risk of harm to his daughter. The Court of Appeal affirmed the order and held that there is substantial evidence of risk of great harm to daughter—no matter how low the probability— that father will sexually abuse his daughter if he is provided unfettered access to her.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Bell

Court: California Courts of Appeal
Docket: B288528(Second Appellate District)
Opinion Date: April 23, 2020
Judge: Stratton
Areas of Law: Criminal Law

Defendant was convicted of one count of attempted robbery, one count of second degree murder, and one count of hit and run driving. The jury found not true the allegation that a principal was armed in the commission of the attempted robbery. The trial court found true the allegations that defendant had served four prior prison terms within the meaning of Penal Code section 667.5, subdivision (b). Defendant raised 13 claims of error on appeal. The Court of Appeal held that the section 667.5, subdivision (b) enhancement terms must be stricken and the matter remanded to the trial court for resentencing. The court also held that defendant forfeited some of his substantive claims and other lack merit. Finally, the court held that, if there is instructional error, the errors are harmless under any standard of review. Accordingly, the court affirmed the judgment of conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Drayton

Court: California Courts of Appeal
Docket: H046928(Sixth Appellate District)

Opinion Date: April 17, 2020
Judge: Danner
Areas of Law: Criminal Law

In 1991, the Wards and their teenage daughter awoke and discovered four men, including Drayton, inside their house. Two were armed. One told the daughter he was going to rape her and placed a firearm inside her vagina. Drayton told the man not to do it. Drayton had a gun and held Mrs. Ward down during the robbery. Two others shot and killed Mr. Ward. Drayton and the others left without seeking help for the Wards. Drayton did not shoot Mr. Ward or threaten to rape the daughter. Drayton surrendered the next day. Drayton's sole prior conviction was a misdemeanor; he had no reported history of violence. Drayton was sentenced to 29 years to life imprisonment. In 2019, Drayton sought resentencing under Penal Code 1170.95, declaring that he "was not a major participant ... or did not act with reckless indifference to human life." Senate Bill 1437, effective January 1, 2019, restricted the circumstances under which a person can be liable for felony murder and enacted Penal Code 1170.95, which allows an individual, previously convicted of felony murder, to petition to have his murder conviction vacated and to be resentenced. The court of appeal directed the trial court to hold a hearing under section 1170.95(d) and to accept the assertions in the petition as true unless facts in the record conclusively refute them as a matter of law. If, accepting the petitioner's assertions as true, he meets section 1170.95(a)'s requirements for relief, the court must issue an order to show cause. In assessing the prima facie showing, the trial court should not weigh evidence or make credibility determinations.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Robinson

Court: California Courts of Appeal
Docket: B293746(Second Appellate District)
Opinion Date: April 20, 2020
Judge: Wiley
Areas of Law: Criminal Law

After defendant penetrated an unconscious woman with his fingers, he challenged evidentiary rulings and requests a presentence conduct credit. The Court of Appeal held that the trial court properly excluded cumulative

evidence about past times the woman was intoxicated at the relevant bar, and any error in allowing a drug recognition expert to testify about whether the woman was incapacitated was harmless. However, the court held that the trial court undercalculated defendant's presentence custody credit because he was not convicted of a violent felony under Penal Code section 2933.1, which would otherwise limit those credits. Accordingly, the court directed the trial court to award defendant 104 days of presentence custody credit and to amend the abstract of judgment, affirming in all other respects.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Torres

Court: California Courts of Appeal
Docket: B292551(Second Appellate District)
Opinion Date: April 20, 2020
Judge: Kenneth R. Yegan
Areas of Law: Criminal Law

Where, as here, the trial court factually finds that a self-represented defendant has engaged in an attempt to intimidate a witness, the constitutional right of self-representation can, in the exercise of the trial court's sound discretion, be revoked. The Court of Appeal affirmed defendant's conviction and sentence for two counts of battery on an ex-girlfriend. In this case, the trial court did not abuse its discretion in revoking defendant's pro se status after he asked his sister to contact the victim and have her say that she was coerced by the police detective to "press charges."

Read Opinion Are you a lawyer? **Annotate this case**.

Colorado v. Lujan

Court: Colorado Supreme Court
Citation: 2020 CO 26
Opinion Date: April 20, 2020
Judge: Brian D. Boatright
Areas of Law: Constitutional Law, Criminal Law

Abel Lujan was charged with first-degree murder for the death of his girlfriend after she was found beaten and strangled behind a friend's house. At trial, two women testified for the State about Lujan's prior violent behavior towards them. Prior to admitting this evidence, the trial court read a limiting instruction, telling the jury that it could only consider the evidence for the purposes of establishing Lujan's motive, intent, or common plan. A copy of this instruction was not given to the jury for deliberations; however, the jury did receive an instruction at the close of the evidence explaining that certain evidence could only be considered for the limited purposes for which it was admitted. While deliberating, the jury submitted a question seeking clarification about the limiting instruction. Over defense counsel's objection, the trial court cleared the courtroom of the public and parties, leaving only the judge, bailiff, and court reporter; the judge then brought in the jury and reread the limiting instruction that it had previously read twice in open court. The jury ultimately found Lujan guilty of second-degree murder. Lujan appealed, arguing that the court's actions when rereading the jury instruction constituted a courtroom closure that violated his Sixth Amendment right to a public trial. A division of the court of appeals agreed and reversed Lujan's conviction. The State argued on certiorari review that the Colorado Supreme Court adopt a triviality standard, under which a defendant's constitutional right to a public trial was not violated when the closure at issue was trivial. In so doing, the State argued that the brief courtroom closure here was trivial and therefore did not violate Lujan's public trial right. The Court concurred with the State, adopted the standard and reversed the appellate court's decision.

Read Opinion Are you a lawyer? **Annotate this case**.

Archer v. State

Court: Florida Supreme Court
Docket: SC19-841
Opinion Date: April 23, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the order of the circuit court denying Appellant's successive motion to vacate his sentence of death under Fla. R. Crim. P. 3.851, holding that the circuit court did not err in denying the Rule

3.851 motion. Appellant was convicted of first-degree murder, armed robbery, and grand theft. Appellant was sentenced to death for the murder. The Supreme Court affirmed the convictions but reversed Appellant's death sentence and remanded the case for a new penalty phase. After a new penalty phase, Appellant was again sentenced to death. In his successive Rule 3.851 motion, Appellant raised three claims. The circuit court denied relief. The Supreme Court affirmed, holding that the circuit court (1) properly denied Appellant's claim that his death sentence violated the Sixth and Eighth Amendments in light of Hurst v. Florida, 136 S. Ct. 616 (2016), and Hurst v. State, 202 So. 3d 40 (Fla. 2016); (2) correctly denied Appellant's claim that his sentence violated the Eighth Amendment; and (3) did not err in denying Appellant's claim of newly discovered evidence.

Read Opinion Are you a lawyer? **Annotate this case**.

Collins v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0158
Opinion Date: April 20, 2020
Judge: David E. Nahmias
Areas of Law: Constitutional Law, Criminal Law

Appellant Tommy Collins was convicted of felony murder in connection with the stabbing death of 14-year-old Rueben Hand. Friends gathered to watch the Peach Drop on New Year's Eve 2010; a disagreement ensued and Hand was stabbed near the Five Points MARTS station shortly after midnight. Appellant's only argument on appeal was that the trial court plainly erred when it gave the jury the State's requested instruction on "revenge for a prior wrong." Seeing no error, "much less plain error," the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Heyward v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0399
Opinion Date: April 20, 2020

Judge: Peterson
Areas of Law: Constitutional Law, Criminal Law

Larmell Heyward was convicted by jury of malice murder and possession of a firearm during the commission of a felony in connection with the 2007 shooting death of Ramon Rogers. Heyward argued on appeal of those convictions that the trial court erred in denying his request to charge the jury on voluntary manslaughter. After review, the Georgia Supreme Court determined the trial court's refusal to give the charge was harmless, since, in the Court's estimation, there was no realistic probability that the jury would have accepted the "slight" evidence of voluntary manslaughter in the light of the strong evidence of malice murder.

Read Opinion Are you a lawyer? **Annotate this case**.

Howard v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0819
Opinion Date: April 20, 2020
Judge: Keith R. Blackwell
Areas of Law: Constitutional Law, Criminal Law

Kenneth Howard was tried by jury and convicted of the murder of Emily Ann Smith Newbegin. Howard appealed, contending that the evidence was legally insufficient to sustain his conviction. Upon its review of the record and briefs, the Georgia Supreme Court found no merit in Howard's claim of error, and affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Keller v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0006
Opinion Date: April 20, 2020
Judge: Boggs
Areas of Law: Constitutional Law, Criminal Law

Randall Keller was convicted of felony murder and related crimes arising out

of the beating death of his ex-wife's two-year-old son, William Powell. On appeal, Keller raised numerous claims of error, including ineffective assistance of counsel, the trial court's rulings on motions before and during trial, several evidentiary rulings, and alleged bias on the part of the trial judge. However, finding no reversible error, the Georgia Supreme Court affirmed Keller's convictions.

Read Opinion Are you a lawyer? **Annotate this case**.

Mills v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0364
Opinion Date: April 20, 2020
Judge: Ellington
Areas of Law: Constitutional Law, Criminal Law

Roger Mills was found guilty by jury of malice murder and aggravated assault in connection with the death of Masuto Garrett. Mills contended that the trial court erred when, during jury deliberations, it excused a holdout juror without sufficient inquiry or good cause. After review, the Georgia Supreme Court concurred with that contention, and reversed Mills's convictions. The Court also concluded the evidence presented at trial was legally sufficient to support the convictions, so the State could retry Mills if it chose.

Read Opinion Are you a lawyer? **Annotate this case**.

Moore v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0344
Opinion Date: April 20, 2020
Judge: David E. Nahmias
Areas of Law: Constitutional Law, Criminal Law

Appellant Carzell Moore, proceeding pro se, appealed a trial court's denial of his motion to set aside a September 2017 order denying his motion for an out-of-time appeal of his 2002 resentencing on his 1977 convictions for murder and rape. Moore contended the trial court abused its discretion by

denying his motion to set aside because he was not given proper notice of the September 2017 order. Finding that the record supported the trial court's ruling, the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Morris v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0176
Opinion Date: April 20, 2020
Judge: Bethel
Areas of Law: Constitutional Law, Criminal Law

Darius Morris was found guilty by jury of malice murder and other offenses in connection with the shooting death of Jameson Bush. Morris appealed, arguing he was denied the right to a timely appeal, that the trial court erred in restricting voir dire as to the religious beliefs and connections of potential jurors, that the trial court erred by giving a confusing jury charge regarding statements of co-conspirators, that the trial court erred by violating his right to a public trial by ordering that the courtroom doors be closed and locked during the court's charge to the jury, and that his trial counsel provided ineffective assistance by not objecting to the closure of the courtroom. Finding no error, the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Rickman v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0127
Opinion Date: April 20, 2020
Judge: Harold D. Melton
Areas of Law: Constitutional Law, Criminal Law

Victoria Rickman was convicted by jury of malice murder and a related firearm offense in connection with the shooting death of William Carter, Jr. Rickman and Carter had a tumultuous on-again, off-again relationship with a history of verbal and physical abuse, false accusations of sexual assault, empty threats to obtain temporary protective orders, and numerous calls to

911. In the days leading up to Carter's death, the pair was talking and meeting again despite a recent break-up. On one such 911 call, officers went to Rickman's residence responding to claims shots were fired. Rickman responded holding her small dog, hair wet, and in pajamas. She did not appear to be injured, and nothing in the home looked disturbed or out of place. Rickman told the officers, "he raped me again and I shot him." Officers found Carter laying face up on the bed naked with multiple gunshot wounds to his body. An autopsy revealed that Carter was shot ten times – four times in the chest, three times in the back, once on the arm, and twice in the head. Rickman's examining physician testified that he found no injuries on Rickman consistent with her description of events, and no signs of trauma to her vaginal cavity. Rickman appealed her convictions, arguing she was denied effective assistance of counsel and that the trial court erred in admitting improper character evidence. Finding no reversible error, the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Robinson v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0265
Opinion Date: April 20, 2020
Judge: Peterson
Areas of Law: Constitutional Law, Criminal Law

Herbert Robinson appealed his convictions for malice murder, armed robbery, and possession of a firearm during the commission of a felony in connection with the death of Michael Moore. On appeal, he argued the trial court erred by allowing the State to use two firearms for demonstrative purposes during trial, and by allowing body-camera footage to be shown at trial. He also argued his trial counsel was ineffective for failing to object to a letter written by Robinson's cellmate being available to the jury for review during deliberations, and for failing to object to a visual aid used by the State during closing arguments. Because Robinson failed to show ineffective assistance of counsel or reversible error by the trial court, the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Santana v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0563
Opinion Date: April 20, 2020
Judge: Warren
Areas of Law: Constitutional Law, Criminal Law

Cuevas Carlos Santana was convicted by jury of malice murder and other crimes in connection with the 2010 shooting deaths of Israel Espinoza Mendoza, Vincente Soto Chavez, and Renato Soto Valencia. On appeal, Santana argues that the evidence was insufficient to support his convictions, that the trial court erred by declining to grant Santana a new trial on the general grounds, and that trial counsel provided ineffective assistance. Finding no reversible error, the Georgia Supreme Court affirmed Santana's convictions.

Read Opinion Are you a lawyer? **Annotate this case**.

Sullivan v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0056
Opinion Date: April 20, 2020
Judge: Warren
Areas of Law: Constitutional Law, Criminal Law

A jury convicted Antonio Sullivan of malice murder and other crimes in connection with the shooting death of Wava Benton. On appeal, Sullivan contended his trial counsel was constitutionally ineffective by failing to present evidence at trial to corroborate Sullivan's testimony about prior difficulties between Sullivan and Benton, and by failing to procure expert testimony about Sullivan's mental health—specifically about post-traumatic stress disorder— to be presented to the jury. The Georgia Supreme Court determined Sullivan failed to establish that his trial counsel was deficient in either respect, and therefore affirmed his convictions.

Read Opinion Are you a lawyer? **Annotate this case**.

Turner v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0247
Opinion Date: April 20, 2020
Judge: Warren
Areas of Law: Constitutional Law, Criminal Law

Appellant Ronald Turner appeals from his conviction for malice murder stemming from the stabbing death of William King. The stabbing took place outside an apartment at which Turner had driven in order to trade food for drugs. Turner testified in his own defense at trial and claimed that King hit him in the head with a beer bottle because Turner owed money to King from a prior drug transaction. Turner testified that he tried to get away from King, but that King chased him down and grabbed his jacket. According to Turner, King was getting ready to hit him again when Turner stabbed King in self-defense. Appealing his ultimate conviction, Turner contended he was denied the effective assistance of counsel in three respects. Seeing no reversible error after a review of the trial court record, the Georgia Supreme Court affirmed Turner's conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Valrie v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0380
Opinion Date: April 20, 2020
Judge: Keith R. Blackwell
Areas of Law: Constitutional Law, Criminal Law

Reuben Valrie was tried by jury and convicted of murder and other crimes in connection with the death of his infant daughter Aliyana. Valrie appealed, claiming that he was denied the effective assistance of counsel. Aliyana died as a result of closed head trauma, with a blunt-force abdominal injury as a secondary cause of death, which investigators determined was consistent with being shaken or dropped. At trial, Valrie presented the testimony of four expert witnesses who testified that Aliyana died of natural causes and that the injuries to her brain and abdomen were caused by

events such as post-mortem CPR and the “rough” handling of her body by first responders. The jury rejected this defense and found Valrie guilty of murder and the other charges. Valrie contended that his trial lawyer should have raised a hearsay objection to the admission of recorded statements that his girlfriend (and Aliyana's mother) made to police investigators (as well as the testimony of one of those investigators about some of those statements). Alternatively, Valrie argued that his lawyer should have sought the redaction of certain portions of the recorded statements that impugned his character. The Georgia Supreme Court concluded Valrie failed to present evidence that his trial counsel was deficient, or that he was prejudiced by any alleged failures. According, the Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Williams v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0241
Opinion Date: April 20, 2020
Judge: Keith R. Blackwell
Areas of Law: Constitutional Law, Criminal Law

Richard Williams, II, was tried by jury and convicted of murder in connection with the strangulation death of Cory Robinson. Williams and Robinson were involved in a sexual relationship and had been living together at an extended-stay hotel. Kelvin Spencer was a close friend of both Williams and Robinson. When Spencer met Williams at the hotel room, Williams looked angry and had scratches on his neck. Spencer saw Robinson lying on the floor in a “praying position.” Spencer did not believe Robinson was dead, and he helped Williams move clothes and other things to a U-Haul truck parked outside, in preparation for a move. Williams did not testify or present any evidence. Based on his lawyer’s opening and closing arguments, the defense theory was that Spencer killed Robinson because he was jealous of Williams’s relationship with Robinson. Williams’s sole claim on appeal was that he was denied the effective assistance of counsel when his trial lawyer failed to present as a defense that Williams accidentally killed Robinson during consensual erotic asphyxiation. He argued that his lawyer's discomfort with the topic of homosexual BDSM activity, and his own problems with the Georgia State Bar, precluded presentation of the "true"

version of events, and that Williams acceded to the lawyer's defense strategy only "through ignorance and that he did not know that a defense based on consensual erotic asphyxiation was available." Finding no reversible error, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Malave

Court: Supreme Court of Hawaii
Docket: SCWC-18-0000332
Opinion Date: April 20, 2020
Judge: Mark E. Recktenwald
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the intermediate court of appeals (ICA) affirming Defendant's conviction of sexual assault in the first degree on the complaining witness pursuant to Haw. Rev. Stat. 707-730(1)(b), holding that the ICA did not err in affirming the family court. Specifically, the Supreme Court held (1) the jury should have been instructed to determine jurisdictional facts, but the error was harmless beyond a reasonable doubt; and (2) the ICA did not err in finding that there was no rational basis in the record to support providing the jury instruction of the lesser included offense of sexual assault in the third degree.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Malave

Court: Supreme Court of Hawaii
Docket: SCWC-18-0000332
Opinion Date: April 22, 2020
Judge: Mark E. Recktenwald
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the intermediate court of appeals (ICA) affirming the judgment of the family court convicting Defendant on two counts of sexual assault in the first degree, holding that the ICA did not err in affirming the family court. At issue on appeal was the jurisdiction of the family court to try Defendant and the propriety of

instructing the jury on a lesser included offense. The ICA affirmed, concluding that the family court had subject matter jurisdiction pursuant to Haw. Rev. Stat. 571-14(a)(1) and that there was no rational basis to support an instruction of the lesser included offense of sexual assault in the third degree. The Supreme Court affirmed, holding (1) although the jury should have been instructed to determine jurisdictional facts, the error was harmless; and (2) the family court was not obligated to instruct the jury on the lesser included offense of sexual assault in the third degree.

Read Opinion Are you a lawyer? **Annotate this case**.

Idaho v. Burke

Court: Idaho Supreme Court - Criminal
Docket: 46841
Opinion Date: April 22, 2020
Judge: Moeller
Areas of Law: Constitutional Law, Criminal Law

Prior to sentencing, defendant James Burke was committed to the state mental hospital for 56 days to restore him to competency. After being evaluated and deemed competent to proceed to trial, Burke was returned to the county jail and later pleaded guilty pursuant to a plea agreement. At the conclusion of his sentencing hearing, Burke sought credit for the 56 days of time spent in court-ordered commitment. The district court denied the motion, concluding that commitment to a state mental hospital did not fall under the definition of 'incarceration' in Idaho Code section 18-309. After reviewing this issue carefully, the Idaho Supreme Court disagreed with the district court's "thorough and thoughtful analysis," holding that court-ordered commitment to state custody pursuant to Idaho Code sections 18-210 and 18-211 met the functional and legal definition of "incarceration" under Idaho Code section 18-309. "The extent of the liberty interests restricted by Burke's court-ordered commitment to State Hospital North are just too similar to imprisonment to conclude otherwise." Accordingly, the Court reversed the district court's order denying Burke's request for credit for time served and remanded the case for the district court to enter an order crediting him with the fifty-six days he spent committed to State Hospital North while the State restored his competency to face criminal charges.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Gibbs

Court: Iowa Supreme Court
Docket: 18-1298
Opinion Date: April 17, 2020
Judge: Edward M. Mansfield
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction of murder in the second degree, holding that Defendant's Fifth Amendment rights were invaded when the trial judge instructed the jury that Defendant was required to notify law enforcement of his use of deadly force, but the error was harmless. During trial, Defendant asserted the defense of justification in his shooting of the victim. At issue on appeal was whether the district court abused its discretion by giving a jury instruction incorporating the terms of Iowa Code 704.2B. The instruction included a statement that a person using deadly force is required to notify law enforcement about his use of deadly force. Defendant argued before the Supreme Court that both section 704.2B and the jury instruction incorporating that section violated his Fifth Amendment rights. The Supreme Court affirmed, holding (1) instructing the jury that a homicide defendant is required to notify a law enforcement agency of his use of deadly force violates the defendant's Fifth Amendment rights; but (2) any error in this case was harmless beyond a reasonable doubt.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Broxton

Court: Kansas Supreme Court
Docket: 114675
Opinion Date: April 17, 2020
Judge: Stegall
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's convictions for second-degree murder, burglary, and theft but reversed Defendant's sentences, holding

that any error during the guilt phase was harmless but that the district court erred by scoring Defendant's prior Florida burglary conviction as a person felony instead of a nonperson felony. On appeal, the court of appeals concluded that a trial court may instruct the jury on felony murder even though the State only charged the defendant with premeditated first degree murder. The Supreme Court disagreed, holding (1) the court of appeals erred in concluding that a district court may elect to provide a felony-murder instruction when that crime was not charged, and the district court properly found that the felony-murder instruction was not legally appropriate in this case; (2) the district court erred by excluding from evidence an exculpatory document from a Florida homicide investigation on the ground it was not relevant, but the error was harmless; and (3) the district court improperly scored Defendant's prior Florida burglary conviction as a person felony.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Corbin

Court: Kansas Supreme Court
Docket: 119665
Opinion Date: April 17, 2020
Judge: Dan Biles
Areas of Law: Criminal Law

The Supreme Court affirmed the ruling of the district court on remand resentencing Defendant to his original mandatory term of imprisonment after once again finding he was not a person with intellectual disability, holding that the district court did not abuse its discretion when it rejected Defendant's intellectual disability motion and imposed a mandatory term of imprisonment. Defendant pled no contest to first-degree premeditated murder. Before sentencing, Defendant filed a motion pursuant to Kan. Stat. Ann. 21-6622(b) asserting that he was a person with intellectual disability and was thus not subject to a mandatory minimum prison term. The district court denied the motion and sentenced Defendant to a hard twenty-five life sentence. While Defendant's appeal was pending, the Legislature amended Kan. Stat. Ann. 76-12b01(i), which provides new standards for deciding intellectual disability. The Supreme Court reversed and remanded for reconsideration of Defendant's motion using the new criteria. On remand, the district court reaffirmed its earlier ruling and again sentenced Defendant

to a hard twenty-five life sentence. The Supreme Court affirmed, holding that the district court's ruling was reasonably based on the law and was supported by substantial competent evidence.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Frazier

Court: Kansas Supreme Court
Docket: 117456
Opinion Date: April 17, 2020
Judge: Wilson
Areas of Law: Criminal Law

The Supreme Court reversed the decision of the district court affirming the judgment of the district court denying Defendant's motion to withdraw plea of no contest to one count of possession of heroin with intent to distribute, holding that the district court's decision in finding no good cause for Defendant to withdraw his plea was based on errors of fact and law, which were grounds for finding abuse of discretion. On appeal, Defendant argued that the district court abused its discretion in denying his motion to withdraw his plea of no contest based on misleading or false statements contained in the plea agreement. The court of appeals affirmed the district court. The Supreme Court reversed, holding (1) there was enough uncertainty in this case to indicate that Defendant's plea agreement was not understandingly made; and (2) therefore, Defendant must be allowed to withdraw his plea.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Harris

Court: Kansas Supreme Court
Docket: 117362
Opinion Date: April 17, 2020
Judge: Wilson
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court reversed the judgment of the court of appeals affirming Defendant's conviction of possession fo marijuana, holding that Defendant's waiver of jury trial was legally insufficient. On appeal, Defendant argued that

he did not properly waive his right to a jury and asserted three other issues. The Supreme Court reversed the judgment of the court of appeals affirming Defendant's convictions without addressing the three remaining issues, holding that because the district court failed properly to apprise Defendant of his right to a jury trial and failed to ensure that Defendant understood the nature of the right he was giving up, Defendant's constitutional right to a jury trial was violated in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Uk

Court: Kansas Supreme Court
Docket: 119712
Opinion Date: April 17, 2020
Judge: Wilson
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's conviction for first-degree premeditated murder, holding that the district court did not err in its challenged instructions to the jury. Specifically, the Supreme Court held (1) the district court did not err in refusing to give the jury Defendant's requested instruction on voluntary manslaughter as a lesser included offense of first-degree murder because the instruction was not factually appropriate; and (2) the district court did not commit clear error in issuing an unmodified version of Instruction No. 11, which contained the definition of "premeditation" and mirrored PIK Crim. 4th 54.150(d) because the instruction was legally appropriate.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Catruch

Court: Maine Supreme Judicial Court
Citation: 2020 ME 52
Opinion Date: April 23, 2020
Judge: Andrew M. Mead
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed the judgments of the trial court

terminating Appellant's participation in the Co-Occurring Disorders and Veterans Court (Veterans Court), holding that the court did not err or abuse its discretion in terminating Appellant's participation in the Veterans Court. The Veterans Court is a criminal docket that provides judicial monitoring, specialized treatment, and other services for military veterans who have disorders often attributable to their military service. Appellant was charged with leaving the scene of an accident and three other offenses. Appellant was admitted to the Veterans Court. Agreeing to sentencing outcomes in a plea agreement and entering into a bail contract, Appellant pleaded guilty to all charges against him. The court later terminated Appellant's participation in the Veterans Court, finding that Appellant had violated the conditions of his bail contract. The Supreme Judicial Court affirmed, holding (1) this matter was properly before the Court; and (2) given Appellant's failure to comply with the requirements for participation in the treatment court and his violations of the agreements, his termination from the Veterans Court was warranted.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Paquin

Court: Maine Supreme Judicial Court
Citation: 2020 ME 53
Opinion Date: April 23, 2020
Judge: Andrew M. Mead
Areas of Law: Constitutional Law, Criminal Law

In this appeal from Defendant's conviction for eleven counts of gross sexual misconduct, the Supreme Judicial Court vacated the judgment of conviction on one count, vacated the dismissal of other counts and remanded for entry of a judgment of acquittal on those counts, and affirmed in all other respects, holding that Defendant's convictions on both Counts 5 and 30 violated his double jeopardy protections and that the court erred in allowing the State to dismiss Counts 27, 28, and 29 during trial without Defendant's consent. The indictment charged Defendant with fifteen counts (Counts 1-13, 30-31) of gross sexual misconduct against the victim and sixteen counts (Counts 14-29) of gross sexual misconduct against a second alleged victim. During trial, the court granted Defendant's motion for a judgment of acquittal on Counts 10-13, and the State dismissed Counts 27-29. Defendant was

found guilty of Counts 1-9 and 30-31 and not guilty on the remaining counts. The court entered judgment in accordance with the verdict. The Supreme Judicial Court held that the trial court erred in failing to rule that the Double Jeopardy Clause barred convictions on both Counts 5 and 30 and allowing the State to dismiss Counts 27, 28, and 29 rather than entering a judgment of acquittal on those counts.

Read Opinion Are you a lawyer? **Annotate this case**.

Watson v. State

Court: Maine Supreme Judicial Court
Citation: 2020 ME 51
Opinion Date: April 21, 2020
Judge: Joseph Jabar
Areas of Law: Criminal Law

The Supreme Judicial Court vacated the judgment of the unified criminal docket denying Appellant's petition for post-conviction review, holding that Appellant was deprived of the effective assistance of counsel when his trial attorney played a video of the ten-year-old victim's interview with police and that Appellant was adversely affected. Appellant was convicted of two counts of gross sexual assault, one count of unlawful sexual contact, and one count of visual sexual aggression against a child. The Supreme Court affirmed. Appellant later filed a petition for post-conviction review claiming that his trial attorney's representation was deficient because introducing the videotaped recording of the victim's entire interview with law enforcement was unnecessary to provide evidence supporting the victim's potential motive to fabricate the allegations. The post-conviction court denied denied the petition. The Supreme Court vacated the judgment below, holding that trial counsel's conduct was deficient and that counsel's actions rose to the level of comprising the reliability of Appellant's conviction and undermining confidence in it.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. Mazza

Court: Massachusetts Supreme Judicial Court

Docket: SJC-11363
Opinion Date: April 21, 2020
Judge: Budd
Areas of Law: Criminal Law

The Supreme Judicial Court reversed the order of the superior court denying Defendant's motion for a new trial and set aside the jury's verdicts of first degree murder and robbery, holding that a recently discovered witness statement made to the police ago constituted newly discovered evidence that "would probably have been a real factor in the jury's deliberations." At issue was Defendant's sixth motion for a new trial, which was predicated on newly discovered evidence consisting of, among other things, a recently discovered statement made to the police in 1972. The superior court denied the motion. As to the police statement, the judge found that it did not constitute newly discovered evidence because Defendant failed to establish that defense counsel did not have possession of it at the time of trial. The Supreme Judicial Court reversed and remanded the case for a new trial, holding (1) Defendant sustained his burden of establishing that defense counsel did not have the 1972 police statement prior to or at trial, and therefore, the statement constituted newly discovered evidence; and (2) there was a substantial risk that the jury would have reached a different conclusion had the evidence been admitted at trial.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. McCarthy

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12750
Opinion Date: April 16, 2020
Judge: Gaziano
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Judicial Court affirmed the judgment of the district court denying Defendant's motions to suppress, holding that the limited use of automatic license plate readers (ALPRs) in this case did not implicate constitutional protections against unreasonable searches. While police were investigating Defendant on suspicion of drug distribution they used ALPRs on two bridges to track Defendant's movements. The police accessed historical data via ALPR technology and received real-time alerts, the last of

which led to Defendant's arrest. Defendant filed motions to suppress the ALPR data and the fruits of the arrest. The superior court denied the motions. The Supreme Judicial Court affirmed, holding that while the widespread use of ALPRs in the Commonwealth could implicate a defendant's constitutional protected expectation of privacy in the whole of his public movements, that interest was not invaded by the limited extent and use of the ALPR data in the instant case.

Read Opinion Are you a lawyer? **Annotate this case**.

Garden v. Commonwealth

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12821
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed the judgment of a single justice of the court denying Petitioner's petition for extraordinary relief under Mass. Gen. Laws ch. 211, 3 seeking an order vacating Petitioner's plea to aggravated rape and dismissing the underlying indictment, holding that the single justice did not err or abuse his discretion in denying relief. The issues raised by Petitioner had all been raised and adjudicated through the normal appellate process. Petitioner then filed a motion to withdraw his guilty plea. The motion was denied, and the Appeals Court affirmed. In this petition for extraordinary relief, Petitioner sought an order vacating his plea to aggravated rape and dismissing the underlying indictment. The single justice denied relief. The Supreme Judicial Court affirmed, holding that the superintendence power was not available as an additional layer of appellate review once all other avenues had been exhausted.

Read Opinion Are you a lawyer? **Annotate this case**.

In re Mitchell

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12910
Opinion Date: April 22, 2020

Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed the judgment of the county court denying, without a hearing, Petitioner's petition for relief under Mass. Gen. Laws ch. 211, 3, holding that the single justice did not err or abuse his discretion in denying relief. Defendant was convicted of several offenses. The Appeals Court reversed the convictions and remanded the matter for a new trial. Thereafter, the Commonwealth filed a nolle prosequi as to all the charges. In his Mass. Gen. Laws ch. 211, 3 petition, Defendant alleged that no crime had been committed and that he was wrongfully prosecuted. The single justice denied relief. The Supreme Judicial Court affirmed, holding that Defendant did not demonstrate entitlement to the exercise of this Court's superintendence powers.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Reek

Court: Minnesota Supreme Court
Docket: A19-0153
Opinion Date: April 22, 2020
Judge: G. Barry Anderson
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction for first-degree murder, holding that there was no error in the proceedings below. Specifically, the Supreme Court held (1) Appellant's right to a fair trial before an impartial tribunal was not violated when the district court stated that it might reconsider its prior Spreigl ruling if the defense presented certain witnesses; (2) the jury instructions on accomplice liability were plainly erroneous, but Appellant failed to establish that there was a reasonable likelihood that the error had a significant effect on the verdict; (3) the prosecutor did not commit misconduct in his closing arguments regarding the law of accomplice liability; (4) the district court did not abuse its discretion by granting the State's motion to admit evidence of appellant's past convictions for impeachment purposes, including by allowing the specific convictions to be disclosed to the jury; and (5) Appellant's pro se arguments were without merit.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Woodard

Court: Minnesota Supreme Court
Docket: A18-1886
Opinion Date: April 22, 2020
Judge: Hudson
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the district court convicting Defendant of first-degree murder and sentencing him to life in prison without the possibility of release, holding that the district court did not err in denying Defendant's motion to present an alternative-perpetrator defense. Specifically, the Supreme Court held (1) the district court did not abuse its discretion in holding that Defendant's proffered evidence in support of his motion to present alternative-perpetrator evidence for lack of sufficient foundation; and (2) the district court committed an error that was plain in instructing the jury on the order in which to consider the charges against Defendant, but there was no reasonable likelihood that the instruction affected the jury's verdict and therefore did not affect Defendant's substantial rights.

Read Opinion Are you a lawyer? **Annotate this case**.

Huff v. Brown

Court: Nebraska Supreme Court
Citation: 305 Neb. 648
Opinion Date: April 23, 2020
Judge: Lindsey Miller-Lerman
Areas of Law: Communications Law, Criminal Law

The Supreme Court reversed the portion of the district court's order granting in part a writ of mandamus requiring Doug Brown, the sheriff of Furnas County, to provide records to Herchel Huff pursuant to the public records statutes, holding that the district court erred when it determined that Huff had shown that Brown had a clear duty to provide the requested records. Huff, an inmate, sought, among other documents, the criminal history

records of jurors who had convicted hims. Furnas County sheriff Kurt Kapperman required a deposit of $750 before fulfilling the request. Huff subsequently filed a petition for writ of mandamus naming Kapperman as the defendant and seeking an order compelling Kapperman to release all requested documents. The court permitted Huff to substitute Brown, the current sheriff, in the caption of the case in place of Kapperman and granted in part mandamus. The Supreme Court reversed in part, holding that the district court (1) did not err when it substituted Brown's name for Kapperman's; but (2) erred in issuing mandamus because Huff failed to demonstrate a prima facie case that he had been denied a request for public records that the sheriff had a clear duty to provide under Neb. Rev. Stat. 84-712.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Montoya

Court: Nebraska Supreme Court
Citation: 305 Neb. 581
Opinion Date: April 17, 2020
Judge: Freudenberg
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the judgment of the district court affirming Defendant's conviction and sentence for driving under the influence, holding that there was no error in the challenged rulings by the trial court. Specifically, the Supreme Court held that the district court did not err by (1) affirming the county court's order denying Defendant's motion to suppress fruits of the stop; (2) affirming the county court's order that denied Defendant's motion to suppress the fruits of his arrest; (3) affirming the county court's order that denied Defendant's motion to suppress the results of the test of his breath alcohol content; (4) finding sufficient evidence to support the conviction; and (5) finding that Defendant's sentence was not excessive.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Schroeder

Court: Nebraska Supreme Court
Citation: 305 Neb. 527
Opinion Date: April 17, 2020
Judge: Funke
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's sentence of death for first degree murder, holding that there was no error in the sentence imposed by the sentencing panel. Specifically, the Supreme Court held that the sentencing panel did not err in (1) allowing the State to introduce evidence on the existence of mitigating circumstances; (2) acknowledging and weighing mitigating evidence from the presentence investigation report; (3) not requesting that documentation from the Department of Correctional Services regarding Defendant's time in custody for mitigation purposes be included in the presentence investigation report; (4) sentencing Defendant to death, where the Legislature has enacted safeguards to ensure fairness and accuracy in the resulting sentence; and (5) finding Defendant should be sentenced to death after balancing the aggravating evidence and mitigating evidence.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Kendrick v. Parker

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1509
Opinion Date: April 21, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals denying Appellant's request for a writ of prohibition and/or mandamus against Montgomery County Court of Common Pleas Judge E. Gerald Parker Jr., holding that the court of appeals correctly determined that Appellant's claim was barred by res judicata. Appellant sought a petition for writ of prohibition and/or mandamus against Judge Erik Blaine, the successor to the judge who sentenced Appellant, alleging that the sentencing court patently and unambiguously lacked jurisdiction to sentence him. Judge Parker, who had succeeded Judge Blaine, subsequently filed a motion for summary judgment. The court of appeals granted summary judgment for Judge

Parker, concluding that Appellant failed to demonstrate that the sentencing court patently and unambiguously lacked jurisdiction or that he lacked an adequate remedy at law and that res judicata barred Appellant's claim. The Supreme Court affirmed, holding that Appellant's claim was barred by res judicata.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Nelson v. Russo

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1541
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals dismissing Appellant's petition for a writ of mandamus seeking to compel Cuyahoga County Court of Common Pleas Judge Nancy Margaret Russo to vacate the consecutive prison sentences imposed on Appellant in 1987, holding that Appellant had an adequate remedy at law and was barred from asserting additional claims of sentencing error he could have raised in his previous mandamus action. In 1987, Appellant was convicted of four counts of rape and one count of kidnapping. Appellant was sentenced to prison terms of fifteen to twenty-five years for each of the five counts, to be served consecutively. In 2019, Appellant sought a writ of mandamus to compel Judge Russo to vacate his consecutive sentences. The court of appeals dismissed the writ action, concluding that res judicata barred Appellant's claim and that his prior appeals were an adequate remedy at law to address the alleged defect in his consecutive sentences. The Supreme Court affirmed, holding that Appellant was not entitled to a writ of mandamus in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Roberts v. Marsh

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1540

Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals dismissing Appellant's original action seeking a writ of procedendo and/or mandamus to compel Hamilton County Court of Common Pleas Judge Melba Marsh to issue a corrected sentencing entry, holding that the court of appeals correctly dismissed the petition as moot. Appellant was convicted of murder with a repeat-violent-offender specification. Appellant later asked the trial court to correct his sentence, arguing that he had improperly been sentenced to postrelease control. On remand, Judge Marsh vacated the postrelease-control sentence. Appellant appealed that order. The court of appeals noted that the trial court had not set forth all the information required under Crim.R. 32(C) in a single document and dismissed the appeal for lack of a final, appealable order. Appellant then filed this original action seeking to compel Judge Marsh to issue a corrected sentencing entry that constitutes a final, appealable order. Judge Marsh issued a nunc pro tunc sentencing entry that constituted a final, appealable order. The court of appeals then dismissed the petition as moot. The Supreme Court affirmed, holding that because Judge Marsh performed the act Appellant requested, the court of appeals dismissed the petition as moot.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Steiner v. Rinfret

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1510
Opinion Date: April 21, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals dismissing Appellant's petition for a writ of mandamus against Holmes County Court of Common Pleas Judge Robert D. Rinfret, holding that the court of appeals correctly determined that Appellant had an adequate remedy in the ordinary course of the law. Appellant, who was serving consecutive prison terms for five convictions, filed a petition for a writ of mandamus arguing that Judge Rinfret improperly sentenced him to a prison

term of nine years for his attempted rape conviction instead of the maximum term of eleven years. The court of appeals dismissed the petition, determining that Appellant had failed to file a mandatory affidavit of his prior civil actions and had an adequate remedy in the ordinary course of the law. The Supreme Court affirmed, holding that relief in mandamus was not available because Petitioner had an adequate remedy in the ordinary course of the law.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Jeffries

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1539
Opinion Date: April 22, 2020
Judge: Donnelly
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals upholding Defendant's convictions of four counts related to two specific instances of sexual abuse of D.S., holding that the trial court and court of appeals correctly applied Ohio's rape-shield law and determined that evidence of D.S.'s prior nonconsensual sexual assault was inadmissible. On appeal, Defendant asserted that the trial court erred in prohibiting him from introducing evidence during trial that D.S. had previously been sexually assaulted by another person, arguing that the rape-shield law applies only to an accuser's prior consensual sexual activity. The lower court held that Ohio's rape-shield law addresses all sexual activity, not only consensual sexual activity. The court of appeals affirmed. The Supreme Court affirmed, holding (1) the plain meaning of the term "sexual activity" as used in the rape-shield law includes both consensual and nonconsensual sexual activity; and (2) therefore, all sexual activity is barred from admission into evidence by the rape-shield, absent certain exceptions listed in the law.

Read Opinion Are you a lawyer? **Annotate this case**.

Pennsylvania v. Britton

Court: Supreme Court of Pennsylvania

Docket: 55 MAP 2018
Opinion Date: April 22, 2020
Judge: Max Baer
Areas of Law: Constitutional Law, Criminal Law

California law enforcement officers interviewed Appellant Stacy Britton in her California residence and, unbeknownst to her, recorded those interviews. Over Appellant's objection, Pennsylvania used those recordings as evidence to help convict Appellant of murder in Pennsylvania. The Pennsylvania Supreme Court granted allowance of appeal to examine whether the California law enforcement officers were acting as agents of the Pennsylvania State Police when they recorded the interviews with Appellant in her California home, and if so, whether Pennsylvania's constitutional and statutory protections were available to Appellant under those circumstances. The Court concluded the California law enforcement officers were not acting as agents of the Pennsylvania State Police when they interviewed Appellant, making analysis of whether any Pennsylvania-specific constitutional or statutory protections unwarranted. Because the Supreme Court concluded the Pennsylvania trial court reached the proper result in this matter, it affirmed that court's judgment.

Read Opinion Are you a lawyer? **Annotate this case**.

Pennsylvania v. Copenhaver

Court: Supreme Court of Pennsylvania
Docket: 48 MAP 2019
Opinion Date: April 22, 2020
Judge: Thomas G. Saylor
Areas of Law: Constitutional Law, Criminal Law

In August 2015, a deputy sheriff conducted a vehicle stop of Appellant Victor Copenhaver's pickup truck. Upon approaching the truck, the deputy noticed an odor of alcohol and marijuana emanating from the passenger compartment. After administering field sobriety tests, he arrested Appellant for suspected driving under the influence of alcohol and controlled substances ("DUI"). Appellant was ultimately charged with DUI and other offenses. Appellant challenged the deputy's authority to conduct a traffic stop and sought suppression of all evidence obtained during the encounter. Rather than presenting testimony at a suppression hearing, the parties

stipulated that Appellant was driving the vehicle in question and that the deputy had training and qualifications equivalent to that of a police officer. The parties also agreed that the vehicle stop occurred as a result of the deputy observing the tailgate to the pickup truck being in a down position, which caught the deputy's attention. The deputy further observed the registration on the pickup truck was expired, and additionally, the registration number was identified as belonging to a vehicle other than the one on which it was attached. The issue this case presented for the Pennsylvania Supreme Court's review was whether the deputy could lawfully conduct the traffic stop based on the expired registration sticker, on a theory that such a violation amounts to a breach of the peace. The Supreme Court concluded driving a vehicle with an expired registration did not entail a breach of the peace. It vacated the superior court's order insofar as it held that the expired registration was a breach of the peace, thus alone authorizing the deputy to stop Appellant's vehicle. Notably, in light of its holding, the Supreme Court found the superior court did not proceed to consider other relevant questions, such as whether the parties' factual stipulation should have been read as indicating that the officer's understanding that the registration sticker was associated with a different vehicle arose in the pre-stop timeframe – consistent with the Commonwealth's position throughout this litigation. "These issues should be resolved in the first instance by the intermediate court on remand."

Read Opinion Are you a lawyer? **Annotate this case**.

Pennsylvania v. Tedford

Court: Supreme Court of Pennsylvania
Docket: 773 CAP
Opinion Date: April 22, 2020
Judge: Donohue
Areas of Law: Constitutional Law, Criminal Law

Appellant Donald Tedford was convicted of first-degree murder and rape on February 6, 1987. He appealed the dismissal of his second petition for relief filed pursuant to the Post Conviction Relief Act ("PCRA"), on December 2, 2014, as amended by a counseled petition on May 5, 2015, and a supplemental petition filed on June 9, 2015. In connection with his initial filings, Tedford sought wholesale discovery of the prosecution's entire file,

but the PCRA court concluded that the petition (as amended) was not timely filed. Tedford also appealed the PCRA court's order denying his supplemental PCRA petition, in which he requested discovery, an evidentiary hearing, and/or a new trial based upon the admission of expert testimony presented at trial related to microscopic hair analysis. The PCRA court concluded that pursuant to PCRA Section 9545(b)(1)(ii), it had jurisdiction to consider the merits of Tedford's newly-discovered-facts claims, but ultimately it concluded Tedford had not asserted a meritorious claim in accordance with Section 9543(a)(2)(vi). Finding no reversible error in that analysis, the Pennsylvania Supreme Court affirmed dismissal of the petition for relief.

Read Opinion Are you a lawyer? **Annotate this case**.

Pennsylvania v. Trahey

Court: Supreme Court of Pennsylvania
Docket: 38 EAP 2018
Opinion Date: April 22, 2020
Judge: Wecht
Areas of Law: Constitutional Law, Criminal Law

The trial court granted Timothy Trahey's motion to suppress the results of a blood test that revealed his blood alcohol concentration ("BAC"), finding no justification for the investigating officers' failure to obtain a search warrant before conducting the test. On the Commonwealth's appeal, the Superior Court reversed, opining that the Commonwealth's evidence sufficiently established the existence of exigent circumstances, thus excusing the absence of a warrant. The Pennsylvania Supreme Court reversed, finding that while the exigency analysis is an objective one, "even disregarding the officers' subjective motivations, or their candid acknowledgment that they would have obtained a search warrant if they thought it necessary, there was no time-sensitive need to conduct a warrantless blood test under the circumstances of this case. Accordingly, the Superior Court's conclusion that the test was justified by exigent circumstances was drawn in error."

Read Opinion Are you a lawyer? **Annotate this case**.

In re Greg Abbott

Court: Supreme Court of Texas
Docket: 20-0291
Opinion Date: April 23, 2020
Judge: Per Curiam
Areas of Law: Constitutional Law, Criminal Law

The Supreme Court conditionally granted mandamus relief to the State seeking review of a temporary restraining order (TRO) blocking enforcement of Executive Order GA-13, which changes the rules applicable to judges' decisions regarding pre-trial bail, against judges, holding that the trial court lacked jurisdiction to order the judges' requested relief, even temporarily. GA-13 suspends certain statutes authorizing trial judges to release jail inmates with violent histories during the state of disaster due to the threat of the novel coronavirus. Plaintiffs alleged that GA-13 is unconstitutional and exceeds the governor's statutory emergency powers. Sixteen of the plaintiffs were Texas trial judges alleging that GA-13 improperly interferes with their judicial authority to make individualized bail decisions, and the other plaintiffs were public interest organizations and lawyer associations. The trial court issued a TRO blocking enforcement of GA-13 against judges. The Supreme Court conditionally granted mandamus relief, holding that the alleged threat of a criminal prosecution in this case did not give the judges standing to seek the invalidation of GA-13, and therefore, the trial court lacked jurisdiction to order their requested relief.

Read Opinion Are you a lawyer? **Annotate this case**.

Stahmann v. Texas

Court: Texas Court of Criminal Appeals
Docket: PD-0556-18
Opinion Date: April 22, 2020
Judge: Barbara Hervey
Areas of Law: Constitutional Law, Criminal Law

Appellant Karl Stahmann was involved in an automobile accident, after which he threw a bottle of promethazine, a controlled substance, over a nearby wire fence before law enforcement arrived. The bottle landed two to three feet past the fence in plain view. He was convicted of third-degree

felony tampering with physical evidence and was sentenced to 10 years' confinement and fined $5,000. The judge suspended his sentence and placed him on community supervision for 10 years. Stahmann appealed, arguing in part that the evidence was insufficient to prove that he destroyed, altered, or concealed the prescription bottle. The court of appeals agreed that the evidence was insufficient, but instead of rendering an acquittal, it reformed the judgment to show that Stahmann was convicted of the lesser-included offense of attempted tampering with physical evidence, a state-jail felony. After review of the evidence presented at trial, the Texas Court of Criminal Appeals concluded the evidence was indeed insufficient to prove that Appellant altered the prescription pill bottle when he threw it over the fence because the mere act of throwing the bottle did not change the bottle itself. "While a rational jury could have reasonably inferred that Stahmann intended to conceal the pill bottle when he threw it over the wire fence, the evidence shows that he failed to conceal it as he intended because the bottle landed short of the bush in plain view on top of some grass." The Court affirmed the trial court's judgment.

Read Opinion Are you a lawyer? **Annotate this case**.

Blanke v. Board of Pardons & Parole

Court: Utah Supreme Court
Citation: 2020 UT 16
Opinion Date: April 16, 2020
Judge: Himonas
Areas of Law: Criminal Law

The Supreme Court affirmed the decision of the court of appeals affirming the district court's denial of Appellant's petition for extraordinary relief, holding that, under the circumstances, the Utah Board of Pardons and Parole need not afford Appellant the due process protections explained in Neese v. Utah Board of Pardons and Parole, 416 P.3d 663 (2017), before it could determine that Appellant was a sex offender and condition his parole on sex offender treatment. Appellant was serving a prison sentence for his convictions of attempted child kidnapping and kidnapping. Because he was convicted of attempted child kidnapping Appellant was considered a sex offender under the sex offender registration statute. Further, Appellant admitted in his presentence report that he had sexual intercourse with a

fifteen-year-old. Appellant filed a petition for extraordinary relief alleging that the Parole Board had violated his due process rights by conditioning his parole on completion of sex offender treatment even though he had not committed a sex offense. Summary judgment was granted for the Parole Board. The Supreme Court affirmed, holding that the Parole Board owed Appellant no additional process before it considered unconnected sex offenses in its decision to require Appellant to undergo sex offender treatment.

Read Opinion Are you a lawyer? **Annotate this case**.

Washington v. Escalante

Court: Washington Supreme Court
Docket: 97268-1
Opinion Date: April 23, 2020
Judge: Steven González
Areas of Law: Constitutional Law, Criminal Law

Alejandro Escalante was detained for hours in a secured area at a border crossing and, the State conceded, interrogated by federal agents without Miranda warnings. Statements he made during that interrogation were used by the State to convict him of drug possession. While a traveler briefly detained and questioned at the border was typically not "in custody" for Miranda purposes, "the government's power to detain and question people at the border without implicating Miranda has limits." Here, the Washington Supreme Court determined those limits were reached. "This border detention created the type of inherently coercive environment that demands Miranda warnings to ensure an individual's choice to speak is the product of free will." The Supreme Court held that Escalante was in custody when he was interrogated and reversed.

Read Opinion Are you a lawyer? **Annotate this case**.

Washington v. Haggard

Court: Washington Supreme Court
Docket: 97375-0
Opinion Date: April 23, 2020

Judge: Barbara Madsen
Areas of Law: Constitutional Law, Criminal Law

A class C felony "washes out" and is omitted from a defendant's offender score as long as he or she is not convicted of any crime within five years of the last date of release from confinement. David Haggard was convicted of a misdemeanor offense within this five-year period, which was dismissed pursuant to RCW 3.66.067. When Haggard later pleaded guilty to burglary and arson, the trial court included prior class C felonies in his criminal history, finding that the dismissed misdemeanor conviction interrupted the washout period for those offenses. Haggard contended on appeal this was error. The Washington Supreme Court determined that because a dismissed conviction constituted a "conviction" under the Sentencing Reform Act of 1981 (SRA), and misdemeanor dismissal and vacation were distinct processes, so Haggard's offender score was properly calculated.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Taylor

Court: Supreme Court of Appeals of West Virginia
Docket: 18-0502
Opinion Date: April 21, 2020
Judge: Walker
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the judgment of the circuit court giving Petitioner credit for twelve days of time served toward the sentence he received for his felony conviction although Petitioner spent additional time in confinement for other charges that were dismissed in the universal plea agreement, holding that to grant Petitioner additional credit for time served would do little more than reward Petitioner for habitual criminal behavior. Petitioner was charged with several crimes and agreed to resolve the pending charges against him in a universal plea agreement. Under the terms of the agreement, Petitioner agreed to plea guilty to the charge of felony carrying a concealed firearm by a prohibited person. In exchange, the State agreed to drop the remaining charges. After he was sentenced, Petitioner argued that, in addition to the twelve days of credit for time served he was granted, he was constitutionally entitled to credit for time served

while he was incarcerated for charges that were resolved in the universal plea agreement. The Supreme Court affirmed, holding that Petitioner's circumstances implicated neither double jeopardy nor equal protection of the law such that additional credit for time served was constitutionally mandated.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Harrison

Court: Wisconsin Supreme Court
Dockets: 2017AP002441-CR, 2017AP002440-CR
Opinion Date: April 17, 2020
Judge: Patience D. Roggensack
Areas of Law: Criminal Law

The Supreme Court affirmed in part and reversed in part the decision of the court of appeals reversing an order of the circuit court that granted sentence credit to Defendant, holding that the court of appeals correctly found that Defendant was not entitled to sentence credit but erred by advancing the commencement of Defendant's terms of extended supervision for Defendant's 2007 and 2008 cases. Specifically, the Court held (1) Defendant was not entitled to sentence credit under Wis. Stat. 973.155(1)(a) because the days he spent in custody for which he sought sentence credit were not in connection with the courses of conduct for which those sentences were imposed; and (2) the court of appeals erred by advancing the commencement of Defendant's terms of extended supervision for his 2007 and 2008 cases to the date they would have begun but for Defendant's confinement for unrelated convictions that were later set aside, holding that whether to employ advancement is a public policy decision best left to the legislature.

Read Opinion Are you a lawyer? **Annotate this case**.

About Justia Opinion Summaries

Justia Weekly Opinion Summaries is a free service, with 63 different

newsletters, each covering a different practice area.

Justia also provides 68 daily jurisdictional newsletters, covering every federal appellate court and the highest courts of all US states.

All daily and weekly Justia newsletters are free. Subscribe or modify your newsletter subscription preferences at daily.justia.com.

You may freely redistribute this email in whole.

About Justia

Justia is an online platform that provides the community with open access to the law, legal information, and lawyers.

Contact Us | Privacy Policy

Unsubscribe From This Newsletter
or unsubscribe from all Justia newsletters immediately **here.**

Justia | 1380 Pear Ave #2B, Mountain View, CA 94043

From: Criminal Law - Justia Weekly Opinion Summaries
To: Burton, Ray (POL)
Subject: Latest 101 Cases This Week: Ramos v. Louisiana (U.S.), United States v. Diaz-Rivera (1st Cir.), United States v. Cotto (2d Cir.)
Date: Friday, April 24, 2020 9:01:47 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

If you are unable to see this message, click here to view it in a web browser.

Justia Weekly Opinion Summaries

Criminal Law
April 24, 2020

Table of Contents

Ramos v. Louisiana
Civil Rights, Constitutional Law, Criminal Law
US Supreme Court

United States v. Diaz-Rivera
Criminal Law
US Court of Appeals for the First Circuit

United States v. Cotto
Criminal Law
US Court of Appeals for the Second Circuit

United States v. Rosa
Criminal Law
US Court of Appeals for the Second Circuit

Fogle v. Sokol
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Third Circuit

James v. New Jersey State Police
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Third Circuit

Bazemore v. Best Buy
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Akande
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Chambers
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Ferebee
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Nance
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Johnson
Criminal Law
US Court of Appeals for the Fifth Circuit

United States v. McGinnis
Criminal Law
US Court of Appeals for the Fifth Circuit

Valentine v. Collier
Civil Rights, Constitutional Law, Criminal Law, Government & Administrative Law, Health Law
US Court of Appeals for the Fifth Circuit

United States v. Dowl
Criminal Law
US Court of Appeals for the Sixth Circuit

United States v. Fowler
Criminal Law
US Court of Appeals for the Sixth Circuit

United States v. Sumlin
Criminal Law
US Court of Appeals for the Sixth Circuit

United States v. Vance
Criminal Law, White Collar Crime
US Court of Appeals for the Sixth Circuit

Winburn v. Nagy
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Sixth Circuit

Lund v. City of Rockford
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

United States v. Perez
Criminal Law
US Court of Appeals for the Seventh Circuit

Jackson v. United States
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Bolman
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Boyd
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Gonzalez-Esparsa
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Sanchez-Velasco
Criminal Law, Immigration Law
US Court of Appeals for the Eighth Circuit

Anthony v. TRAX International Corp.
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Ninth Circuit

City of Almaty v. Khrapunov
Criminal Law, International Law, White Collar Crime
US Court of Appeals for the Ninth Circuit

United States v. Baldon
Criminal Law
US Court of Appeals for the Ninth Circuit

United States v. Costanzo
Criminal Law
US Court of Appeals for the Ninth Circuit

United States v. Manzanares
Constitutional Law, Criminal Law
US Court of Appeals for the Tenth Circuit

United States v. Delaney
Criminal Law
US Court of Appeals for the District of Columbia Circuit

Antenor v. Alaska, Department of Corrections
Civil Procedure, Criminal Law, Government & Administrative Law
Alaska Supreme Court

Berger v. Bryant
Criminal Law
Arkansas Supreme Court

Carroll v. State
Criminal Law
Arkansas Supreme Court

Cave v. State
Civil Rights, Constitutional Law, Criminal Law
Arkansas Supreme Court

Chatmon v. Kelley
Criminal Law
Arkansas Supreme Court

McClinton v. State
Criminal Law
Arkansas Supreme Court

Siegel v. State
Criminal Law
Arkansas Supreme Court

Thomas v. State
Civil Rights, Constitutional Law, Criminal Law
Arkansas Supreme Court

California v. Landowski
Constitutional Law, Criminal Law
California Courts of Appeal

California v. May
Constitutional Law, Criminal Law
California Courts of Appeal

California v. Perez
Constitutional Law, Criminal Law
California Courts of Appeal

In re S.R.
Criminal Law
California Courts of Appeal

People v. Bell
Criminal Law
California Courts of Appeal

People v. Drayton
Criminal Law
California Courts of Appeal

People v. Robinson
Criminal Law
California Courts of Appeal

People v. Torres
Criminal Law
California Courts of Appeal

Colorado v. Lujan
Constitutional Law, Criminal Law
Colorado Supreme Court

Archer v. State
Civil Rights, Constitutional Law, Criminal Law
Florida Supreme Court

Collins v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Heyward v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Howard v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Keller v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Mills v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Moore v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Morris v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Rickman v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Robinson v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Santana v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Sullivan v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Turner v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Valrie v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Williams v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

State v. Malave
Criminal Law
Supreme Court of Hawaii

State v. Malave
Criminal Law
Supreme Court of Hawaii

Idaho v. Burke
Constitutional Law, Criminal Law
Idaho Supreme Court - Criminal

State v. Gibbs
Civil Rights, Constitutional Law, Criminal Law
Iowa Supreme Court

State v. Broxton
Criminal Law
Kansas Supreme Court

State v. Corbin
Criminal Law
Kansas Supreme Court

State v. Frazier
Criminal Law
Kansas Supreme Court

State v. Harris
Civil Rights, Constitutional Law, Criminal Law
Kansas Supreme Court

State v. Uk
Criminal Law
Kansas Supreme Court

State v. Catruch
Criminal Law
Maine Supreme Judicial Court

State v. Paquin
Constitutional Law, Criminal Law
Maine Supreme Judicial Court

Watson v. State
Criminal Law
Maine Supreme Judicial Court

Commonwealth v. Mazza
Criminal Law
Massachusetts Supreme Judicial Court

Commonwealth v. McCarthy
Civil Rights, Constitutional Law, Criminal Law
Massachusetts Supreme Judicial Court

Garden v. Commonwealth
Criminal Law
Massachusetts Supreme Judicial Court

In re Mitchell
Criminal Law
Massachusetts Supreme Judicial Court

State v. Reek
Civil Rights, Constitutional Law, Criminal Law
Minnesota Supreme Court

State v. Woodard
Criminal Law
Minnesota Supreme Court

Huff v. Brown
Communications Law, Criminal Law
Nebraska Supreme Court

State v. Montoya
Civil Rights, Constitutional Law, Criminal Law
Nebraska Supreme Court

State v. Schroeder
Criminal Law
Nebraska Supreme Court

State ex rel. Kendrick v. Parker
Criminal Law
Supreme Court of Ohio

State ex rel. Nelson v. Russo
Criminal Law
Supreme Court of Ohio

State ex rel. Roberts v. Marsh
Criminal Law
Supreme Court of Ohio

State ex rel. Steiner v. Rinfret
Criminal Law
Supreme Court of Ohio

State v. Jeffries
Criminal Law
Supreme Court of Ohio

Pennsylvania v. Britton
Constitutional Law, Criminal Law
Supreme Court of Pennsylvania

Pennsylvania v. Copenhaver
Constitutional Law, Criminal Law
Supreme Court of Pennsylvania

Pennsylvania v. Tedford
Constitutional Law, Criminal Law
Supreme Court of Pennsylvania

Pennsylvania v. Trahey
Constitutional Law, Criminal Law
Supreme Court of Pennsylvania

In re Greg Abbott
Constitutional Law, Criminal Law
Supreme Court of Texas

Stahmann v. Texas
Constitutional Law, Criminal Law
Texas Court of Criminal Appeals

Blanke v. Board of Pardons & Parole
Criminal Law
Utah Supreme Court

Washington v. Escalante
Constitutional Law, Criminal Law
Washington Supreme Court

Washington v. Haggard
Constitutional Law, Criminal Law
Washington Supreme Court

State v. Taylor
Civil Rights, Constitutional Law, Criminal Law
Supreme Court of Appeals of West Virginia

State v. Harrison
Criminal Law
Wisconsin Supreme Court

COVID-19 Updates: Law & Legal Resources Related to Coronavirus

Click here to include Verdict article summaries with your newsletter(s).

Criminal Law Opinions

Ramos v. Louisiana

Court: US Supreme Court
Docket: 18-5924
Opinion Date: April 20, 2020
Judge: Neil M. Gorsuch
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

In 48 states and in federal court, a single juror's vote to acquit is enough to

prevent a conviction; Louisiana and Oregon punish people based on 10-to-2 verdicts. Ramos was convicted in a Louisiana court by a 10-to-2 jury verdict and was sentenced to life without parole. The Supreme Court reversed. The Sixth Amendment right to a jury trial, as incorporated against the states by the Fourteenth Amendment, requires a unanimous verdict to convict a defendant of a serious offense. Juror unanimity is a vital common law right. The Court rejected an "invitation" to "perform a cost-benefit analysis on the historic features of common law jury trials and to conclude that unanimity does not make the cut." In overturning its 1972 "Apodaca" decision, the Court stated that the reasoning, in that case, was "gravely mistaken" and "sits uneasily with 120 years of preceding case law." The fact that Louisiana and Oregon may need to retry defendants convicted of felonies by non-unanimous verdicts whose cases are still pending on direct appeal "will surely impose a cost, but new rules of criminal procedure usually do."

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Diaz-Rivera

Court: US Court of Appeals for the First Circuit
Docket: 18-1461
Opinion Date: April 20, 2020
Judge: Torruella
Areas of Law: Criminal Law

The First Circuit affirmed Defendant's upwardly variant sentence for one count of possession with intent to distribute cocaine and one count of using a firearm during and in relation to a drug-trafficking crime, holding that the sentence was neither procedurally nor substantively unreasonable. Pursuant to a plea agreement, Defendant pled guilty to drug-related crimes. After a sentencing hearing, the district court sentenced Defendant to an upwardly variant sentence of 180 months of imprisonment, thus declining to impose the government's requested sentence. On appeal, Defendant challenged both the procedural and substantive reasonableness of his sentence. The First Circuit affirmed, holding that the 180-month sentence was neither procedurally nor substantively unreasonable.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Cotto

Court: US Court of Appeals for the Second Circuit
Docket: 18-2970
Opinion Date: April 20, 2020
Judge: Leval
Areas of Law: Criminal Law

A conviction for retaliating against a witness in violation of 18 U.S.C. 1513 does not require that the Government prove that defendant had knowledge of the federal nature of the proceeding. The Second Circuit rejected defendant's arguments to the contrary and affirmed his conviction for retaliating against a witness. The court remanded for revision of the provision of the sentence relating to the substance abuse treatment condition of supervised release; instructed the district court to consider on remand whether the court's forthcoming order in United States v. Traficante, No. 18-1962 (2d Cir., submitted Oct. 25, 2019) requires modification of the risk notification provision of supervised release; and granted the parties leave to reinstate this appeal to permit review of the district court's decision on remand as to the risk notification provision.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Rosa

Court: US Court of Appeals for the Second Circuit
Docket: 17-2004
Opinion Date: April 17, 2020
Judge: Nardini
Areas of Law: Criminal Law

Where a district court offers no explanation for its sentence, and where neither the adopted presentence report nor the statement of reasons adequately demonstrates the court's reasoning, the court has committed plain error in violation of 18 U.S.C. 3553(c). The Second Circuit vacated defendant's sentence for conspiracy to commit wire fraud and aggravated identity theft. The court held that the district court failed to state its reasons for sentencing defendant as required under section 3553(c); the error is clear or obvious; and the error affected defendant's substantial rights. Accordingly, the court remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

Fogle v. Sokol

Court: US Court of Appeals for the Third Circuit
Docket: 19-1066
Opinion Date: April 21, 2020
Judge: Matey
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

In 1976, the body of 15-year-old “Kathy” was found near her Indiana County, Pennsylvania home. Kathy’s death involved a brutal assault, rape, and a gunshot to the head. Kathy's sisters, ages nine and 12, stated that she had gotten into a car with a man with blue eyes, black hair that came below his ears and curled at the ends, sideburns, heavy eyebrows, and a heavy mustache. Fogle had “straight reddish-blonde hair that dropped down his back and a matching, full beard that reached his waist.” After three years, Fogle became a suspect because a psychiatric patient described seeing Kathy get in a car with Fogle and his brother. The story was largely inconsistent with statements by Kathy’s sisters. Jailhouse informants were recruited and counseled by law enforcement with promises of leniency. The prosecutors “either knew about, encouraged, or permitted” this strategy. A jury found Fogle guilty of second-degree murder. In 2015, Fogle obtained DNA evidence excluding both himself and his brother as the source of semen collected from Kathy. His conviction was vacated. The Commonwealth declined to pursue new charges, describing the case as lacking “prosecutorial merit.” Fogle, having spent three decades in prison, sued the prosecutors and Indiana County under 42 U.S.C. 1983. The Third Circuit affirmed the denial of their motions to dismiss based on absolute immunity. Only truly prosecutorial functions, not investigative conduct, justify complete protection from suit. Fogle’s complaint alleges actions that fall outside the narrow doctrine of absolute immunity.

Read Opinion Are you a lawyer? **Annotate this case**.

James v. New Jersey State Police

Court: US Court of Appeals for the Third Circuit

Docket: 18-1432
Opinion Date: April 21, 2020
Judge: Porter
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Stephens called 911 and reported that Gibbons hit her and had a gun in his truck. The police responded. Stephens obtained a temporary restraining order, prohibiting Gibbons from possessing firearms and from returning to Stephens's house. The next day, Gibbons went to Stephens's house. Stephens was talking on the phone; the friend called the police. Gibbons left Stephens's house. Trooper Conza arrived. Stephens stated that Gibbons had waved a gun throughout their argument. Conza told Stephens to go to the police barracks and reported over the radio that Gibbons had brandished a firearm. Conza, with Troopers Bartelt and Korejko, visited the nearby home of Gibbons's mother, James. James stated that she did not know where Gibbons was and that he might be off his schizophrenia medication. While driving to the barracks, Stephens saw Gibbons walking alongside the road and called 911. The Troopers responded. Bartelt parked his car and, exiting, observed that Gibbons was pointing a gun at his own head. Bartelt drew his weapon, stood behind his car door, and twice told Gibbons to drop his weapon. Gibbons did not comply. Bartelt shot Gibbons twice within seconds of stopping his car. Gibbons died that night. In James' suit under 42 U.S.C. 1983, the Third Circuit held that Bartelt is entitled to qualified immunity because he did not violate Gibbons's clearly established rights. Bartelt's pre-standoff knowledge of Gibbons differs from that of officers involved in cited cases. Bartelt could reasonably conclude that Gibbons posed a threat to others.

Read Opinion Are you a lawyer? **Annotate this case**.

Bazemore v. Best Buy

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-2196
Opinion Date: April 21, 2020
Judge: Quattlebaum
Areas of Law: Criminal Law

Plaintiff filed suit against her employer, Best Buy, claiming that she was harassed because of her race and gender and subjected to a hostile work

environment in violation of Title VII of the Civil Rights Act of 1964. Plaintiff's complaint stemmed from an incident where a coworker made a racist and sexually charged joke to a small group of coworkers that included plaintiff. The Fourth Circuit affirmed the district court's motion to dismiss and held that, in the case of allegedly harassing comments by a co-worker, an employee must allege plausible facts that the employer knew, or should have known, about the harassment and failed to take action reasonably calculated to stop it. Because plaintiff failed to do this, the court affirmed the district court's judgment. In this case, the coworker's conduct was not imputable to Best Buy where Best Buy took steps that were not only reasonably calculated to end such behavior, but that it did in fact end it.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Akande

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-6833
Opinion Date: April 20, 2020
Judge: Diana Jane Gribbon Motz
Areas of Law: Criminal Law

After defendant moved under 28 U.S.C. 2255 to vacate his conviction based on the ineffective assistance of counsel, the district court denied the motion. The Fourth Circuit granted a certificate of appealability and reversed the district court's judgment. The court held that, given counsel's specific misadvice regarding defendant's rights to preserve his appellate rights, on which defendant understandably relied, the district court's general admonishments did not amount to the careful explanation that addresses the particular issue necessary to cure the error. In this case, the plea colloquy did not correct counsel's erroneous advice and the error prejudiced defendant. Accordingly, the court remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Chambers

Court: US Court of Appeals for the Fourth Circuit
Docket: 19-7104

Opinion Date: April 23, 2020
Judge: Floyd
Areas of Law: Criminal Law

After defendant was erroneously sentenced as a career offender, he moved to reduce his sentence to time served under the First Step Act. The district court denied defendant's motion to reduce his custodial sentence, though it granted the motion as to his supervised release term. The Fourth Circuit held that the First Step Act does not constrain courts from recognizing Guidelines errors. The court explained that First Step Act motions fall under 18 U.S.C. 3582(c)(1)(B), a distinct exception to finality, and that section 404(b) of the First Step Act expressly allows a court to impose a reduced sentence in order to give retroactive effect to sections 2 and 3 of the Fair Sentencing Act. Furthermore, 18 U.S.C. 3553(a) sentencing factors apply in the section 404(b) resentencing context, and the resentencing court has discretion within the section 404(b) framework to vary from the Guidelines and, in doing so, to consider movants' post-sentencing conduct. In this case, the district court seemingly believed that it could not vary from the Guidelines range to reflect post-sentencing information. Therefore, the court vacated the district court's sentencing order. Finally, the court held that any Guidelines error deemed retroactive, such as the error in this case, must be corrected in a First Step Act resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Ferebee

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-4266
Opinion Date: April 22, 2020
Judge: Traxler
Areas of Law: Criminal Law

The Fourth Circuit affirmed the denial of defendant's motion to suppress evidence recovered from a backpack, and the district court's conclusion that defendant abandoned the backpack and any legitimate expectation of privacy in its contents. The court rejected defendant's claim that the collective-knowledge doctrine has any bearing on the propriety of the district court's conclusion that defendant abandoned the backpack. The court also held that the district court is not precluded from finding abandonment in

cases where the defendant, as here, has physical possession of the property he has disavowed. In this case, the record supported the district court's conclusion that defendant clearly and unequivocally disavowed ownership of the backpack. Even if the district court erred by finding that defendant abandoned the backpack, reversal would not be required because the search of the backpack was a proper search incident to arrest for which no warrant was required under the facts of this case.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Nance

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-4585
Opinion Date: April 21, 2020
Judge: Pamela Harris
Areas of Law: Criminal Law

The Fourth Circuit affirmed defendant's above-Guidelines sentence imposed after he pleaded guilty to two federal drug- and firearm-related offenses. The court held that defendant's sentence was not procedurally unreasonable where the district court took into account defendant's extensive criminal history; his pattern of reoffending upon release; his disciplinary infractions in custody and inability to comply with the terms of his release; and the fact that the offenses of conviction occurred over the course of days, in which he was arrested once, released, and then arrested again just days later. The court also held that defendant's sentence was substantively reasonable where the district court conducted a thorough, individualized assessment of defendant and his offense conduct in light of the 18 U.S.C. 3553(a) factors, and did not abuse its discretion in formulating the sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Johnson

Court: US Court of Appeals for the Fifth Circuit
Docket: 17-60852
Opinion Date: April 21, 2020

Judge: Priscilla R. Owen
Areas of Law: Criminal Law

The Fifth Circuit vacated defendant's sentence imposed after he pleaded guilty to violating 18 U.S.C. 922(g) and 924(e) by knowingly possessing a firearm after he had been convicted of a misdemeanor crime of domestic violence. The court held that the district court committing plain error by violating Federal Rule of Criminal Procedure 32 when it relied on factual allegations in the confidential sentencing recommendation that were not in the presentence report and that were not disclosed by defendant. The court explained that the use of undisclosed facts to justify an above-guidelines sentence seriously affects the fairness, integrity, and public reputation of judicial proceedings. Therefore, the court remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. McGinnis

Court: US Court of Appeals for the Fifth Circuit
Docket: 19-10197
Opinion Date: April 21, 2020
Judge: Stuart Kyle Duncan
Areas of Law: Criminal Law

18 U.S.C. 922(g)(8), which prohibits individuals subject to certain domestic violence protective orders from possessing firearms or ammunition for any purpose, is facially constitutional under the Fifth Circuit's two-step NRA framework. Even assuming arguendo that the conduct at issue -- the keeping and possessing of firearms by individuals subject to domestic protective orders -- falls within the Second Amendment right, defendant's facial challenge fails. The court applied intermediate scrutiny and held that section 922(g)(8) is reasonably adapted to the government interest of reducing domestic gun abuse. The court also held that if the commonly understood definitions of terms in the protective order include acts involving "physical force," the protective order is sufficient to support a conviction under section 922(g)(8)(C)(ii). In this case, the jury plausibly found that the order satisfied the statute and the court declined to reverse defendant's conviction on this basis. However, the court remanded for the limited purpose of conforming defendant's written judgment to the district court's

oral pronouncement.

Read Opinion Are you a lawyer? **Annotate this case**.

Valentine v. Collier

Court: US Court of Appeals for the Fifth Circuit
Docket: 20-20207
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Criminal Law, Government & Administrative Law, Health Law

Plaintiffs filed suit alleging that TDCJ's adoption and implementation of measures guided by changing CDC recommendations in regards to the COVID-19 pandemic do not go far enough. Plaintiffs filed a class action alleging violations of the Eighth Amendment's prohibition against cruel and unusual punishment, and the Americans with Disabilities Act, seeking a preliminary injunction. The Fifth Circuit granted TDCJ's motion to stay the district court's preliminary injunction, which regulates the cleaning intervals for common areas, the types of bleach-based disinfectants the prison must use, the alcohol content of hand sanitizer that inmates must receive, mask requirements for inmates, and inmates' access to tissues (amongst many other things). The court held that TDCJ is likely to prevail on the merits of its appeal because: (1) after accounting for the protective measures TDCJ has taken, plaintiffs have not shown a "substantial risk of serious harm" that amounts to "cruel and unusual punishment"; and (2) the district court committed legal error in its application of Farmer v. Brennan, by treating inadequate measures as dispositive of defendants' mental state. In this case, even assuming that there is a substantial risk of serious harm, plaintiffs lack evidence of defendants' subjective deliberate indifference to that harm. The court also held that TDCJ has shown that it will be irreparably injured absent a stay, and that the balance of the harms and the public interest favor a stay. Finally, the court held that plaintiffs have not exhausted their administrative remedies as required in the Prison Litigation Reform Act (PLRA), and the district court's injunction goes well beyond the limits of what the PLRA would allow even if plaintiffs had properly exhausted their claims.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Dowl

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-2469
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

Dowl pleaded guilty to presenting false tax returns, 18 U.S.C. 286. He received a sentence of 30 months of imprisonment plus 24 months of supervised release. On supervised release, Dowl was charged with four new state crimes; failing to inform his probation officer that he had police contact; communicating with his co-defendant despite instructions to the contrary; failing to make payments on his restitution, fine, or special assessment; and failing to get a job. At a hearing, the court reviewed the evidence and allowed Dowl to tell his side of the story. The court deferred judgment on three of the four new state criminal law violations and dismissed the fourth and found Dowl gainfully employed. Dowl had failed to notify his probation officer about police contact, impermissibly communicated with his co-defendant, and did not pay his fines. After considering the 18 U.S.C. 3553(a) sentencing factors, the court returned Dowl to prison for 11 months, giving Dowl and his attorney the opportunity to raise any objections. Dowl had none. The Sixth Circuit affirmed, rejecting Dowl's argument that the court committed reversible error by not directly addressing him to solicit an allocution. The court employed the "plain error" standard because Dowl did not raise any objection during his revocation hearing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Fowler

Court: US Court of Appeals for the Sixth Circuit
Dockets: 19-3071, 19-3070
Opinion Date: April 21, 2020
Judge: Donald
Areas of Law: Criminal Law

In 2018, Fowler pled guilty to possession of child pornography and violations of the conditions of his supervised release from a previous conviction for the same. In addition to possessing child pornography, Fowler had failed drug testing, had threatened his parole officer, and had tried to harass his girlfriend to recant her testimony. The district court ordered Fowler to pay a $5,000 special assessment for possession of child pornography under the Justice for Victims of Trafficking Act, 18 U.S.C. 3014. The court also varied upward and sentenced Fowler to the maximum statutory penalty for violating the conditions of his supervised release, imposing a 120-month sentence for possessing child pornography and a consecutive 36-month sentence for violating the terms of his supervised release. The Sixth Circuit vacated as to the assessment and remanded for a determination of indigency. The district court committed plain error by failing to address Fowler's ability to pay; the parties did not contemplate the $5,000 special assessment as a part of the waiver provision in the plea agreement. The court affirmed the sentence. The district court did not consider an impermissible factor (whether Fowler had actually touched a child) and Fowler had no other challenge to the reasonableness of his sentence,

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Sumlin

Court: US Court of Appeals for the Sixth Circuit
Docket: 18-3819
Opinion Date: April 21, 2020
Judge: Bush
Areas of Law: Criminal Law

Sumlin was convicted of the distribution of drugs that caused the 2015 death of Carrie Dobbins, 21 U.S.C. 841(a)(1) and (b)(1)(C), which carries enhanced penalty provisions. The Sixth Circuit affirmed his convictions and his sentence to life in prison. The district court properly denied Sumlin's suppression motion, given that the affidavit established a sufficient nexus between his drug trafficking activity and residence that was searched. The court properly admitted testimony by the victim's sister, Kelly, who was Sumlin's former girlfriend and had purchased drugs from him. Kelly's testimony about Sumlin's drug-trafficking and that Sumlin was with Carrie on

the day of her overdose was intrinsic proof that was relevant for providing background information and contextualizing the government's case against Sumlin. Sufficient evidence supported the jury's verdict that Sumlin distributed the drugs that caused Carrie's death.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Vance

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-5160
Opinion Date: April 17, 2020
Judge: Bush
Areas of Law: Criminal Law, White Collar Crime

The Spriggs' bank account was established to receive social security checks. The Spriggs' great-grandson, Vance, filled out an application in Mr. Spriggs's name for a debit card to draw on the checking account. Mr. Spriggs had never used a debit card. The Spriggses did not authorize Vance to do so. Bank cameras photographed Vance using the card to withdraw cash. Vance also used the card for personal expenses. At another bank, Vance used Mr. Spriggs's social security number to establish an account and obtain a $15,000 cash advance. Vance made other, unsuccessful loan applications. Upon being notified by the banks about suspicious activities involving his identity, Mr. Spriggs filed a police report. The police arrested Vance. While searching Vance's car, the police located a large stash of personal and financial documents belonging to the Spriggses, including bank statements, tax return forms, property-tax bills, and a car title. The Sixth Circuit affirmed Vance's convictions for access-device fraud, 18 U.S.C. 1029(a)(5), and two counts of aggravated identity theft, 18 U.S.C. 1028A(a)(1), and his 65-month sentence. The court rejected arguments that the district court failed to make adequate findings of fact after the bench trial, improperly denied a motion for judgment of acquittal, and failed to correctly calculate the loss amount connected to Vance's charges under Sentencing Guidelines 2B1.1.

Read Opinion Are you a lawyer? **Annotate this case**.

Winburn v. Nagy

Court: US Court of Appeals for the Sixth Circuit
Dockets: 19-2399, 19-2398
Opinion Date: April 23, 2020
Judge: Jeffrey S. Sutton
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Winburn represented himself at his trial for armed robbery, home invasion, and conspiracy. Based on Winburn's disruptive behavior, the judge removed him from the courtroom and revoked Winburn's permission to represent himself, then granted a competency evaluation and a mistrial. While Winburn awaited his second trial, the judge permitted Winburn's stand-by attorney to withdraw because Winburn had sued her and enjoined Winburn from filing complaints or grievances against his new attorney, except to discharge her. Although represented by a new attorney, Winburn moved pro se to dismiss his charges on double jeopardy grounds. The trial judge denied the motion because Winburn's attorney had not filed it. Winburn filed a habeas petition under 28 U.S.C. 2241 challenging his retrial and another section 2241 petition challenging the injunction. The district judges denied both and declined to issue certificates of appealability. Winburn filed a notice of appeal for one petition and sought a certificate of appealability for the other. The Sixth Circuit held that state pretrial detainees proceeding under section 2241 may not appeal without certificates of appealability and granted Winburn a certificate on the injunction claim. A reasonable jurist could conclude that the unusual order was constitutionally infirm. The court denied relief with respect to double jeopardy. Winburn failed to exhaust his state-court remedies by a motion to dismiss.

Read Opinion Are you a lawyer? **Annotate this case**.

Lund v. City of Rockford

Court: US Court of Appeals for the Seventh Circuit
Docket: 19-1945
Opinion Date: April 20, 2020
Judge: ROVNER
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Lund, a reporter for the Rockford Scanner, heard, by police scanner, of multiple traffic stops in Midtown. He did not have a driver's license, so he

rode a motorized bicycle to Midtown to take photographs. He suspected a prostitution sting operation. An officer noticed Lund and radioed the team. Officers Welsh and Campbell knew of Lund's previous anti-police speech. They directed Lund to “move on.” Lund asked if he was breaking any laws. Campbell informed him that he was not, but that his continued presence would constitute obstruction of a police detail and result in arrest. Lund started his bicycle and called out, loudly, “goodbye officers.” Concerned that Lund might post pictures on social media while the sting operation was ongoing and create a danger for unarmed undercover officers, the officers followed Lund and arrested him for driving the wrong way on a one-way street, operating a vehicle without insurance, obstructing a police officer, felony aggravated driving on a revoked license, and operating a motor vehicle without a valid drivers’ license. News stories listed Lund’s name as an arrestee in the prostitution sting. The charges against Lund were dismissed. Lund sued the officers and the city under 42 U.S.C. 1983. The Seventh Circuit affirmed summary judgment for the defendants on First Amendment retaliation and malicious prosecution under Illinois law, citing the Supreme Court’s intervening "Nieves" (2019) holding, that, in most cases, probable cause to arrest defeats a claim of retaliatory arrest. There was probable cause to arrest Lund.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Perez

Court: US Court of Appeals for the Seventh Circuit
Docket: 18-3156
Opinion Date: April 23, 2020
Judge: KANNE
Areas of Law: Criminal Law

Beloit officers facilitated a recorded controlled buy of heroin from Perez, a suspected high-level drug dealer. Perez sold 98 grams of heroin to an informant. Based on that transaction alone, Perez pled guilty to distributing heroin. At Perez’s sentencing hearing, the judge expressed concern that the guidelines range of 33–41 months’ imprisonment did not reflect the full scope of his drug trafficking. The PSR described conduct that suggested that Perez was responsible for distributing large quantities of heroin, methamphetamine, and cocaine. The judge continued the hearing, directing

the government to file a memorandum, detailing which offense conduct it could support by a preponderance of the evidence. When the hearing reconvened, the government presented witness testimony that elaborated on conduct described in the PSR, including drug ledgers, Perez's post-arrest conversation with his girlfriend, large sums of cash, a money counter, cell phones, and Perez's passport. The judge calculated a higher guidelines range and imposed a 121-month sentence. The Seventh Circuit affirmed, rejecting an argument that the sentencing judge should have recused himself. Perez has not demonstrated that a reasonable observer would have questioned the judge's impartiality nor did he allege that the judge was biased based on events outside the proceedings. The judge's continuance was laudable, not prejudicial.

Read Opinion Are you a lawyer? **Annotate this case**.

Jackson v. United States

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1131
Opinion Date: April 20, 2020
Judge: Lavenski R. Smith
Areas of Law: Criminal Law

The Eighth Circuit affirmed the district court's denial of a 28 U.S.C. 2255 motion to vacate, set aside, or correct petitioner's sentence. The court held that the district court did not err in denying an evidentiary hearing as to petitioner's claim that counsel was constitutionally ineffective for failing to conduct adequate pretrial investigations. In this case, petitioner failed to identify any specific witnesses or evidence that counsel failed to uncover. Furthermore, petitioner failed to show that counsel's representation prejudiced his case. The court also held that the district court did not err in denying an evidentiary hearing as to petitioner's claim that his new counsel was ineffective for failing to subpoena witnesses, for convincing petitioner not to testify, for failing to object to or appeal the district court's answer to a jury question, and for failing to object to the district court's designation of petitioner as a career offender.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Bolman

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-2759
Opinion Date: April 21, 2020
Judge: Jane Louise Kelly
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's conviction for involuntary manslaughter after he struck and killed his nephew with his truck. The court held that the evidence was sufficient to support the conviction, because a reasonable jury could find defendant grossly negligent beyond a reasonable doubt. The court also held that the district court did not plainly err by failing to instruct the jury that actual knowledge is an essential element of the offense that is separate from gross negligence, because the instructions, viewed as a whole, accurately and adequately defined the essential elements of the offense.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Boyd

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-3528
Opinion Date: April 17, 2020
Judge: Kobes
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's sentence imposed after he pleaded guilty to being a felon in possession of a firearm. The court held that the facts underlying defendant's prior arrests were part of his history and characteristics under 18 U.S.C. 3553(a), and thus the district court could consider defendant's arrest records and the circumstances of those arrests. The court explained that the arrests were listed in the presentence report and gleaned from prior police reports. Furthermore, specific facts underlying the arrests may be considered for an upward departure and should be considered fair game for a variance where defendant did not object to them. The court also concluded that there is nothing here that suggested a corrected misstatement improperly influenced the district court's sentencing decision. Finally, the court held that the upward variance was not

unreasonable in consideration of defendant's previous assaults, coupled with the facts underlying his arrest in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Gonzalez-Esparsa

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1477
Opinion Date: April 22, 2020
Judge: Grasz
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's conviction for unlawful use of an identification document and misuse of a social security number. The court held that the evidence was sufficient to support defendant's convictions where a reasonable juror could conclude that defendant knew the permanent resident card bearing his name and photograph had been forged, counterfeited, falsely made, or unlawfully obtained when he used it to secure employment. Furthermore, a reasonable juror could conclude that defendant made the false representation regarding his purported social security number in order to deceive Midwest Concrete in order to obtain a job with the company.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Sanchez-Velasco

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-3568
Opinion Date: April 17, 2020
Judge: James B. Loken
Areas of Law: Criminal Law, Immigration Law

The Eighth Circuit affirmed the district court's denial of defendant's motion to suppress his responses to an ICE agent's two questions at the Treasurer's Office, because he was not in custody at the time of questioning. Although defendant was in custody at the ICE facility, the court held that an agent's questions were not custodial interrogation because the agent could not have known his questions were likely to elicit incriminating information regarding

the two criminal charges that were eventually brought against defendant. The court noted that the Attorney General's regulations carefully distinguish between the warrantless arrest of an alien for a criminal violation of the immigration laws, and what is called the "administrative arrest" of an alien who is reasonably believed to be illegally present in the United States. The court agreed with the district court that the agent's questioning was a request for routine information necessary for basic identification purposes that is not interrogation under Miranda, even if the information turns out to be incriminating.

Read Opinion Are you a lawyer? **Annotate this case**.

Anthony v. TRAX International Corp.

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-15662
Opinion Date: April 17, 2020
Judge: Kim McLane Wardlaw
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Ninth Circuit affirmed the district court's grant of summary judgment to TRAX in a disability discrimination action brought by plaintiff under Title I of the Americans with Disabilities Act (ADA). After TRAX terminated plaintiff from her position as a Technical Writer allegedly due to an inability or unwillingness to accommodate her disability, TRAX discovered during the course of litigation that plaintiff lacked the requisite bachelor's degree for her position. The panel held that, although McKennon v. Nashville Banner Publishing Co., 513 U.S. 352 (1995), held that after-acquired evidence cannot establish a superseding, non-discriminatory justification for an employer's challenged actions, after-acquired evidence remains available for other purposes, including to show that an individual is not qualified under the ADA. Because plaintiff did not satisfy one of the prerequisites for her position, she is not "otherwise qualified," and TRAX was not obligated to engage in the interactive process.

Read Opinion Are you a lawyer? **Annotate this case**.

City of Almaty v. Khrapunov

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-56451
Opinion Date: April 22, 2020
Judge: Marbley
Areas of Law: Criminal Law, International Law, White Collar Crime

The City of Almaty, in Kazakhstan, filed suit against defendant and his family under the Racketeer Influenced and Corrupt Organizations Act (RICO), alleging that they engaged in a scheme to defraud the city of millions of dollars. The City claimed that it was forced to spend money and resources in the United States to trace where its money was laundered. The district court dismissed the City's claim on the basis that it failed to state a domestic injury pursuant to the Supreme Court's recent decision in RJR Nabisco, Inc. v. European Community, 136 S. Ct. 2090 (2016). The Ninth Circuit held that the City failed to state any cognizable injury other than the foreign theft of its funds, and its voluntary expenditures were not proximately caused by defendants' acts of money laundering. In this case, the City's expenditure of funds to trace its allegedly stolen funds is a consequential damage of the initial theft suffered in Kazakhstan and is not causally connected to the predicate act of money laundering.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Baldon

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-10411
Opinion Date: April 21, 2020
Judge: Bennett
Areas of Law: Criminal Law

After defendant pleaded guilty to possession with intent to distribute a controlled substance, the district court sentenced him to 184 months in prison. The Ninth Circuit held that defendant's prior convictions for carjacking under section 215 of the California Penal Code are not categorical crimes of violence under USSG 4A1.1(e). Therefore, the district court incorrectly calculated defendant's criminal history by improperly including two points for his prior carjacking convictions. However, the panel held that the district court did not err in finding that defendant possessed a

firearm under USSG 2D1.1(b)(1). Accordingly, the panel affirmed in part, vacated in part, and remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Costanzo

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-10291
Opinion Date: April 17, 2020
Judge: Michael Daly Hawkins
Areas of Law: Criminal Law

The Ninth Circuit affirmed defendant's conviction of five counts of money laundering, holding that a reasonable trier of fact could have found beyond a reasonable doubt that the money laundering transactions, in which payment was made via bitcoin, affected interstate commerce in some way or to some degree. In this case, the transfer involved the use of an Internet or cellular network connected Personal Computer Device (PCD) to transfer bitcoin (together with the digital code necessary to unlock the bitcoin) to the digital wallet of another Internet or cellular network connected PCD.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Manzanares

Court: US Court of Appeals for the Tenth Circuit
Docket: 18-2010
Opinion Date: April 17, 2020
Judge: Mary Beck Briscoe
Areas of Law: Constitutional Law, Criminal Law

Defendant-Appellant Archie Manzanares appealed a district court's denial of his 28 U.S.C. 2255 motion challenging his sentence under the Armed Career Criminal Act (ACCA). Under the ACCA, an offense qualified as a violent felony by satisfying at least one of three definitions, which have come to be known as the Elements Clause, the Enumerated Clause, and the Residual Clause. Manzanares asserted that without the Residual Clause, his underlying New Mexico convictions (armed robbery, aggravated assault with a deadly weapon, and aggravated battery) no longer qualified

as violent felonies. The district court denied the motion, concluding that all three underlying convictions satisfied the Elements Clause. Manzanares appealed the classification of the armed robbery conviction as a violent felony to the Tenth Circuit, and sought to expand the certificate of appealability to allow him to appeal the decision regarding the aggravated assault with a deadly weapon and aggravated battery convictions. After review, the Tenth Circuit affirmed the district court's denial of Manzanares's 2255 motion, and denied his motion to expand the COA.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Delaney

Court: US Court of Appeals for the District of Columbia Circuit
Docket: 18-3093
Opinion Date: April 17, 2020
Judge: David S. Tatel
Areas of Law: Criminal Law

The DC Circuit vacated the district court's denial of defendant's motion to suppress evidence. The court held that officers violated the Fourth Amendment when they seized defendant because they lacked reasonable suspicion to justify the stop. In this case, a seizure occurred when the officers pulled into the parking lot, partially blocked defendant's vehicle, and activated their take-down light. The court held that any inference of suspicion that the officers drew from encountering defendant soon after hearing the nearby gunshots were undermined by the government's failure to identify specific and articulable facts supporting the officers' estimation of where the various shots came from. Accordingly, the court remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

Antenor v. Alaska, Department of Corrections

Court: Alaska Supreme Court
Docket: S-17005
Opinion Date: April 17, 2020
Judge: Carney

Areas of Law: Civil Procedure, Criminal Law, Government & Administrative Law

Several Alaska Department of Corrections inmates challenged the DOC's policy to charge for local telephone calls, arguing the rates they and call recipients had to pay for calls violated their constitutional right to rehabilitation, their statutory right to reasonable telephone access, and DOC's contractual obligations under a prior settlement and consent decree. In addition, one of the prisoners challenged DOC officers' decision to deny him access to a computer programming book he ordered from outside the prison. He contended that DOC placed a content-specific restriction on the educational materials and publications prisoners were allowed, violating the Alaska Constitution's free speech provisions as well as prisoners' right to reformation. Each of these challenges reached the Alaska Supreme Court after inmates exhausted the administrative process from prison. Inmates then appealed to the superior court, which denied relief. The Alaska Supreme Court determined the superior court record did not provide enough evidence for it to meaningfully determine the reasonableness of the rates charged inmates for local telephone calls; therefore the Court reversed denial of relief and remanded for further fact-finding by the trial court. The Court concluded that the facility's restrictions on programming-related books were rationally related to a legitimate interest, and because they did not infringe on the right to rehabilitation, it affirmed denial of a prisoner's motion to enforce his claimed right to a particular text about computer programming.

Read Opinion Are you a lawyer? **Annotate this case**.

Berger v. Bryant

Court: Arkansas Supreme Court
Citation: 2020 Ark. 357
Opinion Date: April 23, 2020
Judge: Rhonda K. Wood
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's petition to proceed in forma pauperis on a petition for writ of mandamus and a motion for declaratory judgment, holding that Appellant failed to state a colorable cause of action. In 1998, Appellant was convicted

of rape. In his petition for a writ of mandamus, Appellant asserted that he sought information pursuant to the Arkansas Freedom of Information Act regarding his rape conviction but received no response. The circuit court denied the petition. The Supreme Court affirmed, holding (1) even if Appellant had requested disclosable information, he would not be entitled to inspect it as an incarcerated person; and (2) Appellant did not demonstrate a legitimate claim given the facts presented and therefore failed to establish a colorable cause of action to support his request to proceed in forma pauperis.

Read Opinion Are you a lawyer? **Annotate this case**.

Carroll v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 360
Opinion Date: April 23, 2020
Judge: Wynne
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's motion for leave to file a petition for writ of error cram knobs, holding that the circuit court did not abuse its discretion in declining to issue the writ. Appellant pled guilty to rape and was sentenced as a habitual offender to 720 months' imprisonment. In his coram nobis petition, Appellant alleged several grounds for relief, including claims of actual innocence, an invalid arrest warrant, a coerced guilty plea, and prosecutorial misconduct. The circuit court denied the motion. The Supreme Court affirmed, holding that Appellant did not demonstrate that that the writ should issue and failed diligently to proceed on his claim for coram nobis relief.

Read Opinion Are you a lawyer? **Annotate this case**.

Cave v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 356
Opinion Date: April 23, 2020
Judge: Josephine L. Hart

Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's pro se petition for writ of habeas corpus, holding that the circuit court did not err in denying the petition. Appellant was found guilty of two counts of delivery of a controlled substance and one count of maintaining a drug premises. In his habeas petition, Appellant argued that he was actually innocent because his arrest and conviction was based on the false testimony of a witness who had a lengthy criminal history. Appellant further argued that the writ should issue because he was not afforded effective assistance of counsel. The circuit court denied the petition. The Supreme Court affirmed, holding (1) Appellant's claims regarding the witness's credibility do not constitute a valid assertion that he was being unlawfully detained; and (2) Appellant did not actually connect an allegation of ineffective assistance of counsel to his allegation that he was unlawfully detained.

Read Opinion Are you a lawyer? **Annotate this case**.

Chatmon v. Kelley

Court: Arkansas Supreme Court
Citation: 2020 Ark. 355
Opinion Date: April 23, 2020
Judge: Josephine L. Hart
Areas of Law: Criminal Law

The Supreme Court denied Appellant's appeal from the order of the circuit court denying his petition to proceed in forma pauperis on the grounds that Appellant failed to state a colorable cause of action in a petition for writ of habeas corpus, holding that the circuit court did not abuse its discretion by denying Appellant's in forma pauperis petition. In his habeas petition, Appellant alleged that the trial court lacked jurisdiction in his criminal case. Before this case was submitted to the Supreme Court, Appellant filed two motions, including a "Judicial Notice of a Void Judgment" and a "Notice to the Court." The Supreme Court denied the motions, holding that neither motion was cognizable under the Court's rules. The Court then affirmed the Supreme Court's denial of Appellant's in forma pauperis petition, holding that the circuit court correctly found that Appellant did not assert a colorable

cause of action.

Read Opinion Are you a lawyer? **Annotate this case**.

McClinton v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 353
Opinion Date: April 23, 2020
Judge: Karen R. Baker
Areas of Law: Criminal Law

The Supreme Court denied Petitioner's second petition requesting permission to proceed in the trial court with a petition for writ of error coram nobis, holding that Petitioner's proposed attack on the judgment had no merit. Petitioner was convicted of raping a mentally handicapped sixteen-year-old girl and was sentenced to life imprisonment. In his first petition for writ of error coram nobis Petitioner alleged a number of errors in the trial procedure. The first petition was denied. In his second coram nobis petition, Petitioner alleged violations of Brady v. Maryland, 373 U.S. 83 (1963). The Supreme Court denied the writ, holding that Petitioner failed to meet his burden of demonstrating a fundamental error of fact extrinsic to the record.

Read Opinion Are you a lawyer? **Annotate this case**.

Siegel v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 359
Opinion Date: April 23, 2020
Judge: Wynne
Areas of Law: Criminal Law

The Supreme Court dismissed Appellant's appeal from the circuit court's orders denying her motions to declare Ark. Code Ann. 5-62-106 (disposition of animal) and Ark. Code Ann. 5-62-111 (prevention of cruelty) unconstitutional and conditionally granting her motion for return of seized property, holding that there was no final, appealable order in this case. Appellant was convicted of thirty-one misdemeanor counts of cruelty to animals. The circuit court subsequently dismissed the charges on speedy-

trial grounds. The State appealed, and the Supreme Court dismissed the appeal on the grounds that it was not authorized. Appellant had filed motions seeking a declaration that sections 5-62-106 and -111 are unconstitutional and seeking the return of her seized property. The circuit court denied the constitutional claims and entered a conditional order granting Appellant's motion for return of seized property. Appellant appealed. The Supreme Court dismissed the appeal, holding that because the conditional order did not make specific findings as to the return of the property or as to damages and because it expressly left open the possibility of further proceedings, there was no final, appealable order in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

Thomas v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 354
Opinion Date: April 23, 2020
Judge: Josephine L. Hart
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Appellant's conviction of capital murder, holding that the evidence was sufficient to sustain the conviction and that the circuit court did not err in denying Appellant's motion to suppress tracking data generated by his cellphone. On appeal, Appellant argued that the trial court erred by denying his directed-verdict motion because the evidence supported the defense's theory of the case that he did not intend to shoot the victim. Further, Appellant argued that the court abused its discretion in denying his motion to suppress evidence obtained from the seizure of AT&T phone records. The Supreme Court disagreed, holding (1) the evidence was sufficient to support the capital murder conviction; and (2) the circuit court correctly denied the motion to suppress.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. Landowski

Court: California Courts of Appeal
Docket: C080210(Third Appellate District)

Opinion Date: April 23, 2020
Judge: Andrea Lynn Hoch
Areas of Law: Constitutional Law, Criminal Law

Defendant Michael Reyes, Jr., an active Norteno gang member (from the Broderick Boys subset), confronted a former Norteno gang member (from the Franklin Boys subset), "S.," about a physical altercation that occurred between S. and Reyes's stepfather over a debt. That earlier altercation had taken place in front of Reyes's autistic younger brother. Reyes pulled out a handgun and asked S. if he had a problem. S., who was riding his bicycle with his wife, "R.," when Reyes confronted him with the gun, stopped briefly, told Reyes to put the gun down if he wanted to fight, and then started to ride away. This angered Reyes, prompting him to fire six rounds at S. from behind. S. Was hit but survived. R. Was a short distance in front of S., but was not hit. Defendants Liberty Landowski and Lisa Humble were with Reyes at the time of the shooting and aided in his efforts to avoid being apprehended by law enforcement authorities. Reyes, Landowski, and Humble were tried together before the same jury. Reyes was convicted of one count of attempted murder (Count 1), two counts of assault with a semiautomatic firearm (Counts 2 and 4), one count of possession of a firearm by a convicted felon (Count 5), and one count of possession of ammunition by a convicted felon (Count 6). In addition to various firearm and other enhancements, the jury found Reyes committed the crimes for the benefit of, at the direction of, or in association with a criminal street gang with the specific intent to promote, further, or assist in criminal conduct by gang members. The jury convicted Landowski and Humble of being accessories to Reyes's criminal conduct (Count 9) and also found true gang enhancement allegations attached to that crime. Reyes challenged the sufficiency of the firearm evidence presented to support his conviction, and all defendants challenged the sufficiency of the evidence supporting their gang enhancements. The Court of Appeal determined Senate Bill 620 (2017-2018 Reg. Sess.) gave the trial court discretion to strike firearm enhancements in the interest of justice and applied retroactively; and Senate Bill 136 (2019-2020 Reg. Sess.) eliminated such enhancements, and also applied retroactively. To these issues, the Court remanded for the trial court's consideration. The Court affirmed the trial court in all other respects.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. May

Court: California Courts of Appeal
Docket: C084302(Third Appellate District)
Opinion Date: April 20, 2020
Judge: Ronald B. Robie
Areas of Law: Constitutional Law, Criminal Law

Defendant Raymond May was found guilty by jury of possessing an assault weapon and a machine gun based on his possession of a single AK-47 assault rifle while guarding a marijuana plantation. He was sentenced to probation, which included an electronic search condition. On appeal, defendant argued there was a lack of sufficient evidence corroborating his accomplice's testimony and demonstrating he knew of the firearm's illegal character. He further alleged the trial court erred in instructing the jury: that the accomplice instruction should have included language specifying that the accomplice testimony needed to prove more than defendant's mere presence or access to the firearm. Furthermore, defendant argued the electronic search condition imposed as part of his probation failed under the standards announced in California v. Lent, 15 Cal.3d 481 (1975). The Court of Appeal agreed defendant's electronic search condition should have been stricken, but otherwise affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. Perez

Court: California Courts of Appeal
Docket: E072260(Fourth Appellate District)
Opinion Date: April 20, 2020
Judge: Miller
Areas of Law: Constitutional Law, Criminal Law

In 2009, defendant-appellant Rudy Perez pled guilty to active gang participation under Penal Code section 186.22(a), and unlawful possession of a firearm under section 12025(b)(6). In 2010, defendant pled guilty to residential burglary under section 459, and active gang participation under section 186.22(a). In August of 2018, the State filed a new felony complaint, alleging one of the prior gang participation convictions as a strike prior. In

2018, defendant moved to vacate the two prior gang participation convictions based upon changes in the law that rendered them invalid. The trial court denied defendant's motion. In 2019, defendant asked for reconsideration, which was again denied. Thereafter, defendant filed a timely notice of appeal from the denial of his motion to vacate the convictions. The Court of Appeal found that defendant pled guilty to street terrorism under Penal Code section 186.22(a) in 2009 and 2010, and it was undisputed that while committing these offenses, defendant acted alone. However, subsequent to defendant's guilty pleas, in 2012, the California Supreme Court held that a defendant had to act in concert with a fellow gang member in order to be guilty of street terrorism. At that time, defendant could have filed a state habeas petition requesting relief, but failed to do so. "Defendants can lose remedies that are established by law when they fail to invoke such remedies in time." Section 1473.7 became effective in 2017. In defendant's motion filed in the trial court, defendant failed to state what new evidence was discovered, instead arguing that the trial court was allowed "to vacate a conviction where the defendant is innocent as a matter of law or where vacating the conviction is in the interest of justice, even though the defendant is no longer in custody or otherwise restrained by the conviction." The Court of Appeal concurred with the trial court's reason to deny relief, determining that "while the outcome in this case may be unfortunate for defendant, we are not here to rewrite legislation. The Legislature could amend section 1473.7 to address issues raised in this case. However, under the laws, as written, we must uphold the trial court's order."

Read Opinion Are you a lawyer? **Annotate this case**.

In re S.R.

Court: California Courts of Appeal
Docket: B300214(Second Appellate District)
Opinion Date: April 23, 2020
Judge: Bendix
Areas of Law: Criminal Law

Father appealed the juvenile court's dispositional ruling removing daughter from his custody, arguing that his mere possession of child pornography does not demonstrate that he poses a substantial risk of harm to his daughter. The Court of Appeal affirmed the order and held that there is

substantial evidence of risk of great harm to daughter—no matter how low the probability— that father will sexually abuse his daughter if he is provided unfettered access to her.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Bell

Court: California Courts of Appeal
Docket: B288528(Second Appellate District)
Opinion Date: April 23, 2020
Judge: Stratton
Areas of Law: Criminal Law

Defendant was convicted of one count of attempted robbery, one count of second degree murder, and one count of hit and run driving. The jury found not true the allegation that a principal was armed in the commission of the attempted robbery. The trial court found true the allegations that defendant had served four prior prison terms within the meaning of Penal Code section 667.5, subdivision (b). Defendant raised 13 claims of error on appeal. The Court of Appeal held that the section 667.5, subdivision (b) enhancement terms must be stricken and the matter remanded to the trial court for resentencing. The court also held that defendant forfeited some of his substantive claims and other lack merit. Finally, the court held that, if there is instructional error, the errors are harmless under any standard of review. Accordingly, the court affirmed the judgment of conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Drayton

Court: California Courts of Appeal
Docket: H046928(Sixth Appellate District)
Opinion Date: April 17, 2020
Judge: Danner
Areas of Law: Criminal Law

In 1991, the Wards and their teenage daughter awoke and discovered four men, including Drayton, inside their house. Two were armed. One told the daughter he was going to rape her and placed a firearm inside her vagina.

Drayton told the man not to do it. Drayton had a gun and held Mrs. Ward down during the robbery. Two others shot and killed Mr. Ward. Drayton and the others left without seeking help for the Wards. Drayton did not shoot Mr. Ward or threaten to rape the daughter. Drayton surrendered the next day. Drayton's sole prior conviction was a misdemeanor; he had no reported history of violence. Drayton was sentenced to 29 years to life imprisonment. In 2019, Drayton sought resentencing under Penal Code 1170.95, declaring that he "was not a major participant ... or did not act with reckless indifference to human life." Senate Bill 1437, effective January 1, 2019, restricted the circumstances under which a person can be liable for felony murder and enacted Penal Code 1170.95, which allows an individual, previously convicted of felony murder, to petition to have his murder conviction vacated and to be resentenced. The court of appeal directed the trial court to hold a hearing under section 1170.95(d) and to accept the assertions in the petition as true unless facts in the record conclusively refute them as a matter of law. If, accepting the petitioner's assertions as true, he meets section 1170.95(a)'s requirements for relief, the court must issue an order to show cause. In assessing the prima facie showing, the trial court should not weigh evidence or make credibility determinations.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Robinson

Court: California Courts of Appeal
Docket: B293746(Second Appellate District)
Opinion Date: April 20, 2020
Judge: Wiley
Areas of Law: Criminal Law

After defendant penetrated an unconscious woman with his fingers, he challenged evidentiary rulings and requests a presentence conduct credit. The Court of Appeal held that the trial court properly excluded cumulative evidence about past times the woman was intoxicated at the relevant bar, and any error in allowing a drug recognition expert to testify about whether the woman was incapacitated was harmless. However, the court held that the trial court undercalculated defendant's presentence custody credit because he was not convicted of a violent felony under Penal Code section 2933.1, which would otherwise limit those credits. Accordingly, the court

directed the trial court to award defendant 104 days of presentence custody credit and to amend the abstract of judgment, affirming in all other respects.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Torres

Court: California Courts of Appeal
Docket: B292551(Second Appellate District)
Opinion Date: April 20, 2020
Judge: Kenneth R. Yegan
Areas of Law: Criminal Law

Where, as here, the trial court factually finds that a self-represented defendant has engaged in an attempt to intimidate a witness, the constitutional right of self-representation can, in the exercise of the trial court's sound discretion, be revoked. The Court of Appeal affirmed defendant's conviction and sentence for two counts of battery on an ex-girlfriend. In this case, the trial court did not abuse its discretion in revoking defendant's pro se status after he asked his sister to contact the victim and have her say that she was coerced by the police detective to "press charges."

Read Opinion Are you a lawyer? **Annotate this case**.

Colorado v. Lujan

Court: Colorado Supreme Court
Citation: 2020 CO 26
Opinion Date: April 20, 2020
Judge: Brian D. Boatright
Areas of Law: Constitutional Law, Criminal Law

Abel Lujan was charged with first-degree murder for the death of his girlfriend after she was found beaten and strangled behind a friend's house. At trial, two women testified for the State about Lujan's prior violent behavior towards them. Prior to admitting this evidence, the trial court read a limiting instruction, telling the jury that it could only consider the evidence for the purposes of establishing Lujan's motive, intent, or common plan. A copy of

this instruction was not given to the jury for deliberations; however, the jury did receive an instruction at the close of the evidence explaining that certain evidence could only be considered for the limited purposes for which it was admitted. While deliberating, the jury submitted a question seeking clarification about the limiting instruction. Over defense counsel's objection, the trial court cleared the courtroom of the public and parties, leaving only the judge, bailiff, and court reporter; the judge then brought in the jury and reread the limiting instruction that it had previously read twice in open court. The jury ultimately found Lujan guilty of second-degree murder. Lujan appealed, arguing that the court's actions when rereading the jury instruction constituted a courtroom closure that violated his Sixth Amendment right to a public trial. A division of the court of appeals agreed and reversed Lujan's conviction. The State argued on certiorari review that the Colorado Supreme Court adopt a triviality standard, under which a defendant's constitutional right to a public trial was not violated when the closure at issue was trivial. In so doing, the State argued that the brief courtroom closure here was trivial and therefore did not violate Lujan's public trial right. The Court concurred with the State, adopted the standard and reversed the appellate court's decision.

Read Opinion Are you a lawyer? **Annotate this case**.

Archer v. State

Court: Florida Supreme Court
Docket: SC19-841
Opinion Date: April 23, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the order of the circuit court denying Appellant's successive motion to vacate his sentence of death under Fla. R. Crim. P. 3.851, holding that the circuit court did not err in denying the Rule 3.851 motion. Appellant was convicted of first-degree murder, armed robbery, and grand theft. Appellant was sentenced to death for the murder. The Supreme Court affirmed the convictions but reversed Appellant's death sentence and remanded the case for a new penalty phase. After a new penalty phase, Appellant was again sentenced to death. In his successive Rule 3.851 motion, Appellant raised three claims. The circuit court denied

relief. The Supreme Court affirmed, holding that the circuit court (1) properly denied Appellant's claim that his death sentence violated the Sixth and Eighth Amendments in light of Hurst v. Florida, 136 S. Ct. 616 (2016), and Hurst v. State, 202 So. 3d 40 (Fla. 2016); (2) correctly denied Appellant's claim that his sentence violated the Eighth Amendment; and (3) did not err in denying Appellant's claim of newly discovered evidence.

Read Opinion Are you a lawyer? **Annotate this case**.

Collins v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0158
Opinion Date: April 20, 2020
Judge: David E. Nahmias
Areas of Law: Constitutional Law, Criminal Law

Appellant Tommy Collins was convicted of felony murder in connection with the stabbing death of 14-year-old Rueben Hand. Friends gathered to watch the Peach Drop on New Year's Eve 2010; a disagreement ensued and Hand was stabbed near the Five Points MARTS station shortly after midnight. Appellant's only argument on appeal was that the trial court plainly erred when it gave the jury the State's requested instruction on "revenge for a prior wrong." Seeing no error, "much less plain error," the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Heyward v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0399
Opinion Date: April 20, 2020
Judge: Peterson
Areas of Law: Constitutional Law, Criminal Law

Larmell Heyward was convicted by jury of malice murder and possession of a firearm during the commission of a felony in connection with the 2007 shooting death of Ramon Rogers. Heyward argued on appeal of those convictions that the trial court erred in denying his request to charge the jury

on voluntary manslaughter. After review, the Georgia Supreme Court determined the trial court's refusal to give the charge was harmless, since, in the Court's estimation, there was no realistic probability that the jury would have accepted the "slight" evidence of voluntary manslaughter in the light of the strong evidence of malice murder.

Read Opinion Are you a lawyer? **Annotate this case**.

Howard v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0819
Opinion Date: April 20, 2020
Judge: Keith R. Blackwell
Areas of Law: Constitutional Law, Criminal Law

Kenneth Howard was tried by jury and convicted of the murder of Emily Ann Smith Newbegin. Howard appealed, contending that the evidence was legally insufficient to sustain his conviction. Upon its review of the record and briefs, the Georgia Supreme Court found no merit in Howard's claim of error, and affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Keller v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0006
Opinion Date: April 20, 2020
Judge: Boggs
Areas of Law: Constitutional Law, Criminal Law

Randall Keller was convicted of felony murder and related crimes arising out of the beating death of his ex-wife's two-year-old son, William Powell. On appeal, Keller raised numerous claims of error, including ineffective assistance of counsel, the trial court's rulings on motions before and during trial, several evidentiary rulings, and alleged bias on the part of the trial judge. However, finding no reversible error, the Georgia Supreme Court affirmed Keller's convictions.

Read Opinion Are you a lawyer? **Annotate this case**.

Mills v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0364
Opinion Date: April 20, 2020
Judge: Ellington
Areas of Law: Constitutional Law, Criminal Law

Roger Mills was found guilty by jury of malice murder and aggravated assault in connection with the death of Masuto Garrett. Mills contended that the trial court erred when, during jury deliberations, it excused a holdout juror without sufficient inquiry or good cause. After review, the Georgia Supreme Court concurred with that contention, and reversed Mills's convictions. The Court also concluded the evidence presented at trial was legally sufficient to support the convictions, so the State could retry Mills if it chose.

Read Opinion Are you a lawyer? **Annotate this case**.

Moore v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0344
Opinion Date: April 20, 2020
Judge: David E. Nahmias
Areas of Law: Constitutional Law, Criminal Law

Appellant Carzell Moore, proceeding pro se, appealed a trial court's denial of his motion to set aside a September 2017 order denying his motion for an out-of-time appeal of his 2002 resentencing on his 1977 convictions for murder and rape. Moore contended the trial court abused its discretion by denying his motion to set aside because he was not given proper notice of the September 2017 order. Finding that the record supported the trial court's ruling, the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Morris v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0176
Opinion Date: April 20, 2020
Judge: Bethel
Areas of Law: Constitutional Law, Criminal Law

Darius Morris was found guilty by jury of malice murder and other offenses in connection with the shooting death of Jameson Bush. Morris appealed, arguing he was denied the right to a timely appeal, that the trial court erred in restricting voir dire as to the religious beliefs and connections of potential jurors, that the trial court erred by giving a confusing jury charge regarding statements of co-conspirators, that the trial court erred by violating his right to a public trial by ordering that the courtroom doors be closed and locked during the court's charge to the jury, and that his trial counsel provided ineffective assistance by not objecting to the closure of the courtroom. Finding no error, the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Rickman v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0127
Opinion Date: April 20, 2020
Judge: Harold D. Melton
Areas of Law: Constitutional Law, Criminal Law

Victoria Rickman was convicted by jury of malice murder and a related firearm offense in connection with the shooting death of William Carter, Jr. Rickman and Carter had a tumultuous on-again, off-again relationship with a history of verbal and physical abuse, false accusations of sexual assault, empty threats to obtain temporary protective orders, and numerous calls to 911. In the days leading up to Carter's death, the pair was talking and meeting again despite a recent break-up. On one such 911 call, officers went to Rickman's residence responding to claims shots were fired. Rickman responded holding her small dog, hair wet, and in pajamas. She did not appear to be injured, and nothing in the home looked disturbed or out of place. Rickman told the officers, "he raped me again and I shot him."

Officers found Carter laying face up on the bed naked with multiple gunshot wounds to his body. An autopsy revealed that Carter was shot ten times – four times in the chest, three times in the back, once on the arm, and twice in the head. Rickman's examining physician testified that he found no injuries on Rickman consistent with her description of events, and no signs of trauma to her vaginal cavity. Rickman appealed her convictions, arguing she was denied effective assistance of counsel and that the trial court erred in admitting improper character evidence. Finding no reversible error, the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Robinson v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0265
Opinion Date: April 20, 2020
Judge: Peterson
Areas of Law: Constitutional Law, Criminal Law

Herbert Robinson appealed his convictions for malice murder, armed robbery, and possession of a firearm during the commission of a felony in connection with the death of Michael Moore. On appeal, he argued the trial court erred by allowing the State to use two firearms for demonstrative purposes during trial, and by allowing body-camera footage to be shown at trial. He also argued his trial counsel was ineffective for failing to object to a letter written by Robinson's cellmate being available to the jury for review during deliberations, and for failing to object to a visual aid used by the State during closing arguments. Because Robinson failed to show ineffective assistance of counsel or reversible error by the trial court, the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Santana v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0563
Opinion Date: April 20, 2020

Judge: Warren
Areas of Law: Constitutional Law, Criminal Law

Cuevas Carlos Santana was convicted by jury of malice murder and other crimes in connection with the 2010 shooting deaths of Israel Espinoza Mendoza, Vincente Soto Chavez, and Renato Soto Valencia. On appeal, Santana argues that the evidence was insufficient to support his convictions, that the trial court erred by declining to grant Santana a new trial on the general grounds, and that trial counsel provided ineffective assistance. Finding no reversible error, the Georgia Supreme Court affirmed Santana's convictions.

Read Opinion Are you a lawyer? **Annotate this case**.

Sullivan v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0056
Opinion Date: April 20, 2020
Judge: Warren
Areas of Law: Constitutional Law, Criminal Law

A jury convicted Antonio Sullivan of malice murder and other crimes in connection with the shooting death of Wava Benton. On appeal, Sullivan contended his trial counsel was constitutionally ineffective by failing to present evidence at trial to corroborate Sullivan's testimony about prior difficulties between Sullivan and Benton, and by failing to procure expert testimony about Sullivan's mental health—specifically about post-traumatic stress disorder— to be presented to the jury. The Georgia Supreme Court determined Sullivan failed to establish that his trial counsel was deficient in either respect, and therefore affirmed his convictions.

Read Opinion Are you a lawyer? **Annotate this case**.

Turner v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0247
Opinion Date: April 20, 2020
Judge: Warren

Areas of Law: Constitutional Law, Criminal Law

Appellant Ronald Turner appeals from his conviction for malice murder stemming from the stabbing death of William King. The stabbing took place outside an apartment at which Turner had driven in order to trade food for drugs. Turner testified in his own defense at trial and claimed that King hit him in the head with a beer bottle because Turner owed money to King from a prior drug transaction. Turner testified that he tried to get away from King, but that King chased him down and grabbed his jacket. According to Turner, King was getting ready to hit him again when Turner stabbed King in self-defense. Appealing his ultimate conviction, Turner contended he was denied the effective assistance of counsel in three respects. Seeing no reversible error after a review of the trial court record, the Georgia Supreme Court affirmed Turner's conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Valrie v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0380
Opinion Date: April 20, 2020
Judge: Keith R. Blackwell
Areas of Law: Constitutional Law, Criminal Law

Reuben Valrie was tried by jury and convicted of murder and other crimes in connection with the death of his infant daughter Aliyana. Valrie appealed, claiming that he was denied the effective assistance of counsel. Aliyana died as a result of closed head trauma, with a blunt-force abdominal injury as a secondary cause of death, which investigators determined was consistent with being shaken or dropped. At trial, Valrie presented the testimony of four expert witnesses who testified that Aliyana died of natural causes and that the injuries to her brain and abdomen were caused by events such as post-mortem CPR and the “rough” handling of her body by first responders. The jury rejected this defense and found Valrie guilty of murder and the other charges. Valrie contended that his trial lawyer should have raised a hearsay objection to the admission of recorded statements that his girlfriend (and Aliyana's mother) made to police investigators (as well as the testimony of one of those investigators about some of those

statements). Alternatively, Valrie argued that his lawyer should have sought the redaction of certain portions of the recorded statements that impugned his character. The Georgia Supreme Court concluded Valrie failed to present evidence that his trial counsel was deficient, or that he was prejudiced by any alleged failures. According, the Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Williams v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0241
Opinion Date: April 20, 2020
Judge: Keith R. Blackwell
Areas of Law: Constitutional Law, Criminal Law

Richard Williams, II, was tried by jury and convicted of murder in connection with the strangulation death of Cory Robinson. Williams and Robinson were involved in a sexual relationship and had been living together at an extended-stay hotel. Kelvin Spencer was a close friend of both Williams and Robinson. When Spencer met Williams at the hotel room, Williams looked angry and had scratches on his neck. Spencer saw Robinson lying on the floor in a “praying position.” Spencer did not believe Robinson was dead, and he helped Williams move clothes and other things to a U-Haul truck parked outside, in preparation for a move. Williams did not testify or present any evidence. Based on his lawyer’s opening and closing arguments, the defense theory was that Spencer killed Robinson because he was jealous of Williams’s relationship with Robinson. Williams’s sole claim on appeal was that he was denied the effective assistance of counsel when his trial lawyer failed to present as a defense that Williams accidentally killed Robinson during consensual erotic asphyxiation. He argued that his lawyer's discomfort with the topic of homosexual BDSM activity, and his own problems with the Georgia State Bar, precluded presentation of the "true" version of events, and that Williams acceded to the lawyer's defense strategy only "through ignorance and that he did not know that a defense based on consensual erotic asphyxiation was available." Finding no reversible error, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Malave

Court: Supreme Court of Hawaii
Docket: SCWC-18-0000332
Opinion Date: April 20, 2020
Judge: Mark E. Recktenwald
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the intermediate court of appeals (ICA) affirming Defendant's conviction of sexual assault in the first degree on the complaining witness pursuant to Haw. Rev. Stat. 707-730(1)(b), holding that the ICA did not err in affirming the family court. Specifically, the Supreme Court held (1) the jury should have been instructed to determine jurisdictional facts, but the error was harmless beyond a reasonable doubt; and (2) the ICA did not err in finding that there was no rational basis in the record to support providing the jury instruction of the lesser included offense of sexual assault in the third degree.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Malave

Court: Supreme Court of Hawaii
Docket: SCWC-18-0000332
Opinion Date: April 22, 2020
Judge: Mark E. Recktenwald
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the intermediate court of appeals (ICA) affirming the judgment of the family court convicting Defendant on two counts of sexual assault in the first degree, holding that the ICA did not err in affirming the family court. At issue on appeal was the jurisdiction of the family court to try Defendant and the propriety of instructing the jury on a lesser included offense. The ICA affirmed, concluding that the family court had subject matter jurisdiction pursuant to Haw. Rev. Stat. 571-14(a)(1) and that there was no rational basis to support an instruction of the lesser included offense of sexual assault in the third degree. The Supreme Court affirmed, holding (1) although the jury should have been instructed to determine jurisdictional facts, the error was

harmless; and (2) the family court was not obligated to instruct the jury on the lesser included offense of sexual assault in the third degree.

Read Opinion Are you a lawyer? **Annotate this case**.

Idaho v. Burke

Court: Idaho Supreme Court - Criminal
Docket: 46841
Opinion Date: April 22, 2020
Judge: Moeller
Areas of Law: Constitutional Law, Criminal Law

Prior to sentencing, defendant James Burke was committed to the state mental hospital for 56 days to restore him to competency. After being evaluated and deemed competent to proceed to trial, Burke was returned to the county jail and later pleaded guilty pursuant to a plea agreement. At the conclusion of his sentencing hearing, Burke sought credit for the 56 days of time spent in court-ordered commitment. The district court denied the motion, concluding that commitment to a state mental hospital did not fall under the definition of 'incarceration' in Idaho Code section 18-309. After reviewing this issue carefully, the Idaho Supreme Court disagreed with the district court's "thorough and thoughtful analysis," holding that court-ordered commitment to state custody pursuant to Idaho Code sections 18-210 and 18-211 met the functional and legal definition of "incarceration" under Idaho Code section 18-309. "The extent of the liberty interests restricted by Burke's court-ordered commitment to State Hospital North are just too similar to imprisonment to conclude otherwise." Accordingly, the Court reversed the district court's order denying Burke's request for credit for time served and remanded the case for the district court to enter an order crediting him with the fifty-six days he spent committed to State Hospital North while the State restored his competency to face criminal charges.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Gibbs

Court: Iowa Supreme Court
Docket: 18-1298

Opinion Date: April 17, 2020
Judge: Edward M. Mansfield
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction of murder in the second degree, holding that Defendant's Fifth Amendment rights were invaded when the trial judge instructed the jury that Defendant was required to notify law enforcement of his use of deadly force, but the error was harmless. During trial, Defendant asserted the defense of justification in his shooting of the victim. At issue on appeal was whether the district court abused its discretion by giving a jury instruction incorporating the terms of Iowa Code 704.2B. The instruction included a statement that a person using deadly force is required to notify law enforcement about his use of deadly force. Defendant argued before the Supreme Court that both section 704.2B and the jury instruction incorporating that section violated his Fifth Amendment rights. The Supreme Court affirmed, holding (1) instructing the jury that a homicide defendant is required to notify a law enforcement agency of his use of deadly force violates the defendant's Fifth Amendment rights; but (2) any error in this case was harmless beyond a reasonable doubt.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Broxton

Court: Kansas Supreme Court
Docket: 114675
Opinion Date: April 17, 2020
Judge: Stegall
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's convictions for second-degree murder, burglary, and theft but reversed Defendant's sentences, holding that any error during the guilt phase was harmless but that the district court erred by scoring Defendant's prior Florida burglary conviction as a person felony instead of a nonperson felony. On appeal, the court of appeals concluded that a trial court may instruct the jury on felony murder even though the State only charged the defendant with premeditated first degree murder. The Supreme Court disagreed, holding (1) the court of appeals erred in concluding that a district court may elect to provide a felony-murder

instruction when that crime was not charged, and the district court properly found that the felony-murder instruction was not legally appropriate in this case; (2) the district court erred by excluding from evidence an exculpatory document from a Florida homicide investigation on the ground it was not relevant, but the error was harmless; and (3) the district court improperly scored Defendant's prior Florida burglary conviction as a person felony.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Corbin

Court: Kansas Supreme Court
Docket: 119665
Opinion Date: April 17, 2020
Judge: Dan Biles
Areas of Law: Criminal Law

The Supreme Court affirmed the ruling of the district court on remand resentencing Defendant to his original mandatory term of imprisonment after once again finding he was not a person with intellectual disability, holding that the district court did not abuse its discretion when it rejected Defendant's intellectual disability motion and imposed a mandatory term of imprisonment. Defendant pled no contest to first-degree premeditated murder. Before sentencing, Defendant filed a motion pursuant to Kan. Stat. Ann. 21-6622(b) asserting that he was a person with intellectual disability and was thus not subject to a mandatory minimum prison term. The district court denied the motion and sentenced Defendant to a hard twenty-five life sentence. While Defendant's appeal was pending, the Legislature amended Kan. Stat. Ann. 76-12b01(i), which provides new standards for deciding intellectual disability. The Supreme Court reversed and remanded for reconsideration of Defendant's motion using the new criteria. On remand, the district court reaffirmed its earlier ruling and again sentenced Defendant to a hard twenty-five life sentence. The Supreme Court affirmed, holding that the district court's ruling was reasonably based on the law and was supported by substantial competent evidence.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Frazier

Court: Kansas Supreme Court
Docket: 117456
Opinion Date: April 17, 2020
Judge: Wilson
Areas of Law: Criminal Law

The Supreme Court reversed the decision of the district court affirming the judgment of the district court denying Defendant's motion to withdraw plea of no contest to one count of possession of heroin with intent to distribute, holding that the district court's decision in finding no good cause for Defendant to withdraw his plea was based on errors of fact and law, which were grounds for finding abuse of discretion. On appeal, Defendant argued that the district court abused its discretion in denying his motion to withdraw his plea of no contest based on misleading or false statements contained in the plea agreement. The court of appeals affirmed the district court. The Supreme Court reversed, holding (1) there was enough uncertainty in this case to indicate that Defendant's plea agreement was not understandingly made; and (2) therefore, Defendant must be allowed to withdraw his plea.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Harris

Court: Kansas Supreme Court
Docket: 117362
Opinion Date: April 17, 2020
Judge: Wilson
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court reversed the judgment of the court of appeals affirming Defendant's conviction of possession fo marijuana, holding that Defendant's waiver of jury trial was legally insufficient. On appeal, Defendant argued that he did not properly waive his right to a jury and asserted three other issues. The Supreme Court reversed the judgment of the court of appeals affirming Defendant's convictions without addressing the three remaining issues, holding that because the district court failed properly to apprise Defendant of his right to a jury trial and failed to ensure that Defendant understood the nature of the right he was giving up, Defendant's constitutional right to a jury trial was violated in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Uk

Court: Kansas Supreme Court
Docket: 119712
Opinion Date: April 17, 2020
Judge: Wilson
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's conviction for first-degree premeditated murder, holding that the district court did not err in its challenged instructions to the jury. Specifically, the Supreme Court held (1) the district court did not err in refusing to give the jury Defendant's requested instruction on voluntary manslaughter as a lesser included offense of first-degree murder because the instruction was not factually appropriate; and (2) the district court did not commit clear error in issuing an unmodified version of Instruction No. 11, which contained the definition of "premeditation" and mirrored PIK Crim. 4th 54.150(d) because the instruction was legally appropriate.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Catruch

Court: Maine Supreme Judicial Court
Citation: 2020 ME 52
Opinion Date: April 23, 2020
Judge: Andrew M. Mead
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed the judgments of the trial court terminating Appellant's participation in the Co-Occurring Disorders and Veterans Court (Veterans Court), holding that the court did not err or abuse its discretion in terminating Appellant's participation in the Veterans Court. The Veterans Court is a criminal docket that provides judicial monitoring, specialized treatment, and other services for military veterans who have disorders often attributable to their military service. Appellant was charged

with leaving the scene of an accident and three other offenses. Appellant was admitted to the Veterans Court. Agreeing to sentencing outcomes in a plea agreement and entering into a bail contract, Appellant pleaded guilty to all charges against him. The court later terminated Appellant's participation in the Veterans Court, finding that Appellant had violated the conditions of his bail contract. The Supreme Judicial Court affirmed, holding (1) this matter was properly before the Court; and (2) given Appellant's failure to comply with the requirements for participation in the treatment court and his violations of the agreements, his termination from the Veterans Court was warranted.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Paquin

Court: Maine Supreme Judicial Court
Citation: 2020 ME 53
Opinion Date: April 23, 2020
Judge: Andrew M. Mead
Areas of Law: Constitutional Law, Criminal Law

In this appeal from Defendant's conviction for eleven counts of gross sexual misconduct, the Supreme Judicial Court vacated the judgment of conviction on one count, vacated the dismissal of other counts and remanded for entry of a judgment of acquittal on those counts, and affirmed in all other respects, holding that Defendant's convictions on both Counts 5 and 30 violated his double jeopardy protections and that the court erred in allowing the State to dismiss Counts 27, 28, and 29 during trial without Defendant's consent. The indictment charged Defendant with fifteen counts (Counts 1-13, 30-31) of gross sexual misconduct against the victim and sixteen counts (Counts 14-29) of gross sexual misconduct against a second alleged victim. During trial, the court granted Defendant's motion for a judgment of acquittal on Counts 10-13, and the State dismissed Counts 27-29. Defendant was found guilty of Counts 1-9 and 30-31 and not guilty on the remaining counts. The court entered judgment in accordance with the verdict. The Supreme Judicial Court held that the trial court erred in failing to rule that the Double Jeopardy Clause barred convictions on both Counts 5 and 30 and allowing the State to dismiss Counts 27, 28, and 29 rather than entering a judgment of acquittal on those counts.

Read Opinion Are you a lawyer? **Annotate this case**.

Watson v. State

Court: Maine Supreme Judicial Court
Citation: 2020 ME 51
Opinion Date: April 21, 2020
Judge: Joseph Jabar
Areas of Law: Criminal Law

The Supreme Judicial Court vacated the judgment of the unified criminal docket denying Appellant's petition for post-conviction review, holding that Appellant was deprived of the effective assistance of counsel when his trial attorney played a video of the ten-year-old victim's interview with police and that Appellant was adversely affected. Appellant was convicted of two counts of gross sexual assault, one count of unlawful sexual contact, and one count of visual sexual aggression against a child. The Supreme Court affirmed. Appellant later filed a petition for post-conviction review claiming that his trial attorney's representation was deficient because introducing the videotaped recording of the victim's entire interview with law enforcement was unnecessary to provide evidence supporting the victim's potential motive to fabricate the allegations. The post-conviction court denied denied the petition. The Supreme Court vacated the judgment below, holding that trial counsel's conduct was deficient and that counsel's actions rose to the level of comprising the reliability of Appellant's conviction and undermining confidence in it.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. Mazza

Court: Massachusetts Supreme Judicial Court
Docket: SJC-11363
Opinion Date: April 21, 2020
Judge: Budd
Areas of Law: Criminal Law

The Supreme Judicial Court reversed the order of the superior court denying Defendant's motion for a new trial and set aside the jury's verdicts

of first degree murder and robbery, holding that a recently discovered witness statement made to the police ago constituted newly discovered evidence that "would probably have been a real factor in the jury's deliberations." At issue was Defendant's sixth motion for a new trial, which was predicated on newly discovered evidence consisting of, among other things, a recently discovered statement made to the police in 1972. The superior court denied the motion. As to the police statement, the judge found that it did not constitute newly discovered evidence because Defendant failed to establish that defense counsel did not have possession of it at the time of trial. The Supreme Judicial Court reversed and remanded the case for a new trial, holding (1) Defendant sustained his burden of establishing that defense counsel did not have the 1972 police statement prior to or at trial, and therefore, the statement constituted newly discovered evidence; and (2) there was a substantial risk that the jury would have reached a different conclusion had the evidence been admitted at trial.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. McCarthy

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12750
Opinion Date: April 16, 2020
Judge: Gaziano
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Judicial Court affirmed the judgment of the district court denying Defendant's motions to suppress, holding that the limited use of automatic license plate readers (ALPRs) in this case did not implicate constitutional protections against unreasonable searches. While police were investigating Defendant on suspicion of drug distribution they used ALPRs on two bridges to track Defendant's movements. The police accessed historical data via ALPR technology and received real-time alerts, the last of which led to Defendant's arrest. Defendant filed motions to suppress the ALPR data and the fruits of the arrest. The superior court denied the motions. The Supreme Judicial Court affirmed, holding that while the widespread use of ALPRs in the Commonwealth could implicate a defendant's constitutional protected expectation of privacy in the whole of his public movements, that interest was not invaded by the limited extent

and use of the ALPR data in the instant case.

Read Opinion Are you a lawyer? **Annotate this case**.

Garden v. Commonwealth

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12821
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed the judgment of a single justice of the court denying Petitioner's petition for extraordinary relief under Mass. Gen. Laws ch. 211, 3 seeking an order vacating Petitioner's plea to aggravated rape and dismissing the underlying indictment, holding that the single justice did not err or abuse his discretion in denying relief. The issues raised by Petitioner had all been raised and adjudicated through the normal appellate process. Petitioner then filed a motion to withdraw his guilty plea. The motion was denied, and the Appeals Court affirmed. In this petition for extraordinary relief, Petitioner sought an order vacating his plea to aggravated rape and dismissing the underlying indictment. The single justice denied relief. The Supreme Judicial Court affirmed, holding that the superintendence power was not available as an additional layer of appellate review once all other avenues had been exhausted.

Read Opinion Are you a lawyer? **Annotate this case**.

In re Mitchell

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12910
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed the judgment of the county court denying, without a hearing, Petitioner's petition for relief under Mass. Gen. Laws ch. 211, 3, holding that the single justice did not err or abuse his discretion in denying relief. Defendant was convicted of several offenses.

The Appeals Court reversed the convictions and remanded the matter for a new trial. Thereafter, the Commonwealth filed a nolle prosequi as to all the charges. In his Mass. Gen. Laws ch. 211, 3 petition, Defendant alleged that no crime had been committed and that he was wrongfully prosecuted. The single justice denied relief. The Supreme Judicial Court affirmed, holding that Defendant did not demonstrate entitlement to the exercise of this Court's superintendence powers.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Reek

Court: Minnesota Supreme Court
Docket: A19-0153
Opinion Date: April 22, 2020
Judge: G. Barry Anderson
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction for first-degree murder, holding that there was no error in the proceedings below. Specifically, the Supreme Court held (1) Appellant's right to a fair trial before an impartial tribunal was not violated when the district court stated that it might reconsider its prior Spreigl ruling if the defense presented certain witnesses; (2) the jury instructions on accomplice liability were plainly erroneous, but Appellant failed to establish that there was a reasonable likelihood that the error had a significant effect on the verdict; (3) the prosecutor did not commit misconduct in his closing arguments regarding the law of accomplice liability; (4) the district court did not abuse its discretion by granting the State's motion to admit evidence of appellant's past convictions for impeachment purposes, including by allowing the specific convictions to be disclosed to the jury; and (5) Appellant's pro se arguments were without merit.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Woodard

Court: Minnesota Supreme Court
Docket: A18-1886

Opinion Date: April 22, 2020
Judge: Hudson
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the district court convicting Defendant of first-degree murder and sentencing him to life in prison without the possibility of release, holding that the district court did not err in denying Defendant's motion to present an alternative-perpetrator defense. Specifically, the Supreme Court held (1) the district court did not abuse its discretion in holding that Defendant's proffered evidence in support of his motion to present alternative-perpetrator evidence for lack of sufficient foundation; and (2) the district court committed an error that was plain in instructing the jury on the order in which to consider the charges against Defendant, but there was no reasonable likelihood that the instruction affected the jury's verdict and therefore did not affect Defendant's substantial rights.

Read Opinion Are you a lawyer? **Annotate this case**.

Huff v. Brown

Court: Nebraska Supreme Court
Citation: 305 Neb. 648
Opinion Date: April 23, 2020
Judge: Lindsey Miller-Lerman
Areas of Law: Communications Law, Criminal Law

The Supreme Court reversed the portion of the district court's order granting in part a writ of mandamus requiring Doug Brown, the sheriff of Furnas County, to provide records to Herchel Huff pursuant to the public records statutes, holding that the district court erred when it determined that Huff had shown that Brown had a clear duty to provide the requested records. Huff, an inmate, sought, among other documents, the criminal history records of jurors who had convicted hims. Furnas County sheriff Kurt Kapperman required a deposit of $750 before fulfilling the request. Huff subsequently filed a petition for writ of mandamus naming Kapperman as the defendant and seeking an order compelling Kapperman to release all requested documents. The court permitted Huff to substitute Brown, the current sheriff, in the caption of the case in place of Kapperman and granted in part mandamus. The Supreme Court reversed in part, holding that the

district court (1) did not err when it substituted Brown's name for Kapperman's; but (2) erred in issuing mandamus because Huff failed to demonstrate a prima facie case that he had been denied a request for public records that the sheriff had a clear duty to provide under Neb. Rev. Stat. 84-712.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Montoya

Court: Nebraska Supreme Court
Citation: 305 Neb. 581
Opinion Date: April 17, 2020
Judge: Freudenberg
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the judgment of the district court affirming Defendant's conviction and sentence for driving under the influence, holding that there was no error in the challenged rulings by the trial court. Specifically, the Supreme Court held that the district court did not err by (1) affirming the county court's order denying Defendant's motion to suppress fruits of the stop; (2) affirming the county court's order that denied Defendant's motion to suppress the fruits of his arrest; (3) affirming the county court's order that denied Defendant's motion to suppress the results of the test of his breath alcohol content; (4) finding sufficient evidence to support the conviction; and (5) finding that Defendant's sentence was not excessive.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Schroeder

Court: Nebraska Supreme Court
Citation: 305 Neb. 527
Opinion Date: April 17, 2020
Judge: Funke
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's sentence of death for first degree

murder, holding that there was no error in the sentence imposed by the sentencing panel. Specifically, the Supreme Court held that the sentencing panel did not err in (1) allowing the State to introduce evidence on the existence of mitigating circumstances; (2) acknowledging and weighing mitigating evidence from the presentence investigation report; (3) not requesting that documentation from the Department of Correctional Services regarding Defendant's time in custody for mitigation purposes be included in the presentence investigation report; (4) sentencing Defendant to death, where the Legislature has enacted safeguards to ensure fairness and accuracy in the resulting sentence; and (5) finding Defendant should be sentenced to death after balancing the aggravating evidence and mitigating evidence.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Kendrick v. Parker

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1509
Opinion Date: April 21, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals denying Appellant's request for a writ of prohibition and/or mandamus against Montgomery County Court of Common Pleas Judge E. Gerald Parker Jr., holding that the court of appeals correctly determined that Appellant's claim was barred by res judicata. Appellant sought a petition for writ of prohibition and/or mandamus against Judge Erik Blaine, the successor to the judge who sentenced Appellant, alleging that the sentencing court patently and unambiguously lacked jurisdiction to sentence him. Judge Parker, who had succeeded Judge Blaine, subsequently filed a motion for summary judgment. The court of appeals granted summary judgment for Judge Parker, concluding that Appellant failed to demonstrate that the sentencing court patently and unambiguously lacked jurisdiction or that he lacked an adequate remedy at law and that res judicata barred Appellant's claim. The Supreme Court affirmed, holding that Appellant's claim was barred by res judicata.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Nelson v. Russo

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1541
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals dismissing Appellant's petition for a writ of mandamus seeking to compel Cuyahoga County Court of Common Pleas Judge Nancy Margaret Russo to vacate the consecutive prison sentences imposed on Appellant in 1987, holding that Appellant had an adequate remedy at law and was barred from asserting additional claims of sentencing error he could have raised in his previous mandamus action. In 1987, Appellant was convicted of four counts of rape and one count of kidnapping. Appellant was sentenced to prison terms of fifteen to twenty-five years for each of the five counts, to be served consecutively. In 2019, Appellant sought a writ of mandamus to compel Judge Russo to vacate his consecutive sentences. The court of appeals dismissed the writ action, concluding that res judicata barred Appellant's claim and that his prior appeals were an adequate remedy at law to address the alleged defect in his consecutive sentences. The Supreme Court affirmed, holding that Appellant was not entitled to a writ of mandamus in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Roberts v. Marsh

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1540
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals dismissing Appellant's original action seeking a writ of procedendo and/or

mandamus to compel Hamilton County Court of Common Pleas Judge Melba Marsh to issue a corrected sentencing entry, holding that the court of appeals correctly dismissed the petition as moot. Appellant was convicted of murder with a repeat-violent-offender specification. Appellant later asked the trial court to correct his sentence, arguing that he had improperly been sentenced to postrelease control. On remand, Judge Marsh vacated the postrelease-control sentence. Appellant appealed that order. The court of appeals noted that the trial court had not set forth all the information required under Crim.R. 32(C) in a single document and dismissed the appeal for lack of a final, appealable order. Appellant then filed this original action seeking to compel Judge Marsh to issue a corrected sentencing entry that constitutes a final, appealable order. Judge Marsh issued a nunc pro tunc sentencing entry that constituted a final, appealable order. The court of appeals then dismissed the petition as moot. The Supreme Court affirmed, holding that because Judge Marsh performed the act Appellant requested, the court of appeals dismissed the petition as moot.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Steiner v. Rinfret

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1510
Opinion Date: April 21, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals dismissing Appellant's petition for a writ of mandamus against Holmes County Court of Common Pleas Judge Robert D. Rinfret, holding that the court of appeals correctly determined that Appellant had an adequate remedy in the ordinary course of the law. Appellant, who was serving consecutive prison terms for five convictions, filed a petition for a writ of mandamus arguing that Judge Rinfret improperly sentenced him to a prison term of nine years for his attempted rape conviction instead of the maximum term of eleven years. The court of appeals dismissed the petition, determining that Appellant had failed to file a mandatory affidavit of his prior civil actions and had an adequate remedy in the ordinary course of the law. The Supreme Court affirmed, holding that relief in mandamus was not

available because Petitioner had an adequate remedy in the ordinary course of the law.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Jeffries

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1539
Opinion Date: April 22, 2020
Judge: Donnelly
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals upholding Defendant's convictions of four counts related to two specific instances of sexual abuse of D.S., holding that the trial court and court of appeals correctly applied Ohio's rape-shield law and determined that evidence of D.S.'s prior nonconsensual sexual assault was inadmissible. On appeal, Defendant asserted that the trial court erred in prohibiting him from introducing evidence during trial that D.S. had previously been sexually assaulted by another person, arguing that the rape-shield law applies only to an accuser's prior consensual sexual activity. The lower court held that Ohio's rape-shield law addresses all sexual activity, not only consensual sexual activity. The court of appeals affirmed. The Supreme Court affirmed, holding (1) the plain meaning of the term "sexual activity" as used in the rape-shield law includes both consensual and nonconsensual sexual activity; and (2) therefore, all sexual activity is barred from admission into evidence by the rape-shield, absent certain exceptions listed in the law.

Read Opinion Are you a lawyer? **Annotate this case**.

Pennsylvania v. Britton

Court: Supreme Court of Pennsylvania
Docket: 55 MAP 2018
Opinion Date: April 22, 2020
Judge: Max Baer
Areas of Law: Constitutional Law, Criminal Law

California law enforcement officers interviewed Appellant Stacy Britton in

her California residence and, unbeknownst to her, recorded those interviews. Over Appellant's objection, Pennsylvania used those recordings as evidence to help convict Appellant of murder in Pennsylvania. The Pennsylvania Supreme Court granted allowance of appeal to examine whether the California law enforcement officers were acting as agents of the Pennsylvania State Police when they recorded the interviews with Appellant in her California home, and if so, whether Pennsylvania's constitutional and statutory protections were available to Appellant under those circumstances. The Court concluded the California law enforcement officers were not acting as agents of the Pennsylvania State Police when they interviewed Appellant, making analysis of whether any Pennsylvania-specific constitutional or statutory protections unwarranted. Because the Supreme Court concluded the Pennsylvania trial court reached the proper result in this matter, it affirmed that court's judgment.

Read Opinion Are you a lawyer? **Annotate this case**.

Pennsylvania v. Copenhaver

Court: Supreme Court of Pennsylvania
Docket: 48 MAP 2019
Opinion Date: April 22, 2020
Judge: Thomas G. Saylor
Areas of Law: Constitutional Law, Criminal Law

In August 2015, a deputy sheriff conducted a vehicle stop of Appellant Victor Copenhaver's pickup truck. Upon approaching the truck, the deputy noticed an odor of alcohol and marijuana emanating from the passenger compartment. After administering field sobriety tests, he arrested Appellant for suspected driving under the influence of alcohol and controlled substances ("DUI"). Appellant was ultimately charged with DUI and other offenses. Appellant challenged the deputy's authority to conduct a traffic stop and sought suppression of all evidence obtained during the encounter. Rather than presenting testimony at a suppression hearing, the parties stipulated that Appellant was driving the vehicle in question and that the deputy had training and qualifications equivalent to that of a police officer. The parties also agreed that the vehicle stop occurred as a result of the deputy observing the tailgate to the pickup truck being in a down position, which caught the deputy's attention. The deputy further observed the

registration on the pickup truck was expired, and additionally, the registration number was identified as belonging to a vehicle other than the one on which it was attached. The issue this case presented for the Pennsylvania Supreme Court's review was whether the deputy could lawfully conduct the traffic stop based on the expired registration sticker, on a theory that such a violation amounts to a breach of the peace. The Supreme Court concluded driving a vehicle with an expired registration did not entail a breach of the peace. It vacated the superior court's order insofar as it held that the expired registration was a breach of the peace, thus alone authorizing the deputy to stop Appellant's vehicle. Notably, in light of its holding, the Supreme Court found the superior court did not proceed to consider other relevant questions, such as whether the parties' factual stipulation should have been read as indicating that the officer's understanding that the registration sticker was associated with a different vehicle arose in the pre-stop timeframe – consistent with the Commonwealth's position throughout this litigation. "These issues should be resolved in the first instance by the intermediate court on remand."

Read Opinion Are you a lawyer? **Annotate this case**.

Pennsylvania v. Tedford

Court: Supreme Court of Pennsylvania
Docket: 773 CAP
Opinion Date: April 22, 2020
Judge: Donohue
Areas of Law: Constitutional Law, Criminal Law

Appellant Donald Tedford was convicted of first-degree murder and rape on February 6, 1987. He appealed the dismissal of his second petition for relief filed pursuant to the Post Conviction Relief Act ("PCRA"), on December 2, 2014, as amended by a counseled petition on May 5, 2015, and a supplemental petition filed on June 9, 2015. In connection with his initial filings, Tedford sought wholesale discovery of the prosecution's entire file, but the PCRA court concluded that the petition (as amended) was not timely filed. Tedford also appealed the PCRA court's order denying his supplemental PCRA petition, in which he requested discovery, an evidentiary hearing, and/or a new trial based upon the admission of expert testimony presented at trial related to microscopic hair analysis. The PCRA

court concluded that pursuant to PCRA Section 9545(b)(1)(ii), it had jurisdiction to consider the merits of Tedford's newly-discovered-facts claims, but ultimately it concluded Tedford had not asserted a meritorious claim in accordance with Section 9543(a)(2)(vi). Finding no reversible error in that analysis, the Pennsylvania Supreme Court affirmed dismissal of the petition for relief.

Read Opinion Are you a lawyer? **Annotate this case**.

Pennsylvania v. Trahey

Court: Supreme Court of Pennsylvania
Docket: 38 EAP 2018
Opinion Date: April 22, 2020
Judge: Wecht
Areas of Law: Constitutional Law, Criminal Law

The trial court granted Timothy Trahey's motion to suppress the results of a blood test that revealed his blood alcohol concentration ("BAC"), finding no justification for the investigating officers' failure to obtain a search warrant before conducting the test. On the Commonwealth's appeal, the Superior Court reversed, opining that the Commonwealth's evidence sufficiently established the existence of exigent circumstances, thus excusing the absence of a warrant. The Pennsylvania Supreme Court reversed, finding that while the exigency analysis is an objective one, "even disregarding the officers' subjective motivations, or their candid acknowledgment that they would have obtained a search warrant if they thought it necessary, there was no time-sensitive need to conduct a warrantless blood test under the circumstances of this case. Accordingly, the Superior Court's conclusion that the test was justified by exigent circumstances was drawn in error."

Read Opinion Are you a lawyer? **Annotate this case**.

In re Greg Abbott

Court: Supreme Court of Texas
Docket: 20-0291
Opinion Date: April 23, 2020
Judge: Per Curiam

Areas of Law: Constitutional Law, Criminal Law

The Supreme Court conditionally granted mandamus relief to the State seeking review of a temporary restraining order (TRO) blocking enforcement of Executive Order GA-13, which changes the rules applicable to judges' decisions regarding pre-trial bail, against judges, holding that the trial court lacked jurisdiction to order the judges' requested relief, even temporarily. GA-13 suspends certain statutes authorizing trial judges to release jail inmates with violent histories during the state of disaster due to the threat of the novel coronavirus. Plaintiffs alleged that GA-13 is unconstitutional and exceeds the governor's statutory emergency powers. Sixteen of the plaintiffs were Texas trial judges alleging that GA-13 improperly interferes with their judicial authority to make individualized bail decisions, and the other plaintiffs were public interest organizations and lawyer associations. The trial court issued a TRO blocking enforcement of GA-13 against judges. The Supreme Court conditionally granted mandamus relief, holding that the alleged threat of a criminal prosecution in this case did not give the judges standing to seek the invalidation of GA-13, and therefore, the trial court lacked jurisdiction to order their requested relief.

Read Opinion Are you a lawyer? **Annotate this case**.

Stahmann v. Texas

Court: Texas Court of Criminal Appeals
Docket: PD-0556-18
Opinion Date: April 22, 2020
Judge: Barbara Hervey
Areas of Law: Constitutional Law, Criminal Law

Appellant Karl Stahmann was involved in an automobile accident, after which he threw a bottle of promethazine, a controlled substance, over a nearby wire fence before law enforcement arrived. The bottle landed two to three feet past the fence in plain view. He was convicted of third-degree felony tampering with physical evidence and was sentenced to 10 years' confinement and fined $5,000. The judge suspended his sentence and placed him on community supervision for 10 years. Stahmann appealed, arguing in part that the evidence was insufficient to prove that he destroyed, altered, or concealed the prescription bottle. The court of appeals agreed

that the evidence was insufficient, but instead of rendering an acquittal, it reformed the judgment to show that Stahmann was convicted of the lesser-included offense of attempted tampering with physical evidence, a state-jail felony. After review of the evidence presented at trial, the Texas Court of Criminal Appeals concluded the evidence was indeed insufficient to prove that Appellant altered the prescription pill bottle when he threw it over the fence because the mere act of throwing the bottle did not change the bottle itself. "While a rational jury could have reasonably inferred that Stahmann intended to conceal the pill bottle when he threw it over the wire fence, the evidence shows that he failed to conceal it as he intended because the bottle landed short of the bush in plain view on top of some grass." The Court affirmed the trial court's judgment.

Read Opinion Are you a lawyer? **Annotate this case**.

Blanke v. Board of Pardons & Parole

Court: Utah Supreme Court
Citation: 2020 UT 16
Opinion Date: April 16, 2020
Judge: Himonas
Areas of Law: Criminal Law

The Supreme Court affirmed the decision of the court of appeals affirming the district court's denial of Appellant's petition for extraordinary relief, holding that, under the circumstances, the Utah Board of Pardons and Parole need not afford Appellant the due process protections explained in Neese v. Utah Board of Pardons and Parole, 416 P.3d 663 (2017), before it could determine that Appellant was a sex offender and condition his parole on sex offender treatment. Appellant was serving a prison sentence for his convictions of attempted child kidnapping and kidnapping. Because he was convicted of attempted child kidnapping Appellant was considered a sex offender under the sex offender registration statute. Further, Appellant admitted in his presentence report that he had sexual intercourse with a fifteen-year-old. Appellant filed a petition for extraordinary relief alleging that the Parole Board had violated his due process rights by conditioning his parole on completion of sex offender treatment even though he had not committed a sex offense. Summary judgment was granted for the Parole Board. The Supreme Court affirmed, holding that the Parole Board owed

Appellant no additional process before it considered unconnected sex offenses in its decision to require Appellant to undergo sex offender treatment.

Read Opinion Are you a lawyer? **Annotate this case**.

Washington v. Escalante

Court: Washington Supreme Court
Docket: 97268-1
Opinion Date: April 23, 2020
Judge: Steven González
Areas of Law: Constitutional Law, Criminal Law

Alejandro Escalante was detained for hours in a secured area at a border crossing and, the State conceded, interrogated by federal agents without Miranda warnings. Statements he made during that interrogation were used by the State to convict him of drug possession. While a traveler briefly detained and questioned at the border was typically not "in custody" for Miranda purposes, "the government's power to detain and question people at the border without implicating Miranda has limits." Here, the Washington Supreme Court determined those limits were reached. "This border detention created the type of inherently coercive environment that demands Miranda warnings to ensure an individual's choice to speak is the product of free will." The Supreme Court held that Escalante was in custody when he was interrogated and reversed.

Read Opinion Are you a lawyer? **Annotate this case**.

Washington v. Haggard

Court: Washington Supreme Court
Docket: 97375-0
Opinion Date: April 23, 2020
Judge: Barbara Madsen
Areas of Law: Constitutional Law, Criminal Law

A class C felony "washes out" and is omitted from a defendant's offender score as long as he or she is not convicted of any crime within five years of the last date of release from confinement. David Haggard was convicted of

a misdemeanor offense within this five-year period, which was dismissed pursuant to RCW 3.66.067. When Haggard later pleaded guilty to burglary and arson, the trial court included prior class C felonies in his criminal history, finding that the dismissed misdemeanor conviction interrupted the washout period for those offenses. Haggard contended on appeal this was error. The Washington Supreme Court determined that because a dismissed conviction constituted a “conviction” under the Sentencing Reform Act of 1981 (SRA), and misdemeanor dismissal and vacation were distinct processes, so Haggard's offender score was properly calculated.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Taylor

Court: Supreme Court of Appeals of West Virginia
Docket: 18-0502
Opinion Date: April 21, 2020
Judge: Walker
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the judgment of the circuit court giving Petitioner credit for twelve days of time served toward the sentence he received for his felony conviction although Petitioner spent additional time in confinement for other charges that were dismissed in the universal plea agreement, holding that to grant Petitioner additional credit for time served would do little more than reward Petitioner for habitual criminal behavior. Petitioner was charged with several crimes and agreed to resolve the pending charges against him in a universal plea agreement. Under the terms of the agreement, Petitioner agreed to plea guilty to the charge of felony carrying a concealed firearm by a prohibited person. In exchange, the State agreed to drop the remaining charges. After he was sentenced, Petitioner argued that, in addition to the twelve days of credit for time served he was granted, he was constitutionally entitled to credit for time served while he was incarcerated for charges that were resolved in the universal plea agreement. The Supreme Court affirmed, holding that Petitioner's circumstances implicated neither double jeopardy nor equal protection of the law such that additional credit for time served was constitutionally mandated.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Harrison

Court: Wisconsin Supreme Court
Dockets: 2017AP002441-CR, 2017AP002440-CR
Opinion Date: April 17, 2020
Judge: Patience D. Roggensack
Areas of Law: Criminal Law

The Supreme Court affirmed in part and reversed in part the decision of the court of appeals reversing an order of the circuit court that granted sentence credit to Defendant, holding that the court of appeals correctly found that Defendant was not entitled to sentence credit but erred by advancing the commencement of Defendant's terms of extended supervision for Defendant's 2007 and 2008 cases. Specifically, the Court held (1) Defendant was not entitled to sentence credit under Wis. Stat. 973.155(1)(a) because the days he spent in custody for which he sought sentence credit were not in connection with the courses of conduct for which those sentences were imposed; and (2) the court of appeals erred by advancing the commencement of Defendant's terms of extended supervision for his 2007 and 2008 cases to the date they would have begun but for Defendant's confinement for unrelated convictions that were later set aside, holding that whether to employ advancement is a public policy decision best left to the legislature.

Read Opinion Are you a lawyer? **Annotate this case**.

About Justia Opinion Summaries

Justia Weekly Opinion Summaries is a free service, with 63 different newsletters, each covering a different practice area.

Justia also provides 68 daily jurisdictional newsletters, covering every federal appellate court and the highest courts of all US states.

All daily and weekly Justia newsletters are free. Subscribe or modify your newsletter subscription preferences at daily.justia.com.

You may freely redistribute this email in whole.

About Justia

Justia is an online platform that provides the community with open access to the law, legal information, and lawyers.

Contact Us | Privacy Policy

Unsubscribe From This Newsletter
or unsubscribe from all Justia newsletters immediately **here.**

Justia | 1380 Pear Ave #2B, Mountain View, CA 94043

From: Criminal Law - Justia Weekly Opinion Summaries
To: Caravaggio, Suzanne (POL)
Subject: Latest 101 Cases This Week: Ramos v. Louisiana (U.S.), United States v. Diaz-Rivera (1st Cir.), United States v. Cotto (2d Cir.)
Date: Friday, April 24, 2020 9:01:46 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

If you are unable to see this message, click here to view it in a web browser.

Justia Weekly Opinion Summaries

Criminal Law
April 24, 2020

Table of Contents

Ramos v. Louisiana
Civil Rights, Constitutional Law, Criminal Law
US Supreme Court

United States v. Diaz-Rivera
Criminal Law
US Court of Appeals for the First Circuit

United States v. Cotto
Criminal Law
US Court of Appeals for the Second Circuit

United States v. Rosa
Criminal Law
US Court of Appeals for the Second Circuit

Fogle v. Sokol
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Third Circuit

James v. New Jersey State Police
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Third Circuit

Bazemore v. Best Buy
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Akande
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Chambers
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Ferebee
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Nance
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Johnson
Criminal Law
US Court of Appeals for the Fifth Circuit

United States v. McGinnis
Criminal Law
US Court of Appeals for the Fifth Circuit

Valentine v. Collier
Civil Rights, Constitutional Law, Criminal Law, Government & Administrative Law, Health Law
US Court of Appeals for the Fifth Circuit

United States v. Dowl
Criminal Law
US Court of Appeals for the Sixth Circuit

United States v. Fowler
Criminal Law
US Court of Appeals for the Sixth Circuit

United States v. Sumlin
Criminal Law
US Court of Appeals for the Sixth Circuit

United States v. Vance
Criminal Law, White Collar Crime
US Court of Appeals for the Sixth Circuit

Winburn v. Nagy
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Sixth Circuit

Lund v. City of Rockford
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

United States v. Perez
Criminal Law
US Court of Appeals for the Seventh Circuit

Jackson v. United States
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Bolman
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Boyd
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Gonzalez-Esparsa
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Sanchez-Velasco
Criminal Law, Immigration Law
US Court of Appeals for the Eighth Circuit

Anthony v. TRAX International Corp.
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Ninth Circuit

City of Almaty v. Khrapunov
Criminal Law, International Law, White Collar Crime
US Court of Appeals for the Ninth Circuit

United States v. Baldon
Criminal Law
US Court of Appeals for the Ninth Circuit

United States v. Costanzo
Criminal Law
US Court of Appeals for the Ninth Circuit

United States v. Manzanares
Constitutional Law, Criminal Law
US Court of Appeals for the Tenth Circuit

United States v. Delaney
Criminal Law
US Court of Appeals for the District of Columbia Circuit

Antenor v. Alaska, Department of Corrections
Civil Procedure, Criminal Law, Government & Administrative Law
Alaska Supreme Court

Berger v. Bryant
Criminal Law
Arkansas Supreme Court

Carroll v. State
Criminal Law
Arkansas Supreme Court

Cave v. State
Civil Rights, Constitutional Law, Criminal Law
Arkansas Supreme Court

Chatmon v. Kelley
Criminal Law
Arkansas Supreme Court

McClinton v. State
Criminal Law
Arkansas Supreme Court

Siegel v. State
Criminal Law
Arkansas Supreme Court

Thomas v. State
Civil Rights, Constitutional Law, Criminal Law
Arkansas Supreme Court

California v. Landowski
Constitutional Law, Criminal Law
California Courts of Appeal

California v. May
Constitutional Law, Criminal Law
California Courts of Appeal

California v. Perez
Constitutional Law, Criminal Law
California Courts of Appeal

In re S.R.
Criminal Law
California Courts of Appeal

People v. Bell
Criminal Law
California Courts of Appeal

People v. Drayton
Criminal Law
California Courts of Appeal

People v. Robinson
Criminal Law
California Courts of Appeal

People v. Torres
Criminal Law
California Courts of Appeal

Colorado v. Lujan
Constitutional Law, Criminal Law
Colorado Supreme Court

Archer v. State
Civil Rights, Constitutional Law, Criminal Law
Florida Supreme Court

Collins v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Heyward v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Howard v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Keller v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Mills v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Moore v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Morris v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Rickman v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Robinson v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Santana v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Sullivan v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Turner v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Valrie v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Williams v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

State v. Malave
Criminal Law
Supreme Court of Hawaii

State v. Malave
Criminal Law
Supreme Court of Hawaii

Idaho v. Burke
Constitutional Law, Criminal Law
Idaho Supreme Court - Criminal

State v. Gibbs
Civil Rights, Constitutional Law, Criminal Law
Iowa Supreme Court

State v. Broxton
Criminal Law
Kansas Supreme Court

State v. Corbin
Criminal Law
Kansas Supreme Court

State v. Frazier
Criminal Law
Kansas Supreme Court

State v. Harris
Civil Rights, Constitutional Law, Criminal Law
Kansas Supreme Court

State v. Uk
Criminal Law
Kansas Supreme Court

State v. Catruch
Criminal Law
Maine Supreme Judicial Court

State v. Paquin
Constitutional Law, Criminal Law
Maine Supreme Judicial Court

Watson v. State
Criminal Law
Maine Supreme Judicial Court

Commonwealth v. Mazza
Criminal Law
Massachusetts Supreme Judicial Court

Commonwealth v. McCarthy
Civil Rights, Constitutional Law, Criminal Law
Massachusetts Supreme Judicial Court

Garden v. Commonwealth
Criminal Law
Massachusetts Supreme Judicial Court

In re Mitchell
Criminal Law
Massachusetts Supreme Judicial Court

State v. Reek
Civil Rights, Constitutional Law, Criminal Law
Minnesota Supreme Court

State v. Woodard
Criminal Law
Minnesota Supreme Court

Huff v. Brown
Communications Law, Criminal Law
Nebraska Supreme Court

State v. Montoya
Civil Rights, Constitutional Law, Criminal Law
Nebraska Supreme Court

State v. Schroeder
Criminal Law
Nebraska Supreme Court

State ex rel. Kendrick v. Parker
Criminal Law
Supreme Court of Ohio

State ex rel. Nelson v. Russo
Criminal Law
Supreme Court of Ohio

State ex rel. Roberts v. Marsh
Criminal Law
Supreme Court of Ohio

State ex rel. Steiner v. Rinfret
Criminal Law
Supreme Court of Ohio

State v. Jeffries
Criminal Law
Supreme Court of Ohio

Pennsylvania v. Britton
Constitutional Law, Criminal Law
Supreme Court of Pennsylvania

Pennsylvania v. Copenhaver
Constitutional Law, Criminal Law
Supreme Court of Pennsylvania

Pennsylvania v. Tedford
Constitutional Law, Criminal Law
Supreme Court of Pennsylvania

Pennsylvania v. Trahey
Constitutional Law, Criminal Law
Supreme Court of Pennsylvania

In re Greg Abbott
Constitutional Law, Criminal Law
Supreme Court of Texas

Stahmann v. Texas
Constitutional Law, Criminal Law
Texas Court of Criminal Appeals

Blanke v. Board of Pardons & Parole
Criminal Law
Utah Supreme Court

Washington v. Escalante
Constitutional Law, Criminal Law
Washington Supreme Court

Washington v. Haggard
Constitutional Law, Criminal Law
Washington Supreme Court

State v. Taylor
Civil Rights, Constitutional Law, Criminal Law
Supreme Court of Appeals of West Virginia

State v. Harrison
Criminal Law
Wisconsin Supreme Court

COVID-19 Updates: Law & Legal Resources Related to Coronavirus

Click here to remove Verdict from subsequent Justia newsletter(s).

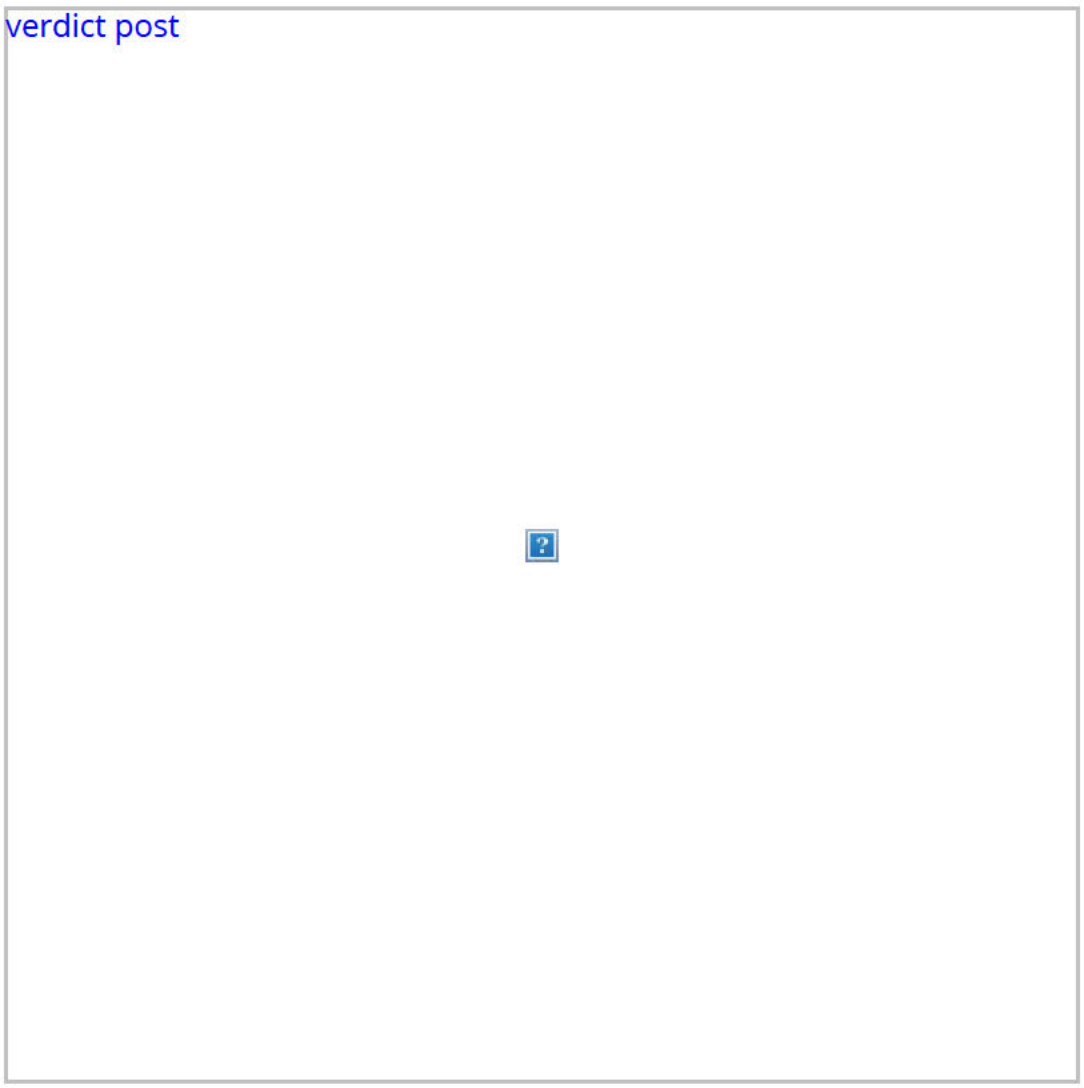
New on Verdict

Legal Analysis and Commentary

Rethinking Retroactivity in Light of the Supreme Court's Jury Unanimity Requirement

MICHAEL C. DORF

verdict post



In light of the U.S. Supreme Court's decision Monday in *Ramos v. Louisiana*, in which it held that the federal Constitution forbids states from convicting defendants except by a unanimous jury, Cornell law professor Michael C. Dorf discusses the Court's jurisprudence on retroactivity. Dorf highlights some costs and benefits of retroactivity and argues that the Court's refusal to issue advisory opinions limits its ability to resolve retroactivity questions in a way that responds to all the relevant considerations.

Read More

Criminal Law Opinions

Ramos v. Louisiana

Court: US Supreme Court
Docket: 18-5924
Opinion Date: April 20, 2020
Judge: Neil M. Gorsuch
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

In 48 states and in federal court, a single juror's vote to acquit is enough to prevent a conviction; Louisiana and Oregon punish people based on 10-to-2 verdicts. Ramos was convicted in a Louisiana court by a 10-to-2 jury verdict and was sentenced to life without parole. The Supreme Court reversed. The Sixth Amendment right to a jury trial, as incorporated against the states by the Fourteenth Amendment, requires a unanimous verdict to convict a defendant of a serious offense. Juror unanimity is a vital common law right. The Court rejected an "invitation" to "perform a cost-benefit analysis on the historic features of common law jury trials and to conclude that unanimity does not make the cut." In overturning its 1972 "Apodaca" decision, the Court stated that the reasoning, in that case, was "gravely mistaken" and "sits uneasily with 120 years of preceding case law." The fact that Louisiana and Oregon may need to retry defendants convicted of felonies by non-unanimous verdicts whose cases are still pending on direct appeal "will surely impose a cost, but new rules of criminal procedure usually do."

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Diaz-Rivera

Court: US Court of Appeals for the First Circuit
Docket: 18-1461
Opinion Date: April 20, 2020
Judge: Torruella
Areas of Law: Criminal Law

The First Circuit affirmed Defendant's upwardly variant sentence for one count of possession with intent to distribute cocaine and one count of using a firearm during and in relation to a drug-trafficking crime, holding that the sentence was neither procedurally nor substantively unreasonable. Pursuant to a plea agreement, Defendant pled guilty to drug-related crimes. After a sentencing hearing, the district court sentenced Defendant to an upwardly variant sentence of 180 months of imprisonment, thus declining to

impose the government's requested sentence. On appeal, Defendant challenged both the procedural and substantive reasonableness of his sentence. The First Circuit affirmed, holding that the 180-month sentence was neither procedurally nor substantively unreasonable.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Cotto

Court: US Court of Appeals for the Second Circuit
Docket: 18-2970
Opinion Date: April 20, 2020
Judge: Leval
Areas of Law: Criminal Law

A conviction for retaliating against a witness in violation of 18 U.S.C. 1513 does not require that the Government prove that defendant had knowledge of the federal nature of the proceeding. The Second Circuit rejected defendant's arguments to the contrary and affirmed his conviction for retaliating against a witness. The court remanded for revision of the provision of the sentence relating to the substance abuse treatment condition of supervised release; instructed the district court to consider on remand whether the court's forthcoming order in United States v. Traficante, No. 18-1962 (2d Cir., submitted Oct. 25, 2019) requires modification of the risk notification provision of supervised release; and granted the parties leave to reinstate this appeal to permit review of the district court's decision on remand as to the risk notification provision.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Rosa

Court: US Court of Appeals for the Second Circuit
Docket: 17-2004
Opinion Date: April 17, 2020
Judge: Nardini
Areas of Law: Criminal Law

Where a district court offers no explanation for its sentence, and where neither the adopted presentence report nor the statement of reasons

adequately demonstrates the court's reasoning, the court has committed plain error in violation of 18 U.S.C. 3553(c). The Second Circuit vacated defendant's sentence for conspiracy to commit wire fraud and aggravated identity theft. The court held that the district court failed to state its reasons for sentencing defendant as required under section 3553(c); the error is clear or obvious; and the error affected defendant's substantial rights. Accordingly, the court remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

Fogle v. Sokol

Court: US Court of Appeals for the Third Circuit
Docket: 19-1066
Opinion Date: April 21, 2020
Judge: Matey
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

In 1976, the body of 15-year-old “Kathy” was found near her Indiana County, Pennsylvania home. Kathy’s death involved a brutal assault, rape, and a gunshot to the head. Kathy's sisters, ages nine and 12, stated that she had gotten into a car with a man with blue eyes, black hair that came below his ears and curled at the ends, sideburns, heavy eyebrows, and a heavy mustache. Fogle had “straight reddish-blonde hair that dropped down his back and a matching, full beard that reached his waist.” After three years, Fogle became a suspect because a psychiatric patient described seeing Kathy get in a car with Fogle and his brother. The story was largely inconsistent with statements by Kathy’s sisters. Jailhouse informants were recruited and counseled by law enforcement with promises of leniency. The prosecutors “either knew about, encouraged, or permitted” this strategy. A jury found Fogle guilty of second-degree murder. In 2015, Fogle obtained DNA evidence excluding both himself and his brother as the source of semen collected from Kathy. His conviction was vacated. The Commonwealth declined to pursue new charges, describing the case as lacking “prosecutorial merit.” Fogle, having spent three decades in prison, sued the prosecutors and Indiana County under 42 U.S.C. 1983. The Third Circuit affirmed the denial of their motions to dismiss based on absolute immunity. Only truly prosecutorial functions, not investigative conduct, justify complete protection from suit. Fogle’s complaint alleges actions that fall

outside the narrow doctrine of absolute immunity.

Read Opinion Are you a lawyer? **Annotate this case**.

James v. New Jersey State Police

Court: US Court of Appeals for the Third Circuit
Docket: 18-1432
Opinion Date: April 21, 2020
Judge: Porter
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Stephens called 911 and reported that Gibbons hit her and had a gun in his truck. The police responded. Stephens obtained a temporary restraining order, prohibiting Gibbons from possessing firearms and from returning to Stephens's house. The next day, Gibbons went to Stephens's house. Stephens was talking on the phone; the friend called the police. Gibbons left Stephens's house. Trooper Conza arrived. Stephens stated that Gibbons had waved a gun throughout their argument. Conza told Stephens to go to the police barracks and reported over the radio that Gibbons had brandished a firearm. Conza, with Troopers Bartelt and Korejko, visited the nearby home of Gibbons's mother, James. James stated that she did not know where Gibbons was and that he might be off his schizophrenia medication. While driving to the barracks, Stephens saw Gibbons walking alongside the road and called 911. The Troopers responded. Bartelt parked his car and, exiting, observed that Gibbons was pointing a gun at his own head. Bartelt drew his weapon, stood behind his car door, and twice told Gibbons to drop his weapon. Gibbons did not comply. Bartelt shot Gibbons twice within seconds of stopping his car. Gibbons died that night. In James' suit under 42 U.S.C. 1983, the Third Circuit held that Bartelt is entitled to qualified immunity because he did not violate Gibbons's clearly established rights. Bartelt's pre-standoff knowledge of Gibbons differs from that of officers involved in cited cases. Bartelt could reasonably conclude that Gibbons posed a threat to others.

Read Opinion Are you a lawyer? **Annotate this case**.

Bazemore v. Best Buy

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-2196
Opinion Date: April 21, 2020
Judge: Quattlebaum
Areas of Law: Criminal Law

Plaintiff filed suit against her employer, Best Buy, claiming that she was harassed because of her race and gender and subjected to a hostile work environment in violation of Title VII of the Civil Rights Act of 1964. Plaintiff's complaint stemmed from an incident where a coworker made a racist and sexually charged joke to a small group of coworkers that included plaintiff. The Fourth Circuit affirmed the district court's motion to dismiss and held that, in the case of allegedly harassing comments by a co-worker, an employee must allege plausible facts that the employer knew, or should have known, about the harassment and failed to take action reasonably calculated to stop it. Because plaintiff failed to do this, the court affirmed the district court's judgment. In this case, the coworker's conduct was not imputable to Best Buy where Best Buy took steps that were not only reasonably calculated to end such behavior, but that it did in fact end it.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Akande

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-6833
Opinion Date: April 20, 2020
Judge: Diana Jane Gribbon Motz
Areas of Law: Criminal Law

After defendant moved under 28 U.S.C. 2255 to vacate his conviction based on the ineffective assistance of counsel, the district court denied the motion. The Fourth Circuit granted a certificate of appealability and reversed the district court's judgment. The court held that, given counsel's specific misadvice regarding defendant's rights to preserve his appellate rights, on which defendant understandably relied, the district court's general admonishments did not amount to the careful explanation that addresses the particular issue necessary to cure the error. In this case, the plea colloquy did not correct counsel's erroneous advice and the error prejudiced defendant. Accordingly, the court remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Chambers

Court: US Court of Appeals for the Fourth Circuit
Docket: 19-7104
Opinion Date: April 23, 2020
Judge: Floyd
Areas of Law: Criminal Law

After defendant was erroneously sentenced as a career offender, he moved to reduce his sentence to time served under the First Step Act. The district court denied defendant's motion to reduce his custodial sentence, though it granted the motion as to his supervised release term. The Fourth Circuit held that the First Step Act does not constrain courts from recognizing Guidelines errors. The court explained that First Step Act motions fall under 18 U.S.C. 3582(c)(1)(B), a distinct exception to finality, and that section 404(b) of the First Step Act expressly allows a court to impose a reduced sentence in order to give retroactive effect to sections 2 and 3 of the Fair Sentencing Act. Furthermore, 18 U.S.C. 3553(a) sentencing factors apply in the section 404(b) resentencing context, and the resentencing court has discretion within the section 404(b) framework to vary from the Guidelines and, in doing so, to consider movants' post-sentencing conduct. In this case, the district court seemingly believed that it could not vary from the Guidelines range to reflect post-sentencing information. Therefore, the court vacated the district court's sentencing order. Finally, the court held that any Guidelines error deemed retroactive, such as the error in this case, must be corrected in a First Step Act resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Ferebee

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-4266
Opinion Date: April 22, 2020
Judge: Traxler
Areas of Law: Criminal Law

The Fourth Circuit affirmed the denial of defendant's motion to suppress evidence recovered from a backpack, and the district court's conclusion that defendant abandoned the backpack and any legitimate expectation of privacy in its contents. The court rejected defendant's claim that the collective-knowledge doctrine has any bearing on the propriety of the district court's conclusion that defendant abandoned the backpack. The court also held that the district court is not precluded from finding abandonment in cases where the defendant, as here, has physical possession of the property he has disavowed. In this case, the record supported the district court's conclusion that defendant clearly and unequivocally disavowed ownership of the backpack. Even if the district court erred by finding that defendant abandoned the backpack, reversal would not be required because the search of the backpack was a proper search incident to arrest for which no warrant was required under the facts of this case.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Nance

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-4585
Opinion Date: April 21, 2020
Judge: Pamela Harris
Areas of Law: Criminal Law

The Fourth Circuit affirmed defendant's above-Guidelines sentence imposed after he pleaded guilty to two federal drug- and firearm-related offenses. The court held that defendant's sentence was not procedurally unreasonable where the district court took into account defendant's extensive criminal history; his pattern of reoffending upon release; his disciplinary infractions in custody and inability to comply with the terms of his release; and the fact that the offenses of conviction occurred over the course of days, in which he was arrested once, released, and then arrested again just days later. The court also held that defendant's sentence was substantively reasonable where the district court conducted a thorough, individualized assessment of defendant and his offense conduct in light of the 18 U.S.C. 3553(a) factors, and did not abuse its discretion in formulating the sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Johnson

Court: US Court of Appeals for the Fifth Circuit
Docket: 17-60852
Opinion Date: April 21, 2020
Judge: Priscilla R. Owen
Areas of Law: Criminal Law

The Fifth Circuit vacated defendant's sentence imposed after he pleaded guilty to violating 18 U.S.C. 922(g) and 924(e) by knowingly possessing a firearm after he had been convicted of a misdemeanor crime of domestic violence. The court held that the district court committing plain error by violating Federal Rule of Criminal Procedure 32 when it relied on factual allegations in the confidential sentencing recommendation that were not in the presentence report and that were not disclosed by defendant. The court explained that the use of undisclosed facts to justify an above-guidelines sentence seriously affects the fairness, integrity, and public reputation of judicial proceedings. Therefore, the court remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. McGinnis

Court: US Court of Appeals for the Fifth Circuit
Docket: 19-10197
Opinion Date: April 21, 2020
Judge: Stuart Kyle Duncan
Areas of Law: Criminal Law

18 U.S.C. 922(g)(8), which prohibits individuals subject to certain domestic violence protective orders from possessing firearms or ammunition for any purpose, is facially constitutional under the Fifth Circuit's two-step NRA framework. Even assuming arguendo that the conduct at issue -- the keeping and possessing of firearms by individuals subject to domestic protective orders -- falls within the Second Amendment right, defendant's facial challenge fails. The court applied intermediate scrutiny and held that section 922(g)(8) is reasonably adapted to the government interest of

reducing domestic gun abuse. The court also held that if the commonly understood definitions of terms in the protective order include acts involving "physical force," the protective order is sufficient to support a conviction under section 922(g)(8)(C)(ii). In this case, the jury plausibly found that the order satisfied the statute and the court declined to reverse defendant's conviction on this basis. However, the court remanded for the limited purpose of conforming defendant's written judgment to the district court's oral pronouncement.

Read Opinion Are you a lawyer? **Annotate this case**.

Valentine v. Collier

Court: US Court of Appeals for the Fifth Circuit
Docket: 20-20207
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Criminal Law, Government & Administrative Law, Health Law

Plaintiffs filed suit alleging that TDCJ's adoption and implementation of measures guided by changing CDC recommendations in regards to the COVID-19 pandemic do not go far enough. Plaintiffs filed a class action alleging violations of the Eighth Amendment's prohibition against cruel and unusual punishment, and the Americans with Disabilities Act, seeking a preliminary injunction. The Fifth Circuit granted TDCJ's motion to stay the district court's preliminary injunction, which regulates the cleaning intervals for common areas, the types of bleach-based disinfectants the prison must use, the alcohol content of hand sanitizer that inmates must receive, mask requirements for inmates, and inmates' access to tissues (amongst many other things). The court held that TDCJ is likely to prevail on the merits of its appeal because: (1) after accounting for the protective measures TDCJ has taken, plaintiffs have not shown a "substantial risk of serious harm" that amounts to "cruel and unusual punishment"; and (2) the district court committed legal error in its application of Farmer v. Brennan, by treating inadequate measures as dispositive of defendants' mental state. In this case, even assuming that there is a substantial risk of serious harm, plaintiffs lack evidence of defendants' subjective deliberate indifference to that harm. The court also held that TDCJ has shown that it will be

irreparably injured absent a stay, and that the balance of the harms and the public interest favor a stay. Finally, the court held that plaintiffs have not exhausted their administrative remedies as required in the Prison Litigation Reform Act (PLRA), and the district court's injunction goes well beyond the limits of what the PLRA would allow even if plaintiffs had properly exhausted their claims.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Dowl

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-2469
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

Dowl pleaded guilty to presenting false tax returns, 18 U.S.C. 286. He received a sentence of 30 months of imprisonment plus 24 months of supervised release. On supervised release, Dowl was charged with four new state crimes; failing to inform his probation officer that he had police contact; communicating with his co-defendant despite instructions to the contrary; failing to make payments on his restitution, fine, or special assessment; and failing to get a job. At a hearing, the court reviewed the evidence and allowed Dowl to tell his side of the story. The court deferred judgment on three of the four new state criminal law violations and dismissed the fourth and found Dowl gainfully employed. Dowl had failed to notify his probation officer about police contact, impermissibly communicated with his co-defendant, and did not pay his fines. After considering the 18 U.S.C. 3553(a) sentencing factors, the court returned Dowl to prison for 11 months, giving Dowl and his attorney the opportunity to raise any objections. Dowl had none. The Sixth Circuit affirmed, rejecting Dowl’s argument that the court committed reversible error by not directly addressing him to solicit an allocution. The court employed the “plain error” standard because Dowl did not raise any objection during his revocation hearing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Fowler

Court: US Court of Appeals for the Sixth Circuit
Dockets: 19-3071, 19-3070
Opinion Date: April 21, 2020
Judge: Donald
Areas of Law: Criminal Law

In 2018, Fowler pled guilty to possession of child pornography and violations of the conditions of his supervised release from a previous conviction for the same. In addition to possessing child pornography, Fowler had failed drug testing, had threatened his parole officer, and had tried to harass his girlfriend to recant her testimony. The district court ordered Fowler to pay a $5,000 special assessment for possession of child pornography under the Justice for Victims of Trafficking Act, 18 U.S.C. 3014. The court also varied upward and sentenced Fowler to the maximum statutory penalty for violating the conditions of his supervised release, imposing a 120-month sentence for possessing child pornography and a consecutive 36-month sentence for violating the terms of his supervised release. The Sixth Circuit vacated as to the assessment and remanded for a determination of indigency. The district court committed plain error by failing to address Fowler's ability to pay; the parties did not contemplate the $5,000 special assessment as a part of the waiver provision in the plea agreement. The court affirmed the sentence. The district court did not consider an impermissible factor (whether Fowler had actually touched a child) and Fowler had no other challenge to the reasonableness of his sentence,

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Sumlin

Court: US Court of Appeals for the Sixth Circuit
Docket: 18-3819
Opinion Date: April 21, 2020
Judge: Bush
Areas of Law: Criminal Law

Sumlin was convicted of the distribution of drugs that caused the 2015 death of Carrie Dobbins, 21 U.S.C. 841(a)(1) and (b)(1)(C), which carries enhanced penalty provisions. The Sixth Circuit affirmed his convictions and

his sentence to life in prison. The district court properly denied Sumlin's suppression motion, given that the affidavit established a sufficient nexus between his drug trafficking activity and residence that was searched. The court properly admitted testimony by the victim's sister, Kelly, who was Sumlin's former girlfriend and had purchased drugs from him. Kelly's testimony about Sumlin's drug-trafficking and that Sumlin was with Carrie on the day of her overdose was intrinsic proof that was relevant for providing background information and contextualizing the government's case against Sumlin. Sufficient evidence supported the jury's verdict that Sumlin distributed the drugs that caused Carrie's death.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Vance

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-5160
Opinion Date: April 17, 2020
Judge: Bush
Areas of Law: Criminal Law, White Collar Crime

The Spriggs' bank account was established to receive social security checks. The Spriggs' great-grandson, Vance, filled out an application in Mr. Spriggs's name for a debit card to draw on the checking account. Mr. Spriggs had never used a debit card. The Spriggses did not authorize Vance to do so. Bank cameras photographed Vance using the card to withdraw cash. Vance also used the card for personal expenses. At another bank, Vance used Mr. Spriggs's social security number to establish an account and obtain a $15,000 cash advance. Vance made other, unsuccessful loan applications. Upon being notified by the banks about suspicious activities involving his identity, Mr. Spriggs filed a police report. The police arrested Vance. While searching Vance's car, the police located a large stash of personal and financial documents belonging to the Spriggses, including bank statements, tax return forms, property-tax bills, and a car title. The Sixth Circuit affirmed Vance's convictions for access-device fraud, 18 U.S.C. 1029(a)(5), and two counts of aggravated identity theft, 18 U.S.C. 1028A(a)(1), and his 65-month sentence. The court rejected arguments that the district court failed to make adequate findings of fact after the bench trial, improperly denied a motion for judgment of acquittal,

and failed to correctly calculate the loss amount connected to Vance's charges under Sentencing Guidelines 2B1.1.

Read Opinion Are you a lawyer? **Annotate this case**.

Winburn v. Nagy

Court: US Court of Appeals for the Sixth Circuit
Dockets: 19-2399, 19-2398
Opinion Date: April 23, 2020
Judge: Jeffrey S. Sutton
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Winburn represented himself at his trial for armed robbery, home invasion, and conspiracy. Based on Winburn's disruptive behavior, the judge removed him from the courtroom and revoked Winburn's permission to represent himself, then granted a competency evaluation and a mistrial. While Winburn awaited his second trial, the judge permitted Winburn's stand-by attorney to withdraw because Winburn had sued her and enjoined Winburn from filing complaints or grievances against his new attorney, except to discharge her. Although represented by a new attorney, Winburn moved pro se to dismiss his charges on double jeopardy grounds. The trial judge denied the motion because Winburn's attorney had not filed it. Winburn filed a habeas petition under 28 U.S.C. 2241 challenging his retrial and another section 2241 petition challenging the injunction. The district judges denied both and declined to issue certificates of appealability. Winburn filed a notice of appeal for one petition and sought a certificate of appealability for the other. The Sixth Circuit held that state pretrial detainees proceeding under section 2241 may not appeal without certificates of appealability and granted Winburn a certificate on the injunction claim. A reasonable jurist could conclude that the unusual order was constitutionally infirm. The court denied relief with respect to double jeopardy. Winburn failed to exhaust his state-court remedies by a motion to dismiss.

Read Opinion Are you a lawyer? **Annotate this case**.

Lund v. City of Rockford

Court: US Court of Appeals for the Seventh Circuit

Docket: 19-1945
Opinion Date: April 20, 2020
Judge: ROVNER
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Lund, a reporter for the Rockford Scanner, heard, by police scanner, of multiple traffic stops in Midtown. He did not have a driver's license, so he rode a motorized bicycle to Midtown to take photographs. He suspected a prostitution sting operation. An officer noticed Lund and radioed the team. Officers Welsh and Campbell knew of Lund's previous anti-police speech. They directed Lund to "move on." Lund asked if he was breaking any laws. Campbell informed him that he was not, but that his continued presence would constitute obstruction of a police detail and result in arrest. Lund started his bicycle and called out, loudly, "goodbye officers." Concerned that Lund might post pictures on social media while the sting operation was ongoing and create a danger for unarmed undercover officers, the officers followed Lund and arrested him for driving the wrong way on a one-way street, operating a vehicle without insurance, obstructing a police officer, felony aggravated driving on a revoked license, and operating a motor vehicle without a valid drivers' license. News stories listed Lund's name as an arrestee in the prostitution sting. The charges against Lund were dismissed. Lund sued the officers and the city under 42 U.S.C. 1983. The Seventh Circuit affirmed summary judgment for the defendants on First Amendment retaliation and malicious prosecution under Illinois law, citing the Supreme Court's intervening "Nieves" (2019) holding, that, in most cases, probable cause to arrest defeats a claim of retaliatory arrest. There was probable cause to arrest Lund.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Perez

Court: US Court of Appeals for the Seventh Circuit
Docket: 18-3156
Opinion Date: April 23, 2020
Judge: KANNE
Areas of Law: Criminal Law

Beloit officers facilitated a recorded controlled buy of heroin from Perez, a suspected high-level drug dealer. Perez sold 98 grams of heroin to an

informant. Based on that transaction alone, Perez pled guilty to distributing heroin. At Perez's sentencing hearing, the judge expressed concern that the guidelines range of 33–41 months' imprisonment did not reflect the full scope of his drug trafficking. The PSR described conduct that suggested that Perez was responsible for distributing large quantities of heroin, methamphetamine, and cocaine. The judge continued the hearing, directing the government to file a memorandum, detailing which offense conduct it could support by a preponderance of the evidence. When the hearing reconvened, the government presented witness testimony that elaborated on conduct described in the PSR, including drug ledgers, Perez's post-arrest conversation with his girlfriend, large sums of cash, a money counter, cell phones, and Perez's passport. The judge calculated a higher guidelines range and imposed a 121-month sentence. The Seventh Circuit affirmed, rejecting an argument that the sentencing judge should have recused himself. Perez has not demonstrated that a reasonable observer would have questioned the judge's impartiality nor did he allege that the judge was biased based on events outside the proceedings. The judge's continuance was laudable, not prejudicial.

Read Opinion Are you a lawyer? **Annotate this case**.

Jackson v. United States

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1131
Opinion Date: April 20, 2020
Judge: Lavenski R. Smith
Areas of Law: Criminal Law

The Eighth Circuit affirmed the district court's denial of a 28 U.S.C. 2255 motion to vacate, set aside, or correct petitioner's sentence. The court held that the district court did not err in denying an evidentiary hearing as to petitioner's claim that counsel was constitutionally ineffective for failing to conduct adequate pretrial investigations. In this case, petitioner failed to identify any specific witnesses or evidence that counsel failed to uncover. Furthermore, petitioner failed to show that counsel's representation prejudiced his case. The court also held that the district court did not err in denying an evidentiary hearing as to petitioner's claim that his new counsel was ineffective for failing to subpoena witnesses, for convincing petitioner

not to testify, for failing to object to or appeal the district court's answer to a jury question, and for failing to object to the district court's designation of petitioner as a career offender.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Bolman

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-2759
Opinion Date: April 21, 2020
Judge: Jane Louise Kelly
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's conviction for involuntary manslaughter after he struck and killed his nephew with his truck. The court held that the evidence was sufficient to support the conviction, because a reasonable jury could find defendant grossly negligent beyond a reasonable doubt. The court also held that the district court did not plainly err by failing to instruct the jury that actual knowledge is an essential element of the offense that is separate from gross negligence, because the instructions, viewed as a whole, accurately and adequately defined the essential elements of the offense.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Boyd

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-3528
Opinion Date: April 17, 2020
Judge: Kobes
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's sentence imposed after he pleaded guilty to being a felon in possession of a firearm. The court held that the facts underlying defendant's prior arrests were part of his history and characteristics under 18 U.S.C. 3553(a), and thus the district court could consider defendant's arrest records and the circumstances of those arrests. The court explained that the arrests were listed in the presentence report

and gleaned from prior police reports. Furthermore, specific facts underlying the arrests may be considered for an upward departure and should be considered fair game for a variance where defendant did not object to them. The court also concluded that there is nothing here that suggested a corrected misstatement improperly influenced the district court's sentencing decision. Finally, the court held that the upward variance was not unreasonable in consideration of defendant's previous assaults, coupled with the facts underlying his arrest in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Gonzalez-Esparsa

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1477
Opinion Date: April 22, 2020
Judge: Grasz
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's conviction for unlawful use of an identification document and misuse of a social security number. The court held that the evidence was sufficient to support defendant's convictions where a reasonable juror could conclude that defendant knew the permanent resident card bearing his name and photograph had been forged, counterfeited, falsely made, or unlawfully obtained when he used it to secure employment. Furthermore, a reasonable juror could conclude that defendant made the false representation regarding his purported social security number in order to deceive Midwest Concrete in order to obtain a job with the company.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Sanchez-Velasco

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-3568
Opinion Date: April 17, 2020
Judge: James B. Loken
Areas of Law: Criminal Law, Immigration Law

The Eighth Circuit affirmed the district court's denial of defendant's motion to suppress his responses to an ICE agent's two questions at the Treasurer's Office, because he was not in custody at the time of questioning. Although defendant was in custody at the ICE facility, the court held that an agent's questions were not custodial interrogation because the agent could not have known his questions were likely to elicit incriminating information regarding the two criminal charges that were eventually brought against defendant. The court noted that the Attorney General's regulations carefully distinguish between the warrantless arrest of an alien for a criminal violation of the immigration laws, and what is called the "administrative arrest" of an alien who is reasonably believed to be illegally present in the United States. The court agreed with the district court that the agent's questioning was a request for routine information necessary for basic identification purposes that is not interrogation under Miranda, even if the information turns out to be incriminating.

Read Opinion Are you a lawyer? **Annotate this case**.

Anthony v. TRAX International Corp.

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-15662
Opinion Date: April 17, 2020
Judge: Kim McLane Wardlaw
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Ninth Circuit affirmed the district court's grant of summary judgment to TRAX in a disability discrimination action brought by plaintiff under Title I of the Americans with Disabilities Act (ADA). After TRAX terminated plaintiff from her position as a Technical Writer allegedly due to an inability or unwillingness to accommodate her disability, TRAX discovered during the course of litigation that plaintiff lacked the requisite bachelor's degree for her position. The panel held that, although McKennon v. Nashville Banner Publishing Co., 513 U.S. 352 (1995), held that after-acquired evidence cannot establish a superseding, non-discriminatory justification for an employer's challenged actions, after-acquired evidence remains available for other purposes, including to show that an individual is not qualified under the ADA. Because plaintiff did not satisfy one of the prerequisites for her

position, she is not "otherwise qualified," and TRAX was not obligated to engage in the interactive process.

Read Opinion Are you a lawyer? **Annotate this case**.

City of Almaty v. Khrapunov

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-56451
Opinion Date: April 22, 2020
Judge: Marbley
Areas of Law: Criminal Law, International Law, White Collar Crime

The City of Almaty, in Kazakhstan, filed suit against defendant and his family under the Racketeer Influenced and Corrupt Organizations Act (RICO), alleging that they engaged in a scheme to defraud the city of millions of dollars. The City claimed that it was forced to spend money and resources in the United States to trace where its money was laundered. The district court dismissed the City's claim on the basis that it failed to state a domestic injury pursuant to the Supreme Court's recent decision in RJR Nabisco, Inc. v. European Community, 136 S. Ct. 2090 (2016). The Ninth Circuit held that the City failed to state any cognizable injury other than the foreign theft of its funds, and its voluntary expenditures were not proximately caused by defendants' acts of money laundering. In this case, the City's expenditure of funds to trace its allegedly stolen funds is a consequential damage of the initial theft suffered in Kazakhstan and is not causally connected to the predicate act of money laundering.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Baldon

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-10411
Opinion Date: April 21, 2020
Judge: Bennett
Areas of Law: Criminal Law

After defendant pleaded guilty to possession with intent to distribute a controlled substance, the district court sentenced him to 184 months in

prison. The Ninth Circuit held that defendant's prior convictions for carjacking under section 215 of the California Penal Code are not categorical crimes of violence under USSG 4A1.1(e). Therefore, the district court incorrectly calculated defendant's criminal history by improperly including two points for his prior carjacking convictions. However, the panel held that the district court did not err in finding that defendant possessed a firearm under USSG 2D1.1(b)(1). Accordingly, the panel affirmed in part, vacated in part, and remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Costanzo

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-10291
Opinion Date: April 17, 2020
Judge: Michael Daly Hawkins
Areas of Law: Criminal Law

The Ninth Circuit affirmed defendant's conviction of five counts of money laundering, holding that a reasonable trier of fact could have found beyond a reasonable doubt that the money laundering transactions, in which payment was made via bitcoin, affected interstate commerce in some way or to some degree. In this case, the transfer involved the use of an Internet or cellular network connected Personal Computer Device (PCD) to transfer bitcoin (together with the digital code necessary to unlock the bitcoin) to the digital wallet of another Internet or cellular network connected PCD.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Manzanares

Court: US Court of Appeals for the Tenth Circuit
Docket: 18-2010
Opinion Date: April 17, 2020
Judge: Mary Beck Briscoe
Areas of Law: Constitutional Law, Criminal Law

Defendant-Appellant Archie Manzanares appealed a district court's denial of his 28 U.S.C. 2255 motion challenging his sentence under the Armed

Career Criminal Act (ACCA). Under the ACCA, an offense qualified as a violent felony by satisfying at least one of three definitions, which have come to be known as the Elements Clause, the Enumerated Clause, and the Residual Clause. Manzanares asserted that without the Residual Clause, his underlying New Mexico convictions (armed robbery, aggravated assault with a deadly weapon, and aggravated battery) no longer qualified as violent felonies. The district court denied the motion, concluding that all three underlying convictions satisfied the Elements Clause. Manzanares appealed the classification of the armed robbery conviction as a violent felony to the Tenth Circuit, and sought to expand the certificate of appealability to allow him to appeal the decision regarding the aggravated assault with a deadly weapon and aggravated battery convictions. After review, the Tenth Circuit affirmed the district court's denial of Manzanares's 2255 motion, and denied his motion to expand the COA.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Delaney

Court: US Court of Appeals for the District of Columbia Circuit
Docket: 18-3093
Opinion Date: April 17, 2020
Judge: David S. Tatel
Areas of Law: Criminal Law

The DC Circuit vacated the district court's denial of defendant's motion to suppress evidence. The court held that officers violated the Fourth Amendment when they seized defendant because they lacked reasonable suspicion to justify the stop. In this case, a seizure occurred when the officers pulled into the parking lot, partially blocked defendant's vehicle, and activated their take-down light. The court held that any inference of suspicion that the officers drew from encountering defendant soon after hearing the nearby gunshots were undermined by the government's failure to identify specific and articulable facts supporting the officers' estimation of where the various shots came from. Accordingly, the court remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

Antenor v. Alaska, Department of Corrections

Court: Alaska Supreme Court
Docket: S-17005
Opinion Date: April 17, 2020
Judge: Carney
Areas of Law: Civil Procedure, Criminal Law, Government & Administrative Law

Several Alaska Department of Corrections inmates challenged the DOC's policy to charge for local telephone calls, arguing the rates they and call recipients had to pay for calls violated their constitutional right to rehabilitation, their statutory right to reasonable telephone access, and DOC's contractual obligations under a prior settlement and consent decree. In addition, one of the prisoners challenged DOC officers' decision to deny him access to a computer programming book he ordered from outside the prison. He contended that DOC placed a content-specific restriction on the educational materials and publications prisoners were allowed, violating the Alaska Constitution's free speech provisions as well as prisoners' right to reformation. Each of these challenges reached the Alaska Supreme Court after inmates exhausted the administrative process from prison. Inmates then appealed to the superior court, which denied relief. The Alaska Supreme Court determined the superior court record did not provide enough evidence for it to meaningfully determine the reasonableness of the rates charged inmates for local telephone calls; therefore the Court reversed denial of relief and remanded for further fact-finding by the trial court. The Court concluded that the facility's restrictions on programming-related books were rationally related to a legitimate interest, and because they did not infringe on the right to rehabilitation, it affirmed denial of a prisoner's motion to enforce his claimed right to a particular text about computer programming.

Read Opinion Are you a lawyer? **Annotate this case**.

Berger v. Bryant

Court: Arkansas Supreme Court
Citation: 2020 Ark. 357
Opinion Date: April 23, 2020
Judge: Rhonda K. Wood

Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's petition to proceed in forma pauperis on a petition for writ of mandamus and a motion for declaratory judgment, holding that Appellant failed to state a colorable cause of action. In 1998, Appellant was convicted of rape. In his petition for a writ of mandamus, Appellant asserted that he sought information pursuant to the Arkansas Freedom of Information Act regarding his rape conviction but received no response. The circuit court denied the petition. The Supreme Court affirmed, holding (1) even if Appellant had requested disclosable information, he would not be entitled to inspect it as an incarcerated person; and (2) Appellant did not demonstrate a legitimate claim given the facts presented and therefore failed to establish a colorable cause of action to support his request to proceed in forma pauperis.

Read Opinion Are you a lawyer? **Annotate this case**.

Carroll v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 360
Opinion Date: April 23, 2020
Judge: Wynne
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's motion for leave to file a petition for writ of error cram knobs, holding that the circuit court did not abuse its discretion in declining to issue the writ. Appellant pled guilty to rape and was sentenced as a habitual offender to 720 months' imprisonment. In his coram nobis petition, Appellant alleged several grounds for relief, including claims of actual innocence, an invalid arrest warrant, a coerced guilty plea, and prosecutorial misconduct. The circuit court denied the motion. The Supreme Court affirmed, holding that Appellant did not demonstrate that that the writ should issue and failed diligently to proceed on his claim for coram nobis relief.

Read Opinion Are you a lawyer? **Annotate this case**.

Cave v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 356
Opinion Date: April 23, 2020
Judge: Josephine L. Hart
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's pro se petition for writ of habeas corpus, holding that the circuit court did not err in denying the petition. Appellant was found guilty of two counts of delivery of a controlled substance and one count of maintaining a drug premises. In his habeas petition, Appellant argued that he was actually innocent because his arrest and conviction was based on the false testimony of a witness who had a lengthy criminal history. Appellant further argued that the writ should issue because he was not afforded effective assistance of counsel. The circuit court denied the petition. The Supreme Court affirmed, holding (1) Appellant's claims regarding the witness's credibility do not constitute a valid assertion that he was being unlawfully detained; and (2) Appellant did not actually connect an allegation of ineffective assistance of counsel to his allegation that he was unlawfully detained.

Read Opinion Are you a lawyer? **Annotate this case**.

Chatmon v. Kelley

Court: Arkansas Supreme Court
Citation: 2020 Ark. 355
Opinion Date: April 23, 2020
Judge: Josephine L. Hart
Areas of Law: Criminal Law

The Supreme Court denied Appellant's appeal from the order of the circuit court denying his petition to proceed in forma pauperis on the grounds that Appellant failed to state a colorable cause of action in a petition for writ of habeas corpus, holding that the circuit court did not abuse its discretion by denying Appellant's in forma pauperis petition. In his habeas petition, Appellant alleged that the trial court lacked jurisdiction in his criminal case. Before this case was submitted to the Supreme Court, Appellant filed two

motions, including a "Judicial Notice of a Void Judgment" and a "Notice to the Court." The Supreme Court denied the motions, holding that neither motion was cognizable under the Court's rules. The Court then affirmed the Supreme Court's denial of Appellant's in forma pauperis petition, holding that the circuit court correctly found that Appellant did not assert a colorable cause of action.

Read Opinion Are you a lawyer? **Annotate this case**.

McClinton v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 353
Opinion Date: April 23, 2020
Judge: Karen R. Baker
Areas of Law: Criminal Law

The Supreme Court denied Petitioner's second petition requesting permission to proceed in the trial court with a petition for writ of error coram nobis, holding that Petitioner's proposed attack on the judgment had no merit. Petitioner was convicted of raping a mentally handicapped sixteen-year-old girl and was sentenced to life imprisonment. In his first petition for writ of error coram nobis Petitioner alleged a number of errors in the trial procedure. The first petition was denied. In his second coram nobis petition, Petitioner alleged violations of Brady v. Maryland, 373 U.S. 83 (1963). The Supreme Court denied the writ, holding that Petitioner failed to meet his burden of demonstrating a fundamental error of fact extrinsic to the record.

Read Opinion Are you a lawyer? **Annotate this case**.

Siegel v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 359
Opinion Date: April 23, 2020
Judge: Wynne
Areas of Law: Criminal Law

The Supreme Court dismissed Appellant's appeal from the circuit court's orders denying her motions to declare Ark. Code Ann. 5-62-106 (disposition

of animal) and Ark. Code Ann. 5-62-111 (prevention of cruelty) unconstitutional and conditionally granting her motion for return of seized property, holding that there was no final, appealable order in this case. Appellant was convicted of thirty-one misdemeanor counts of cruelty to animals. The circuit court subsequently dismissed the charges on speedy-trial grounds. The State appealed, and the Supreme Court dismissed the appeal on the grounds that it was not authorized. Appellant had filed motions seeking a declaration that sections 5-62-106 and -111 are unconstitutional and seeking the return of her seized property. The circuit court denied the constitutional claims and entered a conditional order granting Appellant's motion for return of seized property. Appellant appealed. The Supreme Court dismissed the appeal, holding that because the conditional order did not make specific findings as to the return of the property or as to damages and because it expressly left open the possibility of further proceedings, there was no final, appealable order in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

Thomas v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 354
Opinion Date: April 23, 2020
Judge: Josephine L. Hart
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Appellant's conviction of capital murder, holding that the evidence was sufficient to sustain the conviction and that the circuit court did not err in denying Appellant's motion to suppress tracking data generated by his cellphone. On appeal, Appellant argued that the trial court erred by denying his directed-verdict motion because the evidence supported the defense's theory of the case that he did not intend to shoot the victim. Further, Appellant argued that the court abused its discretion in denying his motion to suppress evidence obtained from the seizure of AT&T phone records. The Supreme Court disagreed, holding (1) the evidence was sufficient to support the capital murder conviction; and (2) the circuit court correctly denied the motion to suppress.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. Landowski

Court: California Courts of Appeal
Docket: C080210(Third Appellate District)
Opinion Date: April 23, 2020
Judge: Andrea Lynn Hoch
Areas of Law: Constitutional Law, Criminal Law

Defendant Michael Reyes, Jr., an active Norteno gang member (from the Broderick Boys subset), confronted a former Norteno gang member (from the Franklin Boys subset), "S.," about a physical altercation that occurred between S. and Reyes's stepfather over a debt. That earlier altercation had taken place in front of Reyes's autistic younger brother. Reyes pulled out a handgun and asked S. if he had a problem. S., who was riding his bicycle with his wife, "R.," when Reyes confronted him with the gun, stopped briefly, told Reyes to put the gun down if he wanted to fight, and then started to ride away. This angered Reyes, prompting him to fire six rounds at S. from behind. S. Was hit but survived. R. Was a short distance in front of S., but was not hit. Defendants Liberty Landowski and Lisa Humble were with Reyes at the time of the shooting and aided in his efforts to avoid being apprehended by law enforcement authorities. Reyes, Landowski, and Humble were tried together before the same jury. Reyes was convicted of one count of attempted murder (Count 1), two counts of assault with a semiautomatic firearm (Counts 2 and 4), one count of possession of a firearm by a convicted felon (Count 5), and one count of possession of ammunition by a convicted felon (Count 6). In addition to various firearm and other enhancements, the jury found Reyes committed the crimes for the benefit of, at the direction of, or in association with a criminal street gang with the specific intent to promote, further, or assist in criminal conduct by gang members. The jury convicted Landowski and Humble of being accessories to Reyes's criminal conduct (Count 9) and also found true gang enhancement allegations attached to that crime. Reyes challenged the sufficiency of the firearm evidence presented to support his conviction, and all defendants challenged the sufficiency of the evidence supporting their gang enhancements. The Court of Appeal determined Senate Bill 620 (2017-2018 Reg. Sess.) gave the trial court discretion to strike firearm enhancements in the interest of justice and applied retroactively; and Senate Bill 136 (2019-2020 Reg. Sess.) eliminated such enhancements,

and also applied retroactively. To these issues, the Court remanded for the trial court's consideration. The Court affirmed the trial court in all other respects.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. May

Court: California Courts of Appeal
Docket: C084302(Third Appellate District)
Opinion Date: April 20, 2020
Judge: Ronald B. Robie
Areas of Law: Constitutional Law, Criminal Law

Defendant Raymond May was found guilty by jury of possessing an assault weapon and a machine gun based on his possession of a single AK-47 assault rifle while guarding a marijuana plantation. He was sentenced to probation, which included an electronic search condition. On appeal, defendant argued there was a lack of sufficient evidence corroborating his accomplice's testimony and demonstrating he knew of the firearm's illegal character. He further alleged the trial court erred in instructing the jury: that the accomplice instruction should have included language specifying that the accomplice testimony needed to prove more than defendant's mere presence or access to the firearm. Furthermore, defendant argued the electronic search condition imposed as part of his probation failed under the standards announced in California v. Lent, 15 Cal.3d 481 (1975). The Court of Appeal agreed defendant's electronic search condition should have been stricken, but otherwise affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. Perez

Court: California Courts of Appeal
Docket: E072260(Fourth Appellate District)
Opinion Date: April 20, 2020
Judge: Miller
Areas of Law: Constitutional Law, Criminal Law

In 2009, defendant-appellant Rudy Perez pled guilty to active gang

participation under Penal Code section 186.22(a), and unlawful possession of a firearm under section 12025(b)(6). In 2010, defendant pled guilty to residential burglary under section 459, and active gang participation under section 186.22(a). In August of 2018, the State filed a new felony complaint, alleging one of the prior gang participation convictions as a strike prior. In 2018, defendant moved to vacate the two prior gang participation convictions based upon changes in the law that rendered them invalid. The trial court denied defendant's motion. In 2019, defendant asked for reconsideration, which was again denied. Thereafter, defendant filed a timely notice of appeal from the denial of his motion to vacate the convictions. The Court of Appeal found that defendant pled guilty to street terrorism under Penal Code section 186.22(a) in 2009 and 2010, and it was undisputed that while committing these offenses, defendant acted alone. However, subsequent to defendant's guilty pleas, in 2012, the California Supreme Court held that a defendant had to act in concert with a fellow gang member in order to be guilty of street terrorism. At that time, defendant could have filed a state habeas petition requesting relief, but failed to do so. "Defendants can lose remedies that are established by law when they fail to invoke such remedies in time." Section 1473.7 became effective in 2017. In defendant's motion filed in the trial court, defendant failed to state what new evidence was discovered, instead arguing that the trial court was allowed "to vacate a conviction where the defendant is innocent as a matter of law or where vacating the conviction is in the interest of justice, even though the defendant is no longer in custody or otherwise restrained by the conviction." The Court of Appeal concurred with the trial court's reason to deny relief, determining that "while the outcome in this case may be unfortunate for defendant, we are not here to rewrite legislation. The Legislature could amend section 1473.7 to address issues raised in this case. However, under the laws, as written, we must uphold the trial court's order."

Read Opinion Are you a lawyer? **Annotate this case**.

In re S.R.

Court: California Courts of Appeal
Docket: B300214(Second Appellate District)
Opinion Date: April 23, 2020
Judge: Bendix

Areas of Law: Criminal Law

Father appealed the juvenile court's dispositional ruling removing daughter from his custody, arguing that his mere possession of child pornography does not demonstrate that he poses a substantial risk of harm to his daughter. The Court of Appeal affirmed the order and held that there is substantial evidence of risk of great harm to daughter—no matter how low the probability— that father will sexually abuse his daughter if he is provided unfettered access to her.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Bell

Court: California Courts of Appeal
Docket: B288528(Second Appellate District)
Opinion Date: April 23, 2020
Judge: Stratton
Areas of Law: Criminal Law

Defendant was convicted of one count of attempted robbery, one count of second degree murder, and one count of hit and run driving. The jury found not true the allegation that a principal was armed in the commission of the attempted robbery. The trial court found true the allegations that defendant had served four prior prison terms within the meaning of Penal Code section 667.5, subdivision (b). Defendant raised 13 claims of error on appeal. The Court of Appeal held that the section 667.5, subdivision (b) enhancement terms must be stricken and the matter remanded to the trial court for resentencing. The court also held that defendant forfeited some of his substantive claims and other lack merit. Finally, the court held that, if there is instructional error, the errors are harmless under any standard of review. Accordingly, the court affirmed the judgment of conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Drayton

Court: California Courts of Appeal
Docket: H046928(Sixth Appellate District)

Opinion Date: April 17, 2020
Judge: Danner
Areas of Law: Criminal Law

In 1991, the Wards and their teenage daughter awoke and discovered four men, including Drayton, inside their house. Two were armed. One told the daughter he was going to rape her and placed a firearm inside her vagina. Drayton told the man not to do it. Drayton had a gun and held Mrs. Ward down during the robbery. Two others shot and killed Mr. Ward. Drayton and the others left without seeking help for the Wards. Drayton did not shoot Mr. Ward or threaten to rape the daughter. Drayton surrendered the next day. Drayton's sole prior conviction was a misdemeanor; he had no reported history of violence. Drayton was sentenced to 29 years to life imprisonment. In 2019, Drayton sought resentencing under Penal Code 1170.95, declaring that he "was not a major participant ... or did not act with reckless indifference to human life." Senate Bill 1437, effective January 1, 2019, restricted the circumstances under which a person can be liable for felony murder and enacted Penal Code 1170.95, which allows an individual, previously convicted of felony murder, to petition to have his murder conviction vacated and to be resentenced. The court of appeal directed the trial court to hold a hearing under section 1170.95(d) and to accept the assertions in the petition as true unless facts in the record conclusively refute them as a matter of law. If, accepting the petitioner's assertions as true, he meets section 1170.95(a)'s requirements for relief, the court must issue an order to show cause. In assessing the prima facie showing, the trial court should not weigh evidence or make credibility determinations.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Robinson

Court: California Courts of Appeal
Docket: B293746(Second Appellate District)
Opinion Date: April 20, 2020
Judge: Wiley
Areas of Law: Criminal Law

After defendant penetrated an unconscious woman with his fingers, he challenged evidentiary rulings and requests a presentence conduct credit. The Court of Appeal held that the trial court properly excluded cumulative

evidence about past times the woman was intoxicated at the relevant bar, and any error in allowing a drug recognition expert to testify about whether the woman was incapacitated was harmless. However, the court held that the trial court undercalculated defendant's presentence custody credit because he was not convicted of a violent felony under Penal Code section 2933.1, which would otherwise limit those credits. Accordingly, the court directed the trial court to award defendant 104 days of presentence custody credit and to amend the abstract of judgment, affirming in all other respects.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Torres

Court: California Courts of Appeal
Docket: B292551(Second Appellate District)
Opinion Date: April 20, 2020
Judge: Kenneth R. Yegan
Areas of Law: Criminal Law

Where, as here, the trial court factually finds that a self-represented defendant has engaged in an attempt to intimidate a witness, the constitutional right of self-representation can, in the exercise of the trial court's sound discretion, be revoked. The Court of Appeal affirmed defendant's conviction and sentence for two counts of battery on an ex-girlfriend. In this case, the trial court did not abuse its discretion in revoking defendant's pro se status after he asked his sister to contact the victim and have her say that she was coerced by the police detective to "press charges."

Read Opinion Are you a lawyer? **Annotate this case**.

Colorado v. Lujan

Court: Colorado Supreme Court
Citation: 2020 CO 26
Opinion Date: April 20, 2020
Judge: Brian D. Boatright
Areas of Law: Constitutional Law, Criminal Law

Abel Lujan was charged with first-degree murder for the death of his girlfriend after she was found beaten and strangled behind a friend's house. At trial, two women testified for the State about Lujan's prior violent behavior towards them. Prior to admitting this evidence, the trial court read a limiting instruction, telling the jury that it could only consider the evidence for the purposes of establishing Lujan's motive, intent, or common plan. A copy of this instruction was not given to the jury for deliberations; however, the jury did receive an instruction at the close of the evidence explaining that certain evidence could only be considered for the limited purposes for which it was admitted. While deliberating, the jury submitted a question seeking clarification about the limiting instruction. Over defense counsel's objection, the trial court cleared the courtroom of the public and parties, leaving only the judge, bailiff, and court reporter; the judge then brought in the jury and reread the limiting instruction that it had previously read twice in open court. The jury ultimately found Lujan guilty of second-degree murder. Lujan appealed, arguing that the court's actions when rereading the jury instruction constituted a courtroom closure that violated his Sixth Amendment right to a public trial. A division of the court of appeals agreed and reversed Lujan's conviction. The State argued on certiorari review that the Colorado Supreme Court adopt a triviality standard, under which a defendant's constitutional right to a public trial was not violated when the closure at issue was trivial. In so doing, the State argued that the brief courtroom closure here was trivial and therefore did not violate Lujan's public trial right. The Court concurred with the State, adopted the standard and reversed the appellate court's decision.

Read Opinion Are you a lawyer? **Annotate this case**.

Archer v. State

Court: Florida Supreme Court
Docket: SC19-841
Opinion Date: April 23, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the order of the circuit court denying Appellant's successive motion to vacate his sentence of death under Fla. R. Crim. P. 3.851, holding that the circuit court did not err in denying the Rule

3.851 motion. Appellant was convicted of first-degree murder, armed robbery, and grand theft. Appellant was sentenced to death for the murder. The Supreme Court affirmed the convictions but reversed Appellant's death sentence and remanded the case for a new penalty phase. After a new penalty phase, Appellant was again sentenced to death. In his successive Rule 3.851 motion, Appellant raised three claims. The circuit court denied relief. The Supreme Court affirmed, holding that the circuit court (1) properly denied Appellant's claim that his death sentence violated the Sixth and Eighth Amendments in light of Hurst v. Florida, 136 S. Ct. 616 (2016), and Hurst v. State, 202 So. 3d 40 (Fla. 2016); (2) correctly denied Appellant's claim that his sentence violated the Eighth Amendment; and (3) did not err in denying Appellant's claim of newly discovered evidence.

Read Opinion Are you a lawyer? **Annotate this case**.

Collins v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0158
Opinion Date: April 20, 2020
Judge: David E. Nahmias
Areas of Law: Constitutional Law, Criminal Law

Appellant Tommy Collins was convicted of felony murder in connection with the stabbing death of 14-year-old Rueben Hand. Friends gathered to watch the Peach Drop on New Year's Eve 2010; a disagreement ensued and Hand was stabbed near the Five Points MARTS station shortly after midnight. Appellant's only argument on appeal was that the trial court plainly erred when it gave the jury the State's requested instruction on "revenge for a prior wrong." Seeing no error, "much less plain error," the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Heyward v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0399
Opinion Date: April 20, 2020

Judge: Peterson
Areas of Law: Constitutional Law, Criminal Law

Larmell Heyward was convicted by jury of malice murder and possession of a firearm during the commission of a felony in connection with the 2007 shooting death of Ramon Rogers. Heyward argued on appeal of those convictions that the trial court erred in denying his request to charge the jury on voluntary manslaughter. After review, the Georgia Supreme Court determined the trial court's refusal to give the charge was harmless, since, in the Court's estimation, there was no realistic probability that the jury would have accepted the "slight" evidence of voluntary manslaughter in the light of the strong evidence of malice murder.

Read Opinion Are you a lawyer? **Annotate this case**.

Howard v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0819
Opinion Date: April 20, 2020
Judge: Keith R. Blackwell
Areas of Law: Constitutional Law, Criminal Law

Kenneth Howard was tried by jury and convicted of the murder of Emily Ann Smith Newbegin. Howard appealed, contending that the evidence was legally insufficient to sustain his conviction. Upon its review of the record and briefs, the Georgia Supreme Court found no merit in Howard's claim of error, and affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Keller v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0006
Opinion Date: April 20, 2020
Judge: Boggs
Areas of Law: Constitutional Law, Criminal Law

Randall Keller was convicted of felony murder and related crimes arising out

of the beating death of his ex-wife's two-year-old son, William Powell. On appeal, Keller raised numerous claims of error, including ineffective assistance of counsel, the trial court's rulings on motions before and during trial, several evidentiary rulings, and alleged bias on the part of the trial judge. However, finding no reversible error, the Georgia Supreme Court affirmed Keller's convictions.

Read Opinion Are you a lawyer? **Annotate this case**.

Mills v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0364
Opinion Date: April 20, 2020
Judge: Ellington
Areas of Law: Constitutional Law, Criminal Law

Roger Mills was found guilty by jury of malice murder and aggravated assault in connection with the death of Masuto Garrett. Mills contended that the trial court erred when, during jury deliberations, it excused a holdout juror without sufficient inquiry or good cause. After review, the Georgia Supreme Court concurred with that contention, and reversed Mills's convictions. The Court also concluded the evidence presented at trial was legally sufficient to support the convictions, so the State could retry Mills if it chose.

Read Opinion Are you a lawyer? **Annotate this case**.

Moore v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0344
Opinion Date: April 20, 2020
Judge: David E. Nahmias
Areas of Law: Constitutional Law, Criminal Law

Appellant Carzell Moore, proceeding pro se, appealed a trial court's denial of his motion to set aside a September 2017 order denying his motion for an out-of-time appeal of his 2002 resentencing on his 1977 convictions for murder and rape. Moore contended the trial court abused its discretion by

denying his motion to set aside because he was not given proper notice of the September 2017 order. Finding that the record supported the trial court's ruling, the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Morris v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0176
Opinion Date: April 20, 2020
Judge: Bethel
Areas of Law: Constitutional Law, Criminal Law

Darius Morris was found guilty by jury of malice murder and other offenses in connection with the shooting death of Jameson Bush. Morris appealed, arguing he was denied the right to a timely appeal, that the trial court erred in restricting voir dire as to the religious beliefs and connections of potential jurors, that the trial court erred by giving a confusing jury charge regarding statements of co-conspirators, that the trial court erred by violating his right to a public trial by ordering that the courtroom doors be closed and locked during the court's charge to the jury, and that his trial counsel provided ineffective assistance by not objecting to the closure of the courtroom. Finding no error, the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Rickman v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0127
Opinion Date: April 20, 2020
Judge: Harold D. Melton
Areas of Law: Constitutional Law, Criminal Law

Victoria Rickman was convicted by jury of malice murder and a related firearm offense in connection with the shooting death of William Carter, Jr. Rickman and Carter had a tumultuous on-again, off-again relationship with a history of verbal and physical abuse, false accusations of sexual assault, empty threats to obtain temporary protective orders, and numerous calls to

911. In the days leading up to Carter's death, the pair was talking and meeting again despite a recent break-up. On one such 911 call, officers went to Rickman's residence responding to claims shots were fired. Rickman responded holding her small dog, hair wet, and in pajamas. She did not appear to be injured, and nothing in the home looked disturbed or out of place. Rickman told the officers, "he raped me again and I shot him." Officers found Carter laying face up on the bed naked with multiple gunshot wounds to his body. An autopsy revealed that Carter was shot ten times – four times in the chest, three times in the back, once on the arm, and twice in the head. Rickman's examining physician testified that he found no injuries on Rickman consistent with her description of events, and no signs of trauma to her vaginal cavity. Rickman appealed her convictions, arguing she was denied effective assistance of counsel and that the trial court erred in admitting improper character evidence. Finding no reversible error, the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Robinson v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0265
Opinion Date: April 20, 2020
Judge: Peterson
Areas of Law: Constitutional Law, Criminal Law

Herbert Robinson appealed his convictions for malice murder, armed robbery, and possession of a firearm during the commission of a felony in connection with the death of Michael Moore. On appeal, he argued the trial court erred by allowing the State to use two firearms for demonstrative purposes during trial, and by allowing body-camera footage to be shown at trial. He also argued his trial counsel was ineffective for failing to object to a letter written by Robinson's cellmate being available to the jury for review during deliberations, and for failing to object to a visual aid used by the State during closing arguments. Because Robinson failed to show ineffective assistance of counsel or reversible error by the trial court, the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Santana v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0563
Opinion Date: April 20, 2020
Judge: Warren
Areas of Law: Constitutional Law, Criminal Law

Cuevas Carlos Santana was convicted by jury of malice murder and other crimes in connection with the 2010 shooting deaths of Israel Espinoza Mendoza, Vincente Soto Chavez, and Renato Soto Valencia. On appeal, Santana argues that the evidence was insufficient to support his convictions, that the trial court erred by declining to grant Santana a new trial on the general grounds, and that trial counsel provided ineffective assistance. Finding no reversible error, the Georgia Supreme Court affirmed Santana's convictions.

Read Opinion Are you a lawyer? **Annotate this case**.

Sullivan v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0056
Opinion Date: April 20, 2020
Judge: Warren
Areas of Law: Constitutional Law, Criminal Law

A jury convicted Antonio Sullivan of malice murder and other crimes in connection with the shooting death of Wava Benton. On appeal, Sullivan contended his trial counsel was constitutionally ineffective by failing to present evidence at trial to corroborate Sullivan's testimony about prior difficulties between Sullivan and Benton, and by failing to procure expert testimony about Sullivan's mental health—specifically about post-traumatic stress disorder— to be presented to the jury. The Georgia Supreme Court determined Sullivan failed to establish that his trial counsel was deficient in either respect, and therefore affirmed his convictions.

Read Opinion Are you a lawyer? **Annotate this case**.

Turner v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0247
Opinion Date: April 20, 2020
Judge: Warren
Areas of Law: Constitutional Law, Criminal Law

Appellant Ronald Turner appeals from his conviction for malice murder stemming from the stabbing death of William King. The stabbing took place outside an apartment at which Turner had driven in order to trade food for drugs. Turner testified in his own defense at trial and claimed that King hit him in the head with a beer bottle because Turner owed money to King from a prior drug transaction. Turner testified that he tried to get away from King, but that King chased him down and grabbed his jacket. According to Turner, King was getting ready to hit him again when Turner stabbed King in self-defense. Appealing his ultimate conviction, Turner contended he was denied the effective assistance of counsel in three respects. Seeing no reversible error after a review of the trial court record, the Georgia Supreme Court affirmed Turner's conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Valrie v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0380
Opinion Date: April 20, 2020
Judge: Keith R. Blackwell
Areas of Law: Constitutional Law, Criminal Law

Reuben Valrie was tried by jury and convicted of murder and other crimes in connection with the death of his infant daughter Aliyana. Valrie appealed, claiming that he was denied the effective assistance of counsel. Aliyana died as a result of closed head trauma, with a blunt-force abdominal injury as a secondary cause of death, which investigators determined was consistent with being shaken or dropped. At trial, Valrie presented the testimony of four expert witnesses who testified that Aliyana died of natural causes and that the injuries to her brain and abdomen were caused by

events such as post-mortem CPR and the “rough” handling of her body by first responders. The jury rejected this defense and found Valrie guilty of murder and the other charges. Valrie contended that his trial lawyer should have raised a hearsay objection to the admission of recorded statements that his girlfriend (and Aliyana's mother) made to police investigators (as well as the testimony of one of those investigators about some of those statements). Alternatively, Valrie argued that his lawyer should have sought the redaction of certain portions of the recorded statements that impugned his character. The Georgia Supreme Court concluded Valrie failed to present evidence that his trial counsel was deficient, or that he was prejudiced by any alleged failures. According, the Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Williams v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0241
Opinion Date: April 20, 2020
Judge: Keith R. Blackwell
Areas of Law: Constitutional Law, Criminal Law

Richard Williams, II, was tried by jury and convicted of murder in connection with the strangulation death of Cory Robinson. Williams and Robinson were involved in a sexual relationship and had been living together at an extended-stay hotel. Kelvin Spencer was a close friend of both Williams and Robinson. When Spencer met Williams at the hotel room, Williams looked angry and had scratches on his neck. Spencer saw Robinson lying on the floor in a “praying position.” Spencer did not believe Robinson was dead, and he helped Williams move clothes and other things to a U-Haul truck parked outside, in preparation for a move. Williams did not testify or present any evidence. Based on his lawyer’s opening and closing arguments, the defense theory was that Spencer killed Robinson because he was jealous of Williams’s relationship with Robinson. Williams’s sole claim on appeal was that he was denied the effective assistance of counsel when his trial lawyer failed to present as a defense that Williams accidentally killed Robinson during consensual erotic asphyxiation. He argued that his lawyer's discomfort with the topic of homosexual BDSM activity, and his own problems with the Georgia State Bar, precluded presentation of the "true"

version of events, and that Williams acceded to the lawyer's defense strategy only "through ignorance and that he did not know that a defense based on consensual erotic asphyxiation was available." Finding no reversible error, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Malave

Court: Supreme Court of Hawaii
Docket: SCWC-18-0000332
Opinion Date: April 20, 2020
Judge: Mark E. Recktenwald
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the intermediate court of appeals (ICA) affirming Defendant's conviction of sexual assault in the first degree on the complaining witness pursuant to Haw. Rev. Stat. 707-730(1)(b), holding that the ICA did not err in affirming the family court. Specifically, the Supreme Court held (1) the jury should have been instructed to determine jurisdictional facts, but the error was harmless beyond a reasonable doubt; and (2) the ICA did not err in finding that there was no rational basis in the record to support providing the jury instruction of the lesser included offense of sexual assault in the third degree.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Malave

Court: Supreme Court of Hawaii
Docket: SCWC-18-0000332
Opinion Date: April 22, 2020
Judge: Mark E. Recktenwald
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the intermediate court of appeals (ICA) affirming the judgment of the family court convicting Defendant on two counts of sexual assault in the first degree, holding that the ICA did not err in affirming the family court. At issue on appeal was the jurisdiction of the family court to try Defendant and the propriety of

instructing the jury on a lesser included offense. The ICA affirmed, concluding that the family court had subject matter jurisdiction pursuant to Haw. Rev. Stat. 571-14(a)(1) and that there was no rational basis to support an instruction of the lesser included offense of sexual assault in the third degree. The Supreme Court affirmed, holding (1) although the jury should have been instructed to determine jurisdictional facts, the error was harmless; and (2) the family court was not obligated to instruct the jury on the lesser included offense of sexual assault in the third degree.

Read Opinion Are you a lawyer? **Annotate this case**.

Idaho v. Burke

Court: Idaho Supreme Court - Criminal
Docket: 46841
Opinion Date: April 22, 2020
Judge: Moeller
Areas of Law: Constitutional Law, Criminal Law

Prior to sentencing, defendant James Burke was committed to the state mental hospital for 56 days to restore him to competency. After being evaluated and deemed competent to proceed to trial, Burke was returned to the county jail and later pleaded guilty pursuant to a plea agreement. At the conclusion of his sentencing hearing, Burke sought credit for the 56 days of time spent in court-ordered commitment. The district court denied the motion, concluding that commitment to a state mental hospital did not fall under the definition of 'incarceration' in Idaho Code section 18-309. After reviewing this issue carefully, the Idaho Supreme Court disagreed with the district court's "thorough and thoughtful analysis," holding that court-ordered commitment to state custody pursuant to Idaho Code sections 18-210 and 18-211 met the functional and legal definition of "incarceration" under Idaho Code section 18-309. "The extent of the liberty interests restricted by Burke's court-ordered commitment to State Hospital North are just too similar to imprisonment to conclude otherwise." Accordingly, the Court reversed the district court's order denying Burke's request for credit for time served and remanded the case for the district court to enter an order crediting him with the fifty-six days he spent committed to State Hospital North while the State restored his competency to face criminal charges.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Gibbs

Court: Iowa Supreme Court
Docket: 18-1298
Opinion Date: April 17, 2020
Judge: Edward M. Mansfield
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction of murder in the second degree, holding that Defendant's Fifth Amendment rights were invaded when the trial judge instructed the jury that Defendant was required to notify law enforcement of his use of deadly force, but the error was harmless. During trial, Defendant asserted the defense of justification in his shooting of the victim. At issue on appeal was whether the district court abused its discretion by giving a jury instruction incorporating the terms of Iowa Code 704.2B. The instruction included a statement that a person using deadly force is required to notify law enforcement about his use of deadly force. Defendant argued before the Supreme Court that both section 704.2B and the jury instruction incorporating that section violated his Fifth Amendment rights. The Supreme Court affirmed, holding (1) instructing the jury that a homicide defendant is required to notify a law enforcement agency of his use of deadly force violates the defendant's Fifth Amendment rights; but (2) any error in this case was harmless beyond a reasonable doubt.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Broxton

Court: Kansas Supreme Court
Docket: 114675
Opinion Date: April 17, 2020
Judge: Stegall
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's convictions for second-degree murder, burglary, and theft but reversed Defendant's sentences, holding

that any error during the guilt phase was harmless but that the district court erred by scoring Defendant's prior Florida burglary conviction as a person felony instead of a nonperson felony. On appeal, the court of appeals concluded that a trial court may instruct the jury on felony murder even though the State only charged the defendant with premeditated first degree murder. The Supreme Court disagreed, holding (1) the court of appeals erred in concluding that a district court may elect to provide a felony-murder instruction when that crime was not charged, and the district court properly found that the felony-murder instruction was not legally appropriate in this case; (2) the district court erred by excluding from evidence an exculpatory document from a Florida homicide investigation on the ground it was not relevant, but the error was harmless; and (3) the district court improperly scored Defendant's prior Florida burglary conviction as a person felony.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Corbin

Court: Kansas Supreme Court
Docket: 119665
Opinion Date: April 17, 2020
Judge: Dan Biles
Areas of Law: Criminal Law

The Supreme Court affirmed the ruling of the district court on remand resentencing Defendant to his original mandatory term of imprisonment after once again finding he was not a person with intellectual disability, holding that the district court did not abuse its discretion when it rejected Defendant's intellectual disability motion and imposed a mandatory term of imprisonment. Defendant pled no contest to first-degree premeditated murder. Before sentencing, Defendant filed a motion pursuant to Kan. Stat. Ann. 21-6622(b) asserting that he was a person with intellectual disability and was thus not subject to a mandatory minimum prison term. The district court denied the motion and sentenced Defendant to a hard twenty-five life sentence. While Defendant's appeal was pending, the Legislature amended Kan. Stat. Ann. 76-12b01(i), which provides new standards for deciding intellectual disability. The Supreme Court reversed and remanded for reconsideration of Defendant's motion using the new criteria. On remand, the district court reaffirmed its earlier ruling and again sentenced Defendant

to a hard twenty-five life sentence. The Supreme Court affirmed, holding that the district court's ruling was reasonably based on the law and was supported by substantial competent evidence.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Frazier

Court: Kansas Supreme Court
Docket: 117456
Opinion Date: April 17, 2020
Judge: Wilson
Areas of Law: Criminal Law

The Supreme Court reversed the decision of the district court affirming the judgment of the district court denying Defendant's motion to withdraw plea of no contest to one count of possession of heroin with intent to distribute, holding that the district court's decision in finding no good cause for Defendant to withdraw his plea was based on errors of fact and law, which were grounds for finding abuse of discretion. On appeal, Defendant argued that the district court abused its discretion in denying his motion to withdraw his plea of no contest based on misleading or false statements contained in the plea agreement. The court of appeals affirmed the district court. The Supreme Court reversed, holding (1) there was enough uncertainty in this case to indicate that Defendant's plea agreement was not understandingly made; and (2) therefore, Defendant must be allowed to withdraw his plea.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Harris

Court: Kansas Supreme Court
Docket: 117362
Opinion Date: April 17, 2020
Judge: Wilson
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court reversed the judgment of the court of appeals affirming Defendant's conviction of possession fo marijuana, holding that Defendant's waiver of jury trial was legally insufficient. On appeal, Defendant argued that

he did not properly waive his right to a jury and asserted three other issues. The Supreme Court reversed the judgment of the court of appeals affirming Defendant's convictions without addressing the three remaining issues, holding that because the district court failed properly to apprise Defendant of his right to a jury trial and failed to ensure that Defendant understood the nature of the right he was giving up, Defendant's constitutional right to a jury trial was violated in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Uk

Court: Kansas Supreme Court
Docket: 119712
Opinion Date: April 17, 2020
Judge: Wilson
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's conviction for first-degree premeditated murder, holding that the district court did not err in its challenged instructions to the jury. Specifically, the Supreme Court held (1) the district court did not err in refusing to give the jury Defendant's requested instruction on voluntary manslaughter as a lesser included offense of first-degree murder because the instruction was not factually appropriate; and (2) the district court did not commit clear error in issuing an unmodified version of Instruction No. 11, which contained the definition of "premeditation" and mirrored PIK Crim. 4th 54.150(d) because the instruction was legally appropriate.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Catruch

Court: Maine Supreme Judicial Court
Citation: 2020 ME 52
Opinion Date: April 23, 2020
Judge: Andrew M. Mead
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed the judgments of the trial court

terminating Appellant's participation in the Co-Occurring Disorders and Veterans Court (Veterans Court), holding that the court did not err or abuse its discretion in terminating Appellant's participation in the Veterans Court. The Veterans Court is a criminal docket that provides judicial monitoring, specialized treatment, and other services for military veterans who have disorders often attributable to their military service. Appellant was charged with leaving the scene of an accident and three other offenses. Appellant was admitted to the Veterans Court. Agreeing to sentencing outcomes in a plea agreement and entering into a bail contract, Appellant pleaded guilty to all charges against him. The court later terminated Appellant's participation in the Veterans Court, finding that Appellant had violated the conditions of his bail contract. The Supreme Judicial Court affirmed, holding (1) this matter was properly before the Court; and (2) given Appellant's failure to comply with the requirements for participation in the treatment court and his violations of the agreements, his termination from the Veterans Court was warranted.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Paquin

Court: Maine Supreme Judicial Court
Citation: 2020 ME 53
Opinion Date: April 23, 2020
Judge: Andrew M. Mead
Areas of Law: Constitutional Law, Criminal Law

In this appeal from Defendant's conviction for eleven counts of gross sexual misconduct, the Supreme Judicial Court vacated the judgment of conviction on one count, vacated the dismissal of other counts and remanded for entry of a judgment of acquittal on those counts, and affirmed in all other respects, holding that Defendant's convictions on both Counts 5 and 30 violated his double jeopardy protections and that the court erred in allowing the State to dismiss Counts 27, 28, and 29 during trial without Defendant's consent. The indictment charged Defendant with fifteen counts (Counts 1-13, 30-31) of gross sexual misconduct against the victim and sixteen counts (Counts 14-29) of gross sexual misconduct against a second alleged victim. During trial, the court granted Defendant's motion for a judgment of acquittal on Counts 10-13, and the State dismissed Counts 27-29. Defendant was

found guilty of Counts 1-9 and 30-31 and not guilty on the remaining counts. The court entered judgment in accordance with the verdict. The Supreme Judicial Court held that the trial court erred in failing to rule that the Double Jeopardy Clause barred convictions on both Counts 5 and 30 and allowing the State to dismiss Counts 27, 28, and 29 rather than entering a judgment of acquittal on those counts.

Read Opinion Are you a lawyer? **Annotate this case**.

Watson v. State

Court: Maine Supreme Judicial Court
Citation: 2020 ME 51
Opinion Date: April 21, 2020
Judge: Joseph Jabar
Areas of Law: Criminal Law

The Supreme Judicial Court vacated the judgment of the unified criminal docket denying Appellant's petition for post-conviction review, holding that Appellant was deprived of the effective assistance of counsel when his trial attorney played a video of the ten-year-old victim's interview with police and that Appellant was adversely affected. Appellant was convicted of two counts of gross sexual assault, one count of unlawful sexual contact, and one count of visual sexual aggression against a child. The Supreme Court affirmed. Appellant later filed a petition for post-conviction review claiming that his trial attorney's representation was deficient because introducing the videotaped recording of the victim's entire interview with law enforcement was unnecessary to provide evidence supporting the victim's potential motive to fabricate the allegations. The post-conviction court denied denied the petition. The Supreme Court vacated the judgment below, holding that trial counsel's conduct was deficient and that counsel's actions rose to the level of comprising the reliability of Appellant's conviction and undermining confidence in it.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. Mazza

Court: Massachusetts Supreme Judicial Court

Docket: SJC-11363
Opinion Date: April 21, 2020
Judge: Budd
Areas of Law: Criminal Law

The Supreme Judicial Court reversed the order of the superior court denying Defendant's motion for a new trial and set aside the jury's verdicts of first degree murder and robbery, holding that a recently discovered witness statement made to the police ago constituted newly discovered evidence that "would probably have been a real factor in the jury's deliberations." At issue was Defendant's sixth motion for a new trial, which was predicated on newly discovered evidence consisting of, among other things, a recently discovered statement made to the police in 1972. The superior court denied the motion. As to the police statement, the judge found that it did not constitute newly discovered evidence because Defendant failed to establish that defense counsel did not have possession of it at the time of trial. The Supreme Judicial Court reversed and remanded the case for a new trial, holding (1) Defendant sustained his burden of establishing that defense counsel did not have the 1972 police statement prior to or at trial, and therefore, the statement constituted newly discovered evidence; and (2) there was a substantial risk that the jury would have reached a different conclusion had the evidence been admitted at trial.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. McCarthy

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12750
Opinion Date: April 16, 2020
Judge: Gaziano
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Judicial Court affirmed the judgment of the district court denying Defendant's motions to suppress, holding that the limited use of automatic license plate readers (ALPRs) in this case did not implicate constitutional protections against unreasonable searches. While police were investigating Defendant on suspicion of drug distribution they used ALPRs on two bridges to track Defendant's movements. The police accessed historical data via ALPR technology and received real-time alerts, the last of

which led to Defendant's arrest. Defendant filed motions to suppress the ALPR data and the fruits of the arrest. The superior court denied the motions. The Supreme Judicial Court affirmed, holding that while the widespread use of ALPRs in the Commonwealth could implicate a defendant's constitutional protected expectation of privacy in the whole of his public movements, that interest was not invaded by the limited extent and use of the ALPR data in the instant case.

Read Opinion Are you a lawyer? **Annotate this case**.

Garden v. Commonwealth

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12821
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed the judgment of a single justice of the court denying Petitioner's petition for extraordinary relief under Mass. Gen. Laws ch. 211, 3 seeking an order vacating Petitioner's plea to aggravated rape and dismissing the underlying indictment, holding that the single justice did not err or abuse his discretion in denying relief. The issues raised by Petitioner had all been raised and adjudicated through the normal appellate process. Petitioner then filed a motion to withdraw his guilty plea. The motion was denied, and the Appeals Court affirmed. In this petition for extraordinary relief, Petitioner sought an order vacating his plea to aggravated rape and dismissing the underlying indictment. The single justice denied relief. The Supreme Judicial Court affirmed, holding that the superintendence power was not available as an additional layer of appellate review once all other avenues had been exhausted.

Read Opinion Are you a lawyer? **Annotate this case**.

In re Mitchell

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12910
Opinion Date: April 22, 2020

Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed the judgment of the county court denying, without a hearing, Petitioner's petition for relief under Mass. Gen. Laws ch. 211, 3, holding that the single justice did not err or abuse his discretion in denying relief. Defendant was convicted of several offenses. The Appeals Court reversed the convictions and remanded the matter for a new trial. Thereafter, the Commonwealth filed a nolle prosequi as to all the charges. In his Mass. Gen. Laws ch. 211, 3 petition, Defendant alleged that no crime had been committed and that he was wrongfully prosecuted. The single justice denied relief. The Supreme Judicial Court affirmed, holding that Defendant did not demonstrate entitlement to the exercise of this Court's superintendence powers.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Reek

Court: Minnesota Supreme Court
Docket: A19-0153
Opinion Date: April 22, 2020
Judge: G. Barry Anderson
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction for first-degree murder, holding that there was no error in the proceedings below. Specifically, the Supreme Court held (1) Appellant's right to a fair trial before an impartial tribunal was not violated when the district court stated that it might reconsider its prior Spreigl ruling if the defense presented certain witnesses; (2) the jury instructions on accomplice liability were plainly erroneous, but Appellant failed to establish that there was a reasonable likelihood that the error had a significant effect on the verdict; (3) the prosecutor did not commit misconduct in his closing arguments regarding the law of accomplice liability; (4) the district court did not abuse its discretion by granting the State’s motion to admit evidence of appellant’s past convictions for impeachment purposes, including by allowing the specific convictions to be disclosed to the jury; and (5) Appellant’s pro se arguments were without merit.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Woodard

Court: Minnesota Supreme Court
Docket: A18-1886
Opinion Date: April 22, 2020
Judge: Hudson
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the district court convicting Defendant of first-degree murder and sentencing him to life in prison without the possibility of release, holding that the district court did not err in denying Defendant's motion to present an alternative-perpetrator defense. Specifically, the Supreme Court held (1) the district court did not abuse its discretion in holding that Defendant's proffered evidence in support of his motion to present alternative-perpetrator evidence for lack of sufficient foundation; and (2) the district court committed an error that was plain in instructing the jury on the order in which to consider the charges against Defendant, but there was no reasonable likelihood that the instruction affected the jury's verdict and therefore did not affect Defendant's substantial rights.

Read Opinion Are you a lawyer? **Annotate this case**.

Huff v. Brown

Court: Nebraska Supreme Court
Citation: 305 Neb. 648
Opinion Date: April 23, 2020
Judge: Lindsey Miller-Lerman
Areas of Law: Communications Law, Criminal Law

The Supreme Court reversed the portion of the district court's order granting in part a writ of mandamus requiring Doug Brown, the sheriff of Furnas County, to provide records to Herchel Huff pursuant to the public records statutes, holding that the district court erred when it determined that Huff had shown that Brown had a clear duty to provide the requested records. Huff, an inmate, sought, among other documents, the criminal history

records of jurors who had convicted hims. Furnas County sheriff Kurt Kapperman required a deposit of $750 before fulfilling the request. Huff subsequently filed a petition for writ of mandamus naming Kapperman as the defendant and seeking an order compelling Kapperman to release all requested documents. The court permitted Huff to substitute Brown, the current sheriff, in the caption of the case in place of Kapperman and granted in part mandamus. The Supreme Court reversed in part, holding that the district court (1) did not err when it substituted Brown's name for Kapperman's; but (2) erred in issuing mandamus because Huff failed to demonstrate a prima facie case that he had been denied a request for public records that the sheriff had a clear duty to provide under Neb. Rev. Stat. 84-712.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Montoya

Court: Nebraska Supreme Court
Citation: 305 Neb. 581
Opinion Date: April 17, 2020
Judge: Freudenberg
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the judgment of the district court affirming Defendant's conviction and sentence for driving under the influence, holding that there was no error in the challenged rulings by the trial court. Specifically, the Supreme Court held that the district court did not err by (1) affirming the county court's order denying Defendant's motion to suppress fruits of the stop; (2) affirming the county court's order that denied Defendant's motion to suppress the fruits of his arrest; (3) affirming the county court's order that denied Defendant's motion to suppress the results of the test of his breath alcohol content; (4) finding sufficient evidence to support the conviction; and (5) finding that Defendant's sentence was not excessive.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Schroeder

Court: Nebraska Supreme Court
Citation: 305 Neb. 527
Opinion Date: April 17, 2020
Judge: Funke
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's sentence of death for first degree murder, holding that there was no error in the sentence imposed by the sentencing panel. Specifically, the Supreme Court held that the sentencing panel did not err in (1) allowing the State to introduce evidence on the existence of mitigating circumstances; (2) acknowledging and weighing mitigating evidence from the presentence investigation report; (3) not requesting that documentation from the Department of Correctional Services regarding Defendant's time in custody for mitigation purposes be included in the presentence investigation report; (4) sentencing Defendant to death, where the Legislature has enacted safeguards to ensure fairness and accuracy in the resulting sentence; and (5) finding Defendant should be sentenced to death after balancing the aggravating evidence and mitigating evidence.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Kendrick v. Parker

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1509
Opinion Date: April 21, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals denying Appellant's request for a writ of prohibition and/or mandamus against Montgomery County Court of Common Pleas Judge E. Gerald Parker Jr., holding that the court of appeals correctly determined that Appellant's claim was barred by res judicata. Appellant sought a petition for writ of prohibition and/or mandamus against Judge Erik Blaine, the successor to the judge who sentenced Appellant, alleging that the sentencing court patently and unambiguously lacked jurisdiction to sentence him. Judge Parker, who had succeeded Judge Blaine, subsequently filed a motion for summary judgment. The court of appeals granted summary judgment for Judge

Parker, concluding that Appellant failed to demonstrate that the sentencing court patently and unambiguously lacked jurisdiction or that he lacked an adequate remedy at law and that res judicata barred Appellant's claim. The Supreme Court affirmed, holding that Appellant's claim was barred by res judicata.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Nelson v. Russo

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1541
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals dismissing Appellant's petition for a writ of mandamus seeking to compel Cuyahoga County Court of Common Pleas Judge Nancy Margaret Russo to vacate the consecutive prison sentences imposed on Appellant in 1987, holding that Appellant had an adequate remedy at law and was barred from asserting additional claims of sentencing error he could have raised in his previous mandamus action. In 1987, Appellant was convicted of four counts of rape and one count of kidnapping. Appellant was sentenced to prison terms of fifteen to twenty-five years for each of the five counts, to be served consecutively. In 2019, Appellant sought a writ of mandamus to compel Judge Russo to vacate his consecutive sentences. The court of appeals dismissed the writ action, concluding that res judicata barred Appellant's claim and that his prior appeals were an adequate remedy at law to address the alleged defect in his consecutive sentences. The Supreme Court affirmed, holding that Appellant was not entitled to a writ of mandamus in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Roberts v. Marsh

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1540

Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals dismissing Appellant's original action seeking a writ of procedendo and/or mandamus to compel Hamilton County Court of Common Pleas Judge Melba Marsh to issue a corrected sentencing entry, holding that the court of appeals correctly dismissed the petition as moot. Appellant was convicted of murder with a repeat-violent-offender specification. Appellant later asked the trial court to correct his sentence, arguing that he had improperly been sentenced to postrelease control. On remand, Judge Marsh vacated the postrelease-control sentence. Appellant appealed that order. The court of appeals noted that the trial court had not set forth all the information required under Crim.R. 32(C) in a single document and dismissed the appeal for lack of a final, appealable order. Appellant then filed this original action seeking to compel Judge Marsh to issue a corrected sentencing entry that constitutes a final, appealable order. Judge Marsh issued a nunc pro tunc sentencing entry that constituted a final, appealable order. The court of appeals then dismissed the petition as moot. The Supreme Court affirmed, holding that because Judge Marsh performed the act Appellant requested, the court of appeals dismissed the petition as moot.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Steiner v. Rinfret

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1510
Opinion Date: April 21, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals dismissing Appellant's petition for a writ of mandamus against Holmes County Court of Common Pleas Judge Robert D. Rinfret, holding that the court of appeals correctly determined that Appellant had an adequate remedy in the ordinary course of the law. Appellant, who was serving consecutive prison terms for five convictions, filed a petition for a writ of mandamus arguing that Judge Rinfret improperly sentenced him to a prison

term of nine years for his attempted rape conviction instead of the maximum term of eleven years. The court of appeals dismissed the petition, determining that Appellant had failed to file a mandatory affidavit of his prior civil actions and had an adequate remedy in the ordinary course of the law. The Supreme Court affirmed, holding that relief in mandamus was not available because Petitioner had an adequate remedy in the ordinary course of the law.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Jeffries

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1539
Opinion Date: April 22, 2020
Judge: Donnelly
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals upholding Defendant's convictions of four counts related to two specific instances of sexual abuse of D.S., holding that the trial court and court of appeals correctly applied Ohio's rape-shield law and determined that evidence of D.S.'s prior nonconsensual sexual assault was inadmissible. On appeal, Defendant asserted that the trial court erred in prohibiting him from introducing evidence during trial that D.S. had previously been sexually assaulted by another person, arguing that the rape-shield law applies only to an accuser's prior consensual sexual activity. The lower court held that Ohio's rape-shield law addresses all sexual activity, not only consensual sexual activity. The court of appeals affirmed. The Supreme Court affirmed, holding (1) the plain meaning of the term "sexual activity" as used in the rape-shield law includes both consensual and nonconsensual sexual activity; and (2) therefore, all sexual activity is barred from admission into evidence by the rape-shield, absent certain exceptions listed in the law.

Read Opinion Are you a lawyer? **Annotate this case**.

Pennsylvania v. Britton

Court: Supreme Court of Pennsylvania

Docket: 55 MAP 2018
Opinion Date: April 22, 2020
Judge: Max Baer
Areas of Law: Constitutional Law, Criminal Law

California law enforcement officers interviewed Appellant Stacy Britton in her California residence and, unbeknownst to her, recorded those interviews. Over Appellant's objection, Pennsylvania used those recordings as evidence to help convict Appellant of murder in Pennsylvania. The Pennsylvania Supreme Court granted allowance of appeal to examine whether the California law enforcement officers were acting as agents of the Pennsylvania State Police when they recorded the interviews with Appellant in her California home, and if so, whether Pennsylvania's constitutional and statutory protections were available to Appellant under those circumstances. The Court concluded the California law enforcement officers were not acting as agents of the Pennsylvania State Police when they interviewed Appellant, making analysis of whether any Pennsylvania-specific constitutional or statutory protections unwarranted. Because the Supreme Court concluded the Pennsylvania trial court reached the proper result in this matter, it affirmed that court's judgment.

Read Opinion Are you a lawyer? **Annotate this case**.

Pennsylvania v. Copenhaver

Court: Supreme Court of Pennsylvania
Docket: 48 MAP 2019
Opinion Date: April 22, 2020
Judge: Thomas G. Saylor
Areas of Law: Constitutional Law, Criminal Law

In August 2015, a deputy sheriff conducted a vehicle stop of Appellant Victor Copenhaver's pickup truck. Upon approaching the truck, the deputy noticed an odor of alcohol and marijuana emanating from the passenger compartment. After administering field sobriety tests, he arrested Appellant for suspected driving under the influence of alcohol and controlled substances ("DUI"). Appellant was ultimately charged with DUI and other offenses. Appellant challenged the deputy's authority to conduct a traffic stop and sought suppression of all evidence obtained during the encounter. Rather than presenting testimony at a suppression hearing, the parties

stipulated that Appellant was driving the vehicle in question and that the deputy had training and qualifications equivalent to that of a police officer. The parties also agreed that the vehicle stop occurred as a result of the deputy observing the tailgate to the pickup truck being in a down position, which caught the deputy's attention. The deputy further observed the registration on the pickup truck was expired, and additionally, the registration number was identified as belonging to a vehicle other than the one on which it was attached. The issue this case presented for the Pennsylvania Supreme Court's review was whether the deputy could lawfully conduct the traffic stop based on the expired registration sticker, on a theory that such a violation amounts to a breach of the peace. The Supreme Court concluded driving a vehicle with an expired registration did not entail a breach of the peace. It vacated the superior court's order insofar as it held that the expired registration was a breach of the peace, thus alone authorizing the deputy to stop Appellant's vehicle. Notably, in light of its holding, the Supreme Court found the superior court did not proceed to consider other relevant questions, such as whether the parties' factual stipulation should have been read as indicating that the officer's understanding that the registration sticker was associated with a different vehicle arose in the pre-stop timeframe – consistent with the Commonwealth's position throughout this litigation. "These issues should be resolved in the first instance by the intermediate court on remand."

Read Opinion Are you a lawyer? **Annotate this case**.

Pennsylvania v. Tedford

Court: Supreme Court of Pennsylvania
Docket: 773 CAP
Opinion Date: April 22, 2020
Judge: Donohue
Areas of Law: Constitutional Law, Criminal Law

Appellant Donald Tedford was convicted of first-degree murder and rape on February 6, 1987. He appealed the dismissal of his second petition for relief filed pursuant to the Post Conviction Relief Act ("PCRA"), on December 2, 2014, as amended by a counseled petition on May 5, 2015, and a supplemental petition filed on June 9, 2015. In connection with his initial filings, Tedford sought wholesale discovery of the prosecution's entire file,

but the PCRA court concluded that the petition (as amended) was not timely filed. Tedford also appealed the PCRA court's order denying his supplemental PCRA petition, in which he requested discovery, an evidentiary hearing, and/or a new trial based upon the admission of expert testimony presented at trial related to microscopic hair analysis. The PCRA court concluded that pursuant to PCRA Section 9545(b)(1)(ii), it had jurisdiction to consider the merits of Tedford's newly-discovered-facts claims, but ultimately it concluded Tedford had not asserted a meritorious claim in accordance with Section 9543(a)(2)(vi). Finding no reversible error in that analysis, the Pennsylvania Supreme Court affirmed dismissal of the petition for relief.

Read Opinion Are you a lawyer? **Annotate this case**.

Pennsylvania v. Trahey

Court: Supreme Court of Pennsylvania
Docket: 38 EAP 2018
Opinion Date: April 22, 2020
Judge: Wecht
Areas of Law: Constitutional Law, Criminal Law

The trial court granted Timothy Trahey's motion to suppress the results of a blood test that revealed his blood alcohol concentration ("BAC"), finding no justification for the investigating officers' failure to obtain a search warrant before conducting the test. On the Commonwealth's appeal, the Superior Court reversed, opining that the Commonwealth's evidence sufficiently established the existence of exigent circumstances, thus excusing the absence of a warrant. The Pennsylvania Supreme Court reversed, finding that while the exigency analysis is an objective one, "even disregarding the officers' subjective motivations, or their candid acknowledgment that they would have obtained a search warrant if they thought it necessary, there was no time-sensitive need to conduct a warrantless blood test under the circumstances of this case. Accordingly, the Superior Court's conclusion that the test was justified by exigent circumstances was drawn in error."

Read Opinion Are you a lawyer? **Annotate this case**.

In re Greg Abbott

Court: Supreme Court of Texas
Docket: 20-0291
Opinion Date: April 23, 2020
Judge: Per Curiam
Areas of Law: Constitutional Law, Criminal Law

The Supreme Court conditionally granted mandamus relief to the State seeking review of a temporary restraining order (TRO) blocking enforcement of Executive Order GA-13, which changes the rules applicable to judges' decisions regarding pre-trial bail, against judges, holding that the trial court lacked jurisdiction to order the judges' requested relief, even temporarily. GA-13 suspends certain statutes authorizing trial judges to release jail inmates with violent histories during the state of disaster due to the threat of the novel coronavirus. Plaintiffs alleged that GA-13 is unconstitutional and exceeds the governor's statutory emergency powers. Sixteen of the plaintiffs were Texas trial judges alleging that GA-13 improperly interferes with their judicial authority to make individualized bail decisions, and the other plaintiffs were public interest organizations and lawyer associations. The trial court issued a TRO blocking enforcement of GA-13 against judges. The Supreme Court conditionally granted mandamus relief, holding that the alleged threat of a criminal prosecution in this case did not give the judges standing to seek the invalidation of GA-13, and therefore, the trial court lacked jurisdiction to order their requested relief.

Read Opinion Are you a lawyer? **Annotate this case**.

Stahmann v. Texas

Court: Texas Court of Criminal Appeals
Docket: PD-0556-18
Opinion Date: April 22, 2020
Judge: Barbara Hervey
Areas of Law: Constitutional Law, Criminal Law

Appellant Karl Stahmann was involved in an automobile accident, after which he threw a bottle of promethazine, a controlled substance, over a nearby wire fence before law enforcement arrived. The bottle landed two to three feet past the fence in plain view. He was convicted of third-degree

felony tampering with physical evidence and was sentenced to 10 years' confinement and fined $5,000. The judge suspended his sentence and placed him on community supervision for 10 years. Stahmann appealed, arguing in part that the evidence was insufficient to prove that he destroyed, altered, or concealed the prescription bottle. The court of appeals agreed that the evidence was insufficient, but instead of rendering an acquittal, it reformed the judgment to show that Stahmann was convicted of the lesser-included offense of attempted tampering with physical evidence, a state-jail felony. After review of the evidence presented at trial, the Texas Court of Criminal Appeals concluded the evidence was indeed insufficient to prove that Appellant altered the prescription pill bottle when he threw it over the fence because the mere act of throwing the bottle did not change the bottle itself. "While a rational jury could have reasonably inferred that Stahmann intended to conceal the pill bottle when he threw it over the wire fence, the evidence shows that he failed to conceal it as he intended because the bottle landed short of the bush in plain view on top of some grass." The Court affirmed the trial court's judgment.

Read Opinion Are you a lawyer? **Annotate this case**.

Blanke v. Board of Pardons & Parole

Court: Utah Supreme Court
Citation: 2020 UT 16
Opinion Date: April 16, 2020
Judge: Himonas
Areas of Law: Criminal Law

The Supreme Court affirmed the decision of the court of appeals affirming the district court's denial of Appellant's petition for extraordinary relief, holding that, under the circumstances, the Utah Board of Pardons and Parole need not afford Appellant the due process protections explained in Neese v. Utah Board of Pardons and Parole, 416 P.3d 663 (2017), before it could determine that Appellant was a sex offender and condition his parole on sex offender treatment. Appellant was serving a prison sentence for his convictions of attempted child kidnapping and kidnapping. Because he was convicted of attempted child kidnapping Appellant was considered a sex offender under the sex offender registration statute. Further, Appellant admitted in his presentence report that he had sexual intercourse with a

fifteen-year-old. Appellant filed a petition for extraordinary relief alleging that the Parole Board had violated his due process rights by conditioning his parole on completion of sex offender treatment even though he had not committed a sex offense. Summary judgment was granted for the Parole Board. The Supreme Court affirmed, holding that the Parole Board owed Appellant no additional process before it considered unconnected sex offenses in its decision to require Appellant to undergo sex offender treatment.

Read Opinion Are you a lawyer? **Annotate this case**.

Washington v. Escalante

Court: Washington Supreme Court
Docket: 97268-1
Opinion Date: April 23, 2020
Judge: Steven González
Areas of Law: Constitutional Law, Criminal Law

Alejandro Escalante was detained for hours in a secured area at a border crossing and, the State conceded, interrogated by federal agents without Miranda warnings. Statements he made during that interrogation were used by the State to convict him of drug possession. While a traveler briefly detained and questioned at the border was typically not "in custody" for Miranda purposes, "the government's power to detain and question people at the border without implicating Miranda has limits." Here, the Washington Supreme Court determined those limits were reached. "This border detention created the type of inherently coercive environment that demands Miranda warnings to ensure an individual's choice to speak is the product of free will." The Supreme Court held that Escalante was in custody when he was interrogated and reversed.

Read Opinion Are you a lawyer? **Annotate this case**.

Washington v. Haggard

Court: Washington Supreme Court
Docket: 97375-0
Opinion Date: April 23, 2020

Judge: Barbara Madsen
Areas of Law: Constitutional Law, Criminal Law

A class C felony "washes out" and is omitted from a defendant's offender score as long as he or she is not convicted of any crime within five years of the last date of release from confinement. David Haggard was convicted of a misdemeanor offense within this five-year period, which was dismissed pursuant to RCW 3.66.067. When Haggard later pleaded guilty to burglary and arson, the trial court included prior class C felonies in his criminal history, finding that the dismissed misdemeanor conviction interrupted the washout period for those offenses. Haggard contended on appeal this was error. The Washington Supreme Court determined that because a dismissed conviction constituted a "conviction" under the Sentencing Reform Act of 1981 (SRA), and misdemeanor dismissal and vacation were distinct processes, so Haggard's offender score was properly calculated.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Taylor

Court: Supreme Court of Appeals of West Virginia
Docket: 18-0502
Opinion Date: April 21, 2020
Judge: Walker
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the judgment of the circuit court giving Petitioner credit for twelve days of time served toward the sentence he received for his felony conviction although Petitioner spent additional time in confinement for other charges that were dismissed in the universal plea agreement, holding that to grant Petitioner additional credit for time served would do little more than reward Petitioner for habitual criminal behavior. Petitioner was charged with several crimes and agreed to resolve the pending charges against him in a universal plea agreement. Under the terms of the agreement, Petitioner agreed to plea guilty to the charge of felony carrying a concealed firearm by a prohibited person. In exchange, the State agreed to drop the remaining charges. After he was sentenced, Petitioner argued that, in addition to the twelve days of credit for time served he was granted, he was constitutionally entitled to credit for time served

while he was incarcerated for charges that were resolved in the universal plea agreement. The Supreme Court affirmed, holding that Petitioner's circumstances implicated neither double jeopardy nor equal protection of the law such that additional credit for time served was constitutionally mandated.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Harrison

Court: Wisconsin Supreme Court
Dockets: 2017AP002441-CR, 2017AP002440-CR
Opinion Date: April 17, 2020
Judge: Patience D. Roggensack
Areas of Law: Criminal Law

The Supreme Court affirmed in part and reversed in part the decision of the court of appeals reversing an order of the circuit court that granted sentence credit to Defendant, holding that the court of appeals correctly found that Defendant was not entitled to sentence credit but erred by advancing the commencement of Defendant's terms of extended supervision for Defendant's 2007 and 2008 cases. Specifically, the Court held (1) Defendant was not entitled to sentence credit under Wis. Stat. 973.155(1)(a) because the days he spent in custody for which he sought sentence credit were not in connection with the courses of conduct for which those sentences were imposed; and (2) the court of appeals erred by advancing the commencement of Defendant's terms of extended supervision for his 2007 and 2008 cases to the date they would have begun but for Defendant's confinement for unrelated convictions that were later set aside, holding that whether to employ advancement is a public policy decision best left to the legislature.

Read Opinion Are you a lawyer? **Annotate this case**.

About Justia Opinion Summaries

Justia Weekly Opinion Summaries is a free service, with 63 different

newsletters, each covering a different practice area.

Justia also provides 68 daily jurisdictional newsletters, covering every federal appellate court and the highest courts of all US states.

All daily and weekly Justia newsletters are free. Subscribe or modify your newsletter subscription preferences at daily.justia.com.

You may freely redistribute this email in whole.

About Justia

Justia is an online platform that provides the community with open access to the law, legal information, and lawyers.

Contact Us | Privacy Policy

Unsubscribe From This Newsletter
or unsubscribe from all Justia newsletters immediately **here.**

Justia | 1380 Pear Ave #2B, Mountain View, CA 94043

From: Criminal Law - Justia Weekly Opinion Summaries
To: Kennedy, Kevin (POL)
Subject: Latest 101 Cases This Week: Ramos v. Louisiana (U.S.), United States v. Diaz-Rivera (1st Cir.), United States v. Cotto (2d Cir.)
Date: Friday, April 24, 2020 9:08:32 AM

If you are unable to see this message, click here to view it in a web browser.

Justia Weekly Opinion Summaries

Criminal Law
April 24, 2020

Table of Contents

Ramos v. Louisiana
Civil Rights, Constitutional Law, Criminal Law
US Supreme Court

United States v. Diaz-Rivera
Criminal Law

US Court of Appeals for the First Circuit

United States v. Cotto
Criminal Law
US Court of Appeals for the Second Circuit

United States v. Rosa
Criminal Law
US Court of Appeals for the Second Circuit

Fogle v. Sokol
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Third Circuit

James v. New Jersey State Police
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Third Circuit

Bazemore v. Best Buy
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Akande
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Chambers
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Ferebee
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Nance
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Johnson
Criminal Law
US Court of Appeals for the Fifth Circuit

United States v. McGinnis
Criminal Law
US Court of Appeals for the Fifth Circuit

Valentine v. Collier
Civil Rights, Constitutional Law, Criminal Law, Government & Administrative Law, Health Law
US Court of Appeals for the Fifth Circuit

United States v. Dowl
Criminal Law

US Court of Appeals for the Sixth Circuit

United States v. Fowler
Criminal Law
US Court of Appeals for the Sixth Circuit

United States v. Sumlin
Criminal Law
US Court of Appeals for the Sixth Circuit

United States v. Vance
Criminal Law, White Collar Crime
US Court of Appeals for the Sixth Circuit

Winburn v. Nagy
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Sixth Circuit

Lund v. City of Rockford
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

United States v. Perez
Criminal Law
US Court of Appeals for the Seventh Circuit

Jackson v. United States
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Bolman
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Boyd
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Gonzalez-Esparsa
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Sanchez-Velasco
Criminal Law, Immigration Law
US Court of Appeals for the Eighth Circuit

Anthony v. TRAX International Corp.
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Ninth Circuit

City of Almaty v. Khrapunov
Criminal Law, International Law, White Collar Crime

US Court of Appeals for the Ninth Circuit

United States v. Baldon
Criminal Law
US Court of Appeals for the Ninth Circuit

United States v. Costanzo
Criminal Law
US Court of Appeals for the Ninth Circuit

United States v. Manzanares
Constitutional Law, Criminal Law
US Court of Appeals for the Tenth Circuit

United States v. Delaney
Criminal Law
US Court of Appeals for the District of Columbia Circuit

Antenor v. Alaska, Department of Corrections
Civil Procedure, Criminal Law, Government & Administrative Law
Alaska Supreme Court

Berger v. Bryant
Criminal Law
Arkansas Supreme Court

Carroll v. State
Criminal Law
Arkansas Supreme Court

Cave v. State
Civil Rights, Constitutional Law, Criminal Law
Arkansas Supreme Court

Chatmon v. Kelley
Criminal Law
Arkansas Supreme Court

McClinton v. State
Criminal Law
Arkansas Supreme Court

Siegel v. State
Criminal Law
Arkansas Supreme Court

Thomas v. State
Civil Rights, Constitutional Law, Criminal Law
Arkansas Supreme Court

California v. Landowski
Constitutional Law, Criminal Law

California Courts of Appeal

California v. May
Constitutional Law, Criminal Law
California Courts of Appeal

California v. Perez
Constitutional Law, Criminal Law
California Courts of Appeal

In re S.R.
Criminal Law
California Courts of Appeal

People v. Bell
Criminal Law
California Courts of Appeal

People v. Drayton
Criminal Law
California Courts of Appeal

People v. Robinson
Criminal Law
California Courts of Appeal

People v. Torres
Criminal Law
California Courts of Appeal

Colorado v. Lujan
Constitutional Law, Criminal Law
Colorado Supreme Court

Archer v. State
Civil Rights, Constitutional Law, Criminal Law
Florida Supreme Court

Collins v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Heyward v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Howard v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Keller v. Georgia
Constitutional Law, Criminal Law

Supreme Court of Georgia

Mills v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Moore v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Morris v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Rickman v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Robinson v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Santana v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Sullivan v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Turner v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Valrie v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Williams v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

State v. Malave
Criminal Law
Supreme Court of Hawaii

State v. Malave
Criminal Law
Supreme Court of Hawaii

Idaho v. Burke
Constitutional Law, Criminal Law

Idaho Supreme Court - Criminal

State v. Gibbs
Civil Rights, Constitutional Law, Criminal Law
Iowa Supreme Court

State v. Broxton
Criminal Law
Kansas Supreme Court

State v. Corbin
Criminal Law
Kansas Supreme Court

State v. Frazier
Criminal Law
Kansas Supreme Court

State v. Harris
Civil Rights, Constitutional Law, Criminal Law
Kansas Supreme Court

State v. Uk
Criminal Law
Kansas Supreme Court

State v. Catruch
Criminal Law
Maine Supreme Judicial Court

State v. Paquin
Constitutional Law, Criminal Law
Maine Supreme Judicial Court

Watson v. State
Criminal Law
Maine Supreme Judicial Court

Commonwealth v. Mazza
Criminal Law
Massachusetts Supreme Judicial Court

Commonwealth v. McCarthy
Civil Rights, Constitutional Law, Criminal Law
Massachusetts Supreme Judicial Court

Garden v. Commonwealth
Criminal Law
Massachusetts Supreme Judicial Court

In re Mitchell
Criminal Law

Massachusetts Supreme Judicial Court

State v. Reek
Civil Rights, Constitutional Law, Criminal Law
Minnesota Supreme Court

State v. Woodard
Criminal Law
Minnesota Supreme Court

Huff v. Brown
Communications Law, Criminal Law
Nebraska Supreme Court

State v. Montoya
Civil Rights, Constitutional Law, Criminal Law
Nebraska Supreme Court

State v. Schroeder
Criminal Law
Nebraska Supreme Court

State ex rel. Kendrick v. Parker
Criminal Law
Supreme Court of Ohio

State ex rel. Nelson v. Russo
Criminal Law
Supreme Court of Ohio

State ex rel. Roberts v. Marsh
Criminal Law
Supreme Court of Ohio

State ex rel. Steiner v. Rinfret
Criminal Law
Supreme Court of Ohio

State v. Jeffries
Criminal Law
Supreme Court of Ohio

Pennsylvania v. Britton
Constitutional Law, Criminal Law
Supreme Court of Pennsylvania

Pennsylvania v. Copenhaver
Constitutional Law, Criminal Law
Supreme Court of Pennsylvania

Pennsylvania v. Tedford
Constitutional Law, Criminal Law

Supreme Court of Pennsylvania

Pennsylvania v. Trahey
Constitutional Law, Criminal Law
Supreme Court of Pennsylvania

In re Greg Abbott
Constitutional Law, Criminal Law
Supreme Court of Texas

Stahmann v. Texas
Constitutional Law, Criminal Law
Texas Court of Criminal Appeals

Blanke v. Board of Pardons & Parole
Criminal Law
Utah Supreme Court

Washington v. Escalante
Constitutional Law, Criminal Law
Washington Supreme Court

Washington v. Haggard
Constitutional Law, Criminal Law
Washington Supreme Court

State v. Taylor
Civil Rights, Constitutional Law, Criminal Law
Supreme Court of Appeals of West Virginia

State v. Harrison
Criminal Law
Wisconsin Supreme Court

COVID-19 Updates: Law & Legal Resources Related to Coronavirus

Click here to include Verdict article summaries with your newsletter(s).

Criminal Law Opinions

Ramos v. Louisiana

Court: US Supreme Court
Docket: 18-5924
Opinion Date: April 20, 2020
Judge: Neil M. Gorsuch
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

In 48 states and in federal court, a single juror's vote to acquit is enough to

prevent a conviction; Louisiana and Oregon punish people based on 10-to-2 verdicts. Ramos was convicted in a Louisiana court by a 10-to-2 jury verdict and was sentenced to life without parole. The Supreme Court reversed. The Sixth Amendment right to a jury trial, as incorporated against the states by the Fourteenth Amendment, requires a unanimous verdict to convict a defendant of a serious offense. Juror unanimity is a vital common law right. The Court rejected an "invitation" to "perform a cost-benefit analysis on the historic features of common law jury trials and to conclude that unanimity does not make the cut." In overturning its 1972 "Apodaca" decision, the Court stated that the reasoning, in that case, was "gravely mistaken" and "sits uneasily with 120 years of preceding case law." The fact that Louisiana and Oregon may need to retry defendants convicted of felonies by non-unanimous verdicts whose cases are still pending on direct appeal "will surely impose a cost, but new rules of criminal procedure usually do."

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Diaz-Rivera

Court: US Court of Appeals for the First Circuit
Docket: 18-1461
Opinion Date: April 20, 2020
Judge: Torruella
Areas of Law: Criminal Law

The First Circuit affirmed Defendant's upwardly variant sentence for one count of possession with intent to distribute cocaine and one count of using a firearm during and in relation to a drug-trafficking crime, holding that the sentence was neither procedurally nor substantively unreasonable. Pursuant to a plea agreement, Defendant pled guilty to drug-related crimes. After a sentencing hearing, the district court sentenced Defendant to an upwardly variant sentence of 180 months of imprisonment, thus declining to impose the government's requested sentence. On appeal, Defendant challenged both the procedural and substantive reasonableness of his sentence. The First Circuit affirmed, holding that the 180-month sentence was neither procedurally nor substantively unreasonable.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Cotto

Court: US Court of Appeals for the Second Circuit
Docket: 18-2970
Opinion Date: April 20, 2020
Judge: Leval
Areas of Law: Criminal Law

A conviction for retaliating against a witness in violation of 18 U.S.C. 1513 does not require that the Government prove that defendant had knowledge of the federal nature of the proceeding. The Second Circuit rejected defendant's arguments to the contrary and affirmed his conviction for retaliating against a witness. The court remanded for revision of the provision of the sentence relating to the substance abuse treatment condition of supervised release; instructed the district court to consider on remand whether the court's forthcoming order in United States v. Traficante, No. 18-1962 (2d Cir., submitted Oct. 25, 2019) requires modification of the risk notification provision of supervised release; and granted the parties leave to reinstate this appeal to permit review of the district court's decision on remand as to the risk notification provision.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Rosa

Court: US Court of Appeals for the Second Circuit
Docket: 17-2004
Opinion Date: April 17, 2020
Judge: Nardini
Areas of Law: Criminal Law

Where a district court offers no explanation for its sentence, and where neither the adopted presentence report nor the statement of reasons adequately demonstrates the court's reasoning, the court has committed plain error in violation of 18 U.S.C. 3553(c). The Second Circuit vacated defendant's sentence for conspiracy to commit wire fraud and aggravated identity theft. The court held that the district court failed to state its reasons for sentencing defendant as required under section 3553(c); the error is clear or obvious; and the error affected defendant's substantial rights. Accordingly, the court remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

Fogle v. Sokol

Court: US Court of Appeals for the Third Circuit
Docket: 19-1066
Opinion Date: April 21, 2020
Judge: Matey
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

In 1976, the body of 15-year-old “Kathy” was found near her Indiana County, Pennsylvania home. Kathy’s death involved a brutal assault, rape, and a gunshot to the head. Kathy's sisters, ages nine and 12, stated that she had gotten into a car with a man with blue eyes, black hair that came below his ears and curled at the ends, sideburns, heavy eyebrows, and a heavy mustache. Fogle had “straight reddish-blonde hair that dropped down his back and a matching, full beard that reached his waist.” After three years, Fogle became a suspect because a psychiatric patient described seeing Kathy get in a car with Fogle and his brother. The story was largely inconsistent with statements by Kathy’s sisters. Jailhouse informants were recruited and counseled by law enforcement with promises of leniency. The prosecutors “either knew about, encouraged, or permitted” this strategy. A jury found Fogle guilty of second-degree murder. In 2015, Fogle obtained DNA evidence excluding both himself and his brother as the source of semen collected from Kathy. His conviction was vacated. The Commonwealth declined to pursue new charges, describing the case as lacking “prosecutorial merit.” Fogle, having spent three decades in prison, sued the prosecutors and Indiana County under 42 U.S.C. 1983. The Third Circuit affirmed the denial of their motions to dismiss based on absolute immunity. Only truly prosecutorial functions, not investigative conduct, justify complete protection from suit. Fogle’s complaint alleges actions that fall outside the narrow doctrine of absolute immunity.

Read Opinion Are you a lawyer? **Annotate this case**.

James v. New Jersey State Police

Court: US Court of Appeals for the Third Circuit

Docket: 18-1432
Opinion Date: April 21, 2020
Judge: Porter
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Stephens called 911 and reported that Gibbons hit her and had a gun in his truck. The police responded. Stephens obtained a temporary restraining order, prohibiting Gibbons from possessing firearms and from returning to Stephens's house. The next day, Gibbons went to Stephens's house. Stephens was talking on the phone; the friend called the police. Gibbons left Stephens's house. Trooper Conza arrived. Stephens stated that Gibbons had waved a gun throughout their argument. Conza told Stephens to go to the police barracks and reported over the radio that Gibbons had brandished a firearm. Conza, with Troopers Bartelt and Korejko, visited the nearby home of Gibbons's mother, James. James stated that she did not know where Gibbons was and that he might be off his schizophrenia medication. While driving to the barracks, Stephens saw Gibbons walking alongside the road and called 911. The Troopers responded. Bartelt parked his car and, exiting, observed that Gibbons was pointing a gun at his own head. Bartelt drew his weapon, stood behind his car door, and twice told Gibbons to drop his weapon. Gibbons did not comply. Bartelt shot Gibbons twice within seconds of stopping his car. Gibbons died that night. In James' suit under 42 U.S.C. 1983, the Third Circuit held that Bartelt is entitled to qualified immunity because he did not violate Gibbons's clearly established rights. Bartelt's pre-standoff knowledge of Gibbons differs from that of officers involved in cited cases. Bartelt could reasonably conclude that Gibbons posed a threat to others.

Read Opinion Are you a lawyer? **Annotate this case**.

Bazemore v. Best Buy

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-2196
Opinion Date: April 21, 2020
Judge: Quattlebaum
Areas of Law: Criminal Law

Plaintiff filed suit against her employer, Best Buy, claiming that she was harassed because of her race and gender and subjected to a hostile work

environment in violation of Title VII of the Civil Rights Act of 1964. Plaintiff's complaint stemmed from an incident where a coworker made a racist and sexually charged joke to a small group of coworkers that included plaintiff. The Fourth Circuit affirmed the district court's motion to dismiss and held that, in the case of allegedly harassing comments by a co-worker, an employee must allege plausible facts that the employer knew, or should have known, about the harassment and failed to take action reasonably calculated to stop it. Because plaintiff failed to do this, the court affirmed the district court's judgment. In this case, the coworker's conduct was not imputable to Best Buy where Best Buy took steps that were not only reasonably calculated to end such behavior, but that it did in fact end it.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Akande

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-6833
Opinion Date: April 20, 2020
Judge: Diana Jane Gribbon Motz
Areas of Law: Criminal Law

After defendant moved under 28 U.S.C. 2255 to vacate his conviction based on the ineffective assistance of counsel, the district court denied the motion. The Fourth Circuit granted a certificate of appealability and reversed the district court's judgment. The court held that, given counsel's specific misadvice regarding defendant's rights to preserve his appellate rights, on which defendant understandably relied, the district court's general admonishments did not amount to the careful explanation that addresses the particular issue necessary to cure the error. In this case, the plea colloquy did not correct counsel's erroneous advice and the error prejudiced defendant. Accordingly, the court remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Chambers

Court: US Court of Appeals for the Fourth Circuit
Docket: 19-7104

Opinion Date: April 23, 2020
Judge: Floyd
Areas of Law: Criminal Law

After defendant was erroneously sentenced as a career offender, he moved to reduce his sentence to time served under the First Step Act. The district court denied defendant's motion to reduce his custodial sentence, though it granted the motion as to his supervised release term. The Fourth Circuit held that the First Step Act does not constrain courts from recognizing Guidelines errors. The court explained that First Step Act motions fall under 18 U.S.C. 3582(c)(1)(B), a distinct exception to finality, and that section 404(b) of the First Step Act expressly allows a court to impose a reduced sentence in order to give retroactive effect to sections 2 and 3 of the Fair Sentencing Act. Furthermore, 18 U.S.C. 3553(a) sentencing factors apply in the section 404(b) resentencing context, and the resentencing court has discretion within the section 404(b) framework to vary from the Guidelines and, in doing so, to consider movants' post-sentencing conduct. In this case, the district court seemingly believed that it could not vary from the Guidelines range to reflect post-sentencing information. Therefore, the court vacated the district court's sentencing order. Finally, the court held that any Guidelines error deemed retroactive, such as the error in this case, must be corrected in a First Step Act resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Ferebee

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-4266
Opinion Date: April 22, 2020
Judge: Traxler
Areas of Law: Criminal Law

The Fourth Circuit affirmed the denial of defendant's motion to suppress evidence recovered from a backpack, and the district court's conclusion that defendant abandoned the backpack and any legitimate expectation of privacy in its contents. The court rejected defendant's claim that the collective-knowledge doctrine has any bearing on the propriety of the district court's conclusion that defendant abandoned the backpack. The court also held that the district court is not precluded from finding abandonment in

cases where the defendant, as here, has physical possession of the property he has disavowed. In this case, the record supported the district court's conclusion that defendant clearly and unequivocally disavowed ownership of the backpack. Even if the district court erred by finding that defendant abandoned the backpack, reversal would not be required because the search of the backpack was a proper search incident to arrest for which no warrant was required under the facts of this case.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Nance

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-4585
Opinion Date: April 21, 2020
Judge: Pamela Harris
Areas of Law: Criminal Law

The Fourth Circuit affirmed defendant's above-Guidelines sentence imposed after he pleaded guilty to two federal drug- and firearm-related offenses. The court held that defendant's sentence was not procedurally unreasonable where the district court took into account defendant's extensive criminal history; his pattern of reoffending upon release; his disciplinary infractions in custody and inability to comply with the terms of his release; and the fact that the offenses of conviction occurred over the course of days, in which he was arrested once, released, and then arrested again just days later. The court also held that defendant's sentence was substantively reasonable where the district court conducted a thorough, individualized assessment of defendant and his offense conduct in light of the 18 U.S.C. 3553(a) factors, and did not abuse its discretion in formulating the sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Johnson

Court: US Court of Appeals for the Fifth Circuit
Docket: 17-60852
Opinion Date: April 21, 2020

Judge: Priscilla R. Owen
Areas of Law: Criminal Law

The Fifth Circuit vacated defendant's sentence imposed after he pleaded guilty to violating 18 U.S.C. 922(g) and 924(e) by knowingly possessing a firearm after he had been convicted of a misdemeanor crime of domestic violence. The court held that the district court committing plain error by violating Federal Rule of Criminal Procedure 32 when it relied on factual allegations in the confidential sentencing recommendation that were not in the presentence report and that were not disclosed by defendant. The court explained that the use of undisclosed facts to justify an above-guidelines sentence seriously affects the fairness, integrity, and public reputation of judicial proceedings. Therefore, the court remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. McGinnis

Court: US Court of Appeals for the Fifth Circuit
Docket: 19-10197
Opinion Date: April 21, 2020
Judge: Stuart Kyle Duncan
Areas of Law: Criminal Law

18 U.S.C. 922(g)(8), which prohibits individuals subject to certain domestic violence protective orders from possessing firearms or ammunition for any purpose, is facially constitutional under the Fifth Circuit's two-step NRA framework. Even assuming arguendo that the conduct at issue -- the keeping and possessing of firearms by individuals subject to domestic protective orders -- falls within the Second Amendment right, defendant's facial challenge fails. The court applied intermediate scrutiny and held that section 922(g)(8) is reasonably adapted to the government interest of reducing domestic gun abuse. The court also held that if the commonly understood definitions of terms in the protective order include acts involving "physical force," the protective order is sufficient to support a conviction under section 922(g)(8)(C)(ii). In this case, the jury plausibly found that the order satisfied the statute and the court declined to reverse defendant's conviction on this basis. However, the court remanded for the limited purpose of conforming defendant's written judgment to the district court's

oral pronouncement.

Read Opinion Are you a lawyer? **Annotate this case**.

Valentine v. Collier

Court: US Court of Appeals for the Fifth Circuit
Docket: 20-20207
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Criminal Law, Government & Administrative Law, Health Law

Plaintiffs filed suit alleging that TDCJ's adoption and implementation of measures guided by changing CDC recommendations in regards to the COVID-19 pandemic do not go far enough. Plaintiffs filed a class action alleging violations of the Eighth Amendment's prohibition against cruel and unusual punishment, and the Americans with Disabilities Act, seeking a preliminary injunction. The Fifth Circuit granted TDCJ's motion to stay the district court's preliminary injunction, which regulates the cleaning intervals for common areas, the types of bleach-based disinfectants the prison must use, the alcohol content of hand sanitizer that inmates must receive, mask requirements for inmates, and inmates' access to tissues (amongst many other things). The court held that TDCJ is likely to prevail on the merits of its appeal because: (1) after accounting for the protective measures TDCJ has taken, plaintiffs have not shown a "substantial risk of serious harm" that amounts to "cruel and unusual punishment"; and (2) the district court committed legal error in its application of Farmer v. Brennan, by treating inadequate measures as dispositive of defendants' mental state. In this case, even assuming that there is a substantial risk of serious harm, plaintiffs lack evidence of defendants' subjective deliberate indifference to that harm. The court also held that TDCJ has shown that it will be irreparably injured absent a stay, and that the balance of the harms and the public interest favor a stay. Finally, the court held that plaintiffs have not exhausted their administrative remedies as required in the Prison Litigation Reform Act (PLRA), and the district court's injunction goes well beyond the limits of what the PLRA would allow even if plaintiffs had properly exhausted their claims.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Dowl

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-2469
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

Dowl pleaded guilty to presenting false tax returns, 18 U.S.C. 286. He received a sentence of 30 months of imprisonment plus 24 months of supervised release. On supervised release, Dowl was charged with four new state crimes; failing to inform his probation officer that he had police contact; communicating with his co-defendant despite instructions to the contrary; failing to make payments on his restitution, fine, or special assessment; and failing to get a job. At a hearing, the court reviewed the evidence and allowed Dowl to tell his side of the story. The court deferred judgment on three of the four new state criminal law violations and dismissed the fourth and found Dowl gainfully employed. Dowl had failed to notify his probation officer about police contact, impermissibly communicated with his co-defendant, and did not pay his fines. After considering the 18 U.S.C. 3553(a) sentencing factors, the court returned Dowl to prison for 11 months, giving Dowl and his attorney the opportunity to raise any objections. Dowl had none. The Sixth Circuit affirmed, rejecting Dowl's argument that the court committed reversible error by not directly addressing him to solicit an allocution. The court employed the "plain error" standard because Dowl did not raise any objection during his revocation hearing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Fowler

Court: US Court of Appeals for the Sixth Circuit
Dockets: 19-3071, 19-3070
Opinion Date: April 21, 2020
Judge: Donald
Areas of Law: Criminal Law

In 2018, Fowler pled guilty to possession of child pornography and violations of the conditions of his supervised release from a previous conviction for the same. In addition to possessing child pornography, Fowler had failed drug testing, had threatened his parole officer, and had tried to harass his girlfriend to recant her testimony. The district court ordered Fowler to pay a $5,000 special assessment for possession of child pornography under the Justice for Victims of Trafficking Act, 18 U.S.C. 3014. The court also varied upward and sentenced Fowler to the maximum statutory penalty for violating the conditions of his supervised release, imposing a 120-month sentence for possessing child pornography and a consecutive 36-month sentence for violating the terms of his supervised release. The Sixth Circuit vacated as to the assessment and remanded for a determination of indigency. The district court committed plain error by failing to address Fowler's ability to pay; the parties did not contemplate the $5,000 special assessment as a part of the waiver provision in the plea agreement. The court affirmed the sentence. The district court did not consider an impermissible factor (whether Fowler had actually touched a child) and Fowler had no other challenge to the reasonableness of his sentence,

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Sumlin

Court: US Court of Appeals for the Sixth Circuit
Docket: 18-3819
Opinion Date: April 21, 2020
Judge: Bush
Areas of Law: Criminal Law

Sumlin was convicted of the distribution of drugs that caused the 2015 death of Carrie Dobbins, 21 U.S.C. 841(a)(1) and (b)(1)(C), which carries enhanced penalty provisions. The Sixth Circuit affirmed his convictions and his sentence to life in prison. The district court properly denied Sumlin's suppression motion, given that the affidavit established a sufficient nexus between his drug trafficking activity and residence that was searched. The court properly admitted testimony by the victim's sister, Kelly, who was Sumlin's former girlfriend and had purchased drugs from him. Kelly's testimony about Sumlin's drug-trafficking and that Sumlin was with Carrie on

the day of her overdose was intrinsic proof that was relevant for providing background information and contextualizing the government's case against Sumlin. Sufficient evidence supported the jury's verdict that Sumlin distributed the drugs that caused Carrie's death.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Vance

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-5160
Opinion Date: April 17, 2020
Judge: Bush
Areas of Law: Criminal Law, White Collar Crime

The Spriggs' bank account was established to receive social security checks. The Spriggs' great-grandson, Vance, filled out an application in Mr. Spriggs's name for a debit card to draw on the checking account. Mr. Spriggs had never used a debit card. The Spriggses did not authorize Vance to do so. Bank cameras photographed Vance using the card to withdraw cash. Vance also used the card for personal expenses. At another bank, Vance used Mr. Spriggs's social security number to establish an account and obtain a $15,000 cash advance. Vance made other, unsuccessful loan applications. Upon being notified by the banks about suspicious activities involving his identity, Mr. Spriggs filed a police report. The police arrested Vance. While searching Vance's car, the police located a large stash of personal and financial documents belonging to the Spriggses, including bank statements, tax return forms, property-tax bills, and a car title. The Sixth Circuit affirmed Vance's convictions for access-device fraud, 18 U.S.C. 1029(a)(5), and two counts of aggravated identity theft, 18 U.S.C. 1028A(a)(1), and his 65-month sentence. The court rejected arguments that the district court failed to make adequate findings of fact after the bench trial, improperly denied a motion for judgment of acquittal, and failed to correctly calculate the loss amount connected to Vance's charges under Sentencing Guidelines 2B1.1.

Read Opinion Are you a lawyer? **Annotate this case**.

Winburn v. Nagy

Court: US Court of Appeals for the Sixth Circuit
Dockets: 19-2399, 19-2398
Opinion Date: April 23, 2020
Judge: Jeffrey S. Sutton
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Winburn represented himself at his trial for armed robbery, home invasion, and conspiracy. Based on Winburn's disruptive behavior, the judge removed him from the courtroom and revoked Winburn's permission to represent himself, then granted a competency evaluation and a mistrial. While Winburn awaited his second trial, the judge permitted Winburn's stand-by attorney to withdraw because Winburn had sued her and enjoined Winburn from filing complaints or grievances against his new attorney, except to discharge her. Although represented by a new attorney, Winburn moved pro se to dismiss his charges on double jeopardy grounds. The trial judge denied the motion because Winburn's attorney had not filed it. Winburn filed a habeas petition under 28 U.S.C. 2241 challenging his retrial and another section 2241 petition challenging the injunction. The district judges denied both and declined to issue certificates of appealability. Winburn filed a notice of appeal for one petition and sought a certificate of appealability for the other. The Sixth Circuit held that state pretrial detainees proceeding under section 2241 may not appeal without certificates of appealability and granted Winburn a certificate on the injunction claim. A reasonable jurist could conclude that the unusual order was constitutionally infirm. The court denied relief with respect to double jeopardy. Winburn failed to exhaust his state-court remedies by a motion to dismiss.

Read Opinion Are you a lawyer? **Annotate this case**.

Lund v. City of Rockford

Court: US Court of Appeals for the Seventh Circuit
Docket: 19-1945
Opinion Date: April 20, 2020
Judge: ROVNER
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Lund, a reporter for the Rockford Scanner, heard, by police scanner, of multiple traffic stops in Midtown. He did not have a driver's license, so he

rode a motorized bicycle to Midtown to take photographs. He suspected a prostitution sting operation. An officer noticed Lund and radioed the team. Officers Welsh and Campbell knew of Lund's previous anti-police speech. They directed Lund to “move on.” Lund asked if he was breaking any laws. Campbell informed him that he was not, but that his continued presence would constitute obstruction of a police detail and result in arrest. Lund started his bicycle and called out, loudly, “goodbye officers.” Concerned that Lund might post pictures on social media while the sting operation was ongoing and create a danger for unarmed undercover officers, the officers followed Lund and arrested him for driving the wrong way on a one-way street, operating a vehicle without insurance, obstructing a police officer, felony aggravated driving on a revoked license, and operating a motor vehicle without a valid drivers’ license. News stories listed Lund’s name as an arrestee in the prostitution sting. The charges against Lund were dismissed. Lund sued the officers and the city under 42 U.S.C. 1983. The Seventh Circuit affirmed summary judgment for the defendants on First Amendment retaliation and malicious prosecution under Illinois law, citing the Supreme Court’s intervening "Nieves" (2019) holding, that, in most cases, probable cause to arrest defeats a claim of retaliatory arrest. There was probable cause to arrest Lund.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Perez

Court: US Court of Appeals for the Seventh Circuit
Docket: 18-3156
Opinion Date: April 23, 2020
Judge: KANNE
Areas of Law: Criminal Law

Beloit officers facilitated a recorded controlled buy of heroin from Perez, a suspected high-level drug dealer. Perez sold 98 grams of heroin to an informant. Based on that transaction alone, Perez pled guilty to distributing heroin. At Perez’s sentencing hearing, the judge expressed concern that the guidelines range of 33–41 months’ imprisonment did not reflect the full scope of his drug trafficking. The PSR described conduct that suggested that Perez was responsible for distributing large quantities of heroin, methamphetamine, and cocaine. The judge continued the hearing, directing

the government to file a memorandum, detailing which offense conduct it could support by a preponderance of the evidence. When the hearing reconvened, the government presented witness testimony that elaborated on conduct described in the PSR, including drug ledgers, Perez's post-arrest conversation with his girlfriend, large sums of cash, a money counter, cell phones, and Perez's passport. The judge calculated a higher guidelines range and imposed a 121-month sentence. The Seventh Circuit affirmed, rejecting an argument that the sentencing judge should have recused himself. Perez has not demonstrated that a reasonable observer would have questioned the judge's impartiality nor did he allege that the judge was biased based on events outside the proceedings. The judge's continuance was laudable, not prejudicial.

Read Opinion Are you a lawyer? **Annotate this case**.

Jackson v. United States

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1131
Opinion Date: April 20, 2020
Judge: Lavenski R. Smith
Areas of Law: Criminal Law

The Eighth Circuit affirmed the district court's denial of a 28 U.S.C. 2255 motion to vacate, set aside, or correct petitioner's sentence. The court held that the district court did not err in denying an evidentiary hearing as to petitioner's claim that counsel was constitutionally ineffective for failing to conduct adequate pretrial investigations. In this case, petitioner failed to identify any specific witnesses or evidence that counsel failed to uncover. Furthermore, petitioner failed to show that counsel's representation prejudiced his case. The court also held that the district court did not err in denying an evidentiary hearing as to petitioner's claim that his new counsel was ineffective for failing to subpoena witnesses, for convincing petitioner not to testify, for failing to object to or appeal the district court's answer to a jury question, and for failing to object to the district court's designation of petitioner as a career offender.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Bolman

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-2759
Opinion Date: April 21, 2020
Judge: Jane Louise Kelly
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's conviction for involuntary manslaughter after he struck and killed his nephew with his truck. The court held that the evidence was sufficient to support the conviction, because a reasonable jury could find defendant grossly negligent beyond a reasonable doubt. The court also held that the district court did not plainly err by failing to instruct the jury that actual knowledge is an essential element of the offense that is separate from gross negligence, because the instructions, viewed as a whole, accurately and adequately defined the essential elements of the offense.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Boyd

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-3528
Opinion Date: April 17, 2020
Judge: Kobes
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's sentence imposed after he pleaded guilty to being a felon in possession of a firearm. The court held that the facts underlying defendant's prior arrests were part of his history and characteristics under 18 U.S.C. 3553(a), and thus the district court could consider defendant's arrest records and the circumstances of those arrests. The court explained that the arrests were listed in the presentence report and gleaned from prior police reports. Furthermore, specific facts underlying the arrests may be considered for an upward departure and should be considered fair game for a variance where defendant did not object to them. The court also concluded that there is nothing here that suggested a corrected misstatement improperly influenced the district court's sentencing decision. Finally, the court held that the upward variance was not

unreasonable in consideration of defendant's previous assaults, coupled with the facts underlying his arrest in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Gonzalez-Esparsa

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1477
Opinion Date: April 22, 2020
Judge: Grasz
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's conviction for unlawful use of an identification document and misuse of a social security number. The court held that the evidence was sufficient to support defendant's convictions where a reasonable juror could conclude that defendant knew the permanent resident card bearing his name and photograph had been forged, counterfeited, falsely made, or unlawfully obtained when he used it to secure employment. Furthermore, a reasonable juror could conclude that defendant made the false representation regarding his purported social security number in order to deceive Midwest Concrete in order to obtain a job with the company.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Sanchez-Velasco

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-3568
Opinion Date: April 17, 2020
Judge: James B. Loken
Areas of Law: Criminal Law, Immigration Law

The Eighth Circuit affirmed the district court's denial of defendant's motion to suppress his responses to an ICE agent's two questions at the Treasurer's Office, because he was not in custody at the time of questioning. Although defendant was in custody at the ICE facility, the court held that an agent's questions were not custodial interrogation because the agent could not have known his questions were likely to elicit incriminating information regarding

the two criminal charges that were eventually brought against defendant. The court noted that the Attorney General's regulations carefully distinguish between the warrantless arrest of an alien for a criminal violation of the immigration laws, and what is called the "administrative arrest" of an alien who is reasonably believed to be illegally present in the United States. The court agreed with the district court that the agent's questioning was a request for routine information necessary for basic identification purposes that is not interrogation under Miranda, even if the information turns out to be incriminating.

Read Opinion Are you a lawyer? **Annotate this case**.

Anthony v. TRAX International Corp.

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-15662
Opinion Date: April 17, 2020
Judge: Kim McLane Wardlaw
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Ninth Circuit affirmed the district court's grant of summary judgment to TRAX in a disability discrimination action brought by plaintiff under Title I of the Americans with Disabilities Act (ADA). After TRAX terminated plaintiff from her position as a Technical Writer allegedly due to an inability or unwillingness to accommodate her disability, TRAX discovered during the course of litigation that plaintiff lacked the requisite bachelor's degree for her position. The panel held that, although McKennon v. Nashville Banner Publishing Co., 513 U.S. 352 (1995), held that after-acquired evidence cannot establish a superseding, non-discriminatory justification for an employer's challenged actions, after-acquired evidence remains available for other purposes, including to show that an individual is not qualified under the ADA. Because plaintiff did not satisfy one of the prerequisites for her position, she is not "otherwise qualified," and TRAX was not obligated to engage in the interactive process.

Read Opinion Are you a lawyer? **Annotate this case**.

City of Almaty v. Khrapunov

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-56451
Opinion Date: April 22, 2020
Judge: Marbley
Areas of Law: Criminal Law, International Law, White Collar Crime

The City of Almaty, in Kazakhstan, filed suit against defendant and his family under the Racketeer Influenced and Corrupt Organizations Act (RICO), alleging that they engaged in a scheme to defraud the city of millions of dollars. The City claimed that it was forced to spend money and resources in the United States to trace where its money was laundered. The district court dismissed the City's claim on the basis that it failed to state a domestic injury pursuant to the Supreme Court's recent decision in RJR Nabisco, Inc. v. European Community, 136 S. Ct. 2090 (2016). The Ninth Circuit held that the City failed to state any cognizable injury other than the foreign theft of its funds, and its voluntary expenditures were not proximately caused by defendants' acts of money laundering. In this case, the City's expenditure of funds to trace its allegedly stolen funds is a consequential damage of the initial theft suffered in Kazakhstan and is not causally connected to the predicate act of money laundering.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Baldon

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-10411
Opinion Date: April 21, 2020
Judge: Bennett
Areas of Law: Criminal Law

After defendant pleaded guilty to possession with intent to distribute a controlled substance, the district court sentenced him to 184 months in prison. The Ninth Circuit held that defendant's prior convictions for carjacking under section 215 of the California Penal Code are not categorical crimes of violence under USSG 4A1.1(e). Therefore, the district court incorrectly calculated defendant's criminal history by improperly including two points for his prior carjacking convictions. However, the panel held that the district court did not err in finding that defendant possessed a

firearm under USSG 2D1.1(b)(1). Accordingly, the panel affirmed in part, vacated in part, and remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Costanzo

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-10291
Opinion Date: April 17, 2020
Judge: Michael Daly Hawkins
Areas of Law: Criminal Law

The Ninth Circuit affirmed defendant's conviction of five counts of money laundering, holding that a reasonable trier of fact could have found beyond a reasonable doubt that the money laundering transactions, in which payment was made via bitcoin, affected interstate commerce in some way or to some degree. In this case, the transfer involved the use of an Internet or cellular network connected Personal Computer Device (PCD) to transfer bitcoin (together with the digital code necessary to unlock the bitcoin) to the digital wallet of another Internet or cellular network connected PCD.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Manzanares

Court: US Court of Appeals for the Tenth Circuit
Docket: 18-2010
Opinion Date: April 17, 2020
Judge: Mary Beck Briscoe
Areas of Law: Constitutional Law, Criminal Law

Defendant-Appellant Archie Manzanares appealed a district court's denial of his 28 U.S.C. 2255 motion challenging his sentence under the Armed Career Criminal Act (ACCA). Under the ACCA, an offense qualified as a violent felony by satisfying at least one of three definitions, which have come to be known as the Elements Clause, the Enumerated Clause, and the Residual Clause. Manzanares asserted that without the Residual Clause, his underlying New Mexico convictions (armed robbery, aggravated assault with a deadly weapon, and aggravated battery) no longer qualified

as violent felonies. The district court denied the motion, concluding that all three underlying convictions satisfied the Elements Clause. Manzanares appealed the classification of the armed robbery conviction as a violent felony to the Tenth Circuit, and sought to expand the certificate of appealability to allow him to appeal the decision regarding the aggravated assault with a deadly weapon and aggravated battery convictions. After review, the Tenth Circuit affirmed the district court's denial of Manzanares's 2255 motion, and denied his motion to expand the COA.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Delaney

Court: US Court of Appeals for the District of Columbia Circuit
Docket: 18-3093
Opinion Date: April 17, 2020
Judge: David S. Tatel
Areas of Law: Criminal Law

The DC Circuit vacated the district court's denial of defendant's motion to suppress evidence. The court held that officers violated the Fourth Amendment when they seized defendant because they lacked reasonable suspicion to justify the stop. In this case, a seizure occurred when the officers pulled into the parking lot, partially blocked defendant's vehicle, and activated their take-down light. The court held that any inference of suspicion that the officers drew from encountering defendant soon after hearing the nearby gunshots were undermined by the government's failure to identify specific and articulable facts supporting the officers' estimation of where the various shots came from. Accordingly, the court remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

Antenor v. Alaska, Department of Corrections

Court: Alaska Supreme Court
Docket: S-17005
Opinion Date: April 17, 2020
Judge: Carney

Areas of Law: Civil Procedure, Criminal Law, Government & Administrative Law

Several Alaska Department of Corrections inmates challenged the DOC's policy to charge for local telephone calls, arguing the rates they and call recipients had to pay for calls violated their constitutional right to rehabilitation, their statutory right to reasonable telephone access, and DOC's contractual obligations under a prior settlement and consent decree. In addition, one of the prisoners challenged DOC officers' decision to deny him access to a computer programming book he ordered from outside the prison. He contended that DOC placed a content-specific restriction on the educational materials and publications prisoners were allowed, violating the Alaska Constitution's free speech provisions as well as prisoners' right to reformation. Each of these challenges reached the Alaska Supreme Court after inmates exhausted the administrative process from prison. Inmates then appealed to the superior court, which denied relief. The Alaska Supreme Court determined the superior court record did not provide enough evidence for it to meaningfully determine the reasonableness of the rates charged inmates for local telephone calls; therefore the Court reversed denial of relief and remanded for further fact-finding by the trial court. The Court concluded that the facility's restrictions on programming-related books were rationally related to a legitimate interest, and because they did not infringe on the right to rehabilitation, it affirmed denial of a prisoner's motion to enforce his claimed right to a particular text about computer programming.

Read Opinion Are you a lawyer? **Annotate this case**.

Berger v. Bryant

Court: Arkansas Supreme Court
Citation: 2020 Ark. 357
Opinion Date: April 23, 2020
Judge: Rhonda K. Wood
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's petition to proceed in forma pauperis on a petition for writ of mandamus and a motion for declaratory judgment, holding that Appellant failed to state a colorable cause of action. In 1998, Appellant was convicted

of rape. In his petition for a writ of mandamus, Appellant asserted that he sought information pursuant to the Arkansas Freedom of Information Act regarding his rape conviction but received no response. The circuit court denied the petition. The Supreme Court affirmed, holding (1) even if Appellant had requested disclosable information, he would not be entitled to inspect it as an incarcerated person; and (2) Appellant did not demonstrate a legitimate claim given the facts presented and therefore failed to establish a colorable cause of action to support his request to proceed in forma pauperis.

Read Opinion Are you a lawyer? **Annotate this case**.

Carroll v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 360
Opinion Date: April 23, 2020
Judge: Wynne
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's motion for leave to file a petition for writ of error cram knobs, holding that the circuit court did not abuse its discretion in declining to issue the writ. Appellant pled guilty to rape and was sentenced as a habitual offender to 720 months' imprisonment. In his coram nobis petition, Appellant alleged several grounds for relief, including claims of actual innocence, an invalid arrest warrant, a coerced guilty plea, and prosecutorial misconduct. The circuit court denied the motion. The Supreme Court affirmed, holding that Appellant did not demonstrate that that the writ should issue and failed diligently to proceed on his claim for coram nobis relief.

Read Opinion Are you a lawyer? **Annotate this case**.

Cave v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 356
Opinion Date: April 23, 2020
Judge: Josephine L. Hart

Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's pro se petition for writ of habeas corpus, holding that the circuit court did not err in denying the petition. Appellant was found guilty of two counts of delivery of a controlled substance and one count of maintaining a drug premises. In his habeas petition, Appellant argued that he was actually innocent because his arrest and conviction was based on the false testimony of a witness who had a lengthy criminal history. Appellant further argued that the writ should issue because he was not afforded effective assistance of counsel. The circuit court denied the petition. The Supreme Court affirmed, holding (1) Appellant's claims regarding the witness's credibility do not constitute a valid assertion that he was being unlawfully detained; and (2) Appellant did not actually connect an allegation of ineffective assistance of counsel to his allegation that he was unlawfully detained.

Read Opinion Are you a lawyer? **Annotate this case**.

Chatmon v. Kelley

Court: Arkansas Supreme Court
Citation: 2020 Ark. 355
Opinion Date: April 23, 2020
Judge: Josephine L. Hart
Areas of Law: Criminal Law

The Supreme Court denied Appellant's appeal from the order of the circuit court denying his petition to proceed in forma pauperis on the grounds that Appellant failed to state a colorable cause of action in a petition for writ of habeas corpus, holding that the circuit court did not abuse its discretion by denying Appellant's in forma pauperis petition. In his habeas petition, Appellant alleged that the trial court lacked jurisdiction in his criminal case. Before this case was submitted to the Supreme Court, Appellant filed two motions, including a "Judicial Notice of a Void Judgment" and a "Notice to the Court." The Supreme Court denied the motions, holding that neither motion was cognizable under the Court's rules. The Court then affirmed the Supreme Court's denial of Appellant's in forma pauperis petition, holding that the circuit court correctly found that Appellant did not assert a colorable

cause of action.

Read Opinion Are you a lawyer? **Annotate this case**.

McClinton v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 353
Opinion Date: April 23, 2020
Judge: Karen R. Baker
Areas of Law: Criminal Law

The Supreme Court denied Petitioner's second petition requesting permission to proceed in the trial court with a petition for writ of error coram nobis, holding that Petitioner's proposed attack on the judgment had no merit. Petitioner was convicted of raping a mentally handicapped sixteen-year-old girl and was sentenced to life imprisonment. In his first petition for writ of error coram nobis Petitioner alleged a number of errors in the trial procedure. The first petition was denied. In his second coram nobis petition, Petitioner alleged violations of Brady v. Maryland, 373 U.S. 83 (1963). The Supreme Court denied the writ, holding that Petitioner failed to meet his burden of demonstrating a fundamental error of fact extrinsic to the record.

Read Opinion Are you a lawyer? **Annotate this case**.

Siegel v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 359
Opinion Date: April 23, 2020
Judge: Wynne
Areas of Law: Criminal Law

The Supreme Court dismissed Appellant's appeal from the circuit court's orders denying her motions to declare Ark. Code Ann. 5-62-106 (disposition of animal) and Ark. Code Ann. 5-62-111 (prevention of cruelty) unconstitutional and conditionally granting her motion for return of seized property, holding that there was no final, appealable order in this case. Appellant was convicted of thirty-one misdemeanor counts of cruelty to animals. The circuit court subsequently dismissed the charges on speedy-

trial grounds. The State appealed, and the Supreme Court dismissed the appeal on the grounds that it was not authorized. Appellant had filed motions seeking a declaration that sections 5-62-106 and -111 are unconstitutional and seeking the return of her seized property. The circuit court denied the constitutional claims and entered a conditional order granting Appellant's motion for return of seized property. Appellant appealed. The Supreme Court dismissed the appeal, holding that because the conditional order did not make specific findings as to the return of the property or as to damages and because it expressly left open the possibility of further proceedings, there was no final, appealable order in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

Thomas v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 354
Opinion Date: April 23, 2020
Judge: Josephine L. Hart
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Appellant's conviction of capital murder, holding that the evidence was sufficient to sustain the conviction and that the circuit court did not err in denying Appellant's motion to suppress tracking data generated by his cellphone. On appeal, Appellant argued that the trial court erred by denying his directed-verdict motion because the evidence supported the defense's theory of the case that he did not intend to shoot the victim. Further, Appellant argued that the court abused its discretion in denying his motion to suppress evidence obtained from the seizure of AT&T phone records. The Supreme Court disagreed, holding (1) the evidence was sufficient to support the capital murder conviction; and (2) the circuit court correctly denied the motion to suppress.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. Landowski

Court: California Courts of Appeal
Docket: C080210(Third Appellate District)

Opinion Date: April 23, 2020
Judge: Andrea Lynn Hoch
Areas of Law: Constitutional Law, Criminal Law

Defendant Michael Reyes, Jr., an active Norteno gang member (from the Broderick Boys subset), confronted a former Norteno gang member (from the Franklin Boys subset), "S.," about a physical altercation that occurred between S. and Reyes's stepfather over a debt. That earlier altercation had taken place in front of Reyes's autistic younger brother. Reyes pulled out a handgun and asked S. if he had a problem. S., who was riding his bicycle with his wife, "R.," when Reyes confronted him with the gun, stopped briefly, told Reyes to put the gun down if he wanted to fight, and then started to ride away. This angered Reyes, prompting him to fire six rounds at S. from behind. S. Was hit but survived. R. Was a short distance in front of S., but was not hit. Defendants Liberty Landowski and Lisa Humble were with Reyes at the time of the shooting and aided in his efforts to avoid being apprehended by law enforcement authorities. Reyes, Landowski, and Humble were tried together before the same jury. Reyes was convicted of one count of attempted murder (Count 1), two counts of assault with a semiautomatic firearm (Counts 2 and 4), one count of possession of a firearm by a convicted felon (Count 5), and one count of possession of ammunition by a convicted felon (Count 6). In addition to various firearm and other enhancements, the jury found Reyes committed the crimes for the benefit of, at the direction of, or in association with a criminal street gang with the specific intent to promote, further, or assist in criminal conduct by gang members. The jury convicted Landowski and Humble of being accessories to Reyes's criminal conduct (Count 9) and also found true gang enhancement allegations attached to that crime. Reyes challenged the sufficiency of the firearm evidence presented to support his conviction, and all defendants challenged the sufficiency of the evidence supporting their gang enhancements. The Court of Appeal determined Senate Bill 620 (2017-2018 Reg. Sess.) gave the trial court discretion to strike firearm enhancements in the interest of justice and applied retroactively; and Senate Bill 136 (2019-2020 Reg. Sess.) eliminated such enhancements, and also applied retroactively. To these issues, the Court remanded for the trial court's consideration. The Court affirmed the trial court in all other respects.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. May

Court: California Courts of Appeal
Docket: C084302(Third Appellate District)
Opinion Date: April 20, 2020
Judge: Ronald B. Robie
Areas of Law: Constitutional Law, Criminal Law

Defendant Raymond May was found guilty by jury of possessing an assault weapon and a machine gun based on his possession of a single AK-47 assault rifle while guarding a marijuana plantation. He was sentenced to probation, which included an electronic search condition. On appeal, defendant argued there was a lack of sufficient evidence corroborating his accomplice's testimony and demonstrating he knew of the firearm's illegal character. He further alleged the trial court erred in instructing the jury: that the accomplice instruction should have included language specifying that the accomplice testimony needed to prove more than defendant's mere presence or access to the firearm. Furthermore, defendant argued the electronic search condition imposed as part of his probation failed under the standards announced in California v. Lent, 15 Cal.3d 481 (1975). The Court of Appeal agreed defendant's electronic search condition should have been stricken, but otherwise affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. Perez

Court: California Courts of Appeal
Docket: E072260(Fourth Appellate District)
Opinion Date: April 20, 2020
Judge: Miller
Areas of Law: Constitutional Law, Criminal Law

In 2009, defendant-appellant Rudy Perez pled guilty to active gang participation under Penal Code section 186.22(a), and unlawful possession of a firearm under section 12025(b)(6). In 2010, defendant pled guilty to residential burglary under section 459, and active gang participation under section 186.22(a). In August of 2018, the State filed a new felony complaint, alleging one of the prior gang participation convictions as a strike prior. In

2018, defendant moved to vacate the two prior gang participation convictions based upon changes in the law that rendered them invalid. The trial court denied defendant's motion. In 2019, defendant asked for reconsideration, which was again denied. Thereafter, defendant filed a timely notice of appeal from the denial of his motion to vacate the convictions. The Court of Appeal found that defendant pled guilty to street terrorism under Penal Code section 186.22(a) in 2009 and 2010, and it was undisputed that while committing these offenses, defendant acted alone. However, subsequent to defendant's guilty pleas, in 2012, the California Supreme Court held that a defendant had to act in concert with a fellow gang member in order to be guilty of street terrorism. At that time, defendant could have filed a state habeas petition requesting relief, but failed to do so. "Defendants can lose remedies that are established by law when they fail to invoke such remedies in time." Section 1473.7 became effective in 2017. In defendant's motion filed in the trial court, defendant failed to state what new evidence was discovered, instead arguing that the trial court was allowed "to vacate a conviction where the defendant is innocent as a matter of law or where vacating the conviction is in the interest of justice, even though the defendant is no longer in custody or otherwise restrained by the conviction." The Court of Appeal concurred with the trial court's reason to deny relief, determining that "while the outcome in this case may be unfortunate for defendant, we are not here to rewrite legislation. The Legislature could amend section 1473.7 to address issues raised in this case. However, under the laws, as written, we must uphold the trial court's order."

Read Opinion Are you a lawyer? **Annotate this case**.

In re S.R.

Court: California Courts of Appeal
Docket: B300214(Second Appellate District)
Opinion Date: April 23, 2020
Judge: Bendix
Areas of Law: Criminal Law

Father appealed the juvenile court's dispositional ruling removing daughter from his custody, arguing that his mere possession of child pornography does not demonstrate that he poses a substantial risk of harm to his daughter. The Court of Appeal affirmed the order and held that there is

substantial evidence of risk of great harm to daughter—no matter how low the probability— that father will sexually abuse his daughter if he is provided unfettered access to her.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Bell

Court: California Courts of Appeal
Docket: B288528(Second Appellate District)
Opinion Date: April 23, 2020
Judge: Stratton
Areas of Law: Criminal Law

Defendant was convicted of one count of attempted robbery, one count of second degree murder, and one count of hit and run driving. The jury found not true the allegation that a principal was armed in the commission of the attempted robbery. The trial court found true the allegations that defendant had served four prior prison terms within the meaning of Penal Code section 667.5, subdivision (b). Defendant raised 13 claims of error on appeal. The Court of Appeal held that the section 667.5, subdivision (b) enhancement terms must be stricken and the matter remanded to the trial court for resentencing. The court also held that defendant forfeited some of his substantive claims and other lack merit. Finally, the court held that, if there is instructional error, the errors are harmless under any standard of review. Accordingly, the court affirmed the judgment of conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Drayton

Court: California Courts of Appeal
Docket: H046928(Sixth Appellate District)
Opinion Date: April 17, 2020
Judge: Danner
Areas of Law: Criminal Law

In 1991, the Wards and their teenage daughter awoke and discovered four men, including Drayton, inside their house. Two were armed. One told the daughter he was going to rape her and placed a firearm inside her vagina.

Drayton told the man not to do it. Drayton had a gun and held Mrs. Ward down during the robbery. Two others shot and killed Mr. Ward. Drayton and the others left without seeking help for the Wards. Drayton did not shoot Mr. Ward or threaten to rape the daughter. Drayton surrendered the next day. Drayton's sole prior conviction was a misdemeanor; he had no reported history of violence. Drayton was sentenced to 29 years to life imprisonment. In 2019, Drayton sought resentencing under Penal Code 1170.95, declaring that he "was not a major participant ... or did not act with reckless indifference to human life." Senate Bill 1437, effective January 1, 2019, restricted the circumstances under which a person can be liable for felony murder and enacted Penal Code 1170.95, which allows an individual, previously convicted of felony murder, to petition to have his murder conviction vacated and to be resentenced. The court of appeal directed the trial court to hold a hearing under section 1170.95(d) and to accept the assertions in the petition as true unless facts in the record conclusively refute them as a matter of law. If, accepting the petitioner's assertions as true, he meets section 1170.95(a)'s requirements for relief, the court must issue an order to show cause. In assessing the prima facie showing, the trial court should not weigh evidence or make credibility determinations.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Robinson

Court: California Courts of Appeal
Docket: B293746(Second Appellate District)
Opinion Date: April 20, 2020
Judge: Wiley
Areas of Law: Criminal Law

After defendant penetrated an unconscious woman with his fingers, he challenged evidentiary rulings and requests a presentence conduct credit. The Court of Appeal held that the trial court properly excluded cumulative evidence about past times the woman was intoxicated at the relevant bar, and any error in allowing a drug recognition expert to testify about whether the woman was incapacitated was harmless. However, the court held that the trial court undercalculated defendant's presentence custody credit because he was not convicted of a violent felony under Penal Code section 2933.1, which would otherwise limit those credits. Accordingly, the court

directed the trial court to award defendant 104 days of presentence custody credit and to amend the abstract of judgment, affirming in all other respects.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Torres

Court: California Courts of Appeal
Docket: B292551(Second Appellate District)
Opinion Date: April 20, 2020
Judge: Kenneth R. Yegan
Areas of Law: Criminal Law

Where, as here, the trial court factually finds that a self-represented defendant has engaged in an attempt to intimidate a witness, the constitutional right of self-representation can, in the exercise of the trial court's sound discretion, be revoked. The Court of Appeal affirmed defendant's conviction and sentence for two counts of battery on an ex-girlfriend. In this case, the trial court did not abuse its discretion in revoking defendant's pro se status after he asked his sister to contact the victim and have her say that she was coerced by the police detective to "press charges."

Read Opinion Are you a lawyer? **Annotate this case**.

Colorado v. Lujan

Court: Colorado Supreme Court
Citation: 2020 CO 26
Opinion Date: April 20, 2020
Judge: Brian D. Boatright
Areas of Law: Constitutional Law, Criminal Law

Abel Lujan was charged with first-degree murder for the death of his girlfriend after she was found beaten and strangled behind a friend’s house. At trial, two women testified for the State about Lujan’s prior violent behavior towards them. Prior to admitting this evidence, the trial court read a limiting instruction, telling the jury that it could only consider the evidence for the purposes of establishing Lujan’s motive, intent, or common plan. A copy of

this instruction was not given to the jury for deliberations; however, the jury did receive an instruction at the close of the evidence explaining that certain evidence could only be considered for the limited purposes for which it was admitted. While deliberating, the jury submitted a question seeking clarification about the limiting instruction. Over defense counsel's objection, the trial court cleared the courtroom of the public and parties, leaving only the judge, bailiff, and court reporter; the judge then brought in the jury and reread the limiting instruction that it had previously read twice in open court. The jury ultimately found Lujan guilty of second-degree murder. Lujan appealed, arguing that the court's actions when rereading the jury instruction constituted a courtroom closure that violated his Sixth Amendment right to a public trial. A division of the court of appeals agreed and reversed Lujan's conviction. The State argued on certiorari review that the Colorado Supreme Court adopt a triviality standard, under which a defendant's constitutional right to a public trial was not violated when the closure at issue was trivial. In so doing, the State argued that the brief courtroom closure here was trivial and therefore did not violate Lujan's public trial right. The Court concurred with the State, adopted the standard and reversed the appellate court's decision.

Read Opinion Are you a lawyer? **Annotate this case**.

Archer v. State

Court: Florida Supreme Court
Docket: SC19-841
Opinion Date: April 23, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the order of the circuit court denying Appellant's successive motion to vacate his sentence of death under Fla. R. Crim. P. 3.851, holding that the circuit court did not err in denying the Rule 3.851 motion. Appellant was convicted of first-degree murder, armed robbery, and grand theft. Appellant was sentenced to death for the murder. The Supreme Court affirmed the convictions but reversed Appellant's death sentence and remanded the case for a new penalty phase. After a new penalty phase, Appellant was again sentenced to death. In his successive Rule 3.851 motion, Appellant raised three claims. The circuit court denied

relief. The Supreme Court affirmed, holding that the circuit court (1) properly denied Appellant's claim that his death sentence violated the Sixth and Eighth Amendments in light of Hurst v. Florida, 136 S. Ct. 616 (2016), and Hurst v. State, 202 So. 3d 40 (Fla. 2016); (2) correctly denied Appellant's claim that his sentence violated the Eighth Amendment; and (3) did not err in denying Appellant's claim of newly discovered evidence.

Read Opinion Are you a lawyer? **Annotate this case**.

Collins v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0158
Opinion Date: April 20, 2020
Judge: David E. Nahmias
Areas of Law: Constitutional Law, Criminal Law

Appellant Tommy Collins was convicted of felony murder in connection with the stabbing death of 14-year-old Rueben Hand. Friends gathered to watch the Peach Drop on New Year's Eve 2010; a disagreement ensued and Hand was stabbed near the Five Points MARTS station shortly after midnight. Appellant's only argument on appeal was that the trial court plainly erred when it gave the jury the State's requested instruction on "revenge for a prior wrong." Seeing no error, "much less plain error," the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Heyward v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0399
Opinion Date: April 20, 2020
Judge: Peterson
Areas of Law: Constitutional Law, Criminal Law

Larmell Heyward was convicted by jury of malice murder and possession of a firearm during the commission of a felony in connection with the 2007 shooting death of Ramon Rogers. Heyward argued on appeal of those convictions that the trial court erred in denying his request to charge the jury

on voluntary manslaughter. After review, the Georgia Supreme Court determined the trial court's refusal to give the charge was harmless, since, in the Court's estimation, there was no realistic probability that the jury would have accepted the "slight" evidence of voluntary manslaughter in the light of the strong evidence of malice murder.

Read Opinion Are you a lawyer? **Annotate this case**.

Howard v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0819
Opinion Date: April 20, 2020
Judge: Keith R. Blackwell
Areas of Law: Constitutional Law, Criminal Law

Kenneth Howard was tried by jury and convicted of the murder of Emily Ann Smith Newbegin. Howard appealed, contending that the evidence was legally insufficient to sustain his conviction. Upon its review of the record and briefs, the Georgia Supreme Court found no merit in Howard's claim of error, and affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Keller v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0006
Opinion Date: April 20, 2020
Judge: Boggs
Areas of Law: Constitutional Law, Criminal Law

Randall Keller was convicted of felony murder and related crimes arising out of the beating death of his ex-wife's two-year-old son, William Powell. On appeal, Keller raised numerous claims of error, including ineffective assistance of counsel, the trial court's rulings on motions before and during trial, several evidentiary rulings, and alleged bias on the part of the trial judge. However, finding no reversible error, the Georgia Supreme Court affirmed Keller's convictions.

Read Opinion Are you a lawyer? **Annotate this case**.

Mills v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0364
Opinion Date: April 20, 2020
Judge: Ellington
Areas of Law: Constitutional Law, Criminal Law

Roger Mills was found guilty by jury of malice murder and aggravated assault in connection with the death of Masuto Garrett. Mills contended that the trial court erred when, during jury deliberations, it excused a holdout juror without sufficient inquiry or good cause. After review, the Georgia Supreme Court concurred with that contention, and reversed Mills's convictions. The Court also concluded the evidence presented at trial was legally sufficient to support the convictions, so the State could retry Mills if it chose.

Read Opinion Are you a lawyer? **Annotate this case**.

Moore v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0344
Opinion Date: April 20, 2020
Judge: David E. Nahmias
Areas of Law: Constitutional Law, Criminal Law

Appellant Carzell Moore, proceeding pro se, appealed a trial court's denial of his motion to set aside a September 2017 order denying his motion for an out-of-time appeal of his 2002 resentencing on his 1977 convictions for murder and rape. Moore contended the trial court abused its discretion by denying his motion to set aside because he was not given proper notice of the September 2017 order. Finding that the record supported the trial court's ruling, the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Morris v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0176
Opinion Date: April 20, 2020
Judge: Bethel
Areas of Law: Constitutional Law, Criminal Law

Darius Morris was found guilty by jury of malice murder and other offenses in connection with the shooting death of Jameson Bush. Morris appealed, arguing he was denied the right to a timely appeal, that the trial court erred in restricting voir dire as to the religious beliefs and connections of potential jurors, that the trial court erred by giving a confusing jury charge regarding statements of co-conspirators, that the trial court erred by violating his right to a public trial by ordering that the courtroom doors be closed and locked during the court's charge to the jury, and that his trial counsel provided ineffective assistance by not objecting to the closure of the courtroom. Finding no error, the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Rickman v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0127
Opinion Date: April 20, 2020
Judge: Harold D. Melton
Areas of Law: Constitutional Law, Criminal Law

Victoria Rickman was convicted by jury of malice murder and a related firearm offense in connection with the shooting death of William Carter, Jr. Rickman and Carter had a tumultuous on-again, off-again relationship with a history of verbal and physical abuse, false accusations of sexual assault, empty threats to obtain temporary protective orders, and numerous calls to 911. In the days leading up to Carter's death, the pair was talking and meeting again despite a recent break-up. On one such 911 call, officers went to Rickman's residence responding to claims shots were fired. Rickman responded holding her small dog, hair wet, and in pajamas. She did not appear to be injured, and nothing in the home looked disturbed or out of place. Rickman told the officers, "he raped me again and I shot him."

Officers found Carter laying face up on the bed naked with multiple gunshot wounds to his body. An autopsy revealed that Carter was shot ten times – four times in the chest, three times in the back, once on the arm, and twice in the head. Rickman's examining physician testified that he found no injuries on Rickman consistent with her description of events, and no signs of trauma to her vaginal cavity. Rickman appealed her convictions, arguing she was denied effective assistance of counsel and that the trial court erred in admitting improper character evidence. Finding no reversible error, the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Robinson v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0265
Opinion Date: April 20, 2020
Judge: Peterson
Areas of Law: Constitutional Law, Criminal Law

Herbert Robinson appealed his convictions for malice murder, armed robbery, and possession of a firearm during the commission of a felony in connection with the death of Michael Moore. On appeal, he argued the trial court erred by allowing the State to use two firearms for demonstrative purposes during trial, and by allowing body-camera footage to be shown at trial. He also argued his trial counsel was ineffective for failing to object to a letter written by Robinson's cellmate being available to the jury for review during deliberations, and for failing to object to a visual aid used by the State during closing arguments. Because Robinson failed to show ineffective assistance of counsel or reversible error by the trial court, the Georgia Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Santana v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0563
Opinion Date: April 20, 2020

Judge: Warren
Areas of Law: Constitutional Law, Criminal Law

Cuevas Carlos Santana was convicted by jury of malice murder and other crimes in connection with the 2010 shooting deaths of Israel Espinoza Mendoza, Vincente Soto Chavez, and Renato Soto Valencia. On appeal, Santana argues that the evidence was insufficient to support his convictions, that the trial court erred by declining to grant Santana a new trial on the general grounds, and that trial counsel provided ineffective assistance. Finding no reversible error, the Georgia Supreme Court affirmed Santana's convictions.

Read Opinion Are you a lawyer? **Annotate this case**.

Sullivan v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0056
Opinion Date: April 20, 2020
Judge: Warren
Areas of Law: Constitutional Law, Criminal Law

A jury convicted Antonio Sullivan of malice murder and other crimes in connection with the shooting death of Wava Benton. On appeal, Sullivan contended his trial counsel was constitutionally ineffective by failing to present evidence at trial to corroborate Sullivan's testimony about prior difficulties between Sullivan and Benton, and by failing to procure expert testimony about Sullivan's mental health—specifically about post-traumatic stress disorder— to be presented to the jury. The Georgia Supreme Court determined Sullivan failed to establish that his trial counsel was deficient in either respect, and therefore affirmed his convictions.

Read Opinion Are you a lawyer? **Annotate this case**.

Turner v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0247
Opinion Date: April 20, 2020
Judge: Warren

Areas of Law: Constitutional Law, Criminal Law

Appellant Ronald Turner appeals from his conviction for malice murder stemming from the stabbing death of William King. The stabbing took place outside an apartment at which Turner had driven in order to trade food for drugs. Turner testified in his own defense at trial and claimed that King hit him in the head with a beer bottle because Turner owed money to King from a prior drug transaction. Turner testified that he tried to get away from King, but that King chased him down and grabbed his jacket. According to Turner, King was getting ready to hit him again when Turner stabbed King in self-defense. Appealing his ultimate conviction, Turner contended he was denied the effective assistance of counsel in three respects. Seeing no reversible error after a review of the trial court record, the Georgia Supreme Court affirmed Turner's conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Valrie v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0380
Opinion Date: April 20, 2020
Judge: Keith R. Blackwell
Areas of Law: Constitutional Law, Criminal Law

Reuben Valrie was tried by jury and convicted of murder and other crimes in connection with the death of his infant daughter Aliyana. Valrie appealed, claiming that he was denied the effective assistance of counsel. Aliyana died as a result of closed head trauma, with a blunt-force abdominal injury as a secondary cause of death, which investigators determined was consistent with being shaken or dropped. At trial, Valrie presented the testimony of four expert witnesses who testified that Aliyana died of natural causes and that the injuries to her brain and abdomen were caused by events such as post-mortem CPR and the “rough” handling of her body by first responders. The jury rejected this defense and found Valrie guilty of murder and the other charges. Valrie contended that his trial lawyer should have raised a hearsay objection to the admission of recorded statements that his girlfriend (and Aliyana's mother) made to police investigators (as well as the testimony of one of those investigators about some of those

statements). Alternatively, Valrie argued that his lawyer should have sought the redaction of certain portions of the recorded statements that impugned his character. The Georgia Supreme Court concluded Valrie failed to present evidence that his trial counsel was deficient, or that he was prejudiced by any alleged failures. According, the Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Williams v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0241
Opinion Date: April 20, 2020
Judge: Keith R. Blackwell
Areas of Law: Constitutional Law, Criminal Law

Richard Williams, II, was tried by jury and convicted of murder in connection with the strangulation death of Cory Robinson. Williams and Robinson were involved in a sexual relationship and had been living together at an extended-stay hotel. Kelvin Spencer was a close friend of both Williams and Robinson. When Spencer met Williams at the hotel room, Williams looked angry and had scratches on his neck. Spencer saw Robinson lying on the floor in a “praying position.” Spencer did not believe Robinson was dead, and he helped Williams move clothes and other things to a U-Haul truck parked outside, in preparation for a move. Williams did not testify or present any evidence. Based on his lawyer’s opening and closing arguments, the defense theory was that Spencer killed Robinson because he was jealous of Williams’s relationship with Robinson. Williams’s sole claim on appeal was that he was denied the effective assistance of counsel when his trial lawyer failed to present as a defense that Williams accidentally killed Robinson during consensual erotic asphyxiation. He argued that his lawyer's discomfort with the topic of homosexual BDSM activity, and his own problems with the Georgia State Bar, precluded presentation of the "true" version of events, and that Williams acceded to the lawyer's defense strategy only "through ignorance and that he did not know that a defense based on consensual erotic asphyxiation was available." Finding no reversible error, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Malave

Court: Supreme Court of Hawaii
Docket: SCWC-18-0000332
Opinion Date: April 20, 2020
Judge: Mark E. Recktenwald
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the intermediate court of appeals (ICA) affirming Defendant's conviction of sexual assault in the first degree on the complaining witness pursuant to Haw. Rev. Stat. 707-730(1)(b), holding that the ICA did not err in affirming the family court. Specifically, the Supreme Court held (1) the jury should have been instructed to determine jurisdictional facts, but the error was harmless beyond a reasonable doubt; and (2) the ICA did not err in finding that there was no rational basis in the record to support providing the jury instruction of the lesser included offense of sexual assault in the third degree.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Malave

Court: Supreme Court of Hawaii
Docket: SCWC-18-0000332
Opinion Date: April 22, 2020
Judge: Mark E. Recktenwald
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the intermediate court of appeals (ICA) affirming the judgment of the family court convicting Defendant on two counts of sexual assault in the first degree, holding that the ICA did not err in affirming the family court. At issue on appeal was the jurisdiction of the family court to try Defendant and the propriety of instructing the jury on a lesser included offense. The ICA affirmed, concluding that the family court had subject matter jurisdiction pursuant to Haw. Rev. Stat. 571-14(a)(1) and that there was no rational basis to support an instruction of the lesser included offense of sexual assault in the third degree. The Supreme Court affirmed, holding (1) although the jury should have been instructed to determine jurisdictional facts, the error was

harmless; and (2) the family court was not obligated to instruct the jury on the lesser included offense of sexual assault in the third degree.

Read Opinion Are you a lawyer? **Annotate this case**.

Idaho v. Burke

Court: Idaho Supreme Court - Criminal
Docket: 46841
Opinion Date: April 22, 2020
Judge: Moeller
Areas of Law: Constitutional Law, Criminal Law

Prior to sentencing, defendant James Burke was committed to the state mental hospital for 56 days to restore him to competency. After being evaluated and deemed competent to proceed to trial, Burke was returned to the county jail and later pleaded guilty pursuant to a plea agreement. At the conclusion of his sentencing hearing, Burke sought credit for the 56 days of time spent in court-ordered commitment. The district court denied the motion, concluding that commitment to a state mental hospital did not fall under the definition of 'incarceration' in Idaho Code section 18-309. After reviewing this issue carefully, the Idaho Supreme Court disagreed with the district court's "thorough and thoughtful analysis," holding that court-ordered commitment to state custody pursuant to Idaho Code sections 18-210 and 18-211 met the functional and legal definition of "incarceration" under Idaho Code section 18-309. "The extent of the liberty interests restricted by Burke's court-ordered commitment to State Hospital North are just too similar to imprisonment to conclude otherwise." Accordingly, the Court reversed the district court's order denying Burke's request for credit for time served and remanded the case for the district court to enter an order crediting him with the fifty-six days he spent committed to State Hospital North while the State restored his competency to face criminal charges.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Gibbs

Court: Iowa Supreme Court
Docket: 18-1298

Opinion Date: April 17, 2020
Judge: Edward M. Mansfield
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction of murder in the second degree, holding that Defendant's Fifth Amendment rights were invaded when the trial judge instructed the jury that Defendant was required to notify law enforcement of his use of deadly force, but the error was harmless. During trial, Defendant asserted the defense of justification in his shooting of the victim. At issue on appeal was whether the district court abused its discretion by giving a jury instruction incorporating the terms of Iowa Code 704.2B. The instruction included a statement that a person using deadly force is required to notify law enforcement about his use of deadly force. Defendant argued before the Supreme Court that both section 704.2B and the jury instruction incorporating that section violated his Fifth Amendment rights. The Supreme Court affirmed, holding (1) instructing the jury that a homicide defendant is required to notify a law enforcement agency of his use of deadly force violates the defendant's Fifth Amendment rights; but (2) any error in this case was harmless beyond a reasonable doubt.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Broxton

Court: Kansas Supreme Court
Docket: 114675
Opinion Date: April 17, 2020
Judge: Stegall
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's convictions for second-degree murder, burglary, and theft but reversed Defendant's sentences, holding that any error during the guilt phase was harmless but that the district court erred by scoring Defendant's prior Florida burglary conviction as a person felony instead of a nonperson felony. On appeal, the court of appeals concluded that a trial court may instruct the jury on felony murder even though the State only charged the defendant with premeditated first degree murder. The Supreme Court disagreed, holding (1) the court of appeals erred in concluding that a district court may elect to provide a felony-murder

instruction when that crime was not charged, and the district court properly found that the felony-murder instruction was not legally appropriate in this case; (2) the district court erred by excluding from evidence an exculpatory document from a Florida homicide investigation on the ground it was not relevant, but the error was harmless; and (3) the district court improperly scored Defendant's prior Florida burglary conviction as a person felony.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Corbin

Court: Kansas Supreme Court
Docket: 119665
Opinion Date: April 17, 2020
Judge: Dan Biles
Areas of Law: Criminal Law

The Supreme Court affirmed the ruling of the district court on remand resentencing Defendant to his original mandatory term of imprisonment after once again finding he was not a person with intellectual disability, holding that the district court did not abuse its discretion when it rejected Defendant's intellectual disability motion and imposed a mandatory term of imprisonment. Defendant pled no contest to first-degree premeditated murder. Before sentencing, Defendant filed a motion pursuant to Kan. Stat. Ann. 21-6622(b) asserting that he was a person with intellectual disability and was thus not subject to a mandatory minimum prison term. The district court denied the motion and sentenced Defendant to a hard twenty-five life sentence. While Defendant's appeal was pending, the Legislature amended Kan. Stat. Ann. 76-12b01(i), which provides new standards for deciding intellectual disability. The Supreme Court reversed and remanded for reconsideration of Defendant's motion using the new criteria. On remand, the district court reaffirmed its earlier ruling and again sentenced Defendant to a hard twenty-five life sentence. The Supreme Court affirmed, holding that the district court's ruling was reasonably based on the law and was supported by substantial competent evidence.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Frazier

Court: Kansas Supreme Court
Docket: 117456
Opinion Date: April 17, 2020
Judge: Wilson
Areas of Law: Criminal Law

The Supreme Court reversed the decision of the district court affirming the judgment of the district court denying Defendant's motion to withdraw plea of no contest to one count of possession of heroin with intent to distribute, holding that the district court's decision in finding no good cause for Defendant to withdraw his plea was based on errors of fact and law, which were grounds for finding abuse of discretion. On appeal, Defendant argued that the district court abused its discretion in denying his motion to withdraw his plea of no contest based on misleading or false statements contained in the plea agreement. The court of appeals affirmed the district court. The Supreme Court reversed, holding (1) there was enough uncertainty in this case to indicate that Defendant's plea agreement was not understandingly made; and (2) therefore, Defendant must be allowed to withdraw his plea.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Harris

Court: Kansas Supreme Court
Docket: 117362
Opinion Date: April 17, 2020
Judge: Wilson
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court reversed the judgment of the court of appeals affirming Defendant's conviction of possession fo marijuana, holding that Defendant's waiver of jury trial was legally insufficient. On appeal, Defendant argued that he did not properly waive his right to a jury and asserted three other issues. The Supreme Court reversed the judgment of the court of appeals affirming Defendant's convictions without addressing the three remaining issues, holding that because the district court failed properly to apprise Defendant of his right to a jury trial and failed to ensure that Defendant understood the nature of the right he was giving up, Defendant's constitutional right to a jury trial was violated in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Uk

Court: Kansas Supreme Court
Docket: 119712
Opinion Date: April 17, 2020
Judge: Wilson
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's conviction for first-degree premeditated murder, holding that the district court did not err in its challenged instructions to the jury. Specifically, the Supreme Court held (1) the district court did not err in refusing to give the jury Defendant's requested instruction on voluntary manslaughter as a lesser included offense of first-degree murder because the instruction was not factually appropriate; and (2) the district court did not commit clear error in issuing an unmodified version of Instruction No. 11, which contained the definition of "premeditation" and mirrored PIK Crim. 4th 54.150(d) because the instruction was legally appropriate.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Catruch

Court: Maine Supreme Judicial Court
Citation: 2020 ME 52
Opinion Date: April 23, 2020
Judge: Andrew M. Mead
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed the judgments of the trial court terminating Appellant's participation in the Co-Occurring Disorders and Veterans Court (Veterans Court), holding that the court did not err or abuse its discretion in terminating Appellant's participation in the Veterans Court. The Veterans Court is a criminal docket that provides judicial monitoring, specialized treatment, and other services for military veterans who have disorders often attributable to their military service. Appellant was charged

with leaving the scene of an accident and three other offenses. Appellant was admitted to the Veterans Court. Agreeing to sentencing outcomes in a plea agreement and entering into a bail contract, Appellant pleaded guilty to all charges against him. The court later terminated Appellant's participation in the Veterans Court, finding that Appellant had violated the conditions of his bail contract. The Supreme Judicial Court affirmed, holding (1) this matter was properly before the Court; and (2) given Appellant's failure to comply with the requirements for participation in the treatment court and his violations of the agreements, his termination from the Veterans Court was warranted.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Paquin

Court: Maine Supreme Judicial Court
Citation: 2020 ME 53
Opinion Date: April 23, 2020
Judge: Andrew M. Mead
Areas of Law: Constitutional Law, Criminal Law

In this appeal from Defendant's conviction for eleven counts of gross sexual misconduct, the Supreme Judicial Court vacated the judgment of conviction on one count, vacated the dismissal of other counts and remanded for entry of a judgment of acquittal on those counts, and affirmed in all other respects, holding that Defendant's convictions on both Counts 5 and 30 violated his double jeopardy protections and that the court erred in allowing the State to dismiss Counts 27, 28, and 29 during trial without Defendant's consent. The indictment charged Defendant with fifteen counts (Counts 1-13, 30-31) of gross sexual misconduct against the victim and sixteen counts (Counts 14-29) of gross sexual misconduct against a second alleged victim. During trial, the court granted Defendant's motion for a judgment of acquittal on Counts 10-13, and the State dismissed Counts 27-29. Defendant was found guilty of Counts 1-9 and 30-31 and not guilty on the remaining counts. The court entered judgment in accordance with the verdict. The Supreme Judicial Court held that the trial court erred in failing to rule that the Double Jeopardy Clause barred convictions on both Counts 5 and 30 and allowing the State to dismiss Counts 27, 28, and 29 rather than entering a judgment of acquittal on those counts.

Read Opinion Are you a lawyer? **Annotate this case**.

Watson v. State

Court: Maine Supreme Judicial Court
Citation: 2020 ME 51
Opinion Date: April 21, 2020
Judge: Joseph Jabar
Areas of Law: Criminal Law

The Supreme Judicial Court vacated the judgment of the unified criminal docket denying Appellant's petition for post-conviction review, holding that Appellant was deprived of the effective assistance of counsel when his trial attorney played a video of the ten-year-old victim's interview with police and that Appellant was adversely affected. Appellant was convicted of two counts of gross sexual assault, one count of unlawful sexual contact, and one count of visual sexual aggression against a child. The Supreme Court affirmed. Appellant later filed a petition for post-conviction review claiming that his trial attorney's representation was deficient because introducing the videotaped recording of the victim's entire interview with law enforcement was unnecessary to provide evidence supporting the victim's potential motive to fabricate the allegations. The post-conviction court denied denied the petition. The Supreme Court vacated the judgment below, holding that trial counsel's conduct was deficient and that counsel's actions rose to the level of comprising the reliability of Appellant's conviction and undermining confidence in it.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. Mazza

Court: Massachusetts Supreme Judicial Court
Docket: SJC-11363
Opinion Date: April 21, 2020
Judge: Budd
Areas of Law: Criminal Law

The Supreme Judicial Court reversed the order of the superior court denying Defendant's motion for a new trial and set aside the jury's verdicts

of first degree murder and robbery, holding that a recently discovered witness statement made to the police ago constituted newly discovered evidence that "would probably have been a real factor in the jury's deliberations." At issue was Defendant's sixth motion for a new trial, which was predicated on newly discovered evidence consisting of, among other things, a recently discovered statement made to the police in 1972. The superior court denied the motion. As to the police statement, the judge found that it did not constitute newly discovered evidence because Defendant failed to establish that defense counsel did not have possession of it at the time of trial. The Supreme Judicial Court reversed and remanded the case for a new trial, holding (1) Defendant sustained his burden of establishing that defense counsel did not have the 1972 police statement prior to or at trial, and therefore, the statement constituted newly discovered evidence; and (2) there was a substantial risk that the jury would have reached a different conclusion had the evidence been admitted at trial.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. McCarthy

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12750
Opinion Date: April 16, 2020
Judge: Gaziano
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Judicial Court affirmed the judgment of the district court denying Defendant's motions to suppress, holding that the limited use of automatic license plate readers (ALPRs) in this case did not implicate constitutional protections against unreasonable searches. While police were investigating Defendant on suspicion of drug distribution they used ALPRs on two bridges to track Defendant's movements. The police accessed historical data via ALPR technology and received real-time alerts, the last of which led to Defendant's arrest. Defendant filed motions to suppress the ALPR data and the fruits of the arrest. The superior court denied the motions. The Supreme Judicial Court affirmed, holding that while the widespread use of ALPRs in the Commonwealth could implicate a defendant's constitutional protected expectation of privacy in the whole of his public movements, that interest was not invaded by the limited extent

and use of the ALPR data in the instant case.

Read Opinion Are you a lawyer? **Annotate this case**.

Garden v. Commonwealth

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12821
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed the judgment of a single justice of the court denying Petitioner's petition for extraordinary relief under Mass. Gen. Laws ch. 211, 3 seeking an order vacating Petitioner's plea to aggravated rape and dismissing the underlying indictment, holding that the single justice did not err or abuse his discretion in denying relief. The issues raised by Petitioner had all been raised and adjudicated through the normal appellate process. Petitioner then filed a motion to withdraw his guilty plea. The motion was denied, and the Appeals Court affirmed. In this petition for extraordinary relief, Petitioner sought an order vacating his plea to aggravated rape and dismissing the underlying indictment. The single justice denied relief. The Supreme Judicial Court affirmed, holding that the superintendence power was not available as an additional layer of appellate review once all other avenues had been exhausted.

Read Opinion Are you a lawyer? **Annotate this case**.

In re Mitchell

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12910
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed the judgment of the county court denying, without a hearing, Petitioner's petition for relief under Mass. Gen. Laws ch. 211, 3, holding that the single justice did not err or abuse his discretion in denying relief. Defendant was convicted of several offenses.

The Appeals Court reversed the convictions and remanded the matter for a new trial. Thereafter, the Commonwealth filed a nolle prosequi as to all the charges. In his Mass. Gen. Laws ch. 211, 3 petition, Defendant alleged that no crime had been committed and that he was wrongfully prosecuted. The single justice denied relief. The Supreme Judicial Court affirmed, holding that Defendant did not demonstrate entitlement to the exercise of this Court's superintendence powers.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Reek

Court: Minnesota Supreme Court
Docket: A19-0153
Opinion Date: April 22, 2020
Judge: G. Barry Anderson
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction for first-degree murder, holding that there was no error in the proceedings below. Specifically, the Supreme Court held (1) Appellant's right to a fair trial before an impartial tribunal was not violated when the district court stated that it might reconsider its prior Spreigl ruling if the defense presented certain witnesses; (2) the jury instructions on accomplice liability were plainly erroneous, but Appellant failed to establish that there was a reasonable likelihood that the error had a significant effect on the verdict; (3) the prosecutor did not commit misconduct in his closing arguments regarding the law of accomplice liability; (4) the district court did not abuse its discretion by granting the State's motion to admit evidence of appellant's past convictions for impeachment purposes, including by allowing the specific convictions to be disclosed to the jury; and (5) Appellant's pro se arguments were without merit.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Woodard

Court: Minnesota Supreme Court
Docket: A18-1886

Opinion Date: April 22, 2020
Judge: Hudson
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the district court convicting Defendant of first-degree murder and sentencing him to life in prison without the possibility of release, holding that the district court did not err in denying Defendant's motion to present an alternative-perpetrator defense. Specifically, the Supreme Court held (1) the district court did not abuse its discretion in holding that Defendant's proffered evidence in support of his motion to present alternative-perpetrator evidence for lack of sufficient foundation; and (2) the district court committed an error that was plain in instructing the jury on the order in which to consider the charges against Defendant, but there was no reasonable likelihood that the instruction affected the jury's verdict and therefore did not affect Defendant's substantial rights.

Read Opinion Are you a lawyer? **Annotate this case**.

Huff v. Brown

Court: Nebraska Supreme Court
Citation: 305 Neb. 648
Opinion Date: April 23, 2020
Judge: Lindsey Miller-Lerman
Areas of Law: Communications Law, Criminal Law

The Supreme Court reversed the portion of the district court's order granting in part a writ of mandamus requiring Doug Brown, the sheriff of Furnas County, to provide records to Herchel Huff pursuant to the public records statutes, holding that the district court erred when it determined that Huff had shown that Brown had a clear duty to provide the requested records. Huff, an inmate, sought, among other documents, the criminal history records of jurors who had convicted hims. Furnas County sheriff Kurt Kapperman required a deposit of $750 before fulfilling the request. Huff subsequently filed a petition for writ of mandamus naming Kapperman as the defendant and seeking an order compelling Kapperman to release all requested documents. The court permitted Huff to substitute Brown, the current sheriff, in the caption of the case in place of Kapperman and granted in part mandamus. The Supreme Court reversed in part, holding that the

district court (1) did not err when it substituted Brown's name for Kapperman's; but (2) erred in issuing mandamus because Huff failed to demonstrate a prima facie case that he had been denied a request for public records that the sheriff had a clear duty to provide under Neb. Rev. Stat. 84-712.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Montoya

Court: Nebraska Supreme Court
Citation: 305 Neb. 581
Opinion Date: April 17, 2020
Judge: Freudenberg
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the judgment of the district court affirming Defendant's conviction and sentence for driving under the influence, holding that there was no error in the challenged rulings by the trial court. Specifically, the Supreme Court held that the district court did not err by (1) affirming the county court's order denying Defendant's motion to suppress fruits of the stop; (2) affirming the county court's order that denied Defendant's motion to suppress the fruits of his arrest; (3) affirming the county court's order that denied Defendant's motion to suppress the results of the test of his breath alcohol content; (4) finding sufficient evidence to support the conviction; and (5) finding that Defendant's sentence was not excessive.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Schroeder

Court: Nebraska Supreme Court
Citation: 305 Neb. 527
Opinion Date: April 17, 2020
Judge: Funke
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's sentence of death for first degree

murder, holding that there was no error in the sentence imposed by the sentencing panel. Specifically, the Supreme Court held that the sentencing panel did not err in (1) allowing the State to introduce evidence on the existence of mitigating circumstances; (2) acknowledging and weighing mitigating evidence from the presentence investigation report; (3) not requesting that documentation from the Department of Correctional Services regarding Defendant's time in custody for mitigation purposes be included in the presentence investigation report; (4) sentencing Defendant to death, where the Legislature has enacted safeguards to ensure fairness and accuracy in the resulting sentence; and (5) finding Defendant should be sentenced to death after balancing the aggravating evidence and mitigating evidence.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Kendrick v. Parker

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1509
Opinion Date: April 21, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals denying Appellant's request for a writ of prohibition and/or mandamus against Montgomery County Court of Common Pleas Judge E. Gerald Parker Jr., holding that the court of appeals correctly determined that Appellant's claim was barred by res judicata. Appellant sought a petition for writ of prohibition and/or mandamus against Judge Erik Blaine, the successor to the judge who sentenced Appellant, alleging that the sentencing court patently and unambiguously lacked jurisdiction to sentence him. Judge Parker, who had succeeded Judge Blaine, subsequently filed a motion for summary judgment. The court of appeals granted summary judgment for Judge Parker, concluding that Appellant failed to demonstrate that the sentencing court patently and unambiguously lacked jurisdiction or that he lacked an adequate remedy at law and that res judicata barred Appellant's claim. The Supreme Court affirmed, holding that Appellant's claim was barred by res judicata.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Nelson v. Russo

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1541
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals dismissing Appellant's petition for a writ of mandamus seeking to compel Cuyahoga County Court of Common Pleas Judge Nancy Margaret Russo to vacate the consecutive prison sentences imposed on Appellant in 1987, holding that Appellant had an adequate remedy at law and was barred from asserting additional claims of sentencing error he could have raised in his previous mandamus action. In 1987, Appellant was convicted of four counts of rape and one count of kidnapping. Appellant was sentenced to prison terms of fifteen to twenty-five years for each of the five counts, to be served consecutively. In 2019, Appellant sought a writ of mandamus to compel Judge Russo to vacate his consecutive sentences. The court of appeals dismissed the writ action, concluding that res judicata barred Appellant's claim and that his prior appeals were an adequate remedy at law to address the alleged defect in his consecutive sentences. The Supreme Court affirmed, holding that Appellant was not entitled to a writ of mandamus in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Roberts v. Marsh

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1540
Opinion Date: April 22, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals dismissing Appellant's original action seeking a writ of procedendo and/or

mandamus to compel Hamilton County Court of Common Pleas Judge Melba Marsh to issue a corrected sentencing entry, holding that the court of appeals correctly dismissed the petition as moot. Appellant was convicted of murder with a repeat-violent-offender specification. Appellant later asked the trial court to correct his sentence, arguing that he had improperly been sentenced to postrelease control. On remand, Judge Marsh vacated the postrelease-control sentence. Appellant appealed that order. The court of appeals noted that the trial court had not set forth all the information required under Crim.R. 32(C) in a single document and dismissed the appeal for lack of a final, appealable order. Appellant then filed this original action seeking to compel Judge Marsh to issue a corrected sentencing entry that constitutes a final, appealable order. Judge Marsh issued a nunc pro tunc sentencing entry that constituted a final, appealable order. The court of appeals then dismissed the petition as moot. The Supreme Court affirmed, holding that because Judge Marsh performed the act Appellant requested, the court of appeals dismissed the petition as moot.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Steiner v. Rinfret

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1510
Opinion Date: April 21, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals dismissing Appellant's petition for a writ of mandamus against Holmes County Court of Common Pleas Judge Robert D. Rinfret, holding that the court of appeals correctly determined that Appellant had an adequate remedy in the ordinary course of the law. Appellant, who was serving consecutive prison terms for five convictions, filed a petition for a writ of mandamus arguing that Judge Rinfret improperly sentenced him to a prison term of nine years for his attempted rape conviction instead of the maximum term of eleven years. The court of appeals dismissed the petition, determining that Appellant had failed to file a mandatory affidavit of his prior civil actions and had an adequate remedy in the ordinary course of the law. The Supreme Court affirmed, holding that relief in mandamus was not

available because Petitioner had an adequate remedy in the ordinary course of the law.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Jeffries

Court: Supreme Court of Ohio
Citation: 2020-Ohio-1539
Opinion Date: April 22, 2020
Judge: Donnelly
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the court of appeals upholding Defendant's convictions of four counts related to two specific instances of sexual abuse of D.S., holding that the trial court and court of appeals correctly applied Ohio's rape-shield law and determined that evidence of D.S.'s prior nonconsensual sexual assault was inadmissible. On appeal, Defendant asserted that the trial court erred in prohibiting him from introducing evidence during trial that D.S. had previously been sexually assaulted by another person, arguing that the rape-shield law applies only to an accuser's prior consensual sexual activity. The lower court held that Ohio's rape-shield law addresses all sexual activity, not only consensual sexual activity. The court of appeals affirmed. The Supreme Court affirmed, holding (1) the plain meaning of the term "sexual activity" as used in the rape-shield law includes both consensual and nonconsensual sexual activity; and (2) therefore, all sexual activity is barred from admission into evidence by the rape-shield, absent certain exceptions listed in the law.

Read Opinion Are you a lawyer? **Annotate this case**.

Pennsylvania v. Britton

Court: Supreme Court of Pennsylvania
Docket: 55 MAP 2018
Opinion Date: April 22, 2020
Judge: Max Baer
Areas of Law: Constitutional Law, Criminal Law

California law enforcement officers interviewed Appellant Stacy Britton in

her California residence and, unbeknownst to her, recorded those interviews. Over Appellant's objection, Pennsylvania used those recordings as evidence to help convict Appellant of murder in Pennsylvania. The Pennsylvania Supreme Court granted allowance of appeal to examine whether the California law enforcement officers were acting as agents of the Pennsylvania State Police when they recorded the interviews with Appellant in her California home, and if so, whether Pennsylvania's constitutional and statutory protections were available to Appellant under those circumstances. The Court concluded the California law enforcement officers were not acting as agents of the Pennsylvania State Police when they interviewed Appellant, making analysis of whether any Pennsylvania-specific constitutional or statutory protections unwarranted. Because the Supreme Court concluded the Pennsylvania trial court reached the proper result in this matter, it affirmed that court's judgment.

Read Opinion Are you a lawyer? **Annotate this case**.

Pennsylvania v. Copenhaver

Court: Supreme Court of Pennsylvania
Docket: 48 MAP 2019
Opinion Date: April 22, 2020
Judge: Thomas G. Saylor
Areas of Law: Constitutional Law, Criminal Law

In August 2015, a deputy sheriff conducted a vehicle stop of Appellant Victor Copenhaver's pickup truck. Upon approaching the truck, the deputy noticed an odor of alcohol and marijuana emanating from the passenger compartment. After administering field sobriety tests, he arrested Appellant for suspected driving under the influence of alcohol and controlled substances ("DUI"). Appellant was ultimately charged with DUI and other offenses. Appellant challenged the deputy's authority to conduct a traffic stop and sought suppression of all evidence obtained during the encounter. Rather than presenting testimony at a suppression hearing, the parties stipulated that Appellant was driving the vehicle in question and that the deputy had training and qualifications equivalent to that of a police officer. The parties also agreed that the vehicle stop occurred as a result of the deputy observing the tailgate to the pickup truck being in a down position, which caught the deputy's attention. The deputy further observed the

registration on the pickup truck was expired, and additionally, the registration number was identified as belonging to a vehicle other than the one on which it was attached. The issue this case presented for the Pennsylvania Supreme Court's review was whether the deputy could lawfully conduct the traffic stop based on the expired registration sticker, on a theory that such a violation amounts to a breach of the peace. The Supreme Court concluded driving a vehicle with an expired registration did not entail a breach of the peace. It vacated the superior court's order insofar as it held that the expired registration was a breach of the peace, thus alone authorizing the deputy to stop Appellant's vehicle. Notably, in light of its holding, the Supreme Court found the superior court did not proceed to consider other relevant questions, such as whether the parties' factual stipulation should have been read as indicating that the officer's understanding that the registration sticker was associated with a different vehicle arose in the pre-stop timeframe – consistent with the Commonwealth's position throughout this litigation. "These issues should be resolved in the first instance by the intermediate court on remand."

Read Opinion Are you a lawyer? **Annotate this case**.

Pennsylvania v. Tedford

Court: Supreme Court of Pennsylvania
Docket: 773 CAP
Opinion Date: April 22, 2020
Judge: Donohue
Areas of Law: Constitutional Law, Criminal Law

Appellant Donald Tedford was convicted of first-degree murder and rape on February 6, 1987. He appealed the dismissal of his second petition for relief filed pursuant to the Post Conviction Relief Act ("PCRA"), on December 2, 2014, as amended by a counseled petition on May 5, 2015, and a supplemental petition filed on June 9, 2015. In connection with his initial filings, Tedford sought wholesale discovery of the prosecution's entire file, but the PCRA court concluded that the petition (as amended) was not timely filed. Tedford also appealed the PCRA court's order denying his supplemental PCRA petition, in which he requested discovery, an evidentiary hearing, and/or a new trial based upon the admission of expert testimony presented at trial related to microscopic hair analysis. The PCRA

court concluded that pursuant to PCRA Section 9545(b)(1)(ii), it had jurisdiction to consider the merits of Tedford's newly-discovered-facts claims, but ultimately it concluded Tedford had not asserted a meritorious claim in accordance with Section 9543(a)(2)(vi). Finding no reversible error in that analysis, the Pennsylvania Supreme Court affirmed dismissal of the petition for relief.

Read Opinion Are you a lawyer? **Annotate this case**.

Pennsylvania v. Trahey

Court: Supreme Court of Pennsylvania
Docket: 38 EAP 2018
Opinion Date: April 22, 2020
Judge: Wecht
Areas of Law: Constitutional Law, Criminal Law

The trial court granted Timothy Trahey's motion to suppress the results of a blood test that revealed his blood alcohol concentration ("BAC"), finding no justification for the investigating officers' failure to obtain a search warrant before conducting the test. On the Commonwealth's appeal, the Superior Court reversed, opining that the Commonwealth's evidence sufficiently established the existence of exigent circumstances, thus excusing the absence of a warrant. The Pennsylvania Supreme Court reversed, finding that while the exigency analysis is an objective one, "even disregarding the officers' subjective motivations, or their candid acknowledgment that they would have obtained a search warrant if they thought it necessary, there was no time-sensitive need to conduct a warrantless blood test under the circumstances of this case. Accordingly, the Superior Court's conclusion that the test was justified by exigent circumstances was drawn in error."

Read Opinion Are you a lawyer? **Annotate this case**.

In re Greg Abbott

Court: Supreme Court of Texas
Docket: 20-0291
Opinion Date: April 23, 2020
Judge: Per Curiam

Areas of Law: Constitutional Law, Criminal Law

The Supreme Court conditionally granted mandamus relief to the State seeking review of a temporary restraining order (TRO) blocking enforcement of Executive Order GA-13, which changes the rules applicable to judges' decisions regarding pre-trial bail, against judges, holding that the trial court lacked jurisdiction to order the judges' requested relief, even temporarily. GA-13 suspends certain statutes authorizing trial judges to release jail inmates with violent histories during the state of disaster due to the threat of the novel coronavirus. Plaintiffs alleged that GA-13 is unconstitutional and exceeds the governor's statutory emergency powers. Sixteen of the plaintiffs were Texas trial judges alleging that GA-13 improperly interferes with their judicial authority to make individualized bail decisions, and the other plaintiffs were public interest organizations and lawyer associations. The trial court issued a TRO blocking enforcement of GA-13 against judges. The Supreme Court conditionally granted mandamus relief, holding that the alleged threat of a criminal prosecution in this case did not give the judges standing to seek the invalidation of GA-13, and therefore, the trial court lacked jurisdiction to order their requested relief.

Read Opinion Are you a lawyer? **Annotate this case**.

Stahmann v. Texas

Court: Texas Court of Criminal Appeals
Docket: PD-0556-18
Opinion Date: April 22, 2020
Judge: Barbara Hervey
Areas of Law: Constitutional Law, Criminal Law

Appellant Karl Stahmann was involved in an automobile accident, after which he threw a bottle of promethazine, a controlled substance, over a nearby wire fence before law enforcement arrived. The bottle landed two to three feet past the fence in plain view. He was convicted of third-degree felony tampering with physical evidence and was sentenced to 10 years' confinement and fined $5,000. The judge suspended his sentence and placed him on community supervision for 10 years. Stahmann appealed, arguing in part that the evidence was insufficient to prove that he destroyed, altered, or concealed the prescription bottle. The court of appeals agreed

that the evidence was insufficient, but instead of rendering an acquittal, it reformed the judgment to show that Stahmann was convicted of the lesser-included offense of attempted tampering with physical evidence, a state-jail felony. After review of the evidence presented at trial, the Texas Court of Criminal Appeals concluded the evidence was indeed insufficient to prove that Appellant altered the prescription pill bottle when he threw it over the fence because the mere act of throwing the bottle did not change the bottle itself. "While a rational jury could have reasonably inferred that Stahmann intended to conceal the pill bottle when he threw it over the wire fence, the evidence shows that he failed to conceal it as he intended because the bottle landed short of the bush in plain view on top of some grass." The Court affirmed the trial court's judgment.

Read Opinion Are you a lawyer? **Annotate this case**.

Blanke v. Board of Pardons & Parole

Court: Utah Supreme Court
Citation: 2020 UT 16
Opinion Date: April 16, 2020
Judge: Himonas
Areas of Law: Criminal Law

The Supreme Court affirmed the decision of the court of appeals affirming the district court's denial of Appellant's petition for extraordinary relief, holding that, under the circumstances, the Utah Board of Pardons and Parole need not afford Appellant the due process protections explained in Neese v. Utah Board of Pardons and Parole, 416 P.3d 663 (2017), before it could determine that Appellant was a sex offender and condition his parole on sex offender treatment. Appellant was serving a prison sentence for his convictions of attempted child kidnapping and kidnapping. Because he was convicted of attempted child kidnapping Appellant was considered a sex offender under the sex offender registration statute. Further, Appellant admitted in his presentence report that he had sexual intercourse with a fifteen-year-old. Appellant filed a petition for extraordinary relief alleging that the Parole Board had violated his due process rights by conditioning his parole on completion of sex offender treatment even though he had not committed a sex offense. Summary judgment was granted for the Parole Board. The Supreme Court affirmed, holding that the Parole Board owed

Appellant no additional process before it considered unconnected sex offenses in its decision to require Appellant to undergo sex offender treatment.

Read Opinion Are you a lawyer? **Annotate this case**.

Washington v. Escalante

Court: Washington Supreme Court
Docket: 97268-1
Opinion Date: April 23, 2020
Judge: Steven González
Areas of Law: Constitutional Law, Criminal Law

Alejandro Escalante was detained for hours in a secured area at a border crossing and, the State conceded, interrogated by federal agents without Miranda warnings. Statements he made during that interrogation were used by the State to convict him of drug possession. While a traveler briefly detained and questioned at the border was typically not "in custody" for Miranda purposes, "the government's power to detain and question people at the border without implicating Miranda has limits." Here, the Washington Supreme Court determined those limits were reached. "This border detention created the type of inherently coercive environment that demands Miranda warnings to ensure an individual's choice to speak is the product of free will." The Supreme Court held that Escalante was in custody when he was interrogated and reversed.

Read Opinion Are you a lawyer? **Annotate this case**.

Washington v. Haggard

Court: Washington Supreme Court
Docket: 97375-0
Opinion Date: April 23, 2020
Judge: Barbara Madsen
Areas of Law: Constitutional Law, Criminal Law

A class C felony "washes out" and is omitted from a defendant's offender score as long as he or she is not convicted of any crime within five years of the last date of release from confinement. David Haggard was convicted of

a misdemeanor offense within this five-year period, which was dismissed pursuant to RCW 3.66.067. When Haggard later pleaded guilty to burglary and arson, the trial court included prior class C felonies in his criminal history, finding that the dismissed misdemeanor conviction interrupted the washout period for those offenses. Haggard contended on appeal this was error. The Washington Supreme Court determined that because a dismissed conviction constituted a "conviction" under the Sentencing Reform Act of 1981 (SRA), and misdemeanor dismissal and vacation were distinct processes, so Haggard's offender score was properly calculated.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Taylor

Court: Supreme Court of Appeals of West Virginia
Docket: 18-0502
Opinion Date: April 21, 2020
Judge: Walker
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the judgment of the circuit court giving Petitioner credit for twelve days of time served toward the sentence he received for his felony conviction although Petitioner spent additional time in confinement for other charges that were dismissed in the universal plea agreement, holding that to grant Petitioner additional credit for time served would do little more than reward Petitioner for habitual criminal behavior. Petitioner was charged with several crimes and agreed to resolve the pending charges against him in a universal plea agreement. Under the terms of the agreement, Petitioner agreed to plea guilty to the charge of felony carrying a concealed firearm by a prohibited person. In exchange, the State agreed to drop the remaining charges. After he was sentenced, Petitioner argued that, in addition to the twelve days of credit for time served he was granted, he was constitutionally entitled to credit for time served while he was incarcerated for charges that were resolved in the universal plea agreement. The Supreme Court affirmed, holding that Petitioner's circumstances implicated neither double jeopardy nor equal protection of the law such that additional credit for time served was constitutionally mandated.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Harrison

Court: Wisconsin Supreme Court
Dockets: 2017AP002441-CR, 2017AP002440-CR
Opinion Date: April 17, 2020
Judge: Patience D. Roggensack
Areas of Law: Criminal Law

The Supreme Court affirmed in part and reversed in part the decision of the court of appeals reversing an order of the circuit court that granted sentence credit to Defendant, holding that the court of appeals correctly found that Defendant was not entitled to sentence credit but erred by advancing the commencement of Defendant's terms of extended supervision for Defendant's 2007 and 2008 cases. Specifically, the Court held (1) Defendant was not entitled to sentence credit under Wis. Stat. 973.155(1)(a) because the days he spent in custody for which he sought sentence credit were not in connection with the courses of conduct for which those sentences were imposed; and (2) the court of appeals erred by advancing the commencement of Defendant's terms of extended supervision for his 2007 and 2008 cases to the date they would have begun but for Defendant's confinement for unrelated convictions that were later set aside, holding that whether to employ advancement is a public policy decision best left to the legislature.

Read Opinion Are you a lawyer? **Annotate this case**.

About Justia Opinion Summaries

Justia Weekly Opinion Summaries is a free service, with 63 different newsletters, each covering a different practice area.

Justia also provides 68 daily jurisdictional newsletters, covering every federal appellate court and the highest courts of all US states.

All daily and weekly Justia newsletters are free. Subscribe or modify your newsletter subscription preferences at daily.justia.com.

You may freely redistribute this email in whole.

About Justia

Justia is an online platform that provides the community with open access to the law, legal information, and lawyers.

Contact Us | Privacy Policy

Unsubscribe From This Newsletter
or unsubscribe from all Justia newsletters immediately **here.**

Justia | 1380 Pear Ave #2B, Mountain View, CA 94043

From: Criminal Law - Justia Weekly Opinion Summaries
To: Sullivan, Kristen (POL)
Subject: Latest 111 Cases This Week: Kelly v. United States (U.S.), Gomes v. Silva (1st Cir.), United States v. Perez-Couvertier (1st Cir.)
Date: Friday, May 8, 2020 9:07:28 AM

If you are unable to see this message, click here to view it in a web browser.

Justia Weekly Opinion Summaries

Criminal Law
May 8, 2020

Table of Contents

Kelly v. United States
Criminal Law, Government & Administrative Law, White Collar Crime
US Supreme Court

Gomes v. Silva
Civil Rights, Constitutional Law, Criminal Law

US Court of Appeals for the First Circuit

United States v. Perez-Couvertier
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the First Circuit

United States v. Haverkamp
Criminal Law
US Court of Appeals for the Second Circuit

United States v. Mladen
Criminal Law, Trusts & Estates
US Court of Appeals for the Second Circuit

United States v. Richardson
Criminal Law
US Court of Appeals for the Second Circuit

United States v. Rosemond
Criminal Law
US Court of Appeals for the Second Circuit

United States v. Lacerda
Criminal Law, White Collar Crime
US Court of Appeals for the Third Circuit

Cucalon v. Barr
Criminal Law, Immigration Law
US Court of Appeals for the Fourth Circuit

United States v. Doctor
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Lewis
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Jordan
Criminal Law
US Court of Appeals for the Fifth Circuit

United States v. Longoria
Criminal Law
US Court of Appeals for the Fifth Circuit

United States v. McNabb
Criminal Law
US Court of Appeals for the Fifth Circuit

Andrews v. Wayne County
Civil Rights, Constitutional Law, Criminal Law

US Court of Appeals for the Sixth Circuit

Hicks v. Scott
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Sixth Circuit

Moody v. United States
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Sixth Circuit

United States v. Foreman
Criminal Law
US Court of Appeals for the Sixth Circuit

United States v. Smith
Criminal Law
US Court of Appeals for the Sixth Circuit

Kirkman v. Thompson
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

Tuduj v. Newbold
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

United States v. Gibson
Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

United States v. Howell
Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

United States v. Lewis
Criminal Law
US Court of Appeals for the Seventh Circuit

Bakor v. Barr
Criminal Law, Immigration Law
US Court of Appeals for the Eighth Circuit

Smith v. Titus
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Becerra
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Haynes
Criminal Law

US Court of Appeals for the Eighth Circuit

United States v. Roberts
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Wright
Criminal Law
US Court of Appeals for the Eighth Circuit

Benson v. Chappell
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Ninth Circuit

Mero v. Barr
Criminal Law, Immigration Law
US Court of Appeals for the Ninth Circuit

Romero-Millan v. Barr
Criminal Law
US Court of Appeals for the Ninth Circuit

United States v. Yang
Criminal Law
US Court of Appeals for the Ninth Circuit

United States v. Neugin
Constitutional Law, Criminal Law
US Court of Appeals for the Tenth Circuit

United States v. Ramon
Constitutional Law, Criminal Law
US Court of Appeals for the Tenth Circuit

United States v. Richards
Constitutional Law, Criminal Law
US Court of Appeals for the Tenth Circuit

Andrews v. Warden
Criminal Law
US Court of Appeals for the Eleventh Circuit

Hollis v. United States
Criminal Law
US Court of Appeals for the Eleventh Circuit

Knight v. Florida Department of Corrections
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Eleventh Circuit

United States v. Evans
Criminal Law

US Court of Appeals for the Eleventh Circuit

United States v. McLellan
Criminal Law
US Court of Appeals for the Eleventh Circuit

United States v. Russell
Criminal Law
US Court of Appeals for the Eleventh Circuit

Welch v. United States
Criminal Law
US Court of Appeals for the Eleventh Circuit

State v. Trujillo
Constitutional Law, Criminal Law
Arizona Supreme Court

Barnett v. State
Criminal Law
Arkansas Supreme Court

Mason v. Kelley
Criminal Law
Arkansas Supreme Court

Ray v. Kelley
Criminal Law
Arkansas Supreme Court

Walker v. Kelley
Criminal Law
Arkansas Supreme Court

People v. Flores
Civil Rights, Constitutional Law, Criminal Law
Supreme Court of California

California v. Law
Constitutional Law, Criminal Law
California Courts of Appeal

California v. Sanchez
Constitutional Law, Criminal Law
California Courts of Appeal

Galeotti v. International Union of Operating Engineers
Criminal Law, Labor & Employment Law, White Collar Crime
California Courts of Appeal

In re I.A.
Criminal Law, Juvenile Law

California Courts of Appeal

People v. Edwards
Criminal Law
California Courts of Appeal

People v. Thomkins
Criminal Law
California Courts of Appeal

People v. Torres
Criminal Law
California Courts of Appeal

People v. Triplett
Criminal Law
California Courts of Appeal

Colorado In Interest of G.S.S.
Constitutional Law, Criminal Law, Juvenile Law
Colorado Supreme Court

Barringer v. Halkitis
Criminal Law
Florida Supreme Court

Franqui v. State
Criminal Law
Florida Supreme Court

Hicks v. State
Criminal Law
Florida Supreme Court

Burley v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Carter v. Georgia
Construction Law, Criminal Law
Supreme Court of Georgia

Clarke v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Collins v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Dawson v. Georgia
Constitutional Law, Criminal Law

Supreme Court of Georgia

Evans v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Hill v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Oliver v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Rosser v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Spencer v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Styles v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Whitehead v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Idaho v. Blythe
Constitutional Law, Criminal Law
Idaho Supreme Court - Criminal

Idaho v. Glodowski
Constitutional Law, Criminal Law
Idaho Supreme Court - Criminal

Idaho v. Jones
Constitutional Law, Criminal Law
Idaho Supreme Court - Criminal

State v. Gordon
Civil Rights, Constitutional Law, Criminal Law
Iowa Supreme Court

State v. Craig
Criminal Law
Kansas Supreme Court

State v. Lemmie
Criminal Law

Kansas Supreme Court

State v. Mullen
Criminal Law
Maine Supreme Judicial Court

Commonwealth v. Billingslea
Civil Rights, Constitutional Law, Criminal Law
Massachusetts Supreme Judicial Court

Commonwealth v. Martin
Civil Rights, Constitutional Law, Criminal Law
Massachusetts Supreme Judicial Court

Commonwealth v. Tavares
Criminal Law
Massachusetts Supreme Judicial Court

State v. Branch
Criminal Law
Minnesota Supreme Court

Galloway v. Mississippi
Constitutional Law, Criminal Law
Supreme Court of Mississippi

City of Missoula v. Zerbst
Civil Rights, Constitutional Law, Criminal Law
Montana Supreme Court

State v. Degarmo
Civil Rights, Constitutional Law, Criminal Law
Nebraska Supreme Court

People v. Holz
Civil Rights, Constitutional Law, Criminal Law
New York Court of Appeals

People v. Maffei
Civil Rights, Constitutional Law, Criminal Law
New York Court of Appeals

State v. Bailey
Civil Rights, Constitutional Law, Criminal Law
North Carolina Supreme Court

State v. Ellis
Civil Rights, Constitutional Law, Criminal Law
North Carolina Supreme Court

State v. Hobbs
Civil Rights, Constitutional Law, Criminal Law

North Carolina Supreme Court

State v. Mylett
Criminal Law
North Carolina Supreme Court

Dodge v. North Dakota
Constitutional Law, Criminal Law
North Dakota Supreme Court

Hewitt v. NDDOT
Criminal Law, Government & Administrative Law
North Dakota Supreme Court

Kastet v. NDDOT
Criminal Law, Government & Administrative Law
North Dakota Supreme Court

North Dakota v. Dahl
Constitutional Law, Criminal Law
North Dakota Supreme Court

North Dakota v. Foster
Constitutional Law, Criminal Law
North Dakota Supreme Court

North Dakota v. Kolstad
Constitutional Law, Criminal Law
North Dakota Supreme Court

North Dakota v. Michel
Constitutional Law, Criminal Law
North Dakota Supreme Court

North Dakota v. Wayland
Constitutional Law, Criminal Law
North Dakota Supreme Court

Schwindt v. Sorel
Constitutional Law, Criminal Law, Government & Administrative Law
North Dakota Supreme Court

State ex rel. McDougald v. Greene
Criminal Law
Supreme Court of Ohio

State ex rel. Parker Bey v. Byrd
Criminal Law
Supreme Court of Ohio

State v. Dangler
Criminal Law

Supreme Court of Ohio

Oregon v. Haji
Constitutional Law, Criminal Law
Oregon Supreme Court

South Carolina v. Durant
Constitutional Law, Criminal Law
South Carolina Supreme Court

South Carolina v. Perry
Constitutional Law, Criminal Law
South Carolina Supreme Court

South Carolina v. Quinn
Constitutional Law, Criminal Law, White Collar Crime
South Carolina Supreme Court

Texas v. Arellano
Constitutional Law, Criminal Law
Texas Court of Criminal Appeals

COVID-19 Updates: Law & Legal Resources Related to Coronavirus

Click here to remove Verdict from subsequent Justia newsletter(s).

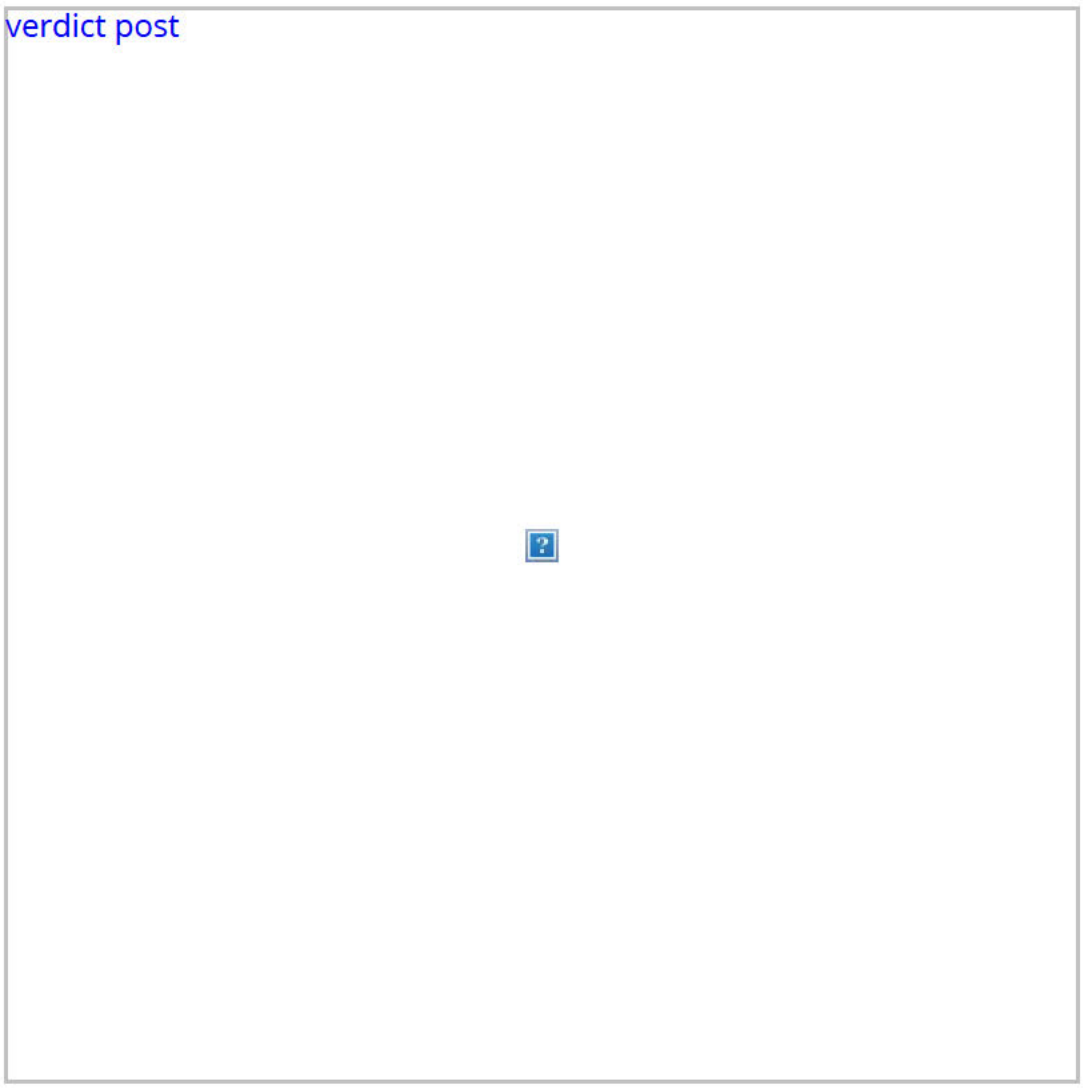
New on Verdict

Legal Analysis and Commentary

Department of Justice Once Again Proves Its Loyalty to the President, Not the Rule of Law

AUSTIN SARAT

verdict post



Austin Sarat—Associate Provost, Associate Dean of the Faculty, and William Nelson Cromwell Professor of Jurisprudence and Political Science at Amherst College—comments on the recent news that the Justice Department will seek dismissal of charges against Michael Flynn. Sarat suggests that because the decision does not seem to advance the fair administration of justice in this case, the court should take the unusual step of refusing to grant the prosecutor's motion to dismiss.

Read More

Criminal Law Opinions

Kelly v. United States

Court: US Supreme Court
Docket: 18-1059
Opinion Date: May 7, 2020
Judge: Elena Kagan
Areas of Law: Criminal Law, Government & Administrative Law, White Collar Crime

During former New Jersey Governor Christie's 2013 reelection campaign, Fort Lee's mayor refused to endorse Christie. Kelly, Christie's Deputy Chief of Staff, Port Authority Deputy Executive Director, Baroni, and another official decided to reduce from three to one the number of lanes reserved at the George Washington Bridge's toll plaza for Fort Lee's commuters. To disguise the political retribution, the lane realignment was said to be for a traffic study. Port Authority traffic engineers were asked to collect some numbers. An extra toll collector was paid overtime. The lane realignment caused four days of gridlock, ending only when the Port Authority's Executive Director learned of the scheme. The Third Circuit affirmed the convictions of Baroni and Kelly for wire fraud, fraud on a federally funded program, and conspiracy to commit those crimes. The Supreme Court reversed. The scheme did not aim to obtain money or property. The wire fraud statute refers to "any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses," 18 U.S.C. 1343. The federal-program fraud statute bars "obtain[ing] by fraud" the "property" (including money) of a federally funded program or entity, section 666(a)(1)(A). The statutes are limited to the protection of property rights and do not authorize federal prosecutors to set standards of good government. The Court rejected arguments that the defendants sought to take control of the Bridge's physical lanes or to deprive the Port Authority of the costs of compensating employees. Their realignment of the access lanes was an exercise of regulatory power; a scheme to alter a regulatory choice is not one to take government property. The time and labor of the employees were an incidental byproduct of that regulatory object. Neither defendant sought to obtain the services that the employees provided.

Read Opinion Are you a lawyer? **Annotate this case**.

Gomes v. Silva

Court: US Court of Appeals for the First Circuit
Docket: 19-1656

Opinion Date: May 1, 2020
Judge: Stahl
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The First Circuit affirmed the judgment of the district court denying Appellant's petition for a writ of habeas corpus, holding that, under the highly deferential standard prescribed by the Antiterrorism and Effective Death Penalty Act for federal habeas review of state criminal convictions, Appellant's claims to habeas relief failed. Appellant was convicted in a Massachusetts superior court of murder in the first degree and related crimes. The Supreme Judicial Court (SJC) affirmed the convictions. Appellant subsequently petitioned the District Court for the District of Massachusetts for a writ of habeas corpus. The district court denied the petition but granted a certificate of appealability. The First Circuit affirmed, holding (1) sufficient evidence supported Appellant's conviction for first-degree murder as a joint venturer, and the SJC's sufficiency determination was not unreasonable; and (2) the SJC reasonably determined that the trial court's admission into evidence of certain items did not constitute error.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Perez-Couvertier

Court: US Court of Appeals for the First Circuit
Docket: 16-2186
Opinion Date: May 7, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The First Circuit affirmed Defendant's conviction of possessing with intent to distribute controlled substances in a protected area and conspiring to distribute controlled substances in a protected area, holding that the district court did not plainly err with respect to any of Defendant's challenges. Specifically, the First Circuit held (1) the district court did not commit plain error in admitting evidence of the conspiracy's activities occurring after he withdrew from the conspiracy or, alternatively, in not instructing the jury to ignore such evidence; (2) the district court did not plainly err in admitting evidence of a drug trafficking organization's violent acts; and (3) the delay between Defendant's indictment and arrest did not violate his Sixth Amendment right to a speedy trial.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Haverkamp

Court: US Court of Appeals for the Second Circuit
Docket: 18-3735
Opinion Date: May 4, 2020
Judge: Barrington D. Parker
Areas of Law: Criminal Law

Defendant pleaded guilty to one count of distribution and receipt of child pornography and one count of possession of child pornography. The district court sentenced him to 121 months of imprisonment, followed by five years of supervised release, and imposed a $200 mandatory special assessment under 18 U.S.C. 3013, as well as a $10,000 assessment under 18 U.S.C. 3014. The Second Circuit held that the district court did not abuse its discretion in sentencing defendant and his sentence was substantively reasonable. The court held that the text of the Justice for Victims of Trafficking Act (JVTA), 18 U.S.C. 3014, taken as a whole and in its context, is straightforwardly meant to be applied on a per-offender, not a per-count, basis. In this case, the district court erroneously applied the special assessment on a per-count, rather than per-offender, basis. Finally, the court held that the computer monitoring condition in question was reasonably related to the nature of defendant's offense. Accordingly, the court affirmed in part, vacated in part, and remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Mladen

Court: US Court of Appeals for the Second Circuit
Docket: 18-0616
Opinion Date: May 6, 2020
Judge: Amalya Lyle Kearse
Areas of Law: Criminal Law, Trusts & Estates

After defendant died while his appeal was pending, counsel moved for

abatement of all incidents of the prosecution, requesting that the appeal be dismissed without a decision on the merits, that defendant's conviction be vacated, and that the matter be remanded to the district court with instructions to dismiss the indictment and order repayment to defendant's estate of the $20,000 fine and $100 special assessment. Because defendant was convicted upon his plea of guilty, and he neither did nor was permitted to challenge on appeal the merits of his conviction, the Second Circuit denied as without merit so much of the motion as seeks (1) vacatur of his conviction, (2) dismissal of the count of the indictment on which he was convicted, and (3) repayment of the mandatory $100 special assessment. The court granted so much of the motion as requests dismissal of this appeal and a remand to the district court for vacatur of the imposed terms of imprisonment and supervised release and for an order requiring that the paid fine of $20,000 be repaid to defendant's estate.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Richardson

Court: US Court of Appeals for the Second Circuit
Docket: 19-412
Opinion Date: May 5, 2020
Judge: Menashi
Areas of Law: Criminal Law

The Second Circuit affirmed defendant's conviction for distribution and possession with intent to distribute a controlled substance. The court held that the district court did not procedurally err by applying the career offender sentencing enhancement pursuant to USSG 4B1.1 because defendant's prior convictions of conspiracy to distribute a controlled substance in violation of 21 U.S.C. 841(a)(1) and 846, and attempted criminal possession of a controlled substance in violation of N.Y. Penal Law 220.16(1), qualify as controlled substance offenses, as defined in USSG 4B1.2(b). The court also held that the district court did not substantively err in sentencing defendant, because it properly considered his criminal history and accounted for his need for mental health and substance abuse treatment.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Rosemond

Court: US Court of Appeals for the Second Circuit
Docket: 18-3561
Opinion Date: May 1, 2020
Judge: Chin
Areas of Law: Criminal Law

The Second Circuit affirmed defendant's conviction for murder-for-hire, conspiracy to commit murder-for-hire, murder through use of a firearm, and possession of a firearm during a murder-for-hire conspiracy. Defendant owned Czar Entertainment, a music management company that represented hip-hop, rap and R&B artists such as Jayceon Taylor, also known as "The Game." Taylor was a member of G-Unit, a rap group run by Curtis Jackson, also known as "50 Cent." Defendant's crimes stemmed from a rivalry with Violator Records, the company that managed G-Unit. The court rejected defendant's contention that his attorney was ineffective because he conceded that defendant paid for the victim to be shot, even though he told counsel not to make this concession. The court held that defendant failed to show that this was objectively unreasonable or that he would have been found not guilty had a different argument been advanced. In this case, there was ample evidence supporting counsel's strategy to concede that defendant ordered a shooting where, among other things, the government's key witness, who participated in the conspiracy and lured the victim to be shot, testified that defendant agreed to pay the shooter. The court also held that the district court did not abuse its broad discretion by admitting prior bad-act evidence under Federal Rule of Evidence 404(b)(1).

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Lacerda

Court: US Court of Appeals for the Third Circuit
Docket: 15-2812
Opinion Date: May 5, 2020
Judge: Porter
Areas of Law: Criminal Law, White Collar Crime

VOG billed itself as an advocacy group helping victims of timeshare fraud get out of their timeshare debts. A jury determined that VOG had actually

defrauded its customers and that three individual defendants (including Lacerda) were each knowing participants in that fraud. Lacerda was sentenced to 324 months' imprisonment for his leading role in the fraudulent enterprise. The Third Circuit affirmed the respective convictions and sentences. The court rejected a claim of impermissible "overview testimony" by an FBI agent; an officer who is familiar with an investigation or was personally involved may tell the story of that investigation—how the investigation began, who was involved, and what techniques were used, and, with a proper foundation, may offer lay opinion testimony and testify about matters within his personal knowledge. The district court did not abuse its discretion when it disqualified defense counsel based on a conflict of interest; when it denied replacement counsel's motion for a continuance; when it excluded from evidence, as hearsay, an email sent by Lacerda to VOG's former CFO; in exercising its sentencing discretion; or by ordering the forfeiture of all VOG's gross proceeds.

Read Opinion Are you a lawyer? **Annotate this case**.

Cucalon v. Barr

Court: US Court of Appeals for the Fourth Circuit
Dockets: 18-1292, 18-2206
Opinion Date: May 7, 2020
Judge: Barbara Milano Keenan
Areas of Law: Criminal Law, Immigration Law

The Fourth Circuit denied petitions for review of the BIA's final order of removal. Applying the modified categorical approach, the court held that defendant's prior conviction for distribution of cocaine under Virginia Code 18.2-248, including distribution of that substance as an accommodation under Virginia Code 18.2-248(D), satisfies the federal definitions of an "aggravated felony" and of a crime "relating to a controlled substance" pursuant to 8 U.S.C. 1227(a)(2)(A)(iii), 1227(a)(2)(B)(i). The court also held that the district court did not abuse its discretion in denying petitioner's motion to reconsider.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Doctor

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-4874
Opinion Date: May 4, 2020
Judge: Roger L. Gregory
Areas of Law: Criminal Law

The Fourth Circuit affirmed the district court's revocation of defendant's supervised release and resulting sentence. The court held that the district court did not clearly err in finding the government proved he committed the assault underlying the supervised release violation; the district court did not commit plain error by adopting the violation report when announcing defendant committed Violation One; and, even if the district court erred in sentencing defendant for a Grade A violation, the error was harmless.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Lewis

Court: US Court of Appeals for the Fourth Circuit
Docket: 19-4028
Opinion Date: May 4, 2020
Judge: Barbara Milano Keenan
Areas of Law: Criminal Law

Defendant was convicted for possessing a firearm as a felon and sentenced to 63 months' imprisonment and a three-year period of supervised release. The district court additionally recommended, without explanation, that defendant receive addiction treatment while incarcerated and ordered, as a special condition of his supervised release, that defendant participate in an addiction treatment program. The Fourth Circuit held that defendant's sentence is procedurally unreasonable because the district court failed to provide an adequate explanation for imposing as a special condition of supervised release the requirement of addiction treatment. The court also held that the district court failed to address defendant's nonfrivolous mitigation arguments. Therefore, the court remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Jordan

Court: US Court of Appeals for the Fifth Circuit
Docket: 19-40499
Opinion Date: May 1, 2020
Judge: Jennifer Walker Elrod
Areas of Law: Criminal Law

The Fifth Circuit affirmed the district court's grant of defendants' motion for a new trial on the basis of prejudicial outside influence on the jury. The court held that the district court did not abuse its broad discretion in granting the motion for a new trial without holding an evidentiary hearing. To the extent there is a bright-line rule applicable to allegations of outside influence on the jury, the court held that it was not applicable to this case. Furthermore, the district court did not abuse its discretion in exercising its prerogative, within broadly defined parameters, to handle the allegation of outside influence in the least disruptive manner possible in this unusual case. Finally, the district court permissibly concluded that the evidence showed a sufficient likelihood of prejudice to shift the burden to the Government, and that the Government did not (and could not) show "no reasonable possibility that the jury's verdict was influenced by" the CSO's comments.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Longoria

Court: US Court of Appeals for the Fifth Circuit
Docket: 19-20201
Opinion Date: May 5, 2020
Judge: Gregg Costa
Areas of Law: Criminal Law

The Fifth Circuit held that the base offense level of 20 was proper for defendant's felon-in-possession crime involving a semiautomatic firearm that is capable of accepting a large capacity magazine. In this case, defendant failed to show that the district court clearly erred in relying on the FBI's agent statement about what was found in the apartment. The court clarified any confusion and held that the 2013 amendment to the commentary on the acceptance-of-responsibility Guideline does not clearly overrule its caselaw allowing the government to withhold the third point for

acceptance of responsibility when it must litigate a suppression motion. The court held that Amendment 775 does not contain the unequivocal override needed to get past the court's precedent. Therefore, the court affirmed defendant's sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. McNabb

Court: US Court of Appeals for the Fifth Circuit
Docket: 19-50265
Opinion Date: May 1, 2020
Judge: Costa
Areas of Law: Criminal Law

The Fifth Circuit affirmed defendant's sentence imposed after he pleaded guilty to possessing a gun after having been convicted of a felony. The court held that defendant is not entitled to relief on his claim that the government breached the plea deal, and thus his appellate waiver remains enforceable. Accordingly, defendant's challenges to his sentence must be dismissed.

Read Opinion Are you a lawyer? **Annotate this case**.

Andrews v. Wayne County

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-1992
Opinion Date: May 4, 2020
Judge: Suhrheinrich
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Canton Police received a 911 call from Andrews, who stated that his fiance, White, had physically attacked him. Officers arrested White. Andrews later took White's medications to the jail; a “KOP” policy allows inmates to keep certain drugs for self-administration. During an intake interview, White admitted to attempting to harm herself or commit suicide in the past but said she was not thinking of harming herself or having suicidal thoughts. An R.N. later evaluated White for nearly two hours, reported White’s chief complaints were “anxiety and depression,” and contacted a pharmacy to verify White’s prescriptions. The R.N. claims White did not exhibit any psychotic behavior,

suicidal ideation, or psychiatric distress but ordered further evaluation. The next day, White was found on the floor with vomit on her face. She stated repeatedly that she took too many pills. The next day, White died in the hospital. The cause of death was Verapamil toxicity. The Sixth Circuit affirmed the rejection of a suit under 42 U.S.C. 1983 on summary judgment. A pretrial detainee does not have an automatic right to a suicide screening. The court rejected an argument that the KOP Policy was deficient because it allows inmates in need of a psychological evaluation to participate before a psychiatrist's assessment of proper housing. The County had no history of suicides relative to the program, so any purported failure to train its employees in suicide risk assessment did not cause White's death.

Read Opinion Are you a lawyer? **Annotate this case**.

Hicks v. Scott

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-3410
Opinion Date: May 1, 2020
Judge: Gibbons
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Cincinnati officers Scott and Moore responded to a reported incident of menacing. Two people alleged that Quandavier had driven by their home that night and threatened to kill them and that Quandavier carried guns. Officer Loreaux identified a vehicle fitting the description. Officers Scott, Moore, Schneider, and Loreaux, standing where the vehicle was parked, heard a voice. Thinking that it was likely Quandavier, they knocked on the exterior door of the residence. It swung open. Three officers entered without a warrant or exigent circumstances. Loreaux remained outside. Neither Scott nor Moore recall announcing their presence or identifying themselves. Inside and upstairs, Scott knocked on a closed door. As it opened, Scott "saw the barrel of a rifle pointed at [her] face." Moore and Schneider also saw Quandavier "nonchalantly" panning the rifle from left to right. Moore reached for its barrel as Scott fired her weapon. Moore did not instruct Quandavier to drop his rifle nor did Scott issue any commands before firing. Quandavier collapsed. The officers immediately radioed for paramedics. Before the officers applied handcuffs or provided first aid, they heard another voice and conducted a sweep. Quandavier died at the scene

without receiving medical attention. In a suit under 42 U.S.C. 1983 for unlawful entry, excessive force, and deliberate indifference to a serious medical need, plus state claims, the district court granted the defendants summary judgment, citing qualified immunity. The Sixth Circuit reversed in part. The district court erred by granting qualified immunity to Scott, Moore, and Schneider on the unlawful entry claim. The court affirmed as to the excessive force, deliberate indifference, and state-law battery claims, and remanded for evaluation of municipal liability and wrongful death claims.

Read Opinion Are you a lawyer? **Annotate this case**.

Moody v. United States

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-5015
Opinion Date: May 6, 2020
Judge: Thapar
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

At Moody's trial, the government produced a video of Moody cooking crack on his stove and waving a handgun while he mused about life in "the game" (drug trafficking). The court ruled that most of the video was admissible. Moody then tried to persuade the jury that the video was filmed more than five years before his indictment, putting it outside the statute of limitations. The jury convicted Moody. Due to prior felony drug convictions, Moody received enhanced, mandatory-minimum life sentences on several counts. He appealed on evidentiary grounds relating to the video. The Sixth Circuit affirmed. Later, Moody raised new claims on collateral review, 28 U.S.C. 2255. The district court found each claim meritless; most were also procedurally defaulted. The court authorized Moody to appeal. The Sixth Circuit dismissed the appeal, stating that none of the claims should have been certified. Reasonable jurists could not doubt that the district court properly denied relief on Moody's claims that he was deprived of his statute-of-limitations defense (violating due process); that the past convictions for his sentencing enhancements were not charged in the indictment or found by the jury; and that his previous lawyers failed to raise the first two claims sooner, violating his right to effective assistance of counsel.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Foreman

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-1827
Opinion Date: May 7, 2020
Judge: Gibbons
Areas of Law: Criminal Law

In 2006, Foreman pled guilty to possession with intent to distribute 50 or more grams of cocaine base, possession with intent to distribute cocaine powder, and possession of a firearm during and in furtherance of a drug trafficking crime. Foreman admitted that he was responsible for approximately 135 grams of crack cocaine and 250 grams of cocaine powder. Foreman had a final Guidelines range of 322-387 months; he was sentenced to 240 months' imprisonment with respect to each drug conviction, to run concurrently, and 60 months' imprisonment for the firearms conviction, to run consecutively. When the First Step Act of 2018 made the Fair Sentencing Act retroactive, Foreman sought relief. The district court held that Foreman was not entitled to a plenary resentencing and declined to revisit his career offender status or hold an in-person hearing, then weighed the new statutory range applicable to Foreman's drug offenses, his recalculated Guidelines range, and the 18 U.S.C. 3553(a) factors, and reduced Foreman's total sentence to 172 months on each drug offense, to run concurrently, plus the mandatory consecutive 60 months on the firearms offense. The Sixth Circuit affirmed. Nothing in the First Step Act entitles a defendant to a plenary resentencing. First Step Act resentencings are not shielded from review for reasonableness; the district court thoroughly explained its rationale, carefully examining Foreman's circumstances, the amended penalty provisions, and the resulting changes to Foreman's Guidelines range.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Smith

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-1724
Opinion Date: May 6, 2020

Judge: Bush
Areas of Law: Criminal Law

In 2006, Smith was convicted of conspiracy to distribute and to possess with intent to distribute 500 grams or more of powder or 50 grams or more of cocaine base (crack cocaine); possession with intent to distribute 50 grams or more of cocaine base (crack cocaine); possession with intent to distribute 500 grams or more of cocaine powder; and being a felon in possession of a firearm. The court imposed a mandatory minimum life sentence. The Fair Sentencing Act subsequently lowered the penalty for cocaine-base offenses, made retroactive through the First Step Act. Smith moved for relief and received a reduced sentence of 360 months, the bottom of the new Guideline range for the counts impacted by the Fair Sentencing Act, to run concurrent to his existing 360-month sentence for his powder cocaine count that was not affected by the Fair Sentencing Act. The Sixth Circuit affirmed, rejecting an argument that the court should have imposed a below-Guideline sentence for all counts. The First Step Act is a limited grant of authority to impose a reduced sentence for certain offenses and does not require a plenary resentencing proceeding. Even assuming the court's obligation to explain its reasons for imposing the modified sentence was akin to that which applies in initial sentencing, the court's use of a modified AO 247 form order to explain its decision was not procedurally unreasonable.

Read Opinion Are you a lawyer? **Annotate this case**.

Kirkman v. Thompson

Court: US Court of Appeals for the Seventh Circuit
Docket: 19-1904
Opinion Date: May 7, 2020
Judge: William Joseph Bauer
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Following a 1992 fight that involved Johnson, Herron, and Walker, two shooters shot the three men. Johnson survived. In the hospital, Johnson described a shooter by the street name "Duke," where Duke lived, and Duke's car. Johnson identified Duke and his accomplice from a photo array. Police pulled over a vehicle matching Johnson's description and arrested

the driver, Kirkman, and the passenger, who matched the general description of the second shooter. Kirkman had a tattoo of Duke on his arm. Police took additional photos and presented a second photo array to Johnson, who identified them as the shooters. At trial, Johnson identified Kirkman and his passenger as the shooters. There was disputed testimony about the cause of the fight. Convicted of murder and aggravated battery with a firearm, Kirkman was sentenced to life in prison. Johnson had a change of heart and submitted an affidavit, identifying Ford and an unknown man as the shooters. At Kirkman's post-conviction hearing, Johnson testified that he and his family had been threatened. Other testimony was inconsistent with Johnson's. Illinois courts denied post-conviction relief, finding that Johnson's recantation lacked credibility. Johnson later pleaded guilty for perjury but failed to specify which statement was false. The Seventh Circuit affirmed the denial of federal habeas relief. Illinois courts found Johnson's recantation lacked credibility. An evidentiary hearing satisfied Kirkman's due process rights. The Illinois trial court's determination defeated Kirkman's innocence and perjured testimony claims.

Read Opinion Are you a lawyer? **Annotate this case**.

Tuduj v. Newbold

Court: US Court of Appeals for the Seventh Circuit
Docket: 19-1699
Opinion Date: May 1, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Illinois prisoner Tuduj, having received extensive dental treatment, filed a "deliberate indifference" suit under 42 U.S.C. 1983 against his dentists and prison officials. The court recruited counsel to assist Tuduj in filing an amended complaint that complied with the Federal Rules of Civil Procedure. Counsel defended against two summary judgment motions, one arguing that Tuduj had not exhausted his administrative remedies and another on the merits While the motions were pending, Tuduj moved "for leave to represent himself," stating that he was "concerned that his counsel has filed a structurally, technically and legally insufficient response doomed to be denied." He asked to file his own brief, except "in the event this Honorable Court deems counsel's response … legally sufficient and Grants same[,]

Plaintiff would be open to continued effective representation." A magistrate denied Tuduj's motion, stating that Tuduj "varie[d] between saying he would like to" represent himself and "indicating that he is happy with counsel's representation as long as he prevails." The district judge granted the motions for summary judgment, citing professional judgment and finding "no competent evidence" of any policy that unlawfully influenced dental-treatment decisions. The Seventh Circuit rejected Tuduj's argument that the court wrongly denied his "unqualified" right to proceed pro se under 28 U.S.C. 1654, the due process clause, the equal protection clause, and the Seventh Amendment. The district court permissibly denied his equivocal request.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Gibson

Court: US Court of Appeals for the Seventh Circuit
Docket: 19-1402
Opinion Date: May 7, 2020
Judge: William Joseph Bauer
Areas of Law: Constitutional Law, Criminal Law

Officer Garrison encountered Gibson, a suspected drug trafficker, walking with a companion. Although initially a consensual encounter, Garrison questioned Gibson and his companion and briefly detained Gibson. After Gibson and his companion departed, Garrison spotted a methamphetamine pipe under his patrol vehicle. Local law enforcement conducted a traffic stop of Gibson's vehicle in the curtilage of his driveway. A drug detection dog signaled the presence of a controlled substance in the vehicle, though nothing was found. Earlier that day, Gibson's wife had met with DEA agents to tell them about methamphetamine inside the home. Police used information Mrs. Gibson had provided to obtain a search warrant. The search of the home uncovered drugs, drug paraphernalia, currency, and AK-47 rifles, which led to Gibson's arrest. Gibson moved to suppress all evidence seized during the search, alleging he was detained without reasonable suspicion, unlawfully frisked, arrested without probable cause, stopped without probable cause or reasonable suspicion, and the traffic stop exceeded a permissible scope. Upon learning of his wife's cooperation, Gibson also argued her statement was insufficiently attenuated to justify the

search warrant. The Seventh Circuit affirmed the denial of the motion. Mrs. Gibson's voluntary statement with DEA agents was independently sufficient to sustain findings of probable cause and sufficiently attenuated from subsequent events to preclude suppression.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Howell

Court: US Court of Appeals for the Seventh Circuit
Docket: 18-3157
Opinion Date: May 4, 2020
Judge: Scudder
Areas of Law: Constitutional Law, Criminal Law

In December 2012, Chicago Police officers responded to an anonymous call reporting a Hispanic man in a black sweater and black hat, carrying a bag, and climbing under a warehouse fence. They found someone who matched the description. After stopping and frisking him, they determined he was not engaged in any crime. Howell, walking toward the police, was white and wearing a black jacket and dark hat. When an officer approached to speak to him, Howell did not answer, looked panicked, and put his hands in his pockets. The officer patted Howell down and found a gun in his jacket. A federal gun charge followed. Howell unsuccessfully moved to suppress the gun. The Seventh Circuit reversed the denial of his suppression motion and vacated his conviction for possessing that gun. The court noted that the facts in the pretrial record differed significantly from those presented at trial, where the arresting officer testified that he decided to proceed with the pat-down only after Howell ignored a directive to remove his hands from his pockets. Viewing the pretrial record as a whole, the police lacked reasonable suspicion to frisk Howell. The court did not reverse Howell's conviction on a second gun charge that resulted from the execution of a warrant to search Howell's apartment three months after the initial stop and the ensuing discovery of more guns and ammunition.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Lewis

Court: US Court of Appeals for the Seventh Circuit
Dockets: 19-1911, 19-1262
Opinion Date: May 7, 2020
Judge: Joel Martin Flaum
Areas of Law: Criminal Law

In 2016-2018, Draheim managed a conspiracy, responsible for at least 38 packages of methamphetamine sent from California to La Crosse, Wisconsin. Draheim supervised at least 11 associates who accepted shipments on her behalf, sent money transfers to California, distributed the meth, rented storage lockers, and collected money owed to her. Draheim provided vehicles. After agents placed a wiretap on her phone and seized several packages of meth en route to Draheim, her California supplier forced Draheim to find a new source. Draheim contacted Lewis, recently out of jail but still involved in the "meth scene." Lewis agreed to purchase meth from a new supplier. During the planned transaction, agents seized the package, which contained 28.6 grams of nearly pure meth. Police subsequently arrested Draheim after they found her daughter dead at home from an overdose; they took Lewis into custody for violating the terms of his state supervision. Both pleaded guilty to meth distribution offenses, 21 U.S.C. 841, 846. Draheim, facing a mandatory-minimum 10-year sentence, unsuccessfully argued that she qualified for "safety-valve relief." The court reasoned that she was the leader of her enterprise. Lewis unsuccessfully contended that he should be sentenced based only on his conviction, not other "relevant conduct." The Seventh Circuit affirmed Draheim's sentence but vacated as to Lewis. The fact that the defendant has engaged in other drug transactions is not, alone, sufficient to justify treating those transactions as relevant conduct for sentencing purposes.

Read Opinion Are you a lawyer? **Annotate this case**.

Bakor v. Barr

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-3011
Opinion Date: May 7, 2020
Judge: Steven M. Colloton
Areas of Law: Criminal Law, Immigration Law

The Eighth Circuit denied a petition for review of the BIA's determination

that defendant committed two crimes involving moral turpitude. The court held that the BIA did not err in determining that petitioner's conviction for the Minnesota crimes of Criminal Sexual Conduct in the Fifth Degree and knowing failure to comply with Minnesota's sex offender registration statute were crimes involving moral turpitude. The court also held that petitioner failed to exhaust his remaining arguments and therefore declined to consider them.

Read Opinion Are you a lawyer? **Annotate this case**.

Smith v. Titus

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-2915
Opinion Date: May 5, 2020
Judge: Steven M. Colloton
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Eighth Circuit affirmed the district court's denial of habeas relief to petitioner based on his claim that the trial court violated his Sixth Amendment right to a public trial when it briefly closed the courtroom to spectators. The district court denied relief based on the ground that the Minnesota Supreme Court’s decision was neither contrary to, nor an unreasonable application of, clearly established federal law. The court agreed and held that it was not objectively unreasonable for the Minnesota Supreme Court to deem it constitutional under the Sixth Amendment for the trial court to explain the parameters of an earlier public order on evidentiary issues in a brief nonpublic proceeding before the jury was sworn.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Becerra

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-2777
Opinion Date: May 7, 2020
Judge: Stras
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's conviction for two counts of being a

felon in possession of a firearm and ammunition. The court held that there was more than enough evidence for defendant's probation officer and other officers to believe defendant had a firearm on him. Therefore, the officers had probable cause to arrest him without a warrant. The court also held that defendant was in custody when he made both statements at issue. In this case, the "request for clarification" of defendant's statement that he had "something" in his car did not require Miranda warnings. Furthermore, because the bulge in defendant's pocket could have been a gun or other weapon that would have posed a danger to the officers and others, they could ask about it without the formality of Miranda warnings. The court joined its sister circuits in declining to recognize the innocent-possessor defense. The court held that the district court did not err in excluding defendant's proposed testimony that he had found the handgun in his car earlier in the day and was about to hand it over to his probation officer. The court reasoned that, even if defendant intended to turn over the gun (or the ammunition) to his probation officer, it is still a crime to knowingly possess it in the first place. Finally, the court held that the district court did not err in denying defendant a sentencing reduction for acceptance of responsibility; the district court considered defendant's mitigation arguments at sentencing; and the district court did not abuse its discretion by imposing a within-Guidelines sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Haynes

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1607
Opinion Date: May 5, 2020
Judge: Raymond W. Gruender
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's conviction and sentence for being a felon in possession of a firearm. The court held that the government did not violate the Speedy Trial Act, and defendant failed to offer any evidence showing that Iowa and federal prosecutors colluded. Furthermore, the district court did not abuse its discretion by failing to hold an evidentiary hearing regarding the existence of collusion. The court also held that the district court did not err in denying the motion to suppress where defendant

was not unlawfully seized. In this case, prior to producing the marijuana cigarette, the officer did not ask defendant any questions but merely ordered him off the bus, particularly as the smell of marijuana alerted the officer that evidence of a more serious crime than failure to use a turn signal might be uncovered during the stop. Finally, the court held that defendant was not unlawfully searched when the officer conducted a pat-down search incident to arrest; the evidence was sufficient to support defendant's conviction; defendant's Rehaif claim failed because there was sufficient evidence that he knew of his prohibited status; and defendant's sentence was not substantively unreasonable nor an abuse of the district court's discretion.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Roberts

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1176
Opinion Date: May 1, 2020
Judge: Steven M. Colloton
Areas of Law: Criminal Law

The Eighth Circuit vacated defendant's sentence imposed after he pleaded guilty to unlawful possession of a firearm as a previously convicted felon. The court held that, although the district court properly applied a four-level increase for possession of a firearm "in connection with another felony offense" under USSG 2K2.1(b)(6)(B), but that a two-level increase for "using a minor to commit a crime" under USSG 3B1.4 should not have applied. In this case, the evidence showed only that defendant engaged in an arm's-length transaction with a minor. The court held that this mere joint participation in an offense as a partner, does not amount to "use" of a minor "to commit the offense" of unlawful possession of a firearm by a felon. Accordingly, the court remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Wright

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1081

Opinion Date: May 5, 2020
Judge: Erickson
Areas of Law: Criminal Law

The Eighth Circuit affirmed the district court's restitution order and certain special conditions of defendant's supervised release imposed after he pleaded guilty to sex trafficking of a child. The court found no error in the district court's restitution amount of $20,000, holding that the evidence supported the amount in light of the aggregate harm to the victim. The court also held that the special conditions -- including a requirement that defendant participate in sex offender treatment including psychological testing and polygraph examinations, a prohibition against contact with any minors without pre-approval, and a requirement that defendant seek prior approval before using temporary commercial lodging, such as a hotel or motel -- where reasonably related to both the offense of conviction and to defendant's history of sexual contact with minor females.

Read Opinion Are you a lawyer? **Annotate this case**.

Benson v. Chappell

Court: US Court of Appeals for the Ninth Circuit
Docket: 13-99004
Opinion Date: May 1, 2020
Judge: Consuelo Maria Callahan
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Ninth Circuit affirmed the district court's denial of petitioner's habeas corpus petition challenging his California conviction and death sentence for murder and other crimes. Petitioner raised two certified claims and two uncertified claims. The panel held that petitioner failed to show that the California Supreme Court's denials of his claims were unreasonable determinations of the facts or contrary to clearly established federal law. In this case, the California Supreme Court reasonably determined that an officer's misstatement during petitioner's interrogation that there was no death penalty in California did not prompt petitioner's confessions. Furthermore, petitioner failed to show that his statements were not knowing, voluntary, and intelligent. Even if petitioner were able to show that trial counsel was ineffective in not fully investigating his abuse as a child or his alleged organic brain injury, the panel held that the state court could

reasonably have determined that any shortcoming in trial counsel's investigation was not prejudicial. Finally, the panel granted a certificate of appealability on petitioner's two uncertified claims and held that the state court reasonably rejected the claims that his trial counsel should have impeached the government's case and the prosecutor withheld material, exculpatory evidence.

Read Opinion Are you a lawyer? **Annotate this case**.

Mero v. Barr

Court: US Court of Appeals for the Ninth Circuit
Docket: 17-70929
Opinion Date: May 1, 2020
Judge: Paul Jeffrey Watford
Areas of Law: Criminal Law, Immigration Law

The Ninth Circuit granted in part a petition for review of the BIA's finding that petitioner was removable based on his conviction for possession of visual presentation depicting sexual conduct of a person under 16 years of age, in violation of Nevada Revised Statutes (N.R.S.) 200.730. Applying the categorical approach, the panel compared the elements of N.R.S. 200.730 with the applicable definition of "sexual abuse of a minor," which requires proof of three elements. The panel held that N.R.S. 200.730 punishes a broader range of conduct because the Nevada statute does not require proof that the offender participated in sexual conduct with a minor. Therefore, petitioner's conviction did not qualify as sexual abuse of a minor. The panel explained that, with a possession-only offense such as N.R.S. 200.730, the minor depicted in the image is not the direct object of the offender's conduct, which is a necessary predicate for the offense to qualify as sexual abuse of a minor.

Read Opinion Are you a lawyer? **Annotate this case**.

Romero-Millan v. Barr

Court: US Court of Appeals for the Ninth Circuit
Dockets: 16-73915, 17-72893, 18-71555
Opinion Date: May 4, 2020

Areas of Law: Criminal Law

The Ninth Circuit certified the following questions of state law to the Arizona Supreme Court: 1. Is Arizona's possession of drug paraphernalia statute, A.R.S. 13-3415, divisible as to drug type? 2. Is Arizona's drug possession statute, A.R.S. 13-3408, divisible as to drug type? 3. Put another way, is jury unanimity (or concurrence) required as to which drug or drugs listed in A.R.S. 13-3401(6), (19), (20), or (23) was involved in an offense under either statute?

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Yang

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-10341
Opinion Date: May 4, 2020
Judge: Piersol
Areas of Law: Criminal Law

The Ninth Circuit affirmed the district court's denial of defendant's motion to suppress after he pleaded guilty to receipt of stolen mail and being a prohibited person in possession of a firearm. Defendant moved to suppress the evidence seized from his residence and the statements he made to law enforcement on the basis that the search warrant obtained by the Postal Inspection Service relied on evidence that was obtained illegally. The panel declined to address the potential Fourth Amendment privacy interests that may be implicated by the warrantless use of this Automatic License Plate Recognition (ALPR) technology, and held that defendant does not have a reasonable expectation of privacy in the historical location data of the Yukon under the facts of this case. The panel found no evidence in the record that Prestige Motors had a policy or practice of allowing lessees to keep cars beyond the rental period and Prestige had made affirmative attempts to repossess the vehicle by activating the GPS unit to locate and disable the vehicle. Therefore, defendant lacked standing to challenge the warrantless search of the database.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Neugin

Court: US Court of Appeals for the Tenth Circuit
Docket: 19-7043
Opinion Date: May 1, 2020
Judge: Scott Milne Matheson, Jr.
Areas of Law: Constitutional Law, Criminal Law

Jack Neugin pled guilty to being a felon in possession of a firearm and ammunition on the condition that he could appeal the district court's denial of his motion to suppress evidence of the ammunition and firearm police found in the bed of his pickup truck. Officers responded to a reported verbal altercation between Neugin and his girlfriend. One of the officers saw ammunition in the back of the truck after he lifted the truck's camper lit do allow the girlfriend to retrieve her belongings. Neugin argued the officers discovered the evidence during an unconstitutional search; the district court concluded the officer was acting "in a lawful position" as "community caretaker," and found no Fourth Amendment violation. The Tenth Circuit reversed, finding that : (1) the officer conducted the without a warrant or probable cause, (2) the community caretaking exception to the warrant requirement does not apply, and (3) the inevitable discovery exception to the exclusionary rule does not apply. The evidence seized should have been suppressed.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Ramon

Court: US Court of Appeals for the Tenth Circuit
Docket: 19-1221
Opinion Date: May 1, 2020
Judge: Gregory Alan Phillips
Areas of Law: Constitutional Law, Criminal Law

In 2016, after serving a federal prison sentence for having possessed a firearm after a felony conviction, Charles Ramon III began serving a mandatory term of supervised release. Before Ramon completed the term, his probation officer filed a petition, soon followed by two superseding petitions, to revoke Ramon’s supervised release. At the revocation hearing, the district court found three violations—two for possessing a controlled

substance and one for again illegally possessing a firearm. Of these, the most serious was Ramon's illegal possession of a firearm—a Grade B violation. For this, the court imposed the statutory maximum sentence of twenty-four months in prison. During the revocation hearing, the government mentioned that it might seek to indict Ramon for illegally possessing a firearm (the conduct in part underlying the revocation). Mindful of this, the district court ordered that Ramon's twenty-four-month sentence run "consecutively to any sentences imposed previously or prospectively in federal or state court." At the hearing, Ramon did not object to the district court's running his sentence consecutively to future federal sentences. On appeal, Ramon argued that the district court exceeded its sentencing authority under 18 U.S.C. 3584(a) by ordering that Ramon's sentence run consecutively to future federal sentences. By the terms of 18 U.S.C. 3584(a), the Tenth Circuit determined the district court did err. But Ramon failed to object to this at trial, and on appeal, failed to show that the error was plain, thus, judgment was affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Richards

Court: US Court of Appeals for the Tenth Circuit
Docket: 19-8044
Opinion Date: May 6, 2020
Judge: Baldock
Areas of Law: Constitutional Law, Criminal Law

In 2018, the Wyoming Division of Criminal Investigation (DCI) obtained a search warrant to review the contents of Defendant–Appellant Joshua Richards' Tumblr account. During the search and subsequent investigation, DCI agents discovered Defendant had re-blogged videos and images of child pornography to his private Tumblr so he could later access and view the materials. Defendant ultimately pleaded guilty to one count of accessing with intent to view child pornography. He was sentenced to twenty-four months' imprisonment followed by five years of supervised release. The district court imposed several special conditions of supervised release, which, as relevant here, related to drugs and alcohol and required Defendant to submit to polygraph testing. On appeal, Defendant argued the district court erred in imposing these special conditions. He also challenged

the length of his prison sentence as substantively unreasonable. The Tenth Circuit determined the alcohol and drug conditions did not directly conflict with the relevant policy statement in the sentencing guidelines, so the district court's decision to impose the conditions was not manifestly unreasonable. And given the circumstances of the case, the Court determined the trial court did not abuse its discretion in imposing Defendant's twenty-four month sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

Andrews v. Warden

Court: US Court of Appeals for the Eleventh Circuit
Docket: 19-12443
Opinion Date: May 5, 2020
Judge: William Holcombe Pryor, Jr.
Areas of Law: Criminal Law

The Eleventh Circuit affirmed the district court's denial of habeas relief under 28 U.S.C. 2241. Plaintiff alleged that President Obama commuted his "total sentence" of imprisonment, which included the 37 months of imprisonment that he served as part of his 2003 sentence. Based on the terms of the commutation order, the Constitution, and Supreme Court precedent, the court could not say that the Bureau erred in excluding the 37-month term of imprisonment from its recalculation.

Read Opinion Are you a lawyer? **Annotate this case**.

Hollis v. United States

Court: US Court of Appeals for the Eleventh Circuit
Docket: 19-11323
Opinion Date: May 6, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Eleventh Circuit affirmed the district court's denial of petitioner's motion to vacate his sentence under 28 U.S.C. 2255. The court held that petitioner cannot prove that his counsel rendered ineffective assistance, because petitioner's prior convictions in Alabama categorically qualify as predicate

offenses under both the Armed Career Criminal Act and the career-offender provision of the Guidelines, and his prior conviction in Georgia qualifies as a predicate offense under the Act. Therefore, counsel did not perform deficiently by failing to raise a meritless objection.

Read Opinion Are you a lawyer? **Annotate this case**.

Knight v. Florida Department of Corrections

Court: US Court of Appeals for the Eleventh Circuit
Docket: 18-12488
Opinion Date: May 1, 2020
Judge: Newsom
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Eleventh Circuit affirmed the district court's denial of a 28 U.S.C. 2254 petition for habeas relief. Petitioner alleged that his counsel rendered ineffective assistance under Strickland v. Washington, 466 U.S. 668 (1984), by failing to adequately investigate and present mitigating evidence during the sentencing phase of his capital-murder trial. The court held that, even assuming that counsel performed deficiently in failing to investigate and present the mitigation evidence that petitioner now raises—thus satisfying the first prong of the two-part Strickland standard that governs ineffective-assistance claims—petitioner failed to carry his burden of demonstrating resulting prejudice.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Evans

Court: US Court of Appeals for the Eleventh Circuit
Docket: 17-15323
Opinion Date: May 6, 2020
Judge: Grant
Areas of Law: Criminal Law

The Eleventh Circuit affirmed defendant's conviction and sentence for being a felon in possession of a firearm. The court held that, given the totality of the circumstances, it was reasonable for officers, mistaking a dog's whimper for a person in distress, to enter defendant's home without a warrant.

Therefore, defendant's challenge to the district court's denial of his motion to suppress evidence failed. The court upheld the district court's imposition of a 22 offense level finding because defendant possessed a semiautomatic firearm capable of accepting a large capacity magazine under USSG 2K2.1(a)(3)(A)(i) (2016). The court also upheld defendant's sentencing enhancement under USSG 2K2.1(b)(4)(B) for possessing a rifle that had an obliterated serial number.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. McLellan

Court: US Court of Appeals for the Eleventh Circuit
Docket: 18-13289
Opinion Date: May 6, 2020
Judge: Boggs
Areas of Law: Criminal Law

The Eleventh Circuit affirmed defendant's conviction for two counts of being a felon in possession of a firearm. The court held that the district court did not abuse its discretion in permitting one of his arresting officers to offer testimony at trial on the correlation between guns and drug activity and to suggest that defendant was selling drugs; the court declined to evaluate the applicability of the Armed Career Criminal Act (ACCA), because the district court would have imposed the same sentence regardless of whether the mandatory minimum applied; and the court rejected defendant's claim under Rehaif v. United States, 139 S. Ct. 2191 (2019), and held that there was no plain error in the district court's failure to instruct the jury of the knowledge-of-status element and any error from the lack of a knowledge-of-status element in defendant's plea colloquy did not affect his substantial rights. Finally, the court remanded for clarification of the judgment to reflect the sentence the district court said it would have imposed if the Armed Career Criminal Act did not apply.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Russell

Court: US Court of Appeals for the Eleventh Circuit

Docket: 18-11202
Opinion Date: May 4, 2020
Judge: Charles R. Wilson
Areas of Law: Criminal Law

Defendant was convicted of possessing a firearm and ammunition as an immigrant illegally or unlawfully in the United States. After defendant appealed his conviction and sentence, the Supreme Court issued its decision in Rehaif v. United States, 588 U.S. ___, 139 S. Ct. 2191 (2019), which reversed a decision from this court and held that under 18 U.S.C. 922(g), the government must prove that a defendant knew "his status as a person barred from possessing a firearm" when he knowingly possessed a firearm. The Eleventh Circuit held that defendant established the necessary prejudice under plain error review and vacated defendant's section 922(g) conviction, remanding for further proceedings. In this case, the district court committed an error that was made plain by the Supreme Court in Rehaif. Furthermore, defendant has sufficiently shown a reasonable probability that but for the error, the outcome of his trial would have been different.

Read Opinion Are you a lawyer? **Annotate this case**.

Welch v. United States

Court: US Court of Appeals for the Eleventh Circuit
Docket: 14-15733
Opinion Date: May 6, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Eleventh Circuit affirmed the district court's denial of petitioner's 28 U.S.C. 2255 motion to vacate his sentence. The court held that defendant's prior 1996 Florida convictions for robbery qualified as violent felonies under the Armed Career Criminal Act's (ACCA) elements clause, and rejected his contention that the court's decision in his direct appeal carved out a narrow exception to pre-1997 Florida robbery convictions obtained in Florida's Fourth District Court of Appeal. The court also held that petitioner's prior Florida felony battery conviction was a violent felony under the ACCA in light of the court's holding in United States v. Vail-Bailon, 868 F.3d 1293 (11th Cir. 2017) (en banc), cert. denied, 138 S. Ct. 2620 (2018).

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Trujillo

Court: Arizona Supreme Court
Docket: CR-18-0531-PR
Opinion Date: May 4, 2020
Judge: Gould
Areas of Law: Constitutional Law, Criminal Law

The Supreme Court held that, for purposes of imposing mandatory sex offender registration under Ariz. Rev. Stat. 13-3821(A)(3), a judge has the authority to make the necessary factual finding that the victim is under the age of eighteen and that Arizona's sex offender registration statutes are civil regulatory statutes, not criminal penalties. Defendant was convicted by a jury of one count of sexual abuse. In reaching its verdict the jury determined that the victim was "fifteen or more years of age." At sentencing, the trial court ordered Defendant to register as a sex offender. Defendant objected, arguing that, pursuant to Apprendi v. New Jersey, 530 U.S. 466 (2000), a jury was required to find whether Defendant was under eighteen pursuant to section 13-3821(A)(3). The trial court denied the objection. The court of appeals affirmed. The Supreme Court affirmed, holding (1) Apprendi does not apply to factual findings that are necessary to impose registration because sex offender registration is a civil regulatory requirement, not a criminal penalty; and (2) the trial judge did not violate Apprendi by determining that the victim was under eighteen.

Read Opinion Are you a lawyer? **Annotate this case**.

Barnett v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 181
Opinion Date: May 7, 2020
Judge: Hudson
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's "motion for credit for time spent in custody," holding that the

circuit court's findings were not clearly erroneous. In his motion, Appellant alleged that he was entitled to 312 days of jail-time credit and that the circuit court should enter a new sentencing order nunc pro tunc that reflected the correct amount of jail-time credit. The circuit court denied the motion. The Supreme Court affirmed, holding that the circuit court's denial of Appellant's motion was not clearly erroneous because Appellant failed to demonstrate a clerical error subject to correction.

Read Opinion Are you a lawyer? **Annotate this case**.

Mason v. Kelley

Court: Arkansas Supreme Court
Citation: 2020 Ark. 182
Opinion Date: May 7, 2020
Judge: Rhonda K. Wood
Areas of Law: Criminal Law

The Supreme Court affirmed the order of the circuit court dismissing Appellant's pro se petition for writ of habeas corpus, holding that Appellant stated no ground on which the writ could issue. Appellant was convicted of aggravated robbery, theft of property, and second-degree battery and sentenced as a habitual offender to an aggregate term of 660 months' imprisonment. The court of appeals affirmed. Appellant later petitioned for writ of habeas corpus, asserting that the trial court misapplied Arkansas's habitual-offender statutes. The circuit court dismissed the petition. The Supreme Court affirmed, holding that the issues Appellant raised in his petition for the writ should have been raised at trial, on direct appeal, or in a petition for postconviction relief.

Read Opinion Are you a lawyer? **Annotate this case**.

Ray v. Kelley

Court: Arkansas Supreme Court
Citation: 2020 Ark. 184
Opinion Date: May 7, 2020
Judge: Wynne
Areas of Law: Criminal Law

The Supreme Court dismissed Appellant's appeal from an order denying his pro se petition for permission to reinvest jurisdiction in the trial court to consider a petition for writ of error coram nobis, holding that the circuit court had no jurisdiction to consider the petition. Appellant entered negotiated guilty pleas to rape and other offenses. Appellant later filed a petition for writ of error coram nobis in the Chicot County Circuit Court, the court where he was incarcerated, setting out two grounds for coram nobis relief. The circuit court denied the petition. The Supreme Court dismissed Appellant's appeal, holding that jurisdiction lay in the trial court where Appellant was convicted, which in this case was the Ashley County Circuit Court. Therefore, the Chicot County Circuit Court was without jurisdiction to address Appellant's coram nobis petition.

Read Opinion Are you a lawyer? **Annotate this case**.

Walker v. Kelley

Court: Arkansas Supreme Court
Citation: 2020 Ark. 183
Opinion Date: May 7, 2020
Judge: Rhonda K. Wood
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's pro se petition for declaratory judgment, holding that Appellant could not use a declaratory-judgment action to collaterally attack his criminal conviction. Appellant was convicted of first-degree murder and second-degree unlawful discharge of a firearm from a vehicle. The court of appeals affirmed. Years later, Appellant filed a petition for declaratory judgment alleging that he was denied due process in his criminal trial when the court admitted the prior testimony of an unavailable witness and that this admission violated the Confrontation Clause. The circuit court denied the petition. The Supreme Court affirmed, holding that a declaratory judgment action provided no relief on these grounds.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Flores

Court: Supreme Court of California
Docket: S116307
Opinion Date: May 4, 2020
Judge: Kruger
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction of three counts of first degree murder and his sentence of death, holding that the three or four minor errors at Defendant's trial were harmless and did not interfere with his due process right to a fair trial. Specifically, the Supreme Court held (1) no error occurred during jury selection; (2) Defendant was not prejudiced by any misstatements by the prosecutor; (3) assuming certain evidence was inadmissible, the court's admonition to the jury and the court's instruction cured the resultant harm; (4) the trial court erred in admitting testimony that the victim was afraid of Defendant, but the error was harmless; and (5) Defendant's remaining allegations of error were without merit.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. Law

Court: California Courts of Appeal
Docket: E072845(Fourth Appellate District)
Opinion Date: May 5, 2020
Judge: Slough
Areas of Law: Constitutional Law, Criminal Law

In 2001, appellant Terrell Law and his codefendant Brett May committed a home invasion robbery, during which one of them shot and killed one of the residents. They were tried jointly in 2006 before two separately empaneled juries who found them both guilty of first degree felony murder with the special circumstance described in Penal Code section 190.2(a)(17(A) and (d). Though Law's jury found he was not the shooter, they nonetheless concluded he was a "major participant" in the underlying robbery and acted "with reckless indifference to human life." In 2018, the Legislature enacted Senate Bill No. 1437 (2017-2018 Reg. Sess.) which, among other things, amended the definition of felony murder in Penal Code section 189. The legislation also added Penal Code section 1170.95, which established a procedure for vacating murder convictions predating the amendment that could not be sustained under the new definition of felony murder. Law

challenged the trial court's summary denial of his section 1170.95 petition to vacate his murder conviction, arguing the trial court erred by reviewing his record of conviction and determining the jury's true finding on the special circumstance rendered him ineligible for relief. The Court of Appeal concluded it was proper for a trial court to review the record of conviction when determining whether a section 1170.95 petitioner had stated a prima facie claim for relief. Additionally, the Court concluded Law "undoubtedly qualifies" as a major participant who acted with reckless indifference to human life, a conclusion that rendered him ineligible for relief under section 1170.95. The Court therefore affirmed the order denying his petition.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. Sanchez

Court: California Courts of Appeal
Docket: E072647(Fourth Appellate District)
Opinion Date: May 7, 2020
Judge: Menetrez
Areas of Law: Constitutional Law, Criminal Law

Victor Sanchez was charged with first degree murder, but pled guilty to voluntary manslaughter. He filed a petition under Penal Code section 1170.95 to vacate that conviction. The trial court denied the petition, concluding that Sanchez was ineligible for relief because he was not convicted of murder. After review, the Court of Appeal joined other courts that held section 1170.95 did not apply to defendants convicted of voluntary manslaughter. The Court also rejected Sanchez's argument that section 1170.95 violated equal protection.

Read Opinion Are you a lawyer? **Annotate this case**.

Galeotti v. International Union of Operating Engineers

Court: California Courts of Appeal
Docket: A157785(First Appellate District)
Opinion Date: May 6, 2020
Judge: Henry E. Needham, Jr.
Areas of Law: Criminal Law, Labor & Employment Law, White Collar Crime

Galeotti, a former Union Local 3 employee, filed a complaint against Local 3 and three of individual union leaders, alleging that the individual defendants required union employees to pay them money to keep their jobs, lied about the reason for collecting the money, and caused Local 3 to terminate Galeotti's employment when he failed to pay the full amount demanded. The trial court dismissed his second amended complaint without leave to amend. The court of appeal reversed in part, reasoning that a threat to terminate employment can provide a basis for an extortion claim and that the allegations of the second amended complaint stated a cause of action for wrongful termination in violation of the public policy underlying the extortion statutes. The complaint stated a cause of action for violations of the Racketeer Influenced and Corrupt Organizations Act (RICO; 18 U.S.C. 1961), based on the predicate acts of extortion, but did not state a cause of action for interference with prospective economic advantage.

Read Opinion Are you a lawyer? **Annotate this case**.

In re I.A.

Court: California Courts of Appeal
Docket: B296549(Second Appellate District)
Opinion Date: May 4, 2020
Judge: Tangeman
Areas of Law: Criminal Law, Juvenile Law

Where a juvenile court vacates its true finding on a generic murder allegation and redesignates it as a finding on an uncharged target offense, and does so before a minor has had the opportunity to contest the court's findings or orders, the minor may challenge the sufficiency of the evidence of the redesignated offense on appeal. The Court of Appeal held that there was insufficient evidence to support the juvenile court's decision sustaining the allegations that I.A. possessed a concealable firearm and committed vandalism. Therefore, the court reversed the juvenile court's findings, vacating the jurisdiction and disposition order and dismissing the Welfare and Institutions Code section 602 petition.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Edwards

Court: California Courts of Appeal
Docket: A158055(First Appellate District)
Opinion Date: May 1, 2020
Judge: Petrou
Areas of Law: Criminal Law

In 2006, Edwards fired an assault weapon into an apartment, killing the victim. Edwards pled guilty to possession of a firearm as a felon and was convicted of second-degree murder and shooting into an inhabited dwelling. Following the enactment of Senate Bill 1437, Edwards filed a Penal Code 1170.95 resentencing petition, checking form boxes indicating that he was convicted under a theory of felony murder or murder under the natural and probable consequences doctrine and that he could not now be convicted of 1st or 2nd-degree murder because of changes to Penal Code 188 and 189. Edwards submitted the jury instructions and the transcript of the prosecutor's closing remarks that Edwards acted with "both express malice, specific intent to kill, as well as implied malice," described as "an intentional act, the natural consequences of which are dangerous to human life, and at the time that the individual acted, they knew of the danger, and they deliberately acted with conscious disregard." The court denied the petition, finding that Edwards was convicted on a valid theory of murder that survived the statutory changes. The court of appeal affirmed. The superior court did not err in considering the record of conviction. Edwards could not meet the statutory prerequisites for even filing a section 1170.95 petition because he was not charged or convicted of second-degree felony murder or murder under the natural or probable consequences doctrine directed at accomplice liability.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Thomkins

Court: California Courts of Appeal
Docket: A141375(First Appellate District)
Opinion Date: May 1, 2020
Judge: Streeter
Areas of Law: Criminal Law

On Easter night in 2011, gunfire erupted at an Oakland bar-restaurant, leaving two people dead and five wounded. Thompkins and Fox were convicted of two counts of first-degree murder for the benefit of a criminal street gang, with firearm discharge enhancements, a multiple-murder special circumstance, and five counts of attempted murder with great bodily injury findings, gang enhancements, and firearm discharge enhancements. Thompkins was convicted as the shooter and Fox as an accomplice. Both were sentenced to life in prison without possibility of parole, plus 224 years to life. After Thompkins was sentenced, Fox stated under oath he was the actual shooter and Thompkins knew nothing about Fox's intentions. Thompkins claimed this new testimony, and his attorney's incompetent reaction entitled him to a new trial and submitted a declaration by another gang member who was present that night. The court of appeal concluded that Thompkins's attorney was not ineffective for failing to bring a motion to recall the sentence followed by a new trial motion because Thompkins failed to show prejudice. The attempted murder convictions and related enhancements must be reversed for both defendants based on the flawed kill zone instruction. Introducing evidence that defendants admitted their gang affiliation at jail intake violated the defendants' privilege against self-incrimination but was harmless. There was some evidentiary error that was harmless due to the wealth of admissible evidence establishing the gang enhancements. Arguments based on the statutory amendments to Penal Code 188 and 189 must be raised in the trial court (section 1170.95). The case must be remanded so the judge may exercise his discretion whether to impose or strike the firearm enhancements on under Penal Code 12022.53.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Torres

Court: California Courts of Appeal
Docket: B295043(Second Appellate District)
Opinion Date: May 4, 2020
Judge: Wiley
Areas of Law: Criminal Law

After the trial court admitted a witness's former testimony, the Court of Appeal applied People v. Roldan (2012) 205 Cal.App.4th 969, 975–985, and reversed. Roldan held that, before invoking the former testimony exception,

prosecutors should react appropriately to the impending deportation risk by following four steps: alert the defense to the risk; videotape the preliminary hearing testimony; use judicial measures to try to delay deportation; and consider an array of other specific measures. In this case, the prosecution conceded that prosecutors were simply unaware of Roldan and did not comply with it. The court held that Roldan controls the court's analysis because the facts about prosecutorial diligence are weaker here than they were in Roldan, where the appellate court held for the defense. In this case, the record before deportation is of prosecutorial inaction where the prosecution's brief in this court admits the investigating officer did not do anything to ensure that the witness would not be deported, nor is there other evidence of prosecutorial efforts to delay the witness's departure or to videotape his testimony at the preliminary hearing.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Triplett

Court: California Courts of Appeal
Docket: B298914(Second Appellate District)
Opinion Date: May 1, 2020
Judge: Frances Rothschild
Areas of Law: Criminal Law

Defendant was convicted of assault with a deadly weapon, carjacking, and attempted murder. In the published portion of the opinion, the Court of Appeal held that the trial court erred by denying defense counsel's request to inform the jurors that they could have testimony of certain witnesses read back to them. The court also held that, under the circumstances in this case, the error was harmless.

Read Opinion Are you a lawyer? **Annotate this case**.

Colorado In Interest of G.S.S.

Court: Colorado Supreme Court
Citation: 2020 CO 32
Opinion Date: May 4, 2020
Judge: Brian D. Boatright

Areas of Law: Constitutional Law, Criminal Law, Juvenile Law

After being charged, fourteen-year-old G.S.S. was detained for more than three months without bail, even though he had not entered a plea and had not been tried on the charges against him. At that point, G.S.S.'s counsel filed a motion to dismiss, arguing that G.S.S.'s "right to a speedy trial" had been violated under section 19-2-509(4)(b), C.R.S. (2019). The trial court agreed and dismissed the case against G.S.S. with prejudice, and the court of appeals affirmed in Colorado in Interest of G.S.S., 2019 COA 4M, __ P.3d __. The Colorado Supreme Court then granted certiorari to determine the proper remedy for a violation of the sixty-day limit in section 19-2-509(4)(b). The Supreme Court determined the remedy for a section 19-2-509(4)(b) violation was for the trial court to immediately hold a bail hearing and order the juvenile's release. Accordingly, the judgment of the court of appeals was reversed.

Read Opinion Are you a lawyer? **Annotate this case**.

Barringer v. Halkitis

Court: Florida Supreme Court
Docket: SC19-1071
Opinion Date: May 7, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court held that Jay Barringer's quo warranto petition filed in this case was a frivolous proceeding brought before the Supreme Court by a state prisoner and sanctioned Barringer by barring him from filing any further pro se requests for relief related to his criminal case. Barringer was convicted of one count of attempted sexual battery of a victim less than twelve years old and sentenced to twenty-five-years' imprisonment. In 2011, Barringer began filing petitions in the Supreme Court. The Court did not grant the relief sought in any of Barringer's filings. In the instant quo warranto petition Barringer challenged his conviction on the ground that the information was defective, a claim Barringer previously raised by way of a habeas petition. The Supreme Court denied the petition and found that Barringer abused the Court's limited judicial resources. The Court sanctioned Barringer by directing the Clerk of Court to reject any future

pleadings or other requests for relief submitted by Barringer that are related to his criminal case, unless such filings are signed by a member of The Florida Bar in good standing.

Read Opinion Are you a lawyer? **Annotate this case**.

Franqui v. State

Court: Florida Supreme Court
Docket: SC19-203
Opinion Date: May 7, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the order of the circuit court denying Appellant's claim of intellectual disability, raised in successive motions for postconviction relief under Fla. R. Crim. P. 3.851, holding that the circuit court did not err in denying relief. Appellant was convicted of first-degree murder and sentenced to death in two separate cases. After the United States Supreme Court decided Hall v. Florida, 572 U.S. 701 (2014), Appellant filed successive motions for postconviction relief in both of his capital cases, asserting that the circuit court's denials of his previous claims of intellectual disability were based on the court's improper interpretation of Florida's intellectual disability statute. The circuit court summarily denied the motions. The Supreme Court reversed and remanded for an evidentiary hearing on the issue of intellectual disability. After a hearing, the circuit court denied the claim. The Supreme Court affirmed, holding (1) the circuit court did not err in denying Appellant's intellectual disability claim; and (2) Appellant was not entitled to relief under Hurst v. Florida, 136 S. Ct. 616 (2016), or Hurst v. State, 202 So. 3d 40 (Fla. 2016).

Read Opinion Are you a lawyer? **Annotate this case**.

Hicks v. State

Court: Florida Supreme Court
Docket: SC19-1978
Opinion Date: May 7, 2020
Judge: Per Curiam

Areas of Law: Criminal Law

The Supreme Court denied the instant mandamus petition filed by Hicks and sanctioned Hicks by barring him from filing any further pro se requests for relief related to his criminal case. Hicks was convicted of one count of lewd and lascivious conduct by a person over eighteen years of age on a victim under sixteen years of age. Since 2016, Hicks filed thirteen pro se requests for relief in the Supreme Court related to his criminal case. The Court did not grant the relief sought in any of Hicks' filings. In the instant petition, Hicks sought a writ of mandamus compelling the circuit court to comply with the requirements of Fla. R. Crim. P. 3.850 by filing a copy of an order denying his second postconviction motion with the clerk of court. The Supreme Court dismissed the petition and found that Hicks abused this Court's limited judicial resources. The Court directed the Clerk of Court to reject any future pleadings or other requests for relief submitted by Hicks that are related to his criminal case, unless such filings are signed by a member of The Florida Bar in good standing.

Read Opinion Are you a lawyer? **Annotate this case**.

Burley v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0356
Opinion Date: May 4, 2020
Judge: Boggs
Areas of Law: Constitutional Law, Criminal Law

In 1992, Douglas Burley pled guilty to malice murder. He moved for an out-of-time appeal in 2019, claiming that his right to appeal was frustrated by his plea counsel's erroneous advice that he could not appeal his conviction because it was the product of a guilty plea. The trial court denied Burley's motion. After review, the Georgia Supreme Court vacated the trial court's judgment and remanded the case with direction to hold a hearing to determine whether ineffective assistance of counsel frustrated Burley's right to appeal.

Read Opinion Are you a lawyer? **Annotate this case**.

Carter v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0022
Opinion Date: May 4, 2020
Judge: David E. Nahmias
Areas of Law: Construction Law, Criminal Law

Brandon Carter was convicted by jury of malice murder and two firearm offenses in connection with the shooting death of Terrance Baker. On appeal, Carter contended the trial court erred by admitting certain hearsay statements into evidence and by violating his constitutional right to be present during his trial. Finding no reversible error, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Clarke v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0258
Opinion Date: May 4, 2020
Judge: Ellington
Areas of Law: Constitutional Law, Criminal Law

Rupert Clark was convicted by jury for the malice murder of his wife, Rosemarie Lebert-Clark. He was also convicted of possession of a firearm during the commission of a felony. On appeal, he argued he received ineffective assistance of trial counsel, and that the trial court erred in admitting certain evidence, violated the continuing witness rule by sending out with the deliberating jury printouts of text messages, and by failing to instruct the jury that a defendant's uncorroborated confession was not alone sufficient to warrant a conviction. Finding no reversible error after reviewing the trial court record, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Collins v. Georgia

Court: Supreme Court of Georgia

Docket: S20A0195
Opinion Date: May 4, 2020
Judge: Harold D. Melton
Areas of Law: Constitutional Law, Criminal Law

Renita Collins was tried for murder along with co-defendant Michael Stallworth. Collins appealed her convictions for murder and possession of a firearm while in commission of a felony in connection with the shooting death of Keith Jacobs. On appeal. Collins contended she was denied a fair trial due to juror misconduct, the trial court abused its discretion by not allowing her to subpoena juror testimony to show that misconduct had occurred, and the trial court abused its discretion when it failed to excuse a prospective juror for cause. Finding no reversible error, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Dawson v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0217
Opinion Date: May 4, 2020
Judge: Warren
Areas of Law: Constitutional Law, Criminal Law

Lavaris Dawson was convicted by jury of felony murder and other crimes in connection with the shooting death of Mamadou Camara. On appeal, Dawson challenged the sufficiency of the evidence supporting his convictions, and argued the trial court erred in admitting Dawson's statements to a detective during an interview because those statements were impermissibly induced by a hope of benefit, and that Dawson was denied his due process right to a timely appeal. After review, the Georgia Supreme Court disagreed and affirmed Dawson's convictions.

Read Opinion Are you a lawyer? **Annotate this case**.

Evans v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0007

Opinion Date: May 4, 2020
Judge: McMillan
Areas of Law: Constitutional Law, Criminal Law

Jimmy Evans was convicted by jury for murder and other crimes relating to the 2006 deaths of Tavoris Calhoun and Dezmon Thomas. On appeal, Evans argued that because he was visibly intoxicated at the time he made statements to law enforcement and consented to a search of his home and person, the statements and consent were involuntarily given and the trial court should have granted his motion for new trial on this ground. Furthermore, Evans argued that his trial counsel was ineffective for failing to file a motion to suppress at trial on the same basis. Because Evans failed to show error or ineffective assistance of counsel, the Georgia Supreme Court affirmed his conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Hill v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0285
Opinion Date: May 4, 2020
Judge: Harold D. Melton
Areas of Law: Constitutional Law, Criminal Law

Esco Hill was convicted by jury of malice murder and other crimes relating to the stabbing death of Alford Morris in 2014. On appeal, Hill argued the trial court committed reversible error by requiring him to be visibly shackled for the duration of his six-day trial. After review of the trial court record, the Georgia Supreme Court concurred this was reversible error, consequently, reversed judgment of conviction. Because the Court concluded the evidence at trial was sufficient to sustain Hill's conviction, the State could re-try him. The Court did not address Hill's remaining enumerations of error, "as they are not likely to recur in the event of a retrial."

Read Opinion Are you a lawyer? **Annotate this case**.

Oliver v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0489
Opinion Date: May 4, 2020
Judge: McMillan
Areas of Law: Constitutional Law, Criminal Law

Jacquan Oliver entered a negotiated plea of guilty to felony murder in connection with the shooting death of Alexander Mixon. He appealed his conviction and sentence, arguing that the trial court abused its discretion in finding a factual basis for his plea, and in determining the plea was voluntarily, knowingly and intelligently made. Finding no merit to these contentions, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Rosser v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0103
Opinion Date: May 4, 2020
Judge: Bethel
Areas of Law: Constitutional Law, Criminal Law

Larry Rosser was convicted by jury of malice murder and other crimes in connection with the death of Alexis Vereen. On appeal, Rosser challenged the sufficiency of the evidence presented against him at trial, and argued the trial court erred by not granting his motion for a mistrial, and by allowing the State to introduce a portion of Rosser's custodial statement to law enforcement. In addition, he argued he received constitutionally ineffective assistance of trial counsel. Finding no reversible error after reviewing the trial court record, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Spencer v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0871
Opinion Date: May 4, 2020
Judge: Keith R. Blackwell

Areas of Law: Constitutional Law, Criminal Law

Christopher Spencer was convicted by jury of murder and other crimes in connection with the fatal shootings of Sylvia Watson and Samuel White. Spencer appealed, claiming only that the evidence was insufficient to support his convictions. Finding no reversible error after reviewing the trial court record, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Styles v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0236
Opinion Date: May 4, 2020
Judge: Ellington
Areas of Law: Constitutional Law, Criminal Law

Derrick Styles was convicted by jury of felony murder and other crimes in connection with the shooting death of Alberto Lumens and the armed robbery fo Juan Lumens Garcia. On appeal, Styles contended the trial court erred in admitting into evidence a recording of an inculpatory telephone conversation between himself and a witness. He also argued his trial counsel was ineffective for failing to object to an allegedly improper comment by the prosecutor during closing argument. Finding no merit to these contentions, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Whitehead v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0171
Opinion Date: May 4, 2020
Judge: Ellington
Areas of Law: Constitutional Law, Criminal Law

Javis Whitehead was convicted by jury of murder and other crimes in connection with the shooting death of Dominique Larry. On appeal, Whitehead challenged the sufficiency of the evidence presented to rebut his

claim of self-defense and to convict him for murder beyond a reasonable doubt. He also argued the trial court erred in denying his motion to suppress his custodial statement, and in refusing to excuse for cause the District Attorney from the panel of prospective jurors prior to the conclusion of voir dire. Finding no merit to these contentions, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Idaho v. Blythe

Court: Idaho Supreme Court - Criminal
Docket: 46992
Opinion Date: May 4, 2020
Judge: Roger S. Burdick
Areas of Law: Constitutional Law, Criminal Law

Nicholas Blythe appealed after he was convicted of possessing a controlled substance. He conditionally pled guilty, reserving the right to challenge his sentence. On appeal, he argued the district court erred in denying his motion to suppress certain evidence found because the evidence presented at trial was found in violation of Blythe's Fourth Amendment rights. After review, the Idaho Supreme Court determined the search at issue took place before an arrest occurred, and because no rationale justifying a search incident to arrest was sufficiently present here, the search of Blythe's shoes was not a valid search incident to arrest. Therefore, the district court erred in holding that the search was reasonable under the Fourth Amendment. Blythe's conviction was vacated, the district court order denying Blythe's motion to suppress was reversed, and the matter remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

Idaho v. Glodowski

Court: Idaho Supreme Court - Criminal
Docket: 47131
Opinion Date: May 6, 2020
Judge: Roger S. Burdick

Areas of Law: Constitutional Law, Criminal Law

David Glodowski appealed after he was convicted for failing to update his sex-offender registration in violation of Idaho Code section 18-8309. He argued the district court erred by ruling that his prior conviction under a Wisconsin statute was "substantially equivalent" to Idaho statutes that required sex-offender registration in Idaho. After review, the Idaho Supreme Court determined the district court improperly allowed the State to seek a redetermination of the "substantially equivalent" element given that the Idaho Bureau of Criminal Identification made a final determination on that element. However, because the State put forth sufficient evidence to prove that element, and the district court's jury instruction accomplished the same purpose, the Supreme Court concluded the error was harmless. Accordingly, the Court found no reversible error in the district court's decision to grant the State's motion and provide the jury instruction. Therefore, judgment of conviction was affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Idaho v. Jones

Court: Idaho Supreme Court - Criminal
Docket: 45905
Opinion Date: May 4, 2020
Judge: Roger S. Burdick
Areas of Law: Constitutional Law, Criminal Law

Timothy Jones was convicted by jury of trafficking heroin and possession of drug paraphernalia. On appeal, he argued the trial court erred in admitting certain evidence regarding his probation status, a knife found in the initial police search of his person, and that the trial court abused its discretion in arriving at his sentence. Finding no reversible error, the Idaho Supreme Court affirmed Jones' conviction and sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Gordon

Court: Iowa Supreme Court

Docket: 18-1099
Opinion Date: May 1, 2020
Judge: Brent R. Appel
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction for assault on a peace officer with a dangerous weapon, a felony, and several misdemeanors, holding that Defendant did not receive ineffective assistance of counsel. After Defendant pleaded guilty, he absconded. He was later returned to custody. On appeal, Defendant argued that he received ineffective assistance of counsel because the plea bargain contained an unlawful term. Specifically, Defendant argued that the plea bargain's provision that he would be released from jail for a forty-eight-hour furlough after pleading guilty was illegal and that his trial counsel committed ineffective assistance in obtaining the illegal benefit for him. The Supreme Court affirmed, holding that where Defendant entered into the plea agreement with the illegally lenient sentence, he could not benefit from that sentence and then attack the plea bargain.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Craig

Court: Kansas Supreme Court
Docket: 119660
Opinion Date: May 1, 2020
Judge: Dan Biles
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's conviction and sentence for first-degree felony murder, holding that there was no error in the proceedings below. A jury found Defendant guilty of both first-degree felony murder and second-degree intentional murder. At sentencing, Defendant moved for a new trial and judgment notwithstanding the verdict, arguing that the jury must have had reasonable doubt on the first-degree felony murder theory because it convicted him of second-degree murder for the same killing. The district court dismissed the second-degree murder conviction and sentenced Defendant for the felony murder over his objection. The Supreme Court affirmed, holding (1) the district court did not err when it sentenced Defendant on felony murder instead of declaring a mistrial because

Defendant did not establish that the jury failed to find each element of the felony murder beyond a reasonable doubt or that the jury's first- and second-degree murder verdicts were so irreconcilable as to require a new trial; and (2) the district court did not err in declining to give an instruction on voluntary intoxication.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Lemmie

Court: Kansas Supreme Court
Docket: 119439
Opinion Date: May 1, 2020
Judge: Carol A. Beier
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's convictions of first-degree felony murder, aggravated robbery, conspiracy to commit aggravated robbery, criminal possession of a firearm, fleeing and eluding, and interference with law enforcement, holding that Defendant's arguments on appeal failed. Specifically, the Supreme Court held (1) any possible violation of Defendant's Fifth Amendment right in the admission of a witness's testimony about Defendant giving the witness phone passcodes was undoubtedly harmless; (2) the district court did not err by admitting hearsay statements as statements of a coconspirator and contemporaneous statements; (3) the State introduced sufficient evidence to convict Defendant of first-degree murder; and (4) the district judge did not abuse its discretion by admitting testimony that Defendant was upset over a meth pipe that went missing.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Mullen

Court: Maine Supreme Judicial Court
Citation: 2020 ME 56
Opinion Date: May 5, 2020
Judge: Connors
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed Defendant's conviction for reckless

conduct and aggravated criminal mischief, holding that the trial court did not abuse its discretion by offering Defendant a continuance of the trial in lieu of excluding his medical records. On appeal, Defendant argued that the trial court abused its discretion by denying his motion to suppress his personal medical records as a sanction for the State's late seizure of the records. The Supreme Judicial Court agreed that the State's conduct undermined the purpose of Maine Rule of Unified Criminal Procedure 18(b) but that the court's offer of a continuance in lieu of the exclusion of the evidence constituted an appropriate response to the State's conduct.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. Billingslea

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12715
Opinion Date: April 30, 2020
Judge: Cypher
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Judicial Court affirmed Defendant's convictions and the decision of the Appeals Court denying Defendant's motion to vacate the entry of his appeal from his convictions in that court and to have the case entered directly in the Supreme Judicial Court, holding that a direct appeal from the third conviction of a habitual offender pursuant to Mass. Gen. Laws ch. 279, 25(b) may be entered in the Appeals Court. Defendant was indicted for serious felonies arising from a brutal attack and rape. In addition to charging the specific felony, each indictment also alleged that the sentence for that felony should be enhanced pursuant to the habitual criminal provision Mass. Gen. Laws ch. 279, 25(a) or the habitual offender provision of section 25(b), or both. After he was convicted, Defendant moved to have the case entered directly in the Supreme Judicial Court. The Appeals Court denied the motion. The Supreme Judicial Court affirmed Defendant's convictions, holding (1) this direct appeal was entitled to the unique review prescribed by Mass Gen. Laws ch. 278, 33E, and the Appeals Court may conduct such section 33E review; (2) Defendant was not impermissibly allowed to waive his right to a jury trial on the sentencing enhancement provisions of the indictments; and (3) Defendant was not entitled to reversal of his convictions on any other ground.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. Martin

Court: Massachusetts Supreme Judicial Court
Docket: SJC-08768
Opinion Date: May 5, 2020
Judge: Ralph D. Gants
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Judicial Court affirmed Defendant's conviction of murder in the first degree and the denial of his motion for a new trial and declined to exercise its authority under Mass. Gen. Laws ch. 278E to reduce Defendant's conviction to murder in the second degree, holding that Defendant was not entitled to relief on any of his allegations of error. Defendant was convicted of murder in the first degree on the theory of felony-murder. Defendant filed a motion for a new trial, which was denied. The Supreme Judicial Court affirmed, holding (1) Defendant's motion for a new trial was correctly denied because Defendant was not prejudiced by counsel's ineffective assistance; (2) this Court declines to extend the reach of the Court's holding in Commonwealth v. Brown, 477 Mass. 805 (2017), to Defendant's case; and (3) trial judge erred when he declined Defendant's request that the jury be instructed on the elements of voluntary and involuntary manslaughter, but the error was not prejudicial in the context of the judge's other instructions.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. Tavares

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12631
Opinion Date: May 6, 2020
Judge: Lowy
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed Defendant's conviction of murder in the first degree on theories of deliberate premeditation and extreme atrocity

or cruelty and declined to exercise its power pursuant to Mass. Gen. Laws ch. 278, 33E to reduce the conviction to manslaughter, holding that there was no reversible error in the proceedings below. Specifically, the Supreme Judicial Court held (1) the trial judge did not err by denying Defendant's requests for a jury instruction pursuant to Commonwealth v. Croft, 345 Mass. 143 (1962); (2) the trial judge did not err by denying Defendant's motions for a required finding of not guilty under Croft because a rational jury could have found that Defendant was guilty of murder in the first degree on both the theories of premeditation and extreme atrocity or cruelty; and (3) there was no basis for reducing Defendant's sentence or ordering a new trial.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Branch

Court: Minnesota Supreme Court
Docket: A18-1055
Opinion Date: May 6, 2020
Judge: Lorie Skjerven Gildea
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's sentences for drive-by shooting at an occupied vehicle and second-degree assault, holding that Minn. Stat. 609.035 did not prohibit the sentences for both offenses when the crimes arose from a single behavioral incident. The district court sentenced Defendant to forty-eight months for drive-by shooting at an occupied vehicle and thirty-six months for second-degree assault and imposed the two sentences to run concurrently. The court of appeals affirmed. The Supreme Court affirmed, holding that, under this Court's analysis in State v. Ferguson, 808 N.W.2d 586 (Minn. 2012), the district court properly imposed multiple sentences in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

Galloway v. Mississippi

Court: Supreme Court of Mississippi
Citation: 2018-CA-01427-SCT

Opinion Date: May 7, 2020
Judge: Beam
Areas of Law: Constitutional Law, Criminal Law

Leslie Galloway appealed the denial of his 2015 petition for post-conviction relief (PCR) pertaining to his 2007 guilty plea to carjacking, a conviction that was used as an aggravating circumstance in Galloway's 2010 capital-murder trial at which Galloway received a death sentence. Galloway claimed in the petition that his defense counsel Wendy Martin had an actual conflict of interest because, before becoming his defense counsel, Martin had served as an assistant district attorney in the same case, unbeknownst to Galloway. The trial court ruled that Galloway's PCR claim was time barred under Mississippi's Uniform Post-Conviction Collateral Relief Act (UPCCRA), having been filed more than seven years after Galloway's conviction for carjacking. The trial court alternatively found no merit to Galloway's PCR claim, time bar notwithstanding. Accordingly, the trial court denied Galloway's PCR petition. The Mississippi Supreme Court agreed with the trial court that Galloway's PCR claim was time barred under the UPCCRA. The Court also agreed there was no merit to Galloway's PCR claim.

Read Opinion Are you a lawyer? **Annotate this case**.

City of Missoula v. Zerbst

Court: Montana Supreme Court
Citation: 2020 MT 108
Opinion Date: May 5, 2020
Judge: Beth Baker
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court reversed Defendant's conviction for sexual assault, holding that the municipal court erred when it instructed the jury on a definition of "consent" from the 2017 sexual assault statute and not the applicable 2015 statute, and the erroneous jury instruction prejudicially affected Defendant's substantial rights. At trial, the court instructed the jury, over Defendant's objection, on the definition of consent contained in recent amendments to the sexual assault statute. On appeal, Defendant argued that the municipal court failed to apply the correct law when instructing the jury on the elements of the claimed offense. The district court denied the

appeal. The Supreme Court reversed, holding (1) the instructions, as a whole, did not fully and fairly instruct the jury on the law applicable to the case; and (2) Defendant's substantial due process right was prejudiced by the erroneous jury instruction.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Degarmo

Court: Nebraska Supreme Court
Citation: 305 Neb. 680
Opinion Date: May 1, 2020
Judge: Stacy
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction of driving under the influence, holding that Defendant consented to a chemical test of his urine and, therefore, the results of the urine test were admissible. A law enforcement officer stopped Defendant for an expired registration. Based on his observations, the officer, a certified drug recognition evaluation expert, administered field sobriety tests. The officer concluded that Defendant was under the influence of marijuana arrested Defendant for driving under the influence and then took him to a detoxification center. Thereafter, a chemical test of Defendant's urine confirmed the presence of marijuana. On appeal, Defendant challenged the admission of the results of the urine test. The Supreme Court affirmed, holding that Defendant voluntarily consented to the warrantless search of his urine, and therefore, the search fell within a recognized exception to the warrant requirement.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Holz

Court: New York Court of Appeals
Citation: 2020 NY Slip Op 02682
Opinion Date: May 7, 2020
Judge: Fahey
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Court of Appeals held that N.Y. Crim. Proc. Law (CPL) 710.70(2) grants a defendant the right to review of a suppression decision when the order related exclusively to a count that was satisfied by a guilty plea but was not one to which the defendant pleaded guilty. Defendant was charged with two counts of burglary in the second degree. The first count related to a laptop computer, and the second count related to jewelry. Defendant moved to suppress the jewelry, but Supreme Court denied the motion. Defendant then pleaded guilty to one count of burglary in the second degree as charged in the count pertaining to the theft of the laptop computer, in satisfaction of the count charging the burglary of jewelry. On appeal, Defendant argued that Supreme Court erred in denying his motion to suppress the jewelry. The Appellate Division affirmed, concluding that it was jurisdictionally precluded from reviewing the suppression order. The Court of Appeals reversed, holding (1) Defendant's right to appellate review of Supreme Court's suppression order was secured by CPL 710.70(2); and (2) because the Appellate Division did not reach the underlying suppression question the case must be remitted to the Appellate Division for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Maffei

Court: New York Court of Appeals
Citation: 2020 NY Slip Op 02680
Opinion Date: May 7, 2020
Judge: DiFiore
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Court of Appeals affirmed the order of the Appellate Division concluding on direct appeal that Defendant was not entitled to relief on his ineffective assistance of counsel claim, holding that Defendant, on this record, did not sustain his burden to establish that counsel was constitutionally ineffective. After a jury trial, Defendant was convicted of second-degree murder. On appeal, Defendant argued that his trial counsel's failure to challenge a prospective juror constituted ineffective assistance of counsel. The Appellate Division affirmed. The Court of Appeals affirmed, holding (1) the record was inadequate to review Defendant's ineffective assistance of counsel claim; and (2) the appropriate procedure for the litigation of Defendant's challenge to his counsel's performance was a N.Y. Crim. Proc.

Law 440.10 motion.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Bailey

Court: North Carolina Supreme Court
Docket: 360A19
Opinion Date: May 1, 2020
Judge: Davis
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the decision of the court of appeals affirming the order of the trial court denying Defendant's motion to suppress evidence seized during the execution of a search warrant, holding that the warrant supported by probable cause. Defendant pled guilty to the offense of trafficking in cocaine while preserving his right to appeal the denial of his motion to suppress. On appeal, Defendant argued that the trial court erred in denying his motion to suppress because the facts contained in the affidavit were insufficient to establish probable cause to search his residence. The court of appeals affirmed. The Supreme Court affirmed, holding that the affidavit contained facts that were sufficient to provide a nexus between the residence and suspected criminal activity, and therefore, the warrant was supported by probable cause.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Ellis

Court: North Carolina Supreme Court
Docket: 340A19
Opinion Date: May 1, 2020
Judge: Robin E. Hudson
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court reversed the decision of the Court of Appeals affirming the trial court's denial of Defendant's motion to suppress evidence, holding that there was no reasonable suspicion to justify the law enforcement officer's stop when Defendant signaled with his middle finger from the passenger side window of a moving vehicle. While assisting a stranded

motorist, the officer turned his attention to another car traveling on the roadway, a white SUV. Defendant had his arm outside the passenger window and gestured with his middle finger, making an up-and-down motion. Believing that Defendant was committing the crime of disorderly conduct, the officer pursued and then stopped the SUV. At trial, Defendant moved to suppress the officer's testimony, arguing that there was no reasonable suspicion to justify the stop. The trial court denied the motion. Defendant pleaded guilty to resisting, delaying, or obstructing a public officer. The court of appeals affirmed the trial court's denial of Defendant's motion to suppress. The Supreme Court reversed, holding that the specific, articulable facts did not establish reasonable suspicion of the crime of disorderly conduct.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Hobbs

Court: North Carolina Supreme Court
Docket: 263PA18
Opinion Date: May 1, 2020
Judge: Earls
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court reversed Defendant's conviction, holding that the trial court clearly erred in ruling that Defendant failed to prove purposeful discrimination with respect to the State's use of peremptory challenges to strike three jurors without considering all of the evidence presented by Defendant. Defendant was found guilty of one count of first-degree murder and other crimes. On appeal, Defendant argued that the trial court erred by failing to grant three objections that he made under Batson v. Kentucky, 476 U.S. 79 (1986). The court of appeals affirmed Defendant's convictions. The Supreme Court reversed, holding (1) the court of appeals erred in its analysis of Defendant's Batson claims with respect to the three jurors; and (2) as to all three jurors, remand was required for reconsideration of whether Defendant proved purposeful discrimination in each case.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Mylett

Court: North Carolina Supreme Court
Docket: 6A19
Opinion Date: May 1, 2020
Judge: Earls
Areas of Law: Criminal Law

The Supreme Court reversed the decision of the court of appeals affirming the trial court's judgment convicting Defendant for conspiracy to commit harassment of a juror, holding that the trial court erred in denying Defendant's motion to dismiss the conspiracy charge for insufficient evidence. Defendant was convicted of conspiracy to commit harassment of a juror because of his actions at a courthouse following his twin brother's conviction for assault on a government official. On appeal, the court of appeals concluded that the trial court did not err in denying Defendant's motion to dismiss the conspiracy charge for insufficient evidence. The Supreme Court reversed, holding that the evidence in Defendant's trial was insufficient to raise anything more than mere conjecture that he had made an agreement with another person to threaten or intimidate a juror.

Read Opinion Are you a lawyer? **Annotate this case**.

Dodge v. North Dakota

Court: North Dakota Supreme Court
Citation: 2020 ND 100
Opinion Date: May 7, 2020
Judge: Gerald W. VandeWalle
Areas of Law: Constitutional Law, Criminal Law

Richard Dodge appealed from a district court order denying his application for post-conviction relief. Dodge was charged with five felonies and a misdemeanor in December 2015. Dodge was appointed counsel. In April 2016, Dodge's counsel moved the court to withdraw because the attorney-client relationship was "irreparably broken and rendered unreasonably difficult." The court granted the motion, and Dodge was appointed substitute counsel in May 2016. In July 2016, Dodge himself filed a "motion to dismiss counsel." The court denied Dodge's motion. Five months after the deadline for motions and plea agreements, Dodge's counsel sought to have Dodge submit to a psychiatric examination. This request was denied, the trial court

found no evidence, and the the court itself made no observations, that Dodge was incompetent to stand trial. After this denial, Dodge himself again moved to dismiss his trial counsel, and due to the allegations Dodge made in his motion, counsel moved to withdraw. The trial court denied both motions, and instead, required the attorney to appear as standby counsel and assist Dodge during trial if requested, but relieved him of any further obligations to consult with Dodge. The case proceeded to trial. At the beginning of trial, the court gave Dodge the option of representing himself or having his attorney represent him. Dodge chose to have his attorney represent him. Because his attorney had not prepared for trial and had no communication with Dodge since he moved to withdraw, Dodge's attorney asked for a brief recess to consult with Dodge. During the recess, a settlement was reached. Dodge agreed to enter Alford pleas on all counts, waived a presentence investigation, and agreed to be sentenced immediately after entering his pleas. Dodge was immediately sentenced following his guilty pleas, and thereafter sought post-conviction relief on grounds he was not competent to enter his pleas, and that he received ineffective assistance of trial counsel. After review, the North Dakota Supreme Court concluded the district court's finding that Dodge was competent when he entered his pleas was not clearly erroneous, and disposed of his claim of ineffective assistance of counsel.

Read Opinion Are you a lawyer? **Annotate this case**.

Hewitt v. NDDOT

Court: North Dakota Supreme Court
Citation: 2020 ND 102
Opinion Date: May 7, 2020
Judge: Lisa K. Fair McEvers
Areas of Law: Criminal Law, Government & Administrative Law

Larry Hewitt appealed a district court judgment affirming the North Dakota Department of Transportation's revocation of his driving privileges. Hewitt claimed the Department's hearing file was improperly admitted at the administrative hearing. After review, the North Dakota Supreme Court affirmed, concluding the hearing file was properly admitted as a self-authenticating copy of an official record.

Read Opinion Are you a lawyer? **Annotate this case**.

Kastet v. NDDOT

Court: North Dakota Supreme Court
Citation: 2020 ND 91
Opinion Date: May 7, 2020
Judge: Daniel J. Crothers
Areas of Law: Criminal Law, Government & Administrative Law

The North Dakota Department of Transportation (Department) appealed the district court's reversing a hearing officer's decision suspending Holden Kastet's driving privileges for 365 days. The Department argued the hearing officer did not abuse his discretion in admitting the chemical breath test, and State Highway Patrol Trooper King scrupulously complied with the approved method for testing Kastet's breath on the Intoxilyzer 8000. After review, the North Dakota Supreme Court concurred with the Department and reversed the district court judgment. The matter was remanded with instructions to reinstate the hearing officer's decision.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Dahl

Court: North Dakota Supreme Court
Citation: 2020 ND 87
Opinion Date: May 7, 2020
Judge: Jerod E. Tufte
Areas of Law: Constitutional Law, Criminal Law

The State of North Dakota appealed a district court order denying its motion to resume prosecution against Matthew Dahl and dismissing the case. In December 2014, the State charged Dahl with two counts of theft. Dahl did not appear on the charges until he was arrested on a bench warrant in February 2017. In mid-April 2017, the State mailed Dahl a pretrial diversion agreement. Dahl signed and returned the notarized agreement dated May 3, 2017. On May 9, 2017, the state's attorney signed and filed the agreement with the district court, and the court approved the agreement the same day. Under the agreement, the State agreed to suspend prosecution for "two

years from the date of execution" conditioned on Dahl's timely payment of restitution. Dahl failed to make minimum monthly restitution payments. On June 6, 2019, the State moved to resume prosecution, alleging Dahl violated the pretrial diversion agreement by his non-payment. The district court held a hearing on the State's motion in August 2019. The court concluded the pretrial agreement was executed when Dahl signed it on May 3, 2017. The court then denied the State's motion to resume prosecution as untimely under N.D.R.Crim.P. 32.2(d)(2), and dismissed the complaint against Dahl. After review, the North Dakota Supreme Court reversed, concluding the district court erred in determining the State's motion was untimely, and remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Foster

Court: North Dakota Supreme Court
Citation: 2020 ND 85
Opinion Date: May 7, 2020
Judge: Jon J. Jensen
Areas of Law: Constitutional Law, Criminal Law

Akeem Foster was convicted by jury of Terrorizing and Carrying a Concealed Weapon. Foster contended on appeal he was denied a fair trial because he was asked during cross-examination if other witnesses were lying and because the prosecutor expressed personal beliefs about the evidence during closing arguments. Foster also argued there was insufficient evidence to convict him of either charge. After review, the North Dakota Supreme Court affirmed Foster's conviction for Carrying a Concealed Weapon, but reversed his conviction for Terrorizing. The Court found Foster was improperly asked to provide an opinion on the veracity and credibility of the State's witnesses. The improper questioning was prejudicial and denied Foster a fair trial on the terrorizing charge.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Kolstad

Court: North Dakota Supreme Court

Citation: 2020 ND 97
Opinion Date: May 7, 2020
Judge: Gerald W. VandeWalle
Areas of Law: Constitutional Law, Criminal Law

In December 2018, Officer Nelson of the University of North Dakota Police Department conducted a traffic stop of Stanley Kolstad for suspicion of driving under the influence. Kolstad performed field sobriety tests and a preliminary breath test (PBT). Prior to performing the PBT, Kolstad informed Nelson that he had asthma. Nelson testified he was unable to obtain a PBT result because Kolstad was filling his cheeks with air while performing the test. Kolstad was arrested for DUI and refusing to submit to a chemical test. Kolstad was transported to the UND police station to be given an Intoxilyzer breath test. Prior to the Intoxilyzer test, Nelson read Kolstad the implied consent advisory. But, because Nelson was not a certified operator of the Intoxilyzer machine, Officer Waltz conducted the test. Prior to the test, Kolstad informed Waltz he had asthma. The Intoxilyzer test results were deficient. Waltz testified Kolstad was not providing enough air for the test machine to provide a valid result. Kolstad was charged with driving under the influence and refusing to submit to a chemical test. Kolstad's counsel made a discovery request to the State seeking copies of any audio or video recordings taken by police officers. Kolstad's counsel also requested the State inform him whether any sound or video recordings taken of Kolstad were subsequently "altered, edited, destroyed, or discarded." The State provided Kolstad's counsel with dash camera footage from Nelson's police car that had been taken at the scene of the arrest, but the State did not provide any body camera footage from either Nelson or Waltz. Upon learning that Waltz's body camera footage was successfully uploaded to UND servers, Kolstad's counsel moved to dismiss the case because the State did not provide any body camera footage in discovery as requested. The district court ultimately dismissed the refusal to submit to a chemical breath test charge as a sanction for failing to provide the body camera footage. The State appealed, arguing the alleged discovery violation did not rise to a constitutional violation of Kolstad's due process rights, and the district court abused its discretion in dismissing the refusal charge. Kolstad argued the district court's order dismissing the refusal charge was not appealable, and if it was, the court did not abuse its discretion in dismissing the charge. The North Dakota Supreme Court concluded there was nothing in the record to indicate the district court adequately considered an

alternative or less severe sanction to dismissal, and by not considering a less severe sanction, the trial court erred. The district court's order dismissing the refusal charge was reversed, and the matter remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Michel

Court: North Dakota Supreme Court
Citation: 2020 ND 101
Opinion Date: May 7, 2020
Judge: Jerod E. Tufte
Areas of Law: Constitutional Law, Criminal Law

Kevin Michel was convicted by jury of knowingly receiving stolen property. Jamestown Police began investigating theft of tires from Northwest Tire in October 2017. About ten months later, Thomas Melland and Andrew Heckelsmiller became suspects in the investigation. Heckelsmiller told police he had sold stolen tires to Michel. In August 2018, Detective LeRoy Gross spoke with Michel about the stolen tires. Michel acknowledged he had bought tires from Heckelsmiller and Melland. Michel also told Detective Gross he stopped buying tires from Heckelsmiller and Melland after seeing a Facebook post from Northwest Tire offering a $500 reward for information regarding stolen tires. Detective Gross told Michel, "There's going to be a lot of restitution these two boys are going to have to come up with unless we can get some tires back." Michel said he had sold several of the tires but still had some of them. Michel turned over seven new tires to Detective Gross. Representatives from Northwest Tire and J&L Service identified the tires as some of those stolen from their shops. During the jury's deliberations, the jury submitted a note with written questions to the court. Michel argued on appeal the district court erred by not specifically answering the jury's questions and instead referring them to the existing jury instructions. After review, the North Dakota Supreme Court affirmed the criminal judgment, except as to the award of restitution. The award was reversed because the district court awarded more than what was required to make the victims whole. The matter was remanded for a redetermination of restitution.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Wayland

Court: North Dakota Supreme Court
Citation: 2020 ND 106
Opinion Date: May 7, 2020
Judge: Jon J. Jensen
Areas of Law: Constitutional Law, Criminal Law

Joey Wayland appealed after he was convicted by jury of Theft of Property and Possession of Drug Paraphernalia. Wayland contended his case should have been dismissed because his right to a speedy trial was violated by a continuance of his trial from March 11, 2019 to April 8, 2019. Wayland also contended the district court violated his right to remain silent by ordering him to submit to a mental health evaluation. Finding no reversible error, the North Dakota Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Schwindt v. Sorel

Court: North Dakota Supreme Court
Citation: 2020 ND 92
Opinion Date: May 7, 2020
Judge: Lisa K. Fair McEvers
Areas of Law: Constitutional Law, Criminal Law, Government & Administrative Law

Gregory Schwindt appealed a district court judgment affirming a Department of Transportation hearing officer's revocation of his driving privileges for 180 days. Schwindt argued North Dakota's implied consent and refusal laws were unconstitutional, the hearing officer erred by considering the results of the horizontal gaze nystagmus (HGN) test, and the hearing officer erred in finding he refused to take a chemical test. After review, the North Dakota Supreme Court concluded the hearing officer's findings of fact were supported by a preponderance of the evidence, the conclusions of law were sustained by the findings of fact, and the decision to revoke Schwindt's driving privileges was in accordance with the law.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. McDougald v. Greene

Court: Supreme Court of Ohio
Citation: 2020-Ohio-2782
Opinion Date: May 6, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court denied a writ of mandamus sought by Relator to compel Respondent, the public-records custodian at the Southern Ohio Correctional Facility (SOCF), to provide Relator with three public records and to pay Relator statutory damages and court costs associated with this litigation, holding that Relator was not entitled to either a writ of mandamus nor statutory damages. When Relator was an inmate at SOCF he submitted a public-records request to Respondent seeking three documents. Respondent provided one of the three documents. Relator then filed a complaint for a writ of mandamus seeking an order compelling Respondent to provide the two documents and to pay statutory damages and court costs associated with this litigation. The Supreme Court denied the writ of mandamus on the merits, holding that Respondent's response to Relator fully satisfied Respondent's obligations under Ohio Rev. Code 149.43, and therefore, Relator was not entitled a writ of mandamus, and there was no basis to award statutory damages.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Parker Bey v. Byrd

Court: Supreme Court of Ohio
Citation: 2020-Ohio-2766
Opinion Date: May 5, 2020
Judge: Maureen O'Connor
Areas of Law: Criminal Law

The Supreme Court affirmed in part and reversed in part the judgment of the court of appeals denying Appellant's complaint for a writ of mandamus to compel the Cuyahoga County Clerk of Courts to produce various court records and denying the clerk's request that Appellant be declared a vexatious litigator, holding that the court of appeals erred in denying Appellant's complaint on the grounds that he did not invoke the Rules of

Superintendence as the basis for his request. Appellant sought copies of journal entries from his criminal case and a copy of the clerk of courts' records-retention schedule. The clerk largely denied the request. Appellant then filed a complaint for a writ of mandamus. The court of appeals denied Appellant's request for mandamus relief, concluding that the clerk had no clear legal duty to provide the requested records. The Supreme Court reversed, holding (1) this action to compel the production of journal entries from a 1995 case was properly brought under the Public Records Act; and (2) this Court declines to impose sanctions on Appellant or to declare him a vexatious litigator.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Dangler

Court: Supreme Court of Ohio
Citation: 2020-Ohio-2765
Opinion Date: May 5, 2020
Judge: DeWine
Areas of Law: Criminal Law

The Supreme Court reversed the judgment of the court of appeals vacating Defendant's conviction and sentence and reinstated the trial court's acceptance of Defendant's plea of no contest to sexual battery, holding that the trial court did not completely fail to comply with Crim.R.11(C)(2)(a), and there was nothing in the record to support a conclusion that Defendant would not have entered his plea had the trial court been more detailed in its explanation. On appeal, Defendant sought to vacate his plea of no contest, arguing that his plea was invalid because the trial court erred by not explaining more fully the obligations and restrictions that went with his status as a sex offender, in violation of Crim. R. 11(C)(2)(a). The court of appeals vacated the conviction without requiring Defendant to show prejudice, concluding that the trial court had completely failed to comply with Crim. R. 11(C)(2)(a). The Supreme Court reversed, holding (1) the trial court did not completely failed to comply with Crim R. 11(C)(2)(a)'s maximum-penalty-advisement requirement; and (2) because Defendant did not establish prejudice, he was not entitled to have his no-contest plea vacated for a failure to comply with Crim.R. 11(C).

Read Opinion Are you a lawyer? **Annotate this case**.

Oregon v. Haji

Court: Oregon Supreme Court
Docket: S066254
Opinion Date: May 7, 2020
Judge: Nakamoto
Areas of Law: Constitutional Law, Criminal Law

After a grand jury issued an indictment charging defendant Hanad Ali Haji with multiple offenses, the district attorney determined that the indictment could be challenged by demurrer because the basis for joining those offenses was not expressly alleged. Instead of seeking another indictment from the grand jury, the district attorney obtained leave from the trial court to amend the indictment by adding allegations specifying the statutory basis for joinder, without adding factual allegations about the crimes. Defendant was convicted on some of the charges at trial, and the Court of Appeals affirmed. The issue this case presented for the Oregon Supreme Court's review centered on whether the district attorney could add allegations specifying the statutory basis for joinder of multiple offenses to an indictment instead of resubmitting the case to the grand jury. The Supreme Court determined that neither the statute permitting joinder of multiple offenses in a single indictment nor Article VII (Amended), section 5(6), of the Oregon Constitution precluded a district attorney, with approval of the trial court, from amending an indictment to add allegations specifying the statutory basis for joinder of multiple offenses. The Supreme Court affirmed the decision of the Court of Appeals, based in part on different reasoning, and affirmed the judgment of the circuit court.

Read Opinion Are you a lawyer? **Annotate this case**.

South Carolina v. Durant

Court: South Carolina Supreme Court
Docket: 27964
Opinion Date: May 6, 2020
Judge: Kaye Gorenflo Hearn
Areas of Law: Constitutional Law, Criminal Law

Appellant Larry Durant was convicted of second-degree criminal sexual conduct (CSC) for sexually abusing a teenage girl in his church office where he served as the pastor. Durant contended the trial court improperly permitted the State to introduce evidence of prior sexual abuse allegations as evidence of a common scheme or plan under Rule 404(b), SCRE, and that the State committed a "Brady" violation by failing to accurately disclose the criminal history of its witness. After review, the South Carolina Supreme Court affirmed the admissibility of the girls' testimony. "[W]hile the State failed to disclose the criminal background information of its witness, we find this information was not material." The Court found Durant exercised his position of trust, authority, and spiritual leadership to hold private prayer meetings with teen girls who had grown up in his church. He told them he was praying for their health and good fortune, and represented that part of this process was touching them sexually and having intercourse. Durant then warned the girls of misfortune if they refused or told anyone. Moreover, he used scripture as a means of grooming the children into performing sex acts. "These facts demonstrate the requisite logical connection between the prior acts of sexual abuse and the one forming the basis of the crime charged." The Court therefore affirmed Durant's conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

South Carolina v. Perry

Court: South Carolina Supreme Court
Docket: 27963
Opinion Date: May 6, 2020
Judge: Few
Areas of Law: Constitutional Law, Criminal Law

Petitioner Wallace Perry was convicted on two counts of criminal sexual conduct (CSC) with a minor in the first degree and two counts of CSC with a minor in the second degree for sexually assaulting two of his biological daughters. Prior to Perry's trial, the State made a motion to admit the testimony of Perry's stepdaughter from an earlier marriage that Perry sexually assaulted her twenty-two to twenty-seven years earlier. The State argued the trial court should not exclude the stepdaughter's testimony under Rule 404(b) of the South Carolina Rules of Evidence because it fit the

"common scheme or plan" exception. Perry objected to this testimony. The trial court initially reserved ruling on the issue, but later indicated it was inclined to allow the stepdaughter to testify. The jury convicted Perry on all counts, and the trial court sentenced him to thirty years in prison. The court of appeals affirmed. The South Carolina Supreme Court determined it was not enough to meet the "logical connection" standard for admission of other crimes under the common scheme or plan exception to Rule 404(b) that the defendant previously committed the same crime. "When evidence of other crimes is admitted based solely on the similarity of a previous crime, the evidence serves only the purpose prohibited by Rule 404(b), and allows the jury to convict the defendant on the improper inference of propensity that because he did it before, he must have done it again. ...The common scheme or plan exception demands more." The Supreme Court held State must show a logical connection between the other crime and the crime charged such that the evidence of other crimes "reasonably tends to prove a material fact in issue." The State must also convince the trial court that the probative force of the evidence when used for this legitimate purpose is not substantially outweighed by the danger of unfair prejudice from the inherent tendency of the evidence to show the defendant's propensity to commit similar crimes. In this case, the State did not meet its burden. Conviction was reversed and the matter remanded for a new trial.

Read Opinion Are you a lawyer? **Annotate this case**.

South Carolina v. Quinn

Court: South Carolina Supreme Court
Docket: 27966
Opinion Date: May 6, 2020
Judge: Kaye Gorenflo Hearn
Areas of Law: Constitutional Law, Criminal Law, White Collar Crime

Respondent Rick Quinn, Jr. was a former member of the South Carolina House of Representatives, representing constituents in Richland and Lexington counties from 1989-2004 and 2010-2017 and serving as House Majority Leader from 1999- 2004. He owned and operated a mail business called Mail Marketing Strategies (MMS) in Columbia, while his father owned and operated a political consulting firm, Richard Quinn & Associates (RQ&A). In 2014, Attorney General Alan Wilson designated First Circuit

Solicitor David Pascoe as special prosecutor to conduct a State grand jury investigation into alleged public corruption committed by current and former members of the South Carolina General Assembly. This case arose from a prior state grand jury investigation of former House Speaker Bobby Harrell, which resulted in six counts of misusing campaign funds, to which he pleaded guilty. During the course of the investigation into Speaker Harrell, SLED uncovered potentially criminal conduct by Representative Jimmy Merrill and Representative Rick Quinn, and a second grand jury investigation was initiated to investigate the conduct of these individuals. The investigation focused on Quinn's practice of using his office as House Majority Leader and leader of the House Republican Caucus to direct mailing and political services to his family's businesses. Quinn only admitted to a limited set of facts supporting the indictment. Believing the plea lacked a sufficient basis, the State moved to vacate Quinn's guilty plea, reconsider the sentence, and for the trial court's recusal. The State appealed the order denying its motions. After review, the South Carolina Supreme Court determined that the State could not appeal the guilty plea, the trial court did not abuse its discretion in sentencing, and there was no evidence of judicial bias or prejudice requiring the court to recuse itself. Therefore, the Court dismissed the State's appeal of the guilty plea, and affirmed as to all other issues.

Read Opinion Are you a lawyer? **Annotate this case**.

Texas v. Arellano

Court: Texas Court of Criminal Appeals
Docket: PD-0287-19
Opinion Date: May 6, 2020
Judge: Slaughter
Areas of Law: Constitutional Law, Criminal Law

After Appellee Cesar Ramiro Arellano was arrested for driving while intoxicated, the arresting officer, Phillip Garcia, prepared a probable cause affidavit to support a search warrant for a blood draw. Officer Garcia submitted his sworn affidavit to the on-duty magistrate. Using a cursive signature, the magistrate signed the blank signature line of a form search warrant authorizing the search and seizure of Appellee's blood. Below the signature line appeared the words, "Magistrate, Victoria County, Texas."

Aside from the cursive signature, the magistrate's name was not typed or handwritten anywhere on the warrant. Upon execution of the search warrant, Appellee was charged with DWI. In the trial court, Appellee filed a motion to suppress all evidence stemming from the blood draw. At the pretrial suppression hearing, Appellee argued that the search warrant to obtain the blood specimen was facially invalid because the magistrate's signature was illegible in violation of the requirements of Code of Criminal Procedure Article 18.04(5). The trial court agreed, the court of appeals concurred, and the evidence was suppressed because of the illegible signature. The Texas Court of Criminal Appeals disagreed with both lower courts, finding the court of appeals erred in holding that reliance on the statutory good-faith exception was automatically precluded based on an illegible magistrate's signature in violation of Code of Criminal Procedure Article 18.04(5). Because the remaining issues in the case were not properly addressed by the court of appeals, judgment was vacated and the matter remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

About Justia Opinion Summaries

Justia Weekly Opinion Summaries is a free service, with 63 different newsletters, each covering a different practice area.

Justia also provides 68 daily jurisdictional newsletters, covering every federal appellate court and the highest courts of all US states.

All daily and weekly Justia newsletters are free. Subscribe or modify your newsletter subscription preferences at daily.justia.com.

You may freely redistribute this email in whole.

About Justia

Justia is an online platform that provides the community with open access to the law, legal information, and lawyers.



Unsubscribe From This Newsletter

or unsubscribe from all Justia newsletters immediately **here.**



Justia | 1380 Pear Ave #2B, Mountain View, CA 94043

From:	Criminal Law - Justia Weekly Opinion Summaries
To:	Burton, Ray (POL)
Subject:	Latest 111 Cases This Week: Kelly v. United States (U.S.), Gomes v. Silva (1st Cir.), United States v. Perez-Couvertier (1st Cir.)
Date:	Friday, May 8, 2020 9:07:12 AM

If you are unable to see this message, click here to view it in a web browser.

Justia Weekly Opinion Summaries



Criminal Law
May 8, 2020

Table of Contents

Kelly v. United States
Criminal Law, Government & Administrative Law, White Collar Crime
US Supreme Court

Gomes v. Silva
Civil Rights, Constitutional Law, Criminal Law

US Court of Appeals for the First Circuit

United States v. Perez-Couvertier
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the First Circuit

United States v. Haverkamp
Criminal Law
US Court of Appeals for the Second Circuit

United States v. Mladen
Criminal Law, Trusts & Estates
US Court of Appeals for the Second Circuit

United States v. Richardson
Criminal Law
US Court of Appeals for the Second Circuit

United States v. Rosemond
Criminal Law
US Court of Appeals for the Second Circuit

United States v. Lacerda
Criminal Law, White Collar Crime
US Court of Appeals for the Third Circuit

Cucalon v. Barr
Criminal Law, Immigration Law
US Court of Appeals for the Fourth Circuit

United States v. Doctor
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Lewis
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Jordan
Criminal Law
US Court of Appeals for the Fifth Circuit

United States v. Longoria
Criminal Law
US Court of Appeals for the Fifth Circuit

United States v. McNabb
Criminal Law
US Court of Appeals for the Fifth Circuit

Andrews v. Wayne County
Civil Rights, Constitutional Law, Criminal Law

US Court of Appeals for the Sixth Circuit

Hicks v. Scott
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Sixth Circuit

Moody v. United States
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Sixth Circuit

United States v. Foreman
Criminal Law
US Court of Appeals for the Sixth Circuit

United States v. Smith
Criminal Law
US Court of Appeals for the Sixth Circuit

Kirkman v. Thompson
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

Tuduj v. Newbold
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

United States v. Gibson
Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

United States v. Howell
Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

United States v. Lewis
Criminal Law
US Court of Appeals for the Seventh Circuit

Bakor v. Barr
Criminal Law, Immigration Law
US Court of Appeals for the Eighth Circuit

Smith v. Titus
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Becerra
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Haynes
Criminal Law

US Court of Appeals for the Eighth Circuit

United States v. Roberts
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Wright
Criminal Law
US Court of Appeals for the Eighth Circuit

Benson v. Chappell
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Ninth Circuit

Mero v. Barr
Criminal Law, Immigration Law
US Court of Appeals for the Ninth Circuit

Romero-Millan v. Barr
Criminal Law
US Court of Appeals for the Ninth Circuit

United States v. Yang
Criminal Law
US Court of Appeals for the Ninth Circuit

United States v. Neugin
Constitutional Law, Criminal Law
US Court of Appeals for the Tenth Circuit

United States v. Ramon
Constitutional Law, Criminal Law
US Court of Appeals for the Tenth Circuit

United States v. Richards
Constitutional Law, Criminal Law
US Court of Appeals for the Tenth Circuit

Andrews v. Warden
Criminal Law
US Court of Appeals for the Eleventh Circuit

Hollis v. United States
Criminal Law
US Court of Appeals for the Eleventh Circuit

Knight v. Florida Department of Corrections
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Eleventh Circuit

United States v. Evans
Criminal Law

US Court of Appeals for the Eleventh Circuit

United States v. McLellan
Criminal Law
US Court of Appeals for the Eleventh Circuit

United States v. Russell
Criminal Law
US Court of Appeals for the Eleventh Circuit

Welch v. United States
Criminal Law
US Court of Appeals for the Eleventh Circuit

State v. Trujillo
Constitutional Law, Criminal Law
Arizona Supreme Court

Barnett v. State
Criminal Law
Arkansas Supreme Court

Mason v. Kelley
Criminal Law
Arkansas Supreme Court

Ray v. Kelley
Criminal Law
Arkansas Supreme Court

Walker v. Kelley
Criminal Law
Arkansas Supreme Court

People v. Flores
Civil Rights, Constitutional Law, Criminal Law
Supreme Court of California

California v. Law
Constitutional Law, Criminal Law
California Courts of Appeal

California v. Sanchez
Constitutional Law, Criminal Law
California Courts of Appeal

Galeotti v. International Union of Operating Engineers
Criminal Law, Labor & Employment Law, White Collar Crime
California Courts of Appeal

In re I.A.
Criminal Law, Juvenile Law

California Courts of Appeal

People v. Edwards
Criminal Law
California Courts of Appeal

People v. Thomkins
Criminal Law
California Courts of Appeal

People v. Torres
Criminal Law
California Courts of Appeal

People v. Triplett
Criminal Law
California Courts of Appeal

Colorado In Interest of G.S.S.
Constitutional Law, Criminal Law, Juvenile Law
Colorado Supreme Court

Barringer v. Halkitis
Criminal Law
Florida Supreme Court

Franqui v. State
Criminal Law
Florida Supreme Court

Hicks v. State
Criminal Law
Florida Supreme Court

Burley v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Carter v. Georgia
Construction Law, Criminal Law
Supreme Court of Georgia

Clarke v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Collins v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Dawson v. Georgia
Constitutional Law, Criminal Law

Supreme Court of Georgia

Evans v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Hill v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Oliver v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Rosser v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Spencer v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Styles v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Whitehead v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Idaho v. Blythe
Constitutional Law, Criminal Law
Idaho Supreme Court - Criminal

Idaho v. Glodowski
Constitutional Law, Criminal Law
Idaho Supreme Court - Criminal

Idaho v. Jones
Constitutional Law, Criminal Law
Idaho Supreme Court - Criminal

State v. Gordon
Civil Rights, Constitutional Law, Criminal Law
Iowa Supreme Court

State v. Craig
Criminal Law
Kansas Supreme Court

State v. Lemmie
Criminal Law

Kansas Supreme Court

State v. Mullen
Criminal Law
Maine Supreme Judicial Court

Commonwealth v. Billingslea
Civil Rights, Constitutional Law, Criminal Law
Massachusetts Supreme Judicial Court

Commonwealth v. Martin
Civil Rights, Constitutional Law, Criminal Law
Massachusetts Supreme Judicial Court

Commonwealth v. Tavares
Criminal Law
Massachusetts Supreme Judicial Court

State v. Branch
Criminal Law
Minnesota Supreme Court

Galloway v. Mississippi
Constitutional Law, Criminal Law
Supreme Court of Mississippi

City of Missoula v. Zerbst
Civil Rights, Constitutional Law, Criminal Law
Montana Supreme Court

State v. Degarmo
Civil Rights, Constitutional Law, Criminal Law
Nebraska Supreme Court

People v. Holz
Civil Rights, Constitutional Law, Criminal Law
New York Court of Appeals

People v. Maffei
Civil Rights, Constitutional Law, Criminal Law
New York Court of Appeals

State v. Bailey
Civil Rights, Constitutional Law, Criminal Law
North Carolina Supreme Court

State v. Ellis
Civil Rights, Constitutional Law, Criminal Law
North Carolina Supreme Court

State v. Hobbs
Civil Rights, Constitutional Law, Criminal Law

North Carolina Supreme Court

State v. Mylett
Criminal Law
North Carolina Supreme Court

Dodge v. North Dakota
Constitutional Law, Criminal Law
North Dakota Supreme Court

Hewitt v. NDDOT
Criminal Law, Government & Administrative Law
North Dakota Supreme Court

Kastet v. NDDOT
Criminal Law, Government & Administrative Law
North Dakota Supreme Court

North Dakota v. Dahl
Constitutional Law, Criminal Law
North Dakota Supreme Court

North Dakota v. Foster
Constitutional Law, Criminal Law
North Dakota Supreme Court

North Dakota v. Kolstad
Constitutional Law, Criminal Law
North Dakota Supreme Court

North Dakota v. Michel
Constitutional Law, Criminal Law
North Dakota Supreme Court

North Dakota v. Wayland
Constitutional Law, Criminal Law
North Dakota Supreme Court

Schwindt v. Sorel
Constitutional Law, Criminal Law, Government & Administrative Law
North Dakota Supreme Court

State ex rel. McDougald v. Greene
Criminal Law
Supreme Court of Ohio

State ex rel. Parker Bey v. Byrd
Criminal Law
Supreme Court of Ohio

State v. Dangler
Criminal Law

Supreme Court of Ohio

Oregon v. Haji
Constitutional Law, Criminal Law
Oregon Supreme Court

South Carolina v. Durant
Constitutional Law, Criminal Law
South Carolina Supreme Court

South Carolina v. Perry
Constitutional Law, Criminal Law
South Carolina Supreme Court

South Carolina v. Quinn
Constitutional Law, Criminal Law, White Collar Crime
South Carolina Supreme Court

Texas v. Arellano
Constitutional Law, Criminal Law
Texas Court of Criminal Appeals

COVID-19 Updates: Law & Legal Resources Related to Coronavirus

Click here to include Verdict article summaries with your newsletter(s).

Criminal Law Opinions

Kelly v. United States

Court: US Supreme Court
Docket: 18-1059
Opinion Date: May 7, 2020
Judge: Elena Kagan
Areas of Law: Criminal Law, Government & Administrative Law, White Collar Crime

During former New Jersey Governor Christie's 2013 reelection campaign,

Fort Lee's mayor refused to endorse Christie. Kelly, Christie's Deputy Chief of Staff, Port Authority Deputy Executive Director, Baroni, and another official decided to reduce from three to one the number of lanes reserved at the George Washington Bridge's toll plaza for Fort Lee's commuters. To disguise the political retribution, the lane realignment was said to be for a traffic study. Port Authority traffic engineers were asked to collect some numbers. An extra toll collector was paid overtime. The lane realignment caused four days of gridlock, ending only when the Port Authority's Executive Director learned of the scheme. The Third Circuit affirmed the convictions of Baroni and Kelly for wire fraud, fraud on a federally funded program, and conspiracy to commit those crimes. The Supreme Court reversed. The scheme did not aim to obtain money or property. The wire fraud statute refers to "any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses," 18 U.S.C. 1343. The federal-program fraud statute bars "obtain[ing] by fraud" the "property" (including money) of a federally funded program or entity, section 666(a)(1)(A). The statutes are limited to the protection of property rights and do not authorize federal prosecutors to set standards of good government. The Court rejected arguments that the defendants sought to take control of the Bridge's physical lanes or to deprive the Port Authority of the costs of compensating employees. Their realignment of the access lanes was an exercise of regulatory power; a scheme to alter a regulatory choice is not one to take government property. The time and labor of the employees were an incidental byproduct of that regulatory object. Neither defendant sought to obtain the services that the employees provided.

Read Opinion Are you a lawyer? **Annotate this case**.

Gomes v. Silva

Court: US Court of Appeals for the First Circuit
Docket: 19-1656
Opinion Date: May 1, 2020
Judge: Stahl
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The First Circuit affirmed the judgment of the district court denying Appellant's petition for a writ of habeas corpus, holding that, under the highly deferential standard prescribed by the Antiterrorism and Effective

Death Penalty Act for federal habeas review of state criminal convictions, Appellant's claims to habeas relief failed. Appellant was convicted in a Massachusetts superior court of murder in the first degree and related crimes. The Supreme Judicial Court (SJC) affirmed the convictions. Appellant subsequently petitioned the District Court for the District of Massachusetts for a writ of habeas corpus. The district court denied the petition but granted a certificate of appealability. The First Circuit affirmed, holding (1) sufficient evidence supported Appellant's conviction for first-degree murder as a joint venturer, and the SJC's sufficiency determination was not unreasonable; and (2) the SJC reasonably determined that the trial court's admission into evidence of certain items did not constitute error.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Perez-Couvertier

Court: US Court of Appeals for the First Circuit
Docket: 16-2186
Opinion Date: May 7, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The First Circuit affirmed Defendant's conviction of possessing with intent to distribute controlled substances in a protected area and conspiring to distribute controlled substances in a protected area, holding that the district court did not plainly err with respect to any of Defendant's challenges. Specifically, the First Circuit held (1) the district court did not commit plain error in admitting evidence of the conspiracy's activities occurring after he withdrew from the conspiracy or, alternatively, in not instructing the jury to ignore such evidence; (2) the district court did not plainly err in admitting evidence of a drug trafficking organization's violent acts; and (3) the delay between Defendant's indictment and arrest did not violate his Sixth Amendment right to a speedy trial.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Haverkamp

Court: US Court of Appeals for the Second Circuit

Docket: 18-3735
Opinion Date: May 4, 2020
Judge: Barrington D. Parker
Areas of Law: Criminal Law

Defendant pleaded guilty to one count of distribution and receipt of child pornography and one count of possession of child pornography. The district court sentenced him to 121 months of imprisonment, followed by five years of supervised release, and imposed a $200 mandatory special assessment under 18 U.S.C. 3013, as well as a $10,000 assessment under 18 U.S.C. 3014. The Second Circuit held that the district court did not abuse its discretion in sentencing defendant and his sentence was substantively reasonable. The court held that the text of the Justice for Victims of Trafficking Act (JVTA), 18 U.S.C. 3014, taken as a whole and in its context, is straightforwardly meant to be applied on a per-offender, not a per-count, basis. In this case, the district court erroneously applied the special assessment on a per-count, rather than per-offender, basis. Finally, the court held that the computer monitoring condition in question was reasonably related to the nature of defendant's offense. Accordingly, the court affirmed in part, vacated in part, and remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Mladen

Court: US Court of Appeals for the Second Circuit
Docket: 18-0616
Opinion Date: May 6, 2020
Judge: Amalya Lyle Kearse
Areas of Law: Criminal Law, Trusts & Estates

After defendant died while his appeal was pending, counsel moved for abatement of all incidents of the prosecution, requesting that the appeal be dismissed without a decision on the merits, that defendant's conviction be vacated, and that the matter be remanded to the district court with instructions to dismiss the indictment and order repayment to defendant's estate of the $20,000 fine and $100 special assessment. Because defendant was convicted upon his plea of guilty, and he neither did nor was permitted to challenge on appeal the merits of his conviction, the Second

Circuit denied as without merit so much of the motion as seeks (1) vacatur of his conviction, (2) dismissal of the count of the indictment on which he was convicted, and (3) repayment of the mandatory $100 special assessment. The court granted so much of the motion as requests dismissal of this appeal and a remand to the district court for vacatur of the imposed terms of imprisonment and supervised release and for an order requiring that the paid fine of $20,000 be repaid to defendant's estate.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Richardson

Court: US Court of Appeals for the Second Circuit
Docket: 19-412
Opinion Date: May 5, 2020
Judge: Menashi
Areas of Law: Criminal Law

The Second Circuit affirmed defendant's conviction for distribution and possession with intent to distribute a controlled substance. The court held that the district court did not procedurally err by applying the career offender sentencing enhancement pursuant to USSG 4B1.1 because defendant's prior convictions of conspiracy to distribute a controlled substance in violation of 21 U.S.C. 841(a)(1) and 846, and attempted criminal possession of a controlled substance in violation of N.Y. Penal Law 220.16(1), qualify as controlled substance offenses, as defined in USSG 4B1.2(b). The court also held that the district court did not substantively err in sentencing defendant, because it properly considered his criminal history and accounted for his need for mental health and substance abuse treatment.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Rosemond

Court: US Court of Appeals for the Second Circuit
Docket: 18-3561
Opinion Date: May 1, 2020
Judge: Chin
Areas of Law: Criminal Law

The Second Circuit affirmed defendant's conviction for murder-for-hire, conspiracy to commit murder-for-hire, murder through use of a firearm, and possession of a firearm during a murder-for-hire conspiracy. Defendant owned Czar Entertainment, a music management company that represented hip-hop, rap and R&B artists such as Jayceon Taylor, also known as "The Game." Taylor was a member of G-Unit, a rap group run by Curtis Jackson, also known as "50 Cent." Defendant's crimes stemmed from a rivalry with Violator Records, the company that managed G-Unit. The court rejected defendant's contention that his attorney was ineffective because he conceded that defendant paid for the victim to be shot, even though he told counsel not to make this concession. The court held that defendant failed to show that this was objectively unreasonable or that he would have been found not guilty had a different argument been advanced. In this case, there was ample evidence supporting counsel's strategy to concede that defendant ordered a shooting where, among other things, the government's key witness, who participated in the conspiracy and lured the victim to be shot, testified that defendant agreed to pay the shooter. The court also held that the district court did not abuse its broad discretion by admitting prior bad-act evidence under Federal Rule of Evidence 404(b)(1).

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Lacerda

Court: US Court of Appeals for the Third Circuit
Docket: 15-2812
Opinion Date: May 5, 2020
Judge: Porter
Areas of Law: Criminal Law, White Collar Crime

VOG billed itself as an advocacy group helping victims of timeshare fraud get out of their timeshare debts. A jury determined that VOG had actually defrauded its customers and that three individual defendants (including Lacerda) were each knowing participants in that fraud. Lacerda was sentenced to 324 months' imprisonment for his leading role in the fraudulent enterprise. The Third Circuit affirmed the respective convictions and sentences. The court rejected a claim of impermissible "overview testimony" by an FBI agent; an officer who is familiar with an investigation or was personally involved may tell the story of that investigation—how the

investigation began, who was involved, and what techniques were used, and, with a proper foundation, may offer lay opinion testimony and testify about matters within his personal knowledge. The district court did not abuse its discretion when it disqualified defense counsel based on a conflict of interest; when it denied replacement counsel's motion for a continuance; when it excluded from evidence, as hearsay, an email sent by Lacerda to VOG's former CFO; in exercising its sentencing discretion; or by ordering the forfeiture of all VOG's gross proceeds.

Read Opinion Are you a lawyer? **Annotate this case**.

Cucalon v. Barr

Court: US Court of Appeals for the Fourth Circuit
Dockets: 18-1292, 18-2206
Opinion Date: May 7, 2020
Judge: Barbara Milano Keenan
Areas of Law: Criminal Law, Immigration Law

The Fourth Circuit denied petitions for review of the BIA's final order of removal. Applying the modified categorical approach, the court held that defendant's prior conviction for distribution of cocaine under Virginia Code 18.2-248, including distribution of that substance as an accommodation under Virginia Code 18.2-248(D), satisfies the federal definitions of an "aggravated felony" and of a crime "relating to a controlled substance" pursuant to 8 U.S.C. 1227(a)(2)(A)(iii), 1227(a)(2)(B)(i). The court also held that the district court did not abuse its discretion in denying petitioner's motion to reconsider.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Doctor

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-4874
Opinion Date: May 4, 2020
Judge: Roger L. Gregory
Areas of Law: Criminal Law

The Fourth Circuit affirmed the district court's revocation of defendant's

supervised release and resulting sentence. The court held that the district court did not clearly err in finding the government proved he committed the assault underlying the supervised release violation; the district court did not commit plain error by adopting the violation report when announcing defendant committed Violation One; and, even if the district court erred in sentencing defendant for a Grade A violation, the error was harmless.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Lewis

Court: US Court of Appeals for the Fourth Circuit
Docket: 19-4028
Opinion Date: May 4, 2020
Judge: Barbara Milano Keenan
Areas of Law: Criminal Law

Defendant was convicted for possessing a firearm as a felon and sentenced to 63 months' imprisonment and a three-year period of supervised release. The district court additionally recommended, without explanation, that defendant receive addiction treatment while incarcerated and ordered, as a special condition of his supervised release, that defendant participate in an addiction treatment program. The Fourth Circuit held that defendant's sentence is procedurally unreasonable because the district court failed to provide an adequate explanation for imposing as a special condition of supervised release the requirement of addiction treatment. The court also held that the district court failed to address defendant's nonfrivolous mitigation arguments. Therefore, the court remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Jordan

Court: US Court of Appeals for the Fifth Circuit
Docket: 19-40499
Opinion Date: May 1, 2020
Judge: Jennifer Walker Elrod
Areas of Law: Criminal Law

The Fifth Circuit affirmed the district court's grant of defendants' motion for a new trial on the basis of prejudicial outside influence on the jury. The court held that the district court did not abuse its broad discretion in granting the motion for a new trial without holding an evidentiary hearing. To the extent there is a bright-line rule applicable to allegations of outside influence on the jury, the court held that it was not applicable to this case. Furthermore, the district court did not abuse its discretion in exercising its prerogative, within broadly defined parameters, to handle the allegation of outside influence in the least disruptive manner possible in this unusual case. Finally, the district court permissibly concluded that the evidence showed a sufficient likelihood of prejudice to shift the burden to the Government, and that the Government did not (and could not) show "no reasonable possibility that the jury's verdict was influenced by" the CSO's comments.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Longoria

Court: US Court of Appeals for the Fifth Circuit
Docket: 19-20201
Opinion Date: May 5, 2020
Judge: Gregg Costa
Areas of Law: Criminal Law

The Fifth Circuit held that the base offense level of 20 was proper for defendant's felon-in-possession crime involving a semiautomatic firearm that is capable of accepting a large capacity magazine. In this case, defendant failed to show that the district court clearly erred in relying on the FBI's agent statement about what was found in the apartment. The court clarified any confusion and held that the 2013 amendment to the commentary on the acceptance-of-responsibility Guideline does not clearly overrule its caselaw allowing the government to withhold the third point for acceptance of responsibility when it must litigate a suppression motion. The court held that Amendment 775 does not contain the unequivocal override needed to get past the court's precedent. Therefore, the court affirmed defendant's sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. McNabb

Court: US Court of Appeals for the Fifth Circuit
Docket: 19-50265
Opinion Date: May 1, 2020
Judge: Costa
Areas of Law: Criminal Law

The Fifth Circuit affirmed defendant's sentence imposed after he pleaded guilty to possessing a gun after having been convicted of a felony. The court held that defendant is not entitled to relief on his claim that the government breached the plea deal, and thus his appellate waiver remains enforceable. Accordingly, defendant's challenges to his sentence must be dismissed.

Read Opinion Are you a lawyer? **Annotate this case**.

Andrews v. Wayne County

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-1992
Opinion Date: May 4, 2020
Judge: Suhrheinrich
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Canton Police received a 911 call from Andrews, who stated that his fiance, White, had physically attacked him. Officers arrested White. Andrews later took White's medications to the jail; a “KOP” policy allows inmates to keep certain drugs for self-administration. During an intake interview, White admitted to attempting to harm herself or commit suicide in the past but said she was not thinking of harming herself or having suicidal thoughts. An R.N. later evaluated White for nearly two hours, reported White’s chief complaints were “anxiety and depression,” and contacted a pharmacy to verify White’s prescriptions. The R.N. claims White did not exhibit any psychotic behavior, suicidal ideation, or psychiatric distress but ordered further evaluation. The next day, White was found on the floor with vomit on her face. She stated repeatedly that she took too many pills. The next day, White died in the hospital. The cause of death was Verapamil toxicity. The Sixth Circuit affirmed the rejection of a suit under 42 U.S.C. 1983 on summary judgment. A pretrial detainee does not have an automatic right to a suicide screening. The court rejected an argument that the KOP Policy was deficient because

it allows inmates in need of a psychological evaluation to participate before a psychiatrist's assessment of proper housing. The County had no history of suicides relative to the program, so any purported failure to train its employees in suicide risk assessment did not cause White's death.

Read Opinion Are you a lawyer? **Annotate this case**.

Hicks v. Scott

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-3410
Opinion Date: May 1, 2020
Judge: Gibbons
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Cincinnati officers Scott and Moore responded to a reported incident of menacing. Two people alleged that Quandavier had driven by their home that night and threatened to kill them and that Quandavier carried guns. Officer Loreaux identified a vehicle fitting the description. Officers Scott, Moore, Schneider, and Loreaux, standing where the vehicle was parked, heard a voice. Thinking that it was likely Quandavier, they knocked on the exterior door of the residence. It swung open. Three officers entered without a warrant or exigent circumstances. Loreaux remained outside. Neither Scott nor Moore recall announcing their presence or identifying themselves. Inside and upstairs, Scott knocked on a closed door. As it opened, Scott "saw the barrel of a rifle pointed at [her] face." Moore and Schneider also saw Quandavier "nonchalantly" panning the rifle from left to right. Moore reached for its barrel as Scott fired her weapon. Moore did not instruct Quandavier to drop his rifle nor did Scott issue any commands before firing. Quandavier collapsed. The officers immediately radioed for paramedics. Before the officers applied handcuffs or provided first aid, they heard another voice and conducted a sweep. Quandavier died at the scene without receiving medical attention. In a suit under 42 U.S.C. 1983 for unlawful entry, excessive force, and deliberate indifference to a serious medical need, plus state claims, the district court granted the defendants summary judgment, citing qualified immunity. The Sixth Circuit reversed in part. The district court erred by granting qualified immunity to Scott, Moore, and Schneider on the unlawful entry claim. The court affirmed as to the excessive force, deliberate indifference, and state-law battery claims, and

remanded for evaluation of municipal liability and wrongful death claims.

Read Opinion Are you a lawyer? **Annotate this case**.

Moody v. United States

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-5015
Opinion Date: May 6, 2020
Judge: Thapar
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

At Moody's trial, the government produced a video of Moody cooking crack on his stove and waving a handgun while he mused about life in "the game" (drug trafficking). The court ruled that most of the video was admissible. Moody then tried to persuade the jury that the video was filmed more than five years before his indictment, putting it outside the statute of limitations. The jury convicted Moody. Due to prior felony drug convictions, Moody received enhanced, mandatory-minimum life sentences on several counts. He appealed on evidentiary grounds relating to the video. The Sixth Circuit affirmed. Later, Moody raised new claims on collateral review, 28 U.S.C. 2255. The district court found each claim meritless; most were also procedurally defaulted. The court authorized Moody to appeal. The Sixth Circuit dismissed the appeal, stating that none of the claims should have been certified. Reasonable jurists could not doubt that the district court properly denied relief on Moody's claims that he was deprived of his statute-of-limitations defense (violating due process); that the past convictions for his sentencing enhancements were not charged in the indictment or found by the jury; and that his previous lawyers failed to raise the first two claims sooner, violating his right to effective assistance of counsel.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Foreman

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-1827
Opinion Date: May 7, 2020
Judge: Gibbons

Areas of Law: Criminal Law

In 2006, Foreman pled guilty to possession with intent to distribute 50 or more grams of cocaine base, possession with intent to distribute cocaine powder, and possession of a firearm during and in furtherance of a drug trafficking crime. Foreman admitted that he was responsible for approximately 135 grams of crack cocaine and 250 grams of cocaine powder. Foreman had a final Guidelines range of 322-387 months; he was sentenced to 240 months' imprisonment with respect to each drug conviction, to run concurrently, and 60 months' imprisonment for the firearms conviction, to run consecutively. When the First Step Act of 2018 made the Fair Sentencing Act retroactive, Foreman sought relief. The district court held that Foreman was not entitled to a plenary resentencing and declined to revisit his career offender status or hold an in-person hearing, then weighed the new statutory range applicable to Foreman's drug offenses, his recalculated Guidelines range, and the 18 U.S.C. 3553(a) factors, and reduced Foreman's total sentence to 172 months on each drug offense, to run concurrently, plus the mandatory consecutive 60 months on the firearms offense. The Sixth Circuit affirmed. Nothing in the First Step Act entitles a defendant to a plenary resentencing. First Step Act resentencings are not shielded from review for reasonableness; the district court thoroughly explained its rationale, carefully examining Foreman's circumstances, the amended penalty provisions, and the resulting changes to Foreman's Guidelines range.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Smith

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-1724
Opinion Date: May 6, 2020
Judge: Bush
Areas of Law: Criminal Law

In 2006, Smith was convicted of conspiracy to distribute and to possess with intent to distribute 500 grams or more of powder or 50 grams or more of cocaine base (crack cocaine); possession with intent to distribute 50 grams or more of cocaine base (crack cocaine); possession with intent to distribute

500 grams or more of cocaine powder; and being a felon in possession of a firearm. The court imposed a mandatory minimum life sentence. The Fair Sentencing Act subsequently lowered the penalty for cocaine-base offenses, made retroactive through the First Step Act. Smith moved for relief and received a reduced sentence of 360 months, the bottom of the new Guideline range for the counts impacted by the Fair Sentencing Act, to run concurrent to his existing 360-month sentence for his powder cocaine count that was not affected by the Fair Sentencing Act. The Sixth Circuit affirmed, rejecting an argument that the court should have imposed a below-Guideline sentence for all counts. The First Step Act is a limited grant of authority to impose a reduced sentence for certain offenses and does not require a plenary resentencing proceeding. Even assuming the court's obligation to explain its reasons for imposing the modified sentence was akin to that which applies in initial sentencing, the court's use of a modified AO 247 form order to explain its decision was not procedurally unreasonable.

Read Opinion Are you a lawyer? **Annotate this case**.

Kirkman v. Thompson

Court: US Court of Appeals for the Seventh Circuit
Docket: 19-1904
Opinion Date: May 7, 2020
Judge: William Joseph Bauer
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Following a 1992 fight that involved Johnson, Herron, and Walker, two shooters shot the three men. Johnson survived. In the hospital, Johnson described a shooter by the street name "Duke," where Duke lived, and Duke's car. Johnson identified Duke and his accomplice from a photo array. Police pulled over a vehicle matching Johnson's description and arrested the driver, Kirkman, and the passenger, who matched the general description of the second shooter. Kirkman had a tattoo of Duke on his arm. Police took additional photos and presented a second photo array to Johnson, who identified them as the shooters. At trial, Johnson identified Kirkman and his passenger as the shooters. There was disputed testimony about the cause of the fight. Convicted of murder and aggravated battery with a firearm, Kirkman was sentenced to life in prison. Johnson had a

change of heart and submitted an affidavit, identifying Ford and an unknown man as the shooters. At Kirkman's post-conviction hearing, Johnson testified that he and his family had been threatened. Other testimony was inconsistent with Johnson's. Illinois courts denied post-conviction relief, finding that Johnson's recantation lacked credibility. Johnson later pleaded guilty for perjury but failed to specify which statement was false. The Seventh Circuit affirmed the denial of federal habeas relief. Illinois courts found Johnson's recantation lacked credibility. An evidentiary hearing satisfied Kirkman's due process rights. The Illinois trial court's determination defeated Kirkman's innocence and perjured testimony claims.

Read Opinion Are you a lawyer? **Annotate this case**.

Tuduj v. Newbold

Court: US Court of Appeals for the Seventh Circuit
Docket: 19-1699
Opinion Date: May 1, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Illinois prisoner Tuduj, having received extensive dental treatment, filed a "deliberate indifference" suit under 42 U.S.C. 1983 against his dentists and prison officials. The court recruited counsel to assist Tuduj in filing an amended complaint that complied with the Federal Rules of Civil Procedure. Counsel defended against two summary judgment motions, one arguing that Tuduj had not exhausted his administrative remedies and another on the merits While the motions were pending, Tuduj moved "for leave to represent himself," stating that he was "concerned that his counsel has filed a structurally, technically and legally insufficient response doomed to be denied." He asked to file his own brief, except "in the event this Honorable Court deems counsel's response … legally sufficient and Grants same[,] Plaintiff would be open to continued effective representation." A magistrate denied Tuduj's motion, stating that Tuduj "varie[d] between saying he would like to" represent himself and "indicating that he is happy with counsel's representation as long as he prevails." The district judge granted the motions for summary judgment, citing professional judgment and finding "no competent evidence" of any policy that unlawfully influenced dental-treatment decisions. The Seventh Circuit rejected Tuduj's argument

that the court wrongly denied his “unqualified” right to proceed pro se under 28 U.S.C. 1654, the due process clause, the equal protection clause, and the Seventh Amendment. The district court permissibly denied his equivocal request.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Gibson

Court: US Court of Appeals for the Seventh Circuit
Docket: 19-1402
Opinion Date: May 7, 2020
Judge: William Joseph Bauer
Areas of Law: Constitutional Law, Criminal Law

Officer Garrison encountered Gibson, a suspected drug trafficker, walking with a companion. Although initially a consensual encounter, Garrison questioned Gibson and his companion and briefly detained Gibson. After Gibson and his companion departed, Garrison spotted a methamphetamine pipe under his patrol vehicle. Local law enforcement conducted a traffic stop of Gibson’s vehicle in the curtilage of his driveway. A drug detection dog signaled the presence of a controlled substance in the vehicle, though nothing was found. Earlier that day, Gibson’s wife had met with DEA agents to tell them about methamphetamine inside the home. Police used information Mrs. Gibson had provided to obtain a search warrant. The search of the home uncovered drugs, drug paraphernalia, currency, and AK-47 rifles, which led to Gibson’s arrest. Gibson moved to suppress all evidence seized during the search, alleging he was detained without reasonable suspicion, unlawfully frisked, arrested without probable cause, stopped without probable cause or reasonable suspicion, and the traffic stop exceeded a permissible scope. Upon learning of his wife’s cooperation, Gibson also argued her statement was insufficiently attenuated to justify the search warrant. The Seventh Circuit affirmed the denial of the motion. Mrs. Gibson’s voluntary statement with DEA agents was independently sufficient to sustain findings of probable cause and sufficiently attenuated from subsequent events to preclude suppression.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Howell

Court: US Court of Appeals for the Seventh Circuit
Docket: 18-3157
Opinion Date: May 4, 2020
Judge: Scudder
Areas of Law: Constitutional Law, Criminal Law

In December 2012, Chicago Police officers responded to an anonymous call reporting a Hispanic man in a black sweater and black hat, carrying a bag, and climbing under a warehouse fence. They found someone who matched the description. After stopping and frisking him, they determined he was not engaged in any crime. Howell, walking toward the police, was white and wearing a black jacket and dark hat. When an officer approached to speak to him, Howell did not answer, looked panicked, and put his hands in his pockets. The officer patted Howell down and found a gun in his jacket. A federal gun charge followed. Howell unsuccessfully moved to suppress the gun. The Seventh Circuit reversed the denial of his suppression motion and vacated his conviction for possessing that gun. The court noted that the facts in the pretrial record differed significantly from those presented at trial, where the arresting officer testified that he decided to proceed with the pat-down only after Howell ignored a directive to remove his hands from his pockets. Viewing the pretrial record as a whole, the police lacked reasonable suspicion to frisk Howell. The court did not reverse Howell's conviction on a second gun charge that resulted from the execution of a warrant to search Howell's apartment three months after the initial stop and the ensuing discovery of more guns and ammunition.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Lewis

Court: US Court of Appeals for the Seventh Circuit
Dockets: 19-1911, 19-1262
Opinion Date: May 7, 2020
Judge: Joel Martin Flaum
Areas of Law: Criminal Law

In 2016-2018, Draheim managed a conspiracy, responsible for at least 38 packages of methamphetamine sent from California to La Crosse,

Wisconsin. Draheim supervised at least 11 associates who accepted shipments on her behalf, sent money transfers to California, distributed the meth, rented storage lockers, and collected money owed to her. Draheim provided vehicles. After agents placed a wiretap on her phone and seized several packages of meth en route to Draheim, her California supplier forced Draheim to find a new source. Draheim contacted Lewis, recently out of jail but still involved in the "meth scene." Lewis agreed to purchase meth from a new supplier. During the planned transaction, agents seized the package, which contained 28.6 grams of nearly pure meth. Police subsequently arrested Draheim after they found her daughter dead at home from an overdose; they took Lewis into custody for violating the terms of his state supervision. Both pleaded guilty to meth distribution offenses, 21 U.S.C. 841, 846. Draheim, facing a mandatory-minimum 10-year sentence, unsuccessfully argued that she qualified for "safety-valve relief." The court reasoned that she was the leader of her enterprise. Lewis unsuccessfully contended that he should be sentenced based only on his conviction, not other "relevant conduct." The Seventh Circuit affirmed Draheim's sentence but vacated as to Lewis. The fact that the defendant has engaged in other drug transactions is not, alone, sufficient to justify treating those transactions as relevant conduct for sentencing purposes.

Read Opinion Are you a lawyer? **Annotate this case**.

Bakor v. Barr

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-3011
Opinion Date: May 7, 2020
Judge: Steven M. Colloton
Areas of Law: Criminal Law, Immigration Law

The Eighth Circuit denied a petition for review of the BIA's determination that defendant committed two crimes involving moral turpitude. The court held that the BIA did not err in determining that petitioner's conviction for the Minnesota crimes of Criminal Sexual Conduct in the Fifth Degree and knowing failure to comply with Minnesota's sex offender registration statute were crimes involving moral turpitude. The court also held that petitioner failed to exhaust his remaining arguments and therefore declined to consider them.

Read Opinion Are you a lawyer? **Annotate this case**.

Smith v. Titus

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-2915
Opinion Date: May 5, 2020
Judge: Steven M. Colloton
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Eighth Circuit affirmed the district court's denial of habeas relief to petitioner based on his claim that the trial court violated his Sixth Amendment right to a public trial when it briefly closed the courtroom to spectators. The district court denied relief based on the ground that the Minnesota Supreme Court's decision was neither contrary to, nor an unreasonable application of, clearly established federal law. The court agreed and held that it was not objectively unreasonable for the Minnesota Supreme Court to deem it constitutional under the Sixth Amendment for the trial court to explain the parameters of an earlier public order on evidentiary issues in a brief nonpublic proceeding before the jury was sworn.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Becerra

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-2777
Opinion Date: May 7, 2020
Judge: Stras
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's conviction for two counts of being a felon in possession of a firearm and ammunition. The court held that there was more than enough evidence for defendant's probation officer and other officers to believe defendant had a firearm on him. Therefore, the officers had probable cause to arrest him without a warrant. The court also held that defendant was in custody when he made both statements at issue. In this case, the "request for clarification" of defendant's statement that he had "something" in his car did not require Miranda warnings. Furthermore,

because the bulge in defendant's pocket could have been a gun or other weapon that would have posed a danger to the officers and others, they could ask about it without the formality of Miranda warnings. The court joined its sister circuits in declining to recognize the innocent-possessor defense. The court held that the district court did not err in excluding defendant's proposed testimony that he had found the handgun in his car earlier in the day and was about to hand it over to his probation officer. The court reasoned that, even if defendant intended to turn over the gun (or the ammunition) to his probation officer, it is still a crime to knowingly possess it in the first place. Finally, the court held that the district court did not err in denying defendant a sentencing reduction for acceptance of responsibility; the district court considered defendant's mitigation arguments at sentencing; and the district court did not abuse its discretion by imposing a within-Guidelines sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Haynes

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1607
Opinion Date: May 5, 2020
Judge: Raymond W. Gruender
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's conviction and sentence for being a felon in possession of a firearm. The court held that the government did not violate the Speedy Trial Act, and defendant failed to offer any evidence showing that Iowa and federal prosecutors colluded. Furthermore, the district court did not abuse its discretion by failing to hold an evidentiary hearing regarding the existence of collusion. The court also held that the district court did not err in denying the motion to suppress where defendant was not unlawfully seized. In this case, prior to producing the marijuana cigarette, the officer did not ask defendant any questions but merely ordered him off the bus, particularly as the smell of marijuana alerted the officer that evidence of a more serious crime than failure to use a turn signal might be uncovered during the stop. Finally, the court held that defendant was not unlawfully searched when the officer conducted a pat-down search incident to arrest; the evidence was sufficient to support defendant's conviction;

defendant's Rehaif claim failed because there was sufficient evidence that he knew of his prohibited status; and defendant's sentence was not substantively unreasonable nor an abuse of the district court's discretion.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Roberts

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1176
Opinion Date: May 1, 2020
Judge: Steven M. Colloton
Areas of Law: Criminal Law

The Eighth Circuit vacated defendant's sentence imposed after he pleaded guilty to unlawful possession of a firearm as a previously convicted felon. The court held that, although the district court properly applied a four-level increase for possession of a firearm "in connection with another felony offense" under USSG 2K2.1(b)(6)(B), but that a two-level increase for "using a minor to commit a crime" under USSG 3B1.4 should not have applied. In this case, the evidence showed only that defendant engaged in an arm's-length transaction with a minor. The court held that this mere joint participation in an offense as a partner, does not amount to "use" of a minor "to commit the offense" of unlawful possession of a firearm by a felon. Accordingly, the court remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Wright

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1081
Opinion Date: May 5, 2020
Judge: Erickson
Areas of Law: Criminal Law

The Eighth Circuit affirmed the district court's restitution order and certain special conditions of defendant's supervised release imposed after he pleaded guilty to sex trafficking of a child. The court found no error in the district court's restitution amount of $20,000, holding that the evidence

supported the amount in light of the aggregate harm to the victim. The court also held that the special conditions -- including a requirement that defendant participate in sex offender treatment including psychological testing and polygraph examinations, a prohibition against contact with any minors without pre-approval, and a requirement that defendant seek prior approval before using temporary commercial lodging, such as a hotel or motel -- where reasonably related to both the offense of conviction and to defendant's history of sexual contact with minor females.

Read Opinion Are you a lawyer? **Annotate this case**.

Benson v. Chappell

Court: US Court of Appeals for the Ninth Circuit
Docket: 13-99004
Opinion Date: May 1, 2020
Judge: Consuelo Maria Callahan
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Ninth Circuit affirmed the district court's denial of petitioner's habeas corpus petition challenging his California conviction and death sentence for murder and other crimes. Petitioner raised two certified claims and two uncertified claims. The panel held that petitioner failed to show that the California Supreme Court's denials of his claims were unreasonable determinations of the facts or contrary to clearly established federal law. In this case, the California Supreme Court reasonably determined that an officer's misstatement during petitioner's interrogation that there was no death penalty in California did not prompt petitioner's confessions. Furthermore, petitioner failed to show that his statements were not knowing, voluntary, and intelligent. Even if petitioner were able to show that trial counsel was ineffective in not fully investigating his abuse as a child or his alleged organic brain injury, the panel held that the state court could reasonably have determined that any shortcoming in trial counsel's investigation was not prejudicial. Finally, the panel granted a certificate of appealability on petitioner's two uncertified claims and held that the state court reasonably rejected the claims that his trial counsel should have impeached the government's case and the prosecutor withheld material, exculpatory evidence.

Read Opinion Are you a lawyer? **Annotate this case**.

Mero v. Barr

Court: US Court of Appeals for the Ninth Circuit
Docket: 17-70929
Opinion Date: May 1, 2020
Judge: Paul Jeffrey Watford
Areas of Law: Criminal Law, Immigration Law

The Ninth Circuit granted in part a petition for review of the BIA's finding that petitioner was removable based on his conviction for possession of visual presentation depicting sexual conduct of a person under 16 years of age, in violation of Nevada Revised Statutes (N.R.S.) 200.730. Applying the categorical approach, the panel compared the elements of N.R.S. 200.730 with the applicable definition of "sexual abuse of a minor," which requires proof of three elements. The panel held that N.R.S. 200.730 punishes a broader range of conduct because the Nevada statute does not require proof that the offender participated in sexual conduct with a minor. Therefore, petitioner's conviction did not qualify as sexual abuse of a minor. The panel explained that, with a possession-only offense such as N.R.S. 200.730, the minor depicted in the image is not the direct object of the offender's conduct, which is a necessary predicate for the offense to qualify as sexual abuse of a minor.

Read Opinion Are you a lawyer? **Annotate this case**.

Romero-Millan v. Barr

Court: US Court of Appeals for the Ninth Circuit
Dockets: 16-73915, 17-72893, 18-71555
Opinion Date: May 4, 2020
Areas of Law: Criminal Law

The Ninth Circuit certified the following questions of state law to the Arizona Supreme Court: 1. Is Arizona's possession of drug paraphernalia statute, A.R.S. 13-3415, divisible as to drug type? 2. Is Arizona's drug possession statute, A.R.S. 13-3408, divisible as to drug type? 3. Put another way, is jury unanimity (or concurrence) required as to which drug or drugs listed in

A.R.S. 13-3401(6), (19), (20), or (23) was involved in an offense under either statute?

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Yang

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-10341
Opinion Date: May 4, 2020
Judge: Piersol
Areas of Law: Criminal Law

The Ninth Circuit affirmed the district court's denial of defendant's motion to suppress after he pleaded guilty to receipt of stolen mail and being a prohibited person in possession of a firearm. Defendant moved to suppress the evidence seized from his residence and the statements he made to law enforcement on the basis that the search warrant obtained by the Postal Inspection Service relied on evidence that was obtained illegally. The panel declined to address the potential Fourth Amendment privacy interests that may be implicated by the warrantless use of this Automatic License Plate Recognition (ALPR) technology, and held that defendant does not have a reasonable expectation of privacy in the historical location data of the Yukon under the facts of this case. The panel found no evidence in the record that Prestige Motors had a policy or practice of allowing lessees to keep cars beyond the rental period and Prestige had made affirmative attempts to repossess the vehicle by activating the GPS unit to locate and disable the vehicle. Therefore, defendant lacked standing to challenge the warrantless search of the database.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Neugin

Court: US Court of Appeals for the Tenth Circuit
Docket: 19-7043
Opinion Date: May 1, 2020
Judge: Scott Milne Matheson, Jr.
Areas of Law: Constitutional Law, Criminal Law

Jack Neugin pled guilty to being a felon in possession of a firearm and ammunition on the condition that he could appeal the district court's denial of his motion to suppress evidence of the ammunition and firearm police found in the bed of his pickup truck. Officers responded to a reported verbal altercation between Neugin and his girlfriend. One of the officers saw ammunition in the back of the truck after he lifted the truck's camper lit do allow the girlfriend to retrieve her belongings. Neugin argued the officers discovered the evidence during an unconstitutional search; the district court concluded the officer was acting "in a lawful position" as "community caretaker," and found no Fourth Amendment violation. The Tenth Circuit reversed, finding that : (1) the officer conducted the without a warrant or probable cause, (2) the community caretaking exception to the warrant requirement does not apply, and (3) the inevitable discovery exception to the exclusionary rule does not apply. The evidence seized should have been suppressed.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Ramon

Court: US Court of Appeals for the Tenth Circuit
Docket: 19-1221
Opinion Date: May 1, 2020
Judge: Gregory Alan Phillips
Areas of Law: Constitutional Law, Criminal Law

In 2016, after serving a federal prison sentence for having possessed a firearm after a felony conviction, Charles Ramon III began serving a mandatory term of supervised release. Before Ramon completed the term, his probation officer filed a petition, soon followed by two superseding petitions, to revoke Ramon's supervised release. At the revocation hearing, the district court found three violations—two for possessing a controlled substance and one for again illegally possessing a firearm. Of these, the most serious was Ramon's illegal possession of a firearm—a Grade B violation. For this, the court imposed the statutory maximum sentence of twenty-four months in prison. During the revocation hearing, the government mentioned that it might seek to indict Ramon for illegally possessing a firearm (the conduct in part underlying the revocation). Mindful of this, the district court ordered that Ramon's twenty-four-month sentence run

"consecutively to any sentences imposed previously or prospectively in federal or state court." At the hearing, Ramon did not object to the district court's running his sentence consecutively to future federal sentences. On appeal, Ramon argued that the district court exceeded its sentencing authority under 18 U.S.C. 3584(a) by ordering that Ramon's sentence run consecutively to future federal sentences. By the terms of 18 U.S.C. 3584(a), the Tenth Circuit determined the district court did err. But Ramon failed to object to this at trial, and on appeal, failed to show that the error was plain, thus, judgment was affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Richards

Court: US Court of Appeals for the Tenth Circuit
Docket: 19-8044
Opinion Date: May 6, 2020
Judge: Baldock
Areas of Law: Constitutional Law, Criminal Law

In 2018, the Wyoming Division of Criminal Investigation (DCI) obtained a search warrant to review the contents of Defendant–Appellant Joshua Richards' Tumblr account. During the search and subsequent investigation, DCI agents discovered Defendant had re-blogged videos and images of child pornography to his private Tumblr so he could later access and view the materials. Defendant ultimately pleaded guilty to one count of accessing with intent to view child pornography. He was sentenced to twenty-four months' imprisonment followed by five years of supervised release. The district court imposed several special conditions of supervised release, which, as relevant here, related to drugs and alcohol and required Defendant to submit to polygraph testing. On appeal, Defendant argued the district court erred in imposing these special conditions. He also challenged the length of his prison sentence as substantively unreasonable. The Tenth Circuit determined the alcohol and drug conditions did not directly conflict with the relevant policy statement in the sentencing guidelines, so the district court's decision to impose the conditions was not manifestly unreasonable. And given the circumstances of the case, the Court determined the trial court did not abuse its discretion in imposing Defendant's twenty-four month sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

Andrews v. Warden

Court: US Court of Appeals for the Eleventh Circuit
Docket: 19-12443
Opinion Date: May 5, 2020
Judge: William Holcombe Pryor, Jr.
Areas of Law: Criminal Law

The Eleventh Circuit affirmed the district court's denial of habeas relief under 28 U.S.C. 2241. Plaintiff alleged that President Obama commuted his "total sentence" of imprisonment, which included the 37 months of imprisonment that he served as part of his 2003 sentence. Based on the terms of the commutation order, the Constitution, and Supreme Court precedent, the court could not say that the Bureau erred in excluding the 37-month term of imprisonment from its recalculation.

Read Opinion Are you a lawyer? **Annotate this case**.

Hollis v. United States

Court: US Court of Appeals for the Eleventh Circuit
Docket: 19-11323
Opinion Date: May 6, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Eleventh Circuit affirmed the district court's denial of petitioner's motion to vacate his sentence under 28 U.S.C. 2255. The court held that petitioner cannot prove that his counsel rendered ineffective assistance, because petitioner's prior convictions in Alabama categorically qualify as predicate offenses under both the Armed Career Criminal Act and the career-offender provision of the Guidelines, and his prior conviction in Georgia qualifies as a predicate offense under the Act. Therefore, counsel did not perform deficiently by failing to raise a meritless objection.

Read Opinion Are you a lawyer? **Annotate this case**.

Knight v. Florida Department of Corrections

Court: US Court of Appeals for the Eleventh Circuit
Docket: 18-12488
Opinion Date: May 1, 2020
Judge: Newsom
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Eleventh Circuit affirmed the district court's denial of a 28 U.S.C. 2254 petition for habeas relief. Petitioner alleged that his counsel rendered ineffective assistance under Strickland v. Washington, 466 U.S. 668 (1984), by failing to adequately investigate and present mitigating evidence during the sentencing phase of his capital-murder trial. The court held that, even assuming that counsel performed deficiently in failing to investigate and present the mitigation evidence that petitioner now raises—thus satisfying the first prong of the two-part Strickland standard that governs ineffective-assistance claims—petitioner failed to carry his burden of demonstrating resulting prejudice.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Evans

Court: US Court of Appeals for the Eleventh Circuit
Docket: 17-15323
Opinion Date: May 6, 2020
Judge: Grant
Areas of Law: Criminal Law

The Eleventh Circuit affirmed defendant's conviction and sentence for being a felon in possession of a firearm. The court held that, given the totality of the circumstances, it was reasonable for officers, mistaking a dog's whimper for a person in distress, to enter defendant's home without a warrant. Therefore, defendant's challenge to the district court's denial of his motion to suppress evidence failed. The court upheld the district court's imposition of a 22 offense level finding because defendant possessed a semiautomatic firearm capable of accepting a large capacity magazine under USSG 2K2.1(a)(3)(A)(i) (2016). The court also upheld defendant's sentencing enhancement under USSG 2K2.1(b)(4)(B) for possessing a rifle that had an

obliterated serial number.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. McLellan

Court: US Court of Appeals for the Eleventh Circuit
Docket: 18-13289
Opinion Date: May 6, 2020
Judge: Boggs
Areas of Law: Criminal Law

The Eleventh Circuit affirmed defendant's conviction for two counts of being a felon in possession of a firearm. The court held that the district court did not abuse its discretion in permitting one of his arresting officers to offer testimony at trial on the correlation between guns and drug activity and to suggest that defendant was selling drugs; the court declined to evaluate the applicability of the Armed Career Criminal Act (ACCA), because the district court would have imposed the same sentence regardless of whether the mandatory minimum applied; and the court rejected defendant's claim under Rehaif v. United States, 139 S. Ct. 2191 (2019), and held that there was no plain error in the district court's failure to instruct the jury of the knowledge-of-status element and any error from the lack of a knowledge-of-status element in defendant's plea colloquy did not affect his substantial rights. Finally, the court remanded for clarification of the judgment to reflect the sentence the district court said it would have imposed if the Armed Career Criminal Act did not apply.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Russell

Court: US Court of Appeals for the Eleventh Circuit
Docket: 18-11202
Opinion Date: May 4, 2020
Judge: Charles R. Wilson
Areas of Law: Criminal Law

Defendant was convicted of possessing a firearm and ammunition as an immigrant illegally or unlawfully in the United States. After defendant

appealed his conviction and sentence, the Supreme Court issued its decision in Rehaif v. United States, 588 U.S. ___, 139 S. Ct. 2191 (2019), which reversed a decision from this court and held that under 18 U.S.C. 922(g), the government must prove that a defendant knew "his status as a person barred from possessing a firearm" when he knowingly possessed a firearm. The Eleventh Circuit held that defendant established the necessary prejudice under plain error review and vacated defendant's section 922(g) conviction, remanding for further proceedings. In this case, the district court committed an error that was made plain by the Supreme Court in Rehaif. Furthermore, defendant has sufficiently shown a reasonable probability that but for the error, the outcome of his trial would have been different.

Read Opinion Are you a lawyer? **Annotate this case**.

Welch v. United States

Court: US Court of Appeals for the Eleventh Circuit
Docket: 14-15733
Opinion Date: May 6, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Eleventh Circuit affirmed the district court's denial of petitioner's 28 U.S.C. 2255 motion to vacate his sentence. The court held that defendant's prior 1996 Florida convictions for robbery qualified as violent felonies under the Armed Career Criminal Act's (ACCA) elements clause, and rejected his contention that the court's decision in his direct appeal carved out a narrow exception to pre-1997 Florida robbery convictions obtained in Florida's Fourth District Court of Appeal. The court also held that petitioner's prior Florida felony battery conviction was a violent felony under the ACCA in light of the court's holding in United States v. Vail-Bailon, 868 F.3d 1293 (11th Cir. 2017) (en banc), cert. denied, 138 S. Ct. 2620 (2018).

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Trujillo

Court: Arizona Supreme Court
Docket: CR-18-0531-PR

Opinion Date: May 4, 2020
Judge: Gould
Areas of Law: Constitutional Law, Criminal Law

The Supreme Court held that, for purposes of imposing mandatory sex offender registration under Ariz. Rev. Stat. 13-3821(A)(3), a judge has the authority to make the necessary factual finding that the victim is under the age of eighteen and that Arizona's sex offender registration statutes are civil regulatory statutes, not criminal penalties. Defendant was convicted by a jury of one count of sexual abuse. In reaching its verdict the jury determined that the victim was "fifteen or more years of age." At sentencing, the trial court ordered Defendant to register as a sex offender. Defendant objected, arguing that, pursuant to Apprendi v. New Jersey, 530 U.S. 466 (2000), a jury was required to find whether Defendant was under eighteen pursuant to section 13-3821(A)(3). The trial court denied the objection. The court of appeals affirmed. The Supreme Court affirmed, holding (1) Apprendi does not apply to factual findings that are necessary to impose registration because sex offender registration is a civil regulatory requirement, not a criminal penalty; and (2) the trial judge did not violate Apprendi by determining that the victim was under eighteen.

Read Opinion Are you a lawyer? **Annotate this case**.

Barnett v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 181
Opinion Date: May 7, 2020
Judge: Hudson
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's "motion for credit for time spent in custody," holding that the circuit court's findings were not clearly erroneous. In his motion, Appellant alleged that he was entitled to 312 days of jail-time credit and that the circuit court should enter a new sentencing order nunc pro tunc that reflected the correct amount of jail-time credit. The circuit court denied the motion. The Supreme Court affirmed, holding that the circuit court's denial of Appellant's motion was not clearly erroneous because Appellant failed to demonstrate a clerical error subject to correction.

Read Opinion Are you a lawyer? **Annotate this case**.

Mason v. Kelley

Court: Arkansas Supreme Court
Citation: 2020 Ark. 182
Opinion Date: May 7, 2020
Judge: Rhonda K. Wood
Areas of Law: Criminal Law

The Supreme Court affirmed the order of the circuit court dismissing Appellant's pro se petition for writ of habeas corpus, holding that Appellant stated no ground on which the writ could issue. Appellant was convicted of aggravated robbery, theft of property, and second-degree battery and sentenced as a habitual offender to an aggregate term of 660 months' imprisonment. The court of appeals affirmed. Appellant later petitioned for writ of habeas corpus, asserting that the trial court misapplied Arkansas's habitual-offender statutes. The circuit court dismissed the petition. The Supreme Court affirmed, holding that the issues Appellant raised in his petition for the writ should have been raised at trial, on direct appeal, or in a petition for postconviction relief.

Read Opinion Are you a lawyer? **Annotate this case**.

Ray v. Kelley

Court: Arkansas Supreme Court
Citation: 2020 Ark. 184
Opinion Date: May 7, 2020
Judge: Wynne
Areas of Law: Criminal Law

The Supreme Court dismissed Appellant's appeal from an order denying his pro se petition for permission to reinvest jurisdiction in the trial court to consider a petition for writ of error coram nobis, holding that the circuit court had no jurisdiction to consider the petition. Appellant entered negotiated guilty pleas to rape and other offenses. Appellant later filed a petition for writ of error coram nobis in the Chicot County Circuit Court, the court where he

was incarcerated, setting out two grounds for coram nobis relief. The circuit court denied the petition. The Supreme Court dismissed Appellant's appeal, holding that jurisdiction lay in the trial court where Appellant was convicted, which in this case was the Ashley County Circuit Court. Therefore, the Chicot County Circuit Court was without jurisdiction to address Appellant's coram nobis petition.

Read Opinion Are you a lawyer? **Annotate this case**.

Walker v. Kelley

Court: Arkansas Supreme Court
Citation: 2020 Ark. 183
Opinion Date: May 7, 2020
Judge: Rhonda K. Wood
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's pro se petition for declaratory judgment, holding that Appellant could not use a declaratory-judgment action to collaterally attack his criminal conviction. Appellant was convicted of first-degree murder and second-degree unlawful discharge of a firearm from a vehicle. The court of appeals affirmed. Years later, Appellant filed a petition for declaratory judgment alleging that he was denied due process in his criminal trial when the court admitted the prior testimony of an unavailable witness and that this admission violated the Confrontation Clause. The circuit court denied the petition. The Supreme Court affirmed, holding that a declaratory judgment action provided no relief on these grounds.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Flores

Court: Supreme Court of California
Docket: S116307
Opinion Date: May 4, 2020
Judge: Kruger
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction of three counts of first

degree murder and his sentence of death, holding that the three or four minor errors at Defendant's trial were harmless and did not interfere with his due process right to a fair trial. Specifically, the Supreme Court held (1) no error occurred during jury selection; (2) Defendant was not prejudiced by any misstatements by the prosecutor; (3) assuming certain evidence was inadmissible, the court's admonition to the jury and the court's instruction cured the resultant harm; (4) the trial court erred in admitting testimony that the victim was afraid of Defendant, but the error was harmless; and (5) Defendant's remaining allegations of error were without merit.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. Law

Court: California Courts of Appeal
Docket: E072845(Fourth Appellate District)
Opinion Date: May 5, 2020
Judge: Slough
Areas of Law: Constitutional Law, Criminal Law

In 2001, appellant Terrell Law and his codefendant Brett May committed a home invasion robbery, during which one of them shot and killed one of the residents. They were tried jointly in 2006 before two separately empaneled juries who found them both guilty of first degree felony murder with the special circumstance described in Penal Code section 190.2(a)(17(A) and (d). Though Law's jury found he was not the shooter, they nonetheless concluded he was a "major participant" in the underlying robbery and acted "with reckless indifference to human life." In 2018, the Legislature enacted Senate Bill No. 1437 (2017-2018 Reg. Sess.) which, among other things, amended the definition of felony murder in Penal Code section 189. The legislation also added Penal Code section 1170.95, which established a procedure for vacating murder convictions predating the amendment that could not be sustained under the new definition of felony murder. Law challenged the trial court's summary denial of his section 1170.95 petition to vacate his murder conviction, arguing the trial court erred by reviewing his record of conviction and determining the jury's true finding on the special circumstance rendered him ineligible for relief. The Court of Appeal concluded it was proper for a trial court to review the record of conviction when determining whether a section 1170.95 petitioner had stated a prima

facie claim for relief. Additionally, the Court concluded Law "undoubtedly qualifies" as a major participant who acted with reckless indifference to human life, a conclusion that rendered him ineligible for relief under section 1170.95. The Court therefore affirmed the order denying his petition.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. Sanchez

Court: California Courts of Appeal
Docket: E072647(Fourth Appellate District)
Opinion Date: May 7, 2020
Judge: Menetrez
Areas of Law: Constitutional Law, Criminal Law

Victor Sanchez was charged with first degree murder, but pled guilty to voluntary manslaughter. He filed a petition under Penal Code section 1170.95 to vacate that conviction. The trial court denied the petition, concluding that Sanchez was ineligible for relief because he was not convicted of murder. After review, the Court of Appeal joined other courts that held section 1170.95 did not apply to defendants convicted of voluntary manslaughter. The Court also rejected Sanchez's argument that section 1170.95 violated equal protection.

Read Opinion Are you a lawyer? **Annotate this case**.

Galeotti v. International Union of Operating Engineers

Court: California Courts of Appeal
Docket: A157785(First Appellate District)
Opinion Date: May 6, 2020
Judge: Henry E. Needham, Jr.
Areas of Law: Criminal Law, Labor & Employment Law, White Collar Crime

Galeotti, a former Union Local 3 employee, filed a complaint against Local 3 and three of individual union leaders, alleging that the individual defendants required union employees to pay them money to keep their jobs, lied about the reason for collecting the money, and caused Local 3 to terminate Galeotti's employment when he failed to pay the full amount demanded. The trial court dismissed his second amended complaint without leave to amend.

The court of appeal reversed in part, reasoning that a threat to terminate employment can provide a basis for an extortion claim and that the allegations of the second amended complaint stated a cause of action for wrongful termination in violation of the public policy underlying the extortion statutes. The complaint stated a cause of action for violations of the Racketeer Influenced and Corrupt Organizations Act (RICO; 18 U.S.C. 1961), based on the predicate acts of extortion, but did not state a cause of action for interference with prospective economic advantage.

Read Opinion Are you a lawyer? **Annotate this case**.

In re I.A.

Court: California Courts of Appeal
Docket: B296549(Second Appellate District)
Opinion Date: May 4, 2020
Judge: Tangeman
Areas of Law: Criminal Law, Juvenile Law

Where a juvenile court vacates its true finding on a generic murder allegation and redesignates it as a finding on an uncharged target offense, and does so before a minor has had the opportunity to contest the court's findings or orders, the minor may challenge the sufficiency of the evidence of the redesignated offense on appeal. The Court of Appeal held that there was insufficient evidence to support the juvenile court's decision sustaining the allegations that I.A. possessed a concealable firearm and committed vandalism. Therefore, the court reversed the juvenile court's findings, vacating the jurisdiction and disposition order and dismissing the Welfare and Institutions Code section 602 petition.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Edwards

Court: California Courts of Appeal
Docket: A158055(First Appellate District)
Opinion Date: May 1, 2020
Judge: Petrou
Areas of Law: Criminal Law

In 2006, Edwards fired an assault weapon into an apartment, killing the victim. Edwards pled guilty to possession of a firearm as a felon and was convicted of second-degree murder and shooting into an inhabited dwelling. Following the enactment of Senate Bill 1437, Edwards filed a Penal Code 1170.95 resentencing petition, checking form boxes indicating that he was convicted under a theory of felony murder or murder under the natural and probable consequences doctrine and that he could not now be convicted of 1st or 2nd-degree murder because of changes to Penal Code 188 and 189. Edwards submitted the jury instructions and the transcript of the prosecutor's closing remarks that Edwards acted with "both express malice, specific intent to kill, as well as implied malice," described as "an intentional act, the natural consequences of which are dangerous to human life, and at the time that the individual acted, they knew of the danger, and they deliberately acted with conscious disregard." The court denied the petition, finding that Edwards was convicted on a valid theory of murder that survived the statutory changes. The court of appeal affirmed. The superior court did not err in considering the record of conviction. Edwards could not meet the statutory prerequisites for even filing a section 1170.95 petition because he was not charged or convicted of second-degree felony murder or murder under the natural or probable consequences doctrine directed at accomplice liability.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Thomkins

Court: California Courts of Appeal
Docket: A141375(First Appellate District)
Opinion Date: May 1, 2020
Judge: Streeter
Areas of Law: Criminal Law

On Easter night in 2011, gunfire erupted at an Oakland bar-restaurant, leaving two people dead and five wounded. Thompkins and Fox were convicted of two counts of first-degree murder for the benefit of a criminal street gang, with firearm discharge enhancements, a multiple-murder special circumstance, and five counts of attempted murder with great bodily injury findings, gang enhancements, and firearm discharge enhancements.

Thompkins was convicted as the shooter and Fox as an accomplice. Both were sentenced to life in prison without possibility of parole, plus 224 years to life. After Thompkins was sentenced, Fox stated under oath he was the actual shooter and Thompkins knew nothing about Fox's intentions. Thompkins claimed this new testimony, and his attorney's incompetent reaction entitled him to a new trial and submitted a declaration by another gang member who was present that night. The court of appeal concluded that Thompkins's attorney was not ineffective for failing to bring a motion to recall the sentence followed by a new trial motion because Thompkins failed to show prejudice. The attempted murder convictions and related enhancements must be reversed for both defendants based on the flawed kill zone instruction. Introducing evidence that defendants admitted their gang affiliation at jail intake violated the defendants' privilege against self-incrimination but was harmless. There was some evidentiary error that was harmless due to the wealth of admissible evidence establishing the gang enhancements. Arguments based on the statutory amendments to Penal Code 188 and 189 must be raised in the trial court (section 1170.95). The case must be remanded so the judge may exercise his discretion whether to impose or strike the firearm enhancements on under Penal Code 12022.53.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Torres

Court: California Courts of Appeal
Docket: B295043(Second Appellate District)
Opinion Date: May 4, 2020
Judge: Wiley
Areas of Law: Criminal Law

After the trial court admitted a witness's former testimony, the Court of Appeal applied People v. Roldan (2012) 205 Cal.App.4th 969, 975–985, and reversed. Roldan held that, before invoking the former testimony exception, prosecutors should react appropriately to the impending deportation risk by following four steps: alert the defense to the risk; videotape the preliminary hearing testimony; use judicial measures to try to delay deportation; and consider an array of other specific measures. In this case, the prosecution conceded that prosecutors were simply unaware of Roldan and did not comply with it. The court held that Roldan controls the court's analysis

because the facts about prosecutorial diligence are weaker here than they were in Roldan, where the appellate court held for the defense. In this case, the record before deportation is of prosecutorial inaction where the prosecution's brief in this court admits the investigating officer did not do anything to ensure that the witness would not be deported, nor is there other evidence of prosecutorial efforts to delay the witness's departure or to videotape his testimony at the preliminary hearing.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Triplett

Court: California Courts of Appeal
Docket: B298914(Second Appellate District)
Opinion Date: May 1, 2020
Judge: Frances Rothschild
Areas of Law: Criminal Law

Defendant was convicted of assault with a deadly weapon, carjacking, and attempted murder. In the published portion of the opinion, the Court of Appeal held that the trial court erred by denying defense counsel's request to inform the jurors that they could have testimony of certain witnesses read back to them. The court also held that, under the circumstances in this case, the error was harmless.

Read Opinion Are you a lawyer? **Annotate this case**.

Colorado In Interest of G.S.S.

Court: Colorado Supreme Court
Citation: 2020 CO 32
Opinion Date: May 4, 2020
Judge: Brian D. Boatright
Areas of Law: Constitutional Law, Criminal Law, Juvenile Law

After being charged, fourteen-year-old G.S.S. was detained for more than three months without bail, even though he had not entered a plea and had not been tried on the charges against him. At that point, G.S.S.'s counsel filed a motion to dismiss, arguing that G.S.S.'s "right to a speedy trial" had been violated under section 19-2-509(4)(b), C.R.S. (2019). The trial court

agreed and dismissed the case against G.S.S. with prejudice, and the court of appeals affirmed in Colorado in Interest of G.S.S., 2019 COA 4M, __ P.3d __. The Colorado Supreme Court then granted certiorari to determine the proper remedy for a violation of the sixty-day limit in section 19-2-509(4)(b). The Supreme Court determined the remedy for a section 19-2-509(4)(b) violation was for the trial court to immediately hold a bail hearing and order the juvenile's release. Accordingly, the judgment of the court of appeals was reversed.

Read Opinion Are you a lawyer? **Annotate this case**.

Barringer v. Halkitis

Court: Florida Supreme Court
Docket: SC19-1071
Opinion Date: May 7, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court held that Jay Barringer's quo warranto petition filed in this case was a frivolous proceeding brought before the Supreme Court by a state prisoner and sanctioned Barringer by barring him from filing any further pro se requests for relief related to his criminal case. Barringer was convicted of one count of attempted sexual battery of a victim less than twelve years old and sentenced to twenty-five-years' imprisonment. In 2011, Barringer began filing petitions in the Supreme Court. The Court did not grant the relief sought in any of Barringer's filings. In the instant quo warranto petition Barringer challenged his conviction on the ground that the information was defective, a claim Barringer previously raised by way of a habeas petition. The Supreme Court denied the petition and found that Barringer abused the Court's limited judicial resources. The Court sanctioned Barringer by directing the Clerk of Court to reject any future pleadings or other requests for relief submitted by Barringer that are related to his criminal case, unless such filings are signed by a member of The Florida Bar in good standing.

Read Opinion Are you a lawyer? **Annotate this case**.

Franqui v. State

Court: Florida Supreme Court
Docket: SC19-203
Opinion Date: May 7, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the order of the circuit court denying Appellant's claim of intellectual disability, raised in successive motions for postconviction relief under Fla. R. Crim. P. 3.851, holding that the circuit court did not err in denying relief. Appellant was convicted of first-degree murder and sentenced to death in two separate cases. After the United States Supreme Court decided Hall v. Florida, 572 U.S. 701 (2014), Appellant filed successive motions for postconviction relief in both of his capital cases, asserting that the circuit court's denials of his previous claims of intellectual disability were based on the court's improper interpretation of Florida's intellectual disability statute. The circuit court summarily denied the motions. The Supreme Court reversed and remanded for an evidentiary hearing on the issue of intellectual disability. After a hearing, the circuit court denied the claim. The Supreme Court affirmed, holding (1) the circuit court did not err in denying Appellant's intellectual disability claim; and (2) Appellant was not entitled to relief under Hurst v. Florida, 136 S. Ct. 616 (2016), or Hurst v. State, 202 So. 3d 40 (Fla. 2016).

Read Opinion Are you a lawyer? **Annotate this case**.

Hicks v. State

Court: Florida Supreme Court
Docket: SC19-1978
Opinion Date: May 7, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court denied the instant mandamus petition filed by Hicks and sanctioned Hicks by barring him from filing any further pro se requests for relief related to his criminal case. Hicks was convicted of one count of lewd and lascivious conduct by a person over eighteen years of age on a victim under sixteen years of age. Since 2016, Hicks filed thirteen pro se requests for relief in the Supreme Court related to his criminal case. The

Court did not grant the relief sought in any of Hicks' filings. In the instant petition, Hicks sought a writ of mandamus compelling the circuit court to comply with the requirements of Fla. R. Crim. P. 3.850 by filing a copy of an order denying his second postconviction motion with the clerk of court. The Supreme Court dismissed the petition and found that Hicks abused this Court's limited judicial resources. The Court directed the Clerk of Court to reject any future pleadings or other requests for relief submitted by Hicks that are related to his criminal case, unless such filings are signed by a member of The Florida Bar in good standing.

Read Opinion Are you a lawyer? **Annotate this case**.

Burley v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0356
Opinion Date: May 4, 2020
Judge: Boggs
Areas of Law: Constitutional Law, Criminal Law

In 1992, Douglas Burley pled guilty to malice murder. He moved for an out-of-time appeal in 2019, claiming that his right to appeal was frustrated by his plea counsel's erroneous advice that he could not appeal his conviction because it was the product of a guilty plea. The trial court denied Burley's motion. After review, the Georgia Supreme Court vacated the trial court's judgment and remanded the case with direction to hold a hearing to determine whether ineffective assistance of counsel frustrated Burley's right to appeal.

Read Opinion Are you a lawyer? **Annotate this case**.

Carter v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0022
Opinion Date: May 4, 2020
Judge: David E. Nahmias
Areas of Law: Construction Law, Criminal Law

Brandon Carter was convicted by jury of malice murder and two firearm offenses in connection with the shooting death of Terrance Baker. On appeal, Carter contended the trial court erred by admitting certain hearsay statements into evidence and by violating his constitutional right to be present during his trial. Finding no reversible error, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Clarke v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0258
Opinion Date: May 4, 2020
Judge: Ellington
Areas of Law: Constitutional Law, Criminal Law

Rupert Clark was convicted by jury for the malice murder of his wife, Rosemarie Lebert-Clark. He was also convicted of possession of a firearm during the commission of a felony. On appeal, he argued he received ineffective assistance of trial counsel, and that the trial court erred in admitting certain evidence, violated the continuing witness rule by sending out with the deliberating jury printouts of text messages, and by failing to instruct the jury that a defendant's uncorroborated confession was not alone sufficient to warrant a conviction. Finding no reversible error after reviewing the trial court record, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Collins v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0195
Opinion Date: May 4, 2020
Judge: Harold D. Melton
Areas of Law: Constitutional Law, Criminal Law

Renita Collins was tried for murder along with co-defendant Michael Stallworth. Collins appealed her convictions for murder and possession of a firearm while in commission of a felony in connection with the shooting

death of Keith Jacobs. On appeal. Collins contended she was denied a fair trial due to juror misconduct, the trial court abused its discretion by not allowing her to subpoena juror testimony to show that misconduct had occurred, and the trial court abused its discretion when it failed to excuse a prospective juror for cause. Finding no reversible error, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Dawson v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0217
Opinion Date: May 4, 2020
Judge: Warren
Areas of Law: Constitutional Law, Criminal Law

Lavaris Dawson was convicted by jury of felony murder and other crimes in connection with the shooting death of Mamadou Camara. On appeal, Dawson challenged the sufficiency of the evidence supporting his convictions, and argued the trial court erred in admitting Dawson's statements to a detective during an interview because those statements were impermissibly induced by a hope of benefit, and that Dawson was denied his due process right to a timely appeal. After review, the Georgia Supreme Court disagreed and affirmed Dawson's convictions.

Read Opinion Are you a lawyer? **Annotate this case**.

Evans v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0007
Opinion Date: May 4, 2020
Judge: McMillan
Areas of Law: Constitutional Law, Criminal Law

Jimmy Evans was convicted by jury for murder and other crimes relating to the 2006 deaths of Tavoris Calhoun and Dezmon Thomas. On appeal, Evans argued that because he was visibly intoxicated at the time he made statements to law enforcement and consented to a search of his home and

person, the statements and consent were involuntarily given and the trial court should have granted his motion for new trial on this ground. Furthermore, Evans argued that his trial counsel was ineffective for failing to file a motion to suppress at trial on the same basis. Because Evans failed to show error or ineffective assistance of counsel, the Georgia Supreme Court affirmed his conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Hill v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0285
Opinion Date: May 4, 2020
Judge: Harold D. Melton
Areas of Law: Constitutional Law, Criminal Law

Esco Hill was convicted by jury of malice murder and other crimes relating to the stabbing death of Alford Morris in 2014. On appeal, Hill argued the trial court committed reversible error by requiring him to be visibly shackled for the duration of his six-day trial. After review of the trial court record, the Georgia Supreme Court concurred this was reversible error, consequently, reversed judgment of conviction. Because the Court concluded the evidence at trial was sufficient to sustain Hill's conviction, the State could re-try him. The Court did not address Hill's remaining enumerations of error, "as they are not likely to recur in the event of a retrial."

Read Opinion Are you a lawyer? **Annotate this case**.

Oliver v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0489
Opinion Date: May 4, 2020
Judge: McMillan
Areas of Law: Constitutional Law, Criminal Law

Jacquan Oliver entered a negotiated plea of guilty to felony murder in connection with the shooting death of Alexander Mixon. He appealed his

conviction and sentence, arguing that the trial court abused its discretion in finding a factual basis for his plea, and in determining the plea was voluntarily, knowingly and intelligently made. Finding no merit to these contentions, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Rosser v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0103
Opinion Date: May 4, 2020
Judge: Bethel
Areas of Law: Constitutional Law, Criminal Law

Larry Rosser was convicted by jury of malice murder and other crimes in connection with the death of Alexis Vereen. On appeal, Rosser challenged the sufficiency of the evidence presented against him at trial, and argued the trial court erred by not granting his motion for a mistrial, and by allowing the State to introduce a portion of Rosser's custodial statement to law enforcement. In addition, he argued he received constitutionally ineffective assistance of trial counsel. Finding no reversible error after reviewing the trial court record, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Spencer v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0871
Opinion Date: May 4, 2020
Judge: Keith R. Blackwell
Areas of Law: Constitutional Law, Criminal Law

Christopher Spencer was convicted by jury of murder and other crimes in connection with the fatal shootings of Sylvia Watson and Samuel White. Spencer appealed, claiming only that the evidence was insufficient to support his convictions. Finding no reversible error after reviewing the trial court record, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Styles v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0236
Opinion Date: May 4, 2020
Judge: Ellington
Areas of Law: Constitutional Law, Criminal Law

Derrick Styles was convicted by jury of felony murder and other crimes in connection with the shooting death of Alberto Lumens and the armed robbery fo Juan Lumens Garcia. On appeal, Styles contended the trial court erred in admitting into evidence a recording of an inculpatory telephone conversation between himself and a witness. He also argued his trial counsel was ineffective for failing to object to an allegedly improper comment by the prosecutor during closing argument. Finding no merit to these contentions, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Whitehead v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0171
Opinion Date: May 4, 2020
Judge: Ellington
Areas of Law: Constitutional Law, Criminal Law

Javis Whitehead was convicted by jury of murder and other crimes in connection with the shooting death of Dominique Larry. On appeal, Whitehead challenged the sufficiency of the evidence presented to rebut his claim of self-defense and to convict him for murder beyond a reasonable doubt. He also argued the trial court erred in denying his motion to suppress his custodial statement, and in refusing to excuse for cause the District Attorney from the panel of prospective jurors prior to the conclusion of voir dire. Finding no merit to these contentions, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Idaho v. Blythe

Court: Idaho Supreme Court - Criminal
Docket: 46992
Opinion Date: May 4, 2020
Judge: Roger S. Burdick
Areas of Law: Constitutional Law, Criminal Law

Nicholas Blythe appealed after he was convicted of possessing a controlled substance. He conditionally pled guilty, reserving the right to challenge his sentence. On appeal, he argued the district court erred in denying his motion to suppress certain evidence found because the evidence presented at trial was found in violation of Blythe's Fourth Amendment rights. After review, the Idaho Supreme Court determined the search at issue took place before an arrest occurred, and because no rationale justifying a search incident to arrest was sufficiently present here, the search of Blythe's shoes was not a valid search incident to arrest. Therefore, the district court erred in holding that the search was reasonable under the Fourth Amendment. Blythe's conviction was vacated, the district court order denying Blythe's motion to suppress was reversed, and the matter remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

Idaho v. Glodowski

Court: Idaho Supreme Court - Criminal
Docket: 47131
Opinion Date: May 6, 2020
Judge: Roger S. Burdick
Areas of Law: Constitutional Law, Criminal Law

David Glodowski appealed after he was convicted for failing to update his sex-offender registration in violation of Idaho Code section 18-8309. He argued the district court erred by ruling that his prior conviction under a Wisconsin statute was "substantially equivalent" to Idaho statutes that required sex-offender registration in Idaho. After review, the Idaho Supreme Court determined the district court improperly allowed the State to seek a

redetermination of the “substantially equivalent” element given that the Idaho Bureau of Criminal Identification made a final determination on that element. However, because the State put forth sufficient evidence to prove that element, and the district court’s jury instruction accomplished the same purpose, the Supreme Court concluded the error was harmless. Accordingly, the Court found no reversible error in the district court’s decision to grant the State’s motion and provide the jury instruction. Therefore, judgment of conviction was affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Idaho v. Jones

Court: Idaho Supreme Court - Criminal
Docket: 45905
Opinion Date: May 4, 2020
Judge: Roger S. Burdick
Areas of Law: Constitutional Law, Criminal Law

Timothy Jones was convicted by jury of trafficking heroin and possession of drug paraphernalia. On appeal, he argued the trial court erred in admitting certain evidence regarding his probation status, a knife found in the initial police search of his person, and that the trial court abused its discretion in arriving at his sentence. Finding no reversible error, the Idaho Supreme Court affirmed Jones' conviction and sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Gordon

Court: Iowa Supreme Court
Docket: 18-1099
Opinion Date: May 1, 2020
Judge: Brent R. Appel
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction for assault on a peace officer with a dangerous weapon, a felony, and several misdemeanors, holding that Defendant did not receive ineffective assistance of counsel. After Defendant pleaded guilty, he absconded. He was later returned to

custody. On appeal, Defendant argued that he received ineffective assistance of counsel because the plea bargain contained an unlawful term. Specifically, Defendant argued that the plea bargain's provision that he would be released from jail for a forty-eight-hour furlough after pleading guilty was illegal and that his trial counsel committed ineffective assistance in obtaining the illegal benefit for him. The Supreme Court affirmed, holding that where Defendant entered into the plea agreement with the illegally lenient sentence, he could not benefit from that sentence and then attack the plea bargain.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Craig

Court: Kansas Supreme Court
Docket: 119660
Opinion Date: May 1, 2020
Judge: Dan Biles
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's conviction and sentence for first-degree felony murder, holding that there was no error in the proceedings below. A jury found Defendant guilty of both first-degree felony murder and second-degree intentional murder. At sentencing, Defendant moved for a new trial and judgment notwithstanding the verdict, arguing that the jury must have had reasonable doubt on the first-degree felony murder theory because it convicted him of second-degree murder for the same killing. The district court dismissed the second-degree murder conviction and sentenced Defendant for the felony murder over his objection. The Supreme Court affirmed, holding (1) the district court did not err when it sentenced Defendant on felony murder instead of declaring a mistrial because Defendant did not establish that the jury failed to find each element of the felony murder beyond a reasonable doubt or that the jury's first- and second-degree murder verdicts were so irreconcilable as to require a new trial; and (2) the district court did not err in declining to give an instruction on voluntary intoxication.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Lemmie

Court: Kansas Supreme Court
Docket: 119439
Opinion Date: May 1, 2020
Judge: Carol A. Beier
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's convictions of first-degree felony murder, aggravated robbery, conspiracy to commit aggravated robbery, criminal possession of a firearm, fleeing and eluding, and interference with law enforcement, holding that Defendant's arguments on appeal failed. Specifically, the Supreme Court held (1) any possible violation of Defendant's Fifth Amendment right in the admission of a witness's testimony about Defendant giving the witness phone passcodes was undoubtedly harmless; (2) the district court did not err by admitting hearsay statements as statements of a coconspirator and contemporaneous statements; (3) the State introduced sufficient evidence to convict Defendant of first-degree murder; and (4) the district judge did not abuse its discretion by admitting testimony that Defendant was upset over a meth pipe that went missing.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Mullen

Court: Maine Supreme Judicial Court
Citation: 2020 ME 56
Opinion Date: May 5, 2020
Judge: Connors
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed Defendant's conviction for reckless conduct and aggravated criminal mischief, holding that the trial court did not abuse its discretion by offering Defendant a continuance of the trial in lieu of excluding his medical records. On appeal, Defendant argued that the trial court abused its discretion by denying his motion to suppress his personal medical records as a sanction for the State's late seizure of the records. The Supreme Judicial Court agreed that the State's conduct undermined the purpose of Maine Rule of Unified Criminal Procedure 18(b) but that the court's offer of a continuance in lieu of the exclusion of the evidence

constituted an appropriate response to the State's conduct.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. Billingslea

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12715
Opinion Date: April 30, 2020
Judge: Cypher
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Judicial Court affirmed Defendant's convictions and the decision of the Appeals Court denying Defendant's motion to vacate the entry of his appeal from his convictions in that court and to have the case entered directly in the Supreme Judicial Court, holding that a direct appeal from the third conviction of a habitual offender pursuant to Mass. Gen. Laws ch. 279, 25(b) may be entered in the Appeals Court. Defendant was indicted for serious felonies arising from a brutal attack and rape. In addition to charging the specific felony, each indictment also alleged that the sentence for that felony should be enhanced pursuant to the habitual criminal provision Mass. Gen. Laws ch. 279, 25(a) or the habitual offender provision of section 25(b), or both. After he was convicted, Defendant moved to have the case entered directly in the Supreme Judicial Court. The Appeals Court denied the motion. The Supreme Judicial Court affirmed Defendant's convictions, holding (1) this direct appeal was entitled to the unique review prescribed by Mass Gen. Laws ch. 278, 33E, and the Appeals Court may conduct such section 33E review; (2) Defendant was not impermissibly allowed to waive his right to a jury trial on the sentencing enhancement provisions of the indictments; and (3) Defendant was not entitled to reversal of his convictions on any other ground.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. Martin

Court: Massachusetts Supreme Judicial Court
Docket: SJC-08768
Opinion Date: May 5, 2020

Judge: Ralph D. Gants
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Judicial Court affirmed Defendant's conviction of murder in the first degree and the denial of his motion for a new trial and declined to exercise its authority under Mass. Gen. Laws ch. 278E to reduce Defendant's conviction to murder in the second degree, holding that Defendant was not entitled to relief on any of his allegations of error. Defendant was convicted of murder in the first degree on the theory of felony-murder. Defendant filed a motion for a new trial, which was denied. The Supreme Judicial Court affirmed, holding (1) Defendant's motion for a new trial was correctly denied because Defendant was not prejudiced by counsel's ineffective assistance; (2) this Court declines to extend the reach of the Court's holding in Commonwealth v. Brown, 477 Mass. 805 (2017), to Defendant's case; and (3) trial judge erred when he declined Defendant's request that the jury be instructed on the elements of voluntary and involuntary manslaughter, but the error was not prejudicial in the context of the judge's other instructions.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. Tavares

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12631
Opinion Date: May 6, 2020
Judge: Lowy
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed Defendant's conviction of murder in the first degree on theories of deliberate premeditation and extreme atrocity or cruelty and declined to exercise its power pursuant to Mass. Gen. Laws ch. 278, 33E to reduce the conviction to manslaughter, holding that there was no reversible error in the proceedings below. Specifically, the Supreme Judicial Court held (1) the trial judge did not err by denying Defendant's requests for a jury instruction pursuant to Commonwealth v. Croft, 345 Mass. 143 (1962); (2) the trial judge did not err by denying Defendant's motions for a required finding of not guilty under Croft because a rational jury could have found that Defendant was guilty of murder in the first degree

on both the theories of premeditation and extreme atrocity or cruelty; and (3) there was no basis for reducing Defendant's sentence or ordering a new trial.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Branch

Court: Minnesota Supreme Court
Docket: A18-1055
Opinion Date: May 6, 2020
Judge: Lorie Skjerven Gildea
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's sentences for drive-by shooting at an occupied vehicle and second-degree assault, holding that Minn. Stat. 609.035 did not prohibit the sentences for both offenses when the crimes arose from a single behavioral incident. The district court sentenced Defendant to forty-eight months for drive-by shooting at an occupied vehicle and thirty-six months for second-degree assault and imposed the two sentences to run concurrently. The court of appeals affirmed. The Supreme Court affirmed, holding that, under this Court's analysis in State v. Ferguson, 808 N.W.2d 586 (Minn. 2012), the district court properly imposed multiple sentences in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

Galloway v. Mississippi

Court: Supreme Court of Mississippi
Citation: 2018-CA-01427-SCT
Opinion Date: May 7, 2020
Judge: Beam
Areas of Law: Constitutional Law, Criminal Law

Leslie Galloway appealed the denial of his 2015 petition for post-conviction relief (PCR) pertaining to his 2007 guilty plea to carjacking, a conviction that was used as an aggravating circumstance in Galloway's 2010 capital-murder trial at which Galloway received a death sentence. Galloway claimed in the petition that his defense counsel Wendy Martin had an actual

conflict of interest because, before becoming his defense counsel, Martin had served as an assistant district attorney in the same case, unbeknownst to Galloway. The trial court ruled that Galloway's PCR claim was time barred under Mississippi's Uniform Post-Conviction Collateral Relief Act (UPCCRA), having been filed more than seven years after Galloway's conviction for carjacking. The trial court alternatively found no merit to Galloway's PCR claim, time bar notwithstanding. Accordingly, the trial court denied Galloway's PCR petition. The Mississippi Supreme Court agreed with the trial court that Galloway's PCR claim was time barred under the UPCCRA. The Court also agreed there was no merit to Galloway's PCR claim.

Read Opinion Are you a lawyer? **Annotate this case**.

City of Missoula v. Zerbst

Court: Montana Supreme Court
Citation: 2020 MT 108
Opinion Date: May 5, 2020
Judge: Beth Baker
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court reversed Defendant's conviction for sexual assault, holding that the municipal court erred when it instructed the jury on a definition of "consent" from the 2017 sexual assault statute and not the applicable 2015 statute, and the erroneous jury instruction prejudicially affected Defendant's substantial rights. At trial, the court instructed the jury, over Defendant's objection, on the definition of consent contained in recent amendments to the sexual assault statute. On appeal, Defendant argued that the municipal court failed to apply the correct law when instructing the jury on the elements of the claimed offense. The district court denied the appeal. The Supreme Court reversed, holding (1) the instructions, as a whole, did not fully and fairly instruct the jury on the law applicable to the case; and (2) Defendant's substantial due process right was prejudiced by the erroneous jury instruction.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Degarmo

Court: Nebraska Supreme Court
Citation: 305 Neb. 680
Opinion Date: May 1, 2020
Judge: Stacy
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction of driving under the influence, holding that Defendant consented to a chemical test of his urine and, therefore, the results of the urine test were admissible. A law enforcement officer stopped Defendant for an expired registration. Based on his observations, the officer, a certified drug recognition evaluation expert, administered field sobriety tests. The officer concluded that Defendant was under the influence of marijuana arrested Defendant for driving under the influence and then took him to a detoxification center. Thereafter, a chemical test of Defendant's urine confirmed the presence of marijuana. On appeal, Defendant challenged the admission of the results of the urine test. The Supreme Court affirmed, holding that Defendant voluntarily consented to the warrantless search of his urine, and therefore, the search fell within a recognized exception to the warrant requirement.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Holz

Court: New York Court of Appeals
Citation: 2020 NY Slip Op 02682
Opinion Date: May 7, 2020
Judge: Fahey
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Court of Appeals held that N.Y. Crim. Proc. Law (CPL) 710.70(2) grants a defendant the right to review of a suppression decision when the order related exclusively to a count that was satisfied by a guilty plea but was not one to which the defendant pleaded guilty. Defendant was charged with two counts of burglary in the second degree. The first count related to a laptop computer, and the second count related to jewelry. Defendant moved to suppress the jewelry, but Supreme Court denied the motion. Defendant then pleaded guilty to one count of burglary in the second degree as charged in the count pertaining to the theft of the laptop computer, in satisfaction of the

count charging the burglary of jewelry. On appeal, Defendant argued that Supreme Court erred in denying his motion to suppress the jewelry. The Appellate Division affirmed, concluding that it was jurisdictionally precluded from reviewing the suppression order. The Court of Appeals reversed, holding (1) Defendant's right to appellate review of Supreme Court's suppression order was secured by CPL 710.70(2); and (2) because the Appellate Division did not reach the underlying suppression question the case must be remitted to the Appellate Division for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Maffei

Court: New York Court of Appeals
Citation: 2020 NY Slip Op 02680
Opinion Date: May 7, 2020
Judge: DiFiore
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Court of Appeals affirmed the order of the Appellate Division concluding on direct appeal that Defendant was not entitled to relief on his ineffective assistance of counsel claim, holding that Defendant, on this record, did not sustain his burden to establish that counsel was constitutionally ineffective. After a jury trial, Defendant was convicted of second-degree murder. On appeal, Defendant argued that his trial counsel's failure to challenge a prospective juror constituted ineffective assistance of counsel. The Appellate Division affirmed. The Court of Appeals affirmed, holding (1) the record was inadequate to review Defendant's ineffective assistance of counsel claim; and (2) the appropriate procedure for the litigation of Defendant's challenge to his counsel's performance was a N.Y. Crim. Proc. Law 440.10 motion.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Bailey

Court: North Carolina Supreme Court
Docket: 360A19
Opinion Date: May 1, 2020

Judge: Davis
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the decision of the court of appeals affirming the order of the trial court denying Defendant's motion to suppress evidence seized during the execution of a search warrant, holding that the warrant supported by probable cause. Defendant pled guilty to the offense of trafficking in cocaine while preserving his right to appeal the denial of his motion to suppress. On appeal, Defendant argued that the trial court erred in denying his motion to suppress because the facts contained in the affidavit were insufficient to establish probable cause to search his residence. The court of appeals affirmed. The Supreme Court affirmed, holding that the affidavit contained facts that were sufficient to provide a nexus between the residence and suspected criminal activity, and therefore, the warrant was supported by probable cause.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Ellis

Court: North Carolina Supreme Court
Docket: 340A19
Opinion Date: May 1, 2020
Judge: Robin E. Hudson
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court reversed the decision of the Court of Appeals affirming the trial court's denial of Defendant's motion to suppress evidence, holding that there was no reasonable suspicion to justify the law enforcement officer's stop when Defendant signaled with his middle finger from the passenger side window of a moving vehicle. While assisting a stranded motorist, the officer turned his attention to another car traveling on the roadway, a white SUV. Defendant had his arm outside the passenger window and gestured with his middle finger, making an up-and-down motion. Believing that Defendant was committing the crime of disorderly conduct, the officer pursued and then stopped the SUV. At trial, Defendant moved to suppress the officer's testimony, arguing that there was no reasonable suspicion to justify the stop. The trial court denied the motion. Defendant pleaded guilty to resisting, delaying, or obstructing a public

officer. The court of appeals affirmed the trial court's denial of Defendant's motion to suppress. The Supreme Court reversed, holding that the specific, articulable facts did not establish reasonable suspicion of the crime of disorderly conduct.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Hobbs

Court: North Carolina Supreme Court
Docket: 263PA18
Opinion Date: May 1, 2020
Judge: Earls
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court reversed Defendant's conviction, holding that the trial court clearly erred in ruling that Defendant failed to prove purposeful discrimination with respect to the State's use of peremptory challenges to strike three jurors without considering all of the evidence presented by Defendant. Defendant was found guilty of one count of first-degree murder and other crimes. On appeal, Defendant argued that the trial court erred by failing to grant three objections that he made under Batson v. Kentucky, 476 U.S. 79 (1986). The court of appeals affirmed Defendant's convictions. The Supreme Court reversed, holding (1) the court of appeals erred in its analysis of Defendant's Batson claims with respect to the three jurors; and (2) as to all three jurors, remand was required for reconsideration of whether Defendant proved purposeful discrimination in each case.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Mylett

Court: North Carolina Supreme Court
Docket: 6A19
Opinion Date: May 1, 2020
Judge: Earls
Areas of Law: Criminal Law

The Supreme Court reversed the decision of the court of appeals affirming the trial court's judgment convicting Defendant for conspiracy to commit

harassment of a juror, holding that the trial court erred in denying Defendant's motion to dismiss the conspiracy charge for insufficient evidence. Defendant was convicted of conspiracy to commit harassment of a juror because of his actions at a courthouse following his twin brother's conviction for assault on a government official. On appeal, the court of appeals concluded that the trial court did not err in denying Defendant's motion to dismiss the conspiracy charge for insufficient evidence. The Supreme Court reversed, holding that the evidence in Defendant's trial was insufficient to raise anything more than mere conjecture that he had made an agreement with another person to threaten or intimidate a juror.

Read Opinion Are you a lawyer? **Annotate this case**.

Dodge v. North Dakota

Court: North Dakota Supreme Court
Citation: 2020 ND 100
Opinion Date: May 7, 2020
Judge: Gerald W. VandeWalle
Areas of Law: Constitutional Law, Criminal Law

Richard Dodge appealed from a district court order denying his application for post-conviction relief. Dodge was charged with five felonies and a misdemeanor in December 2015. Dodge was appointed counsel. In April 2016, Dodge's counsel moved the court to withdraw because the attorney-client relationship was "irreparably broken and rendered unreasonably difficult." The court granted the motion, and Dodge was appointed substitute counsel in May 2016. In July 2016, Dodge himself filed a "motion to dismiss counsel." The court denied Dodge's motion. Five months after the deadline for motions and plea agreements, Dodge's counsel sought to have Dodge submit to a psychiatric examination. This request was denied, the trial court found no evidence, and the the court itself made no observations, that Dodge was incompetent to stand trial. After this denial, Dodge himself again moved to dismiss his trial counsel, and due to the allegations Dodge made in his motion, counsel moved to withdraw. The trial court denied both motions, and instead, required the attorney to appear as standby counsel and assist Dodge during trial if requested, but relieved him of any further obligations to consult with Dodge. The case proceeded to trial. At the beginning of trial, the court gave Dodge the option of representing himself or

having his attorney represent him. Dodge chose to have his attorney represent him. Because his attorney had not prepared for trial and had no communication with Dodge since he moved to withdraw, Dodge's attorney asked for a brief recess to consult with Dodge. During the recess, a settlement was reached. Dodge agreed to enter Alford pleas on all counts, waived a presentence investigation, and agreed to be sentenced immediately after entering his pleas. Dodge was immediately sentenced following his guilty pleas, and thereafter sought post-conviction relief on grounds he was not competent to enter his pleas, and that he received ineffective assistance of trial counsel. After review, the North Dakota Supreme Court concluded the district court's finding that Dodge was competent when he entered his pleas was not clearly erroneous, and disposed of his claim of ineffective assistance of counsel.

Read Opinion Are you a lawyer? **Annotate this case**.

Hewitt v. NDDOT

Court: North Dakota Supreme Court
Citation: 2020 ND 102
Opinion Date: May 7, 2020
Judge: Lisa K. Fair McEvers
Areas of Law: Criminal Law, Government & Administrative Law

Larry Hewitt appealed a district court judgment affirming the North Dakota Department of Transportation's revocation of his driving privileges. Hewitt claimed the Department's hearing file was improperly admitted at the administrative hearing. After review, the North Dakota Supreme Court affirmed, concluding the hearing file was properly admitted as a self-authenticating copy of an official record.

Read Opinion Are you a lawyer? **Annotate this case**.

Kastet v. NDDOT

Court: North Dakota Supreme Court
Citation: 2020 ND 91
Opinion Date: May 7, 2020
Judge: Daniel J. Crothers

Areas of Law: Criminal Law, Government & Administrative Law

The North Dakota Department of Transportation (Department) appealed the district court's reversing a hearing officer's decision suspending Holden Kastet's driving privileges for 365 days. The Department argued the hearing officer did not abuse his discretion in admitting the chemical breath test, and State Highway Patrol Trooper King scrupulously complied with the approved method for testing Kastet's breath on the Intoxilyzer 8000. After review, the North Dakota Supreme Court concurred with the Department and reversed the district court judgment. The matter was remanded with instructions to reinstate the hearing officer's decision.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Dahl

Court: North Dakota Supreme Court
Citation: 2020 ND 87
Opinion Date: May 7, 2020
Judge: Jerod E. Tufte
Areas of Law: Constitutional Law, Criminal Law

The State of North Dakota appealed a district court order denying its motion to resume prosecution against Matthew Dahl and dismissing the case. In December 2014, the State charged Dahl with two counts of theft. Dahl did not appear on the charges until he was arrested on a bench warrant in February 2017. In mid-April 2017, the State mailed Dahl a pretrial diversion agreement. Dahl signed and returned the notarized agreement dated May 3, 2017. On May 9, 2017, the state's attorney signed and filed the agreement with the district court, and the court approved the agreement the same day. Under the agreement, the State agreed to suspend prosecution for "two years from the date of execution" conditioned on Dahl's timely payment of restitution. Dahl failed to make minimum monthly restitution payments. On June 6, 2019, the State moved to resume prosecution, alleging Dahl violated the pretrial diversion agreement by his non-payment. The district court held a hearing on the State's motion in August 2019. The court concluded the pretrial agreement was executed when Dahl signed it on May 3, 2017. The court then denied the State's motion to resume prosecution as untimely under N.D.R.Crim.P. 32.2(d)(2), and dismissed the complaint

against Dahl. After review, the North Dakota Supreme Court reversed, concluding the district court erred in determining the State's motion was untimely, and remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Foster

Court: North Dakota Supreme Court
Citation: 2020 ND 85
Opinion Date: May 7, 2020
Judge: Jon J. Jensen
Areas of Law: Constitutional Law, Criminal Law

Akeem Foster was convicted by jury of Terrorizing and Carrying a Concealed Weapon. Foster contended on appeal he was denied a fair trial because he was asked during cross-examination if other witnesses were lying and because the prosecutor expressed personal beliefs about the evidence during closing arguments. Foster also argued there was insufficient evidence to convict him of either charge. After review, the North Dakota Supreme Court affirmed Foster's conviction for Carrying a Concealed Weapon, but reversed his conviction for Terrorizing. The Court found Foster was improperly asked to provide an opinion on the veracity and credibility of the State's witnesses. The improper questioning was prejudicial and denied Foster a fair trial on the terrorizing charge.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Kolstad

Court: North Dakota Supreme Court
Citation: 2020 ND 97
Opinion Date: May 7, 2020
Judge: Gerald W. VandeWalle
Areas of Law: Constitutional Law, Criminal Law

In December 2018, Officer Nelson of the University of North Dakota Police Department conducted a traffic stop of Stanley Kolstad for suspicion of driving under the influence. Kolstad performed field sobriety tests and a preliminary breath test (PBT). Prior to performing the PBT, Kolstad informed

Nelson that he had asthma. Nelson testified he was unable to obtain a PBT result because Kolstad was filling his cheeks with air while performing the test. Kolstad was arrested for DUI and refusing to submit to a chemical test. Kolstad was transported to the UND police station to be given an Intoxilyzer breath test. Prior to the Intoxilyzer test, Nelson read Kolstad the implied consent advisory. But, because Nelson was not a certified operator of the Intoxilyzer machine, Officer Waltz conducted the test. Prior to the test, Kolstad informed Waltz he had asthma. The Intoxilyzer test results were deficient. Waltz testified Kolstad was not providing enough air for the test machine to provide a valid result. Kolstad was charged with driving under the influence and refusing to submit to a chemical test. Kolstad's counsel made a discovery request to the State seeking copies of any audio or video recordings taken by police officers. Kolstad's counsel also requested the State inform him whether any sound or video recordings taken of Kolstad were subsequently "altered, edited, destroyed, or discarded." The State provided Kolstad's counsel with dash camera footage from Nelson's police car that had been taken at the scene of the arrest, but the State did not provide any body camera footage from either Nelson or Waltz. Upon learning that Waltz's body camera footage was successfully uploaded to UND servers, Kolstad's counsel moved to dismiss the case because the State did not provide any body camera footage in discovery as requested. The district court ultimately dismissed the refusal to submit to a chemical breath test charge as a sanction for failing to provide the body camera footage. The State appealed, arguing the alleged discovery violation did not rise to a constitutional violation of Kolstad's due process rights, and the district court abused its discretion in dismissing the refusal charge. Kolstad argued the district court's order dismissing the refusal charge was not appealable, and if it was, the court did not abuse its discretion in dismissing the charge. The North Dakota Supreme Court concluded there was nothing in the record to indicate the district court adequately considered an alternative or less severe sanction to dismissal, and by not considering a less severe sanction, the trial court erred. The district court's order dismissing the refusal charge was reversed, and the matter remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Michel

Court: North Dakota Supreme Court
Citation: 2020 ND 101
Opinion Date: May 7, 2020
Judge: Jerod E. Tufte
Areas of Law: Constitutional Law, Criminal Law

Kevin Michel was convicted by jury of knowingly receiving stolen property. Jamestown Police began investigating theft of tires from Northwest Tire in October 2017. About ten months later, Thomas Melland and Andrew Heckelsmiller became suspects in the investigation. Heckelsmiller told police he had sold stolen tires to Michel. In August 2018, Detective LeRoy Gross spoke with Michel about the stolen tires. Michel acknowledged he had bought tires from Heckelsmiller and Melland. Michel also told Detective Gross he stopped buying tires from Heckelsmiller and Melland after seeing a Facebook post from Northwest Tire offering a $500 reward for information regarding stolen tires. Detective Gross told Michel, "There's going to be a lot of restitution these two boys are going to have to come up with unless we can get some tires back." Michel said he had sold several of the tires but still had some of them. Michel turned over seven new tires to Detective Gross. Representatives from Northwest Tire and J&L Service identified the tires as some of those stolen from their shops. During the jury's deliberations, the jury submitted a note with written questions to the court. Michel argued on appeal the district court erred by not specifically answering the jury's questions and instead referring them to the existing jury instructions. After review, the North Dakota Supreme Court affirmed the criminal judgment, except as to the award of restitution. The award was reversed because the district court awarded more than what was required to make the victims whole. The matter was remanded for a redetermination of restitution.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Wayland

Court: North Dakota Supreme Court
Citation: 2020 ND 106
Opinion Date: May 7, 2020
Judge: Jon J. Jensen
Areas of Law: Constitutional Law, Criminal Law

Joey Wayland appealed after he was convicted by jury of Theft of Property and Possession of Drug Paraphernalia. Wayland contended his case should have been dismissed because his right to a speedy trial was violated by a continuance of his trial from March 11, 2019 to April 8, 2019. Wayland also contended the district court violated his right to remain silent by ordering him to submit to a mental health evaluation. Finding no reversible error, the North Dakota Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Schwindt v. Sorel

Court: North Dakota Supreme Court
Citation: 2020 ND 92
Opinion Date: May 7, 2020
Judge: Lisa K. Fair McEvers
Areas of Law: Constitutional Law, Criminal Law, Government & Administrative Law

Gregory Schwindt appealed a district court judgment affirming a Department of Transportation hearing officer's revocation of his driving privileges for 180 days. Schwindt argued North Dakota's implied consent and refusal laws were unconstitutional, the hearing officer erred by considering the results of the horizontal gaze nystagmus (HGN) test, and the hearing officer erred in finding he refused to take a chemical test. After review, the North Dakota Supreme Court concluded the hearing officer's findings of fact were supported by a preponderance of the evidence, the conclusions of law were sustained by the findings of fact, and the decision to revoke Schwindt's driving privileges was in accordance with the law.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. McDougald v. Greene

Court: Supreme Court of Ohio
Citation: 2020-Ohio-2782
Opinion Date: May 6, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court denied a writ of mandamus sought by Relator to

compel Respondent, the public-records custodian at the Southern Ohio Correctional Facility (SOCF), to provide Relator with three public records and to pay Relator statutory damages and court costs associated with this litigation, holding that Relator was not entitled to either a writ of mandamus nor statutory damages. When Relator was an inmate at SOCF he submitted a public-records request to Respondent seeking three documents. Respondent provided one of the three documents. Relator then filed a complaint for a writ of mandamus seeking an order compelling Respondent to provide the two documents and to pay statutory damages and court costs associated with this litigation. The Supreme Court denied the writ of mandamus on the merits, holding that Respondent's response to Relator fully satisfied Respondent's obligations under Ohio Rev. Code 149.43, and therefore, Relator was not entitled a writ of mandamus, and there was no basis to award statutory damages.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Parker Bey v. Byrd

Court: Supreme Court of Ohio
Citation: 2020-Ohio-2766
Opinion Date: May 5, 2020
Judge: Maureen O'Connor
Areas of Law: Criminal Law

The Supreme Court affirmed in part and reversed in part the judgment of the court of appeals denying Appellant's complaint for a writ of mandamus to compel the Cuyahoga County Clerk of Courts to produce various court records and denying the clerk's request that Appellant be declared a vexatious litigator, holding that the court of appeals erred in denying Appellant's complaint on the grounds that he did not invoke the Rules of Superintendence as the basis for his request. Appellant sought copies of journal entries from his criminal case and a copy of the clerk of courts' records-retention schedule. The clerk largely denied the request. Appellant then filed a complaint for a writ of mandamus. The court of appeals denied Appellant's request for mandamus relief, concluding that the clerk had no clear legal duty to provide the requested records. The Supreme Court reversed, holding (1) this action to compel the production of journal entries from a 1995 case was properly brought under the Public Records Act; and

(2) this Court declines to impose sanctions on Appellant or to declare him a vexatious litigator.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Dangler

Court: Supreme Court of Ohio
Citation: 2020-Ohio-2765
Opinion Date: May 5, 2020
Judge: DeWine
Areas of Law: Criminal Law

The Supreme Court reversed the judgment of the court of appeals vacating Defendant's conviction and sentence and reinstated the trial court's acceptance of Defendant's plea of no contest to sexual battery, holding that the trial court did not completely fail to comply with Crim.R.11(C)(2)(a), and there was nothing in the record to support a conclusion that Defendant would not have entered his plea had the trial court been more detailed in its explanation. On appeal, Defendant sought to vacate his plea of no contest, arguing that his plea was invalid because the trial court erred by not explaining more fully the obligations and restrictions that went with his status as a sex offender, in violation of Crim. R. 11(C)(2)(a). The court of appeals vacated the conviction without requiring Defendant to show prejudice, concluding that the trial court had completely failed to comply with Crim. R. 11(C)(2)(a). The Supreme Court reversed, holding (1) the trial court did not completely failed to comply with Crim R. 11(C)(2)(a)'s maximum-penalty-advisement requirement; and (2) because Defendant did not establish prejudice, he was not entitled to have his no-contest plea vacated for a failure to comply with Crim.R. 11(C).

Read Opinion Are you a lawyer? **Annotate this case**.

Oregon v. Haji

Court: Oregon Supreme Court
Docket: S066254
Opinion Date: May 7, 2020
Judge: Nakamoto

Areas of Law: Constitutional Law, Criminal Law

After a grand jury issued an indictment charging defendant Hanad Ali Haji with multiple offenses, the district attorney determined that the indictment could be challenged by demurrer because the basis for joining those offenses was not expressly alleged. Instead of seeking another indictment from the grand jury, the district attorney obtained leave from the trial court to amend the indictment by adding allegations specifying the statutory basis for joinder, without adding factual allegations about the crimes. Defendant was convicted on some of the charges at trial, and the Court of Appeals affirmed. The issue this case presented for the Oregon Supreme Court's review centered on whether the district attorney could add allegations specifying the statutory basis for joinder of multiple offenses to an indictment instead of resubmitting the case to the grand jury. The Supreme Court determined that neither the statute permitting joinder of multiple offenses in a single indictment nor Article VII (Amended), section 5(6), of the Oregon Constitution precluded a district attorney, with approval of the trial court, from amending an indictment to add allegations specifying the statutory basis for joinder of multiple offenses. The Supreme Court affirmed the decision of the Court of Appeals, based in part on different reasoning, and affirmed the judgment of the circuit court.

Read Opinion Are you a lawyer? **Annotate this case**.

South Carolina v. Durant

Court: South Carolina Supreme Court
Docket: 27964
Opinion Date: May 6, 2020
Judge: Kaye Gorenflo Hearn
Areas of Law: Constitutional Law, Criminal Law

Appellant Larry Durant was convicted of second-degree criminal sexual conduct (CSC) for sexually abusing a teenage girl in his church office where he served as the pastor. Durant contended the trial court improperly permitted the State to introduce evidence of prior sexual abuse allegations as evidence of a common scheme or plan under Rule 404(b), SCRE, and that the State committed a "Brady" violation by failing to accurately disclose the criminal history of its witness. After review, the South Carolina Supreme

Court affirmed the admissibility of the girls' testimony. "[W]hile the State failed to disclose the criminal background information of its witness, we find this information was not material." The Court found Durant exercised his position of trust, authority, and spiritual leadership to hold private prayer meetings with teen girls who had grown up in his church. He told them he was praying for their health and good fortune, and represented that part of this process was touching them sexually and having intercourse. Durant then warned the girls of misfortune if they refused or told anyone. Moreover, he used scripture as a means of grooming the children into performing sex acts. "These facts demonstrate the requisite logical connection between the prior acts of sexual abuse and the one forming the basis of the crime charged." The Court therefore affirmed Durant's conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

South Carolina v. Perry

Court: South Carolina Supreme Court
Docket: 27963
Opinion Date: May 6, 2020
Judge: Few
Areas of Law: Constitutional Law, Criminal Law

Petitioner Wallace Perry was convicted on two counts of criminal sexual conduct (CSC) with a minor in the first degree and two counts of CSC with a minor in the second degree for sexually assaulting two of his biological daughters. Prior to Perry's trial, the State made a motion to admit the testimony of Perry's stepdaughter from an earlier marriage that Perry sexually assaulted her twenty-two to twenty-seven years earlier. The State argued the trial court should not exclude the stepdaughter's testimony under Rule 404(b) of the South Carolina Rules of Evidence because it fit the "common scheme or plan" exception. Perry objected to this testimony. The trial court initially reserved ruling on the issue, but later indicated it was inclined to allow the stepdaughter to testify. The jury convicted Perry on all counts, and the trial court sentenced him to thirty years in prison. The court of appeals affirmed. The South Carolina Supreme Court determined it was not enough to meet the "logical connection" standard for admission of other crimes under the common scheme or plan exception to Rule 404(b) that the defendant previously committed the same crime. "When evidence of other

crimes is admitted based solely on the similarity of a previous crime, the evidence serves only the purpose prohibited by Rule 404(b), and allows the jury to convict the defendant on the improper inference of propensity that because he did it before, he must have done it again. ...The common scheme or plan exception demands more." The Supreme Court held State must show a logical connection between the other crime and the crime charged such that the evidence of other crimes "reasonably tends to prove a material fact in issue." The State must also convince the trial court that the probative force of the evidence when used for this legitimate purpose is not substantially outweighed by the danger of unfair prejudice from the inherent tendency of the evidence to show the defendant's propensity to commit similar crimes. In this case, the State did not meet its burden. Conviction was reversed and the matter remanded for a new trial.

Read Opinion Are you a lawyer? **Annotate this case**.

South Carolina v. Quinn

Court: South Carolina Supreme Court
Docket: 27966
Opinion Date: May 6, 2020
Judge: Kaye Gorenflo Hearn
Areas of Law: Constitutional Law, Criminal Law, White Collar Crime

Respondent Rick Quinn, Jr. was a former member of the South Carolina House of Representatives, representing constituents in Richland and Lexington counties from 1989-2004 and 2010-2017 and serving as House Majority Leader from 1999- 2004. He owned and operated a mail business called Mail Marketing Strategies (MMS) in Columbia, while his father owned and operated a political consulting firm, Richard Quinn & Associates (RQ&A). In 2014, Attorney General Alan Wilson designated First Circuit Solicitor David Pascoe as special prosecutor to conduct a State grand jury investigation into alleged public corruption committed by current and former members of the South Carolina General Assembly. This case arose from a prior state grand jury investigation of former House Speaker Bobby Harrell, which resulted in six counts of misusing campaign funds, to which he pleaded guilty. During the course of the investigation into Speaker Harrell, SLED uncovered potentially criminal conduct by Representative Jimmy Merrill and Representative Rick Quinn, and a second grand jury

investigation was initiated to investigate the conduct of these individuals. The investigation focused on Quinn's practice of using his office as House Majority Leader and leader of the House Republican Caucus to direct mailing and political services to his family's businesses. Quinn only admitted to a limited set of facts supporting the indictment. Believing the plea lacked a sufficient basis, the State moved to vacate Quinn's guilty plea, reconsider the sentence, and for the trial court's recusal. The State appealed the order denying its motions. After review, the South Carolina Supreme Court determined that the State could not appeal the guilty plea, the trial court did not abuse its discretion in sentencing, and there was no evidence of judicial bias or prejudice requiring the court to recuse itself. Therefore, the Court dismissed the State's appeal of the guilty plea, and affirmed as to all other issues.

Read Opinion Are you a lawyer? **Annotate this case**.

Texas v. Arellano

Court: Texas Court of Criminal Appeals
Docket: PD-0287-19
Opinion Date: May 6, 2020
Judge: Slaughter
Areas of Law: Constitutional Law, Criminal Law

After Appellee Cesar Ramiro Arellano was arrested for driving while intoxicated, the arresting officer, Phillip Garcia, prepared a probable cause affidavit to support a search warrant for a blood draw. Officer Garcia submitted his sworn affidavit to the on-duty magistrate. Using a cursive signature, the magistrate signed the blank signature line of a form search warrant authorizing the search and seizure of Appellee's blood. Below the signature line appeared the words, "Magistrate, Victoria County, Texas." Aside from the cursive signature, the magistrate's name was not typed or handwritten anywhere on the warrant. Upon execution of the search warrant, Appellee was charged with DWI. In the trial court, Appellee filed a motion to suppress all evidence stemming from the blood draw. At the pretrial suppression hearing, Appellee argued that the search warrant to obtain the blood specimen was facially invalid because the magistrate's signature was illegible in violation of the requirements of Code of Criminal Procedure Article 18.04(5). The trial court agreed, the court of appeals

concurred, and the evidence was suppressed because of the illegible signature. The Texas Court of Criminal Appeals disagreed with both lower courts, finding the court of appeals erred in holding that reliance on the statutory good-faith exception was automatically precluded based on an illegible magistrate's signature in violation of Code of Criminal Procedure Article 18.04(5). Because the remaining issues in the case were not properly addressed by the court of appeals, judgment was vacated and the matter remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

About Justia Opinion Summaries

Justia Weekly Opinion Summaries is a free service, with 63 different newsletters, each covering a different practice area.

Justia also provides 68 daily jurisdictional newsletters, covering every federal appellate court and the highest courts of all US states.

All daily and weekly Justia newsletters are free. Subscribe or modify your newsletter subscription preferences at daily.justia.com.

You may freely redistribute this email in whole.

About Justia

Justia is an online platform that provides the community with open access to the law, legal information, and lawyers.

Contact Us | Privacy Policy

Unsubscribe From This Newsletter
or unsubscribe from all Justia newsletters immediately **here.**

Justia | 1380 Pear Ave #2B, Mountain View, CA 94043

From: Criminal Law - Justia Weekly Opinion Summaries
To: Caravaggio, Suzanne (POL)
Subject: Latest 111 Cases This Week: Kelly v. United States (U.S.), Gomes v. Silva (1st Cir.), United States v. Perez-Couvertier (1st Cir.)
Date: Friday, May 8, 2020 9:07:02 AM

If you are unable to see this message, click here to view it in a web browser.

Justia Weekly Opinion Summaries

Criminal Law
May 8, 2020

Table of Contents

Kelly v. United States
Criminal Law, Government & Administrative Law, White Collar Crime
US Supreme Court

Gomes v. Silva
Civil Rights, Constitutional Law, Criminal Law

US Court of Appeals for the First Circuit

United States v. Perez-Couvertier
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the First Circuit

United States v. Haverkamp
Criminal Law
US Court of Appeals for the Second Circuit

United States v. Mladen
Criminal Law, Trusts & Estates
US Court of Appeals for the Second Circuit

United States v. Richardson
Criminal Law
US Court of Appeals for the Second Circuit

United States v. Rosemond
Criminal Law
US Court of Appeals for the Second Circuit

United States v. Lacerda
Criminal Law, White Collar Crime
US Court of Appeals for the Third Circuit

Cucalon v. Barr
Criminal Law, Immigration Law
US Court of Appeals for the Fourth Circuit

United States v. Doctor
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Lewis
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Jordan
Criminal Law
US Court of Appeals for the Fifth Circuit

United States v. Longoria
Criminal Law
US Court of Appeals for the Fifth Circuit

United States v. McNabb
Criminal Law
US Court of Appeals for the Fifth Circuit

Andrews v. Wayne County
Civil Rights, Constitutional Law, Criminal Law

US Court of Appeals for the Sixth Circuit

Hicks v. Scott
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Sixth Circuit

Moody v. United States
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Sixth Circuit

United States v. Foreman
Criminal Law
US Court of Appeals for the Sixth Circuit

United States v. Smith
Criminal Law
US Court of Appeals for the Sixth Circuit

Kirkman v. Thompson
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

Tuduj v. Newbold
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

United States v. Gibson
Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

United States v. Howell
Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

United States v. Lewis
Criminal Law
US Court of Appeals for the Seventh Circuit

Bakor v. Barr
Criminal Law, Immigration Law
US Court of Appeals for the Eighth Circuit

Smith v. Titus
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Becerra
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Haynes
Criminal Law

US Court of Appeals for the Eighth Circuit

United States v. Roberts
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Wright
Criminal Law
US Court of Appeals for the Eighth Circuit

Benson v. Chappell
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Ninth Circuit

Mero v. Barr
Criminal Law, Immigration Law
US Court of Appeals for the Ninth Circuit

Romero-Millan v. Barr
Criminal Law
US Court of Appeals for the Ninth Circuit

United States v. Yang
Criminal Law
US Court of Appeals for the Ninth Circuit

United States v. Neugin
Constitutional Law, Criminal Law
US Court of Appeals for the Tenth Circuit

United States v. Ramon
Constitutional Law, Criminal Law
US Court of Appeals for the Tenth Circuit

United States v. Richards
Constitutional Law, Criminal Law
US Court of Appeals for the Tenth Circuit

Andrews v. Warden
Criminal Law
US Court of Appeals for the Eleventh Circuit

Hollis v. United States
Criminal Law
US Court of Appeals for the Eleventh Circuit

Knight v. Florida Department of Corrections
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Eleventh Circuit

United States v. Evans
Criminal Law

US Court of Appeals for the Eleventh Circuit

United States v. McLellan
Criminal Law
US Court of Appeals for the Eleventh Circuit

United States v. Russell
Criminal Law
US Court of Appeals for the Eleventh Circuit

Welch v. United States
Criminal Law
US Court of Appeals for the Eleventh Circuit

State v. Trujillo
Constitutional Law, Criminal Law
Arizona Supreme Court

Barnett v. State
Criminal Law
Arkansas Supreme Court

Mason v. Kelley
Criminal Law
Arkansas Supreme Court

Ray v. Kelley
Criminal Law
Arkansas Supreme Court

Walker v. Kelley
Criminal Law
Arkansas Supreme Court

People v. Flores
Civil Rights, Constitutional Law, Criminal Law
Supreme Court of California

California v. Law
Constitutional Law, Criminal Law
California Courts of Appeal

California v. Sanchez
Constitutional Law, Criminal Law
California Courts of Appeal

Galeotti v. International Union of Operating Engineers
Criminal Law, Labor & Employment Law, White Collar Crime
California Courts of Appeal

In re I.A.
Criminal Law, Juvenile Law

California Courts of Appeal

People v. Edwards
Criminal Law
California Courts of Appeal

People v. Thomkins
Criminal Law
California Courts of Appeal

People v. Torres
Criminal Law
California Courts of Appeal

People v. Triplett
Criminal Law
California Courts of Appeal

Colorado In Interest of G.S.S.
Constitutional Law, Criminal Law, Juvenile Law
Colorado Supreme Court

Barringer v. Halkitis
Criminal Law
Florida Supreme Court

Franqui v. State
Criminal Law
Florida Supreme Court

Hicks v. State
Criminal Law
Florida Supreme Court

Burley v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Carter v. Georgia
Construction Law, Criminal Law
Supreme Court of Georgia

Clarke v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Collins v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Dawson v. Georgia
Constitutional Law, Criminal Law

Supreme Court of Georgia

Evans v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Hill v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Oliver v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Rosser v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Spencer v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Styles v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Whitehead v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Idaho v. Blythe
Constitutional Law, Criminal Law
Idaho Supreme Court - Criminal

Idaho v. Glodowski
Constitutional Law, Criminal Law
Idaho Supreme Court - Criminal

Idaho v. Jones
Constitutional Law, Criminal Law
Idaho Supreme Court - Criminal

State v. Gordon
Civil Rights, Constitutional Law, Criminal Law
Iowa Supreme Court

State v. Craig
Criminal Law
Kansas Supreme Court

State v. Lemmie
Criminal Law

Kansas Supreme Court

State v. Mullen
Criminal Law
Maine Supreme Judicial Court

Commonwealth v. Billingslea
Civil Rights, Constitutional Law, Criminal Law
Massachusetts Supreme Judicial Court

Commonwealth v. Martin
Civil Rights, Constitutional Law, Criminal Law
Massachusetts Supreme Judicial Court

Commonwealth v. Tavares
Criminal Law
Massachusetts Supreme Judicial Court

State v. Branch
Criminal Law
Minnesota Supreme Court

Galloway v. Mississippi
Constitutional Law, Criminal Law
Supreme Court of Mississippi

City of Missoula v. Zerbst
Civil Rights, Constitutional Law, Criminal Law
Montana Supreme Court

State v. Degarmo
Civil Rights, Constitutional Law, Criminal Law
Nebraska Supreme Court

People v. Holz
Civil Rights, Constitutional Law, Criminal Law
New York Court of Appeals

People v. Maffei
Civil Rights, Constitutional Law, Criminal Law
New York Court of Appeals

State v. Bailey
Civil Rights, Constitutional Law, Criminal Law
North Carolina Supreme Court

State v. Ellis
Civil Rights, Constitutional Law, Criminal Law
North Carolina Supreme Court

State v. Hobbs
Civil Rights, Constitutional Law, Criminal Law

North Carolina Supreme Court

State v. Mylett
Criminal Law
North Carolina Supreme Court

Dodge v. North Dakota
Constitutional Law, Criminal Law
North Dakota Supreme Court

Hewitt v. NDDOT
Criminal Law, Government & Administrative Law
North Dakota Supreme Court

Kastet v. NDDOT
Criminal Law, Government & Administrative Law
North Dakota Supreme Court

North Dakota v. Dahl
Constitutional Law, Criminal Law
North Dakota Supreme Court

North Dakota v. Foster
Constitutional Law, Criminal Law
North Dakota Supreme Court

North Dakota v. Kolstad
Constitutional Law, Criminal Law
North Dakota Supreme Court

North Dakota v. Michel
Constitutional Law, Criminal Law
North Dakota Supreme Court

North Dakota v. Wayland
Constitutional Law, Criminal Law
North Dakota Supreme Court

Schwindt v. Sorel
Constitutional Law, Criminal Law, Government & Administrative Law
North Dakota Supreme Court

State ex rel. McDougald v. Greene
Criminal Law
Supreme Court of Ohio

State ex rel. Parker Bey v. Byrd
Criminal Law
Supreme Court of Ohio

State v. Dangler
Criminal Law

Supreme Court of Ohio

Oregon v. Haji
Constitutional Law, Criminal Law
Oregon Supreme Court

South Carolina v. Durant
Constitutional Law, Criminal Law
South Carolina Supreme Court

South Carolina v. Perry
Constitutional Law, Criminal Law
South Carolina Supreme Court

South Carolina v. Quinn
Constitutional Law, Criminal Law, White Collar Crime
South Carolina Supreme Court

Texas v. Arellano
Constitutional Law, Criminal Law
Texas Court of Criminal Appeals

COVID-19 Updates: Law & Legal Resources Related to Coronavirus

Click here to remove Verdict from subsequent Justia newsletter(s).

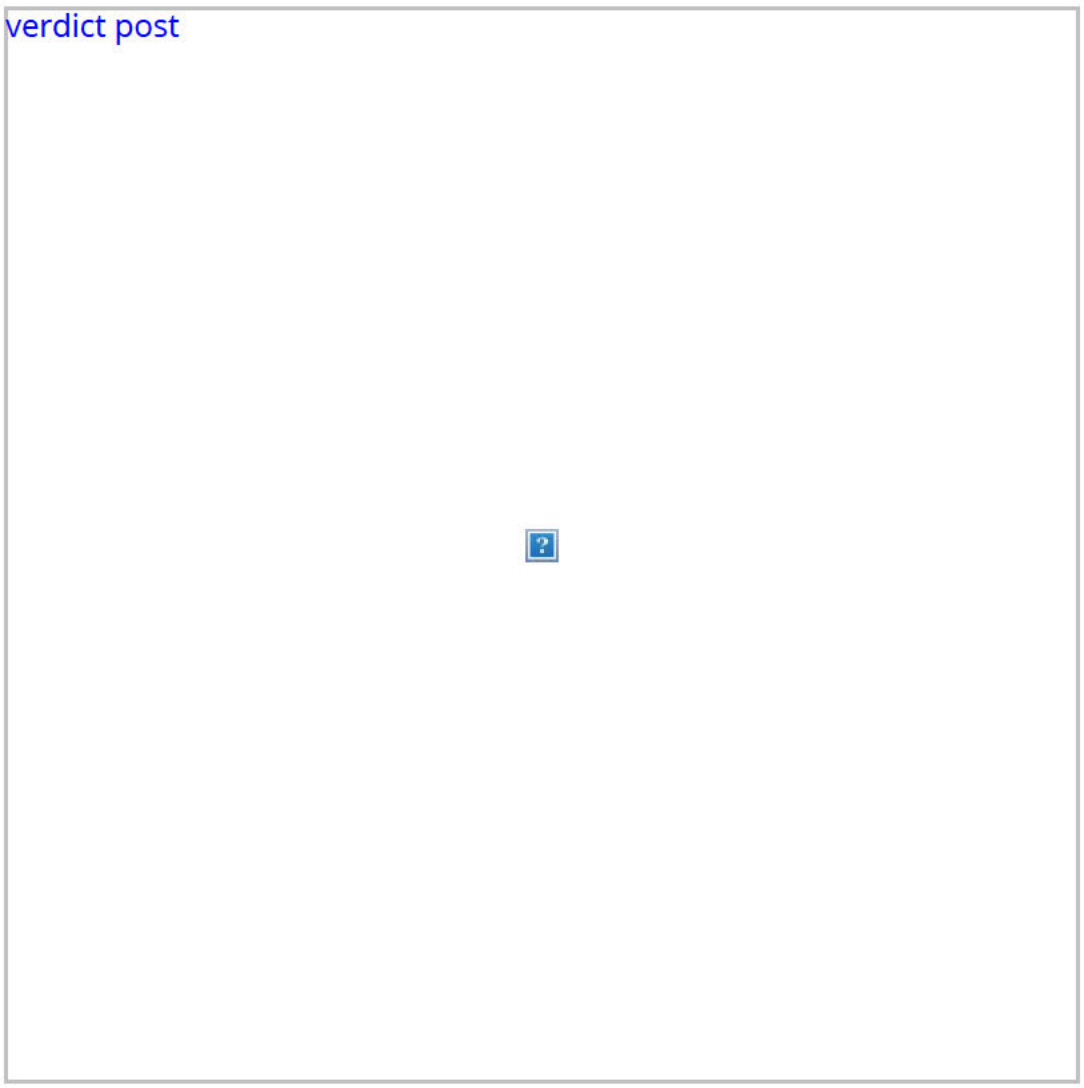
New on Verdict

Legal Analysis and Commentary

Department of Justice Once Again Proves Its Loyalty to the President, Not the Rule of Law

AUSTIN SARAT

verdict post



Austin Sarat—Associate Provost, Associate Dean of the Faculty, and William Nelson Cromwell Professor of Jurisprudence and Political Science at Amherst College—comments on the recent news that the Justice Department will seek dismissal of charges against Michael Flynn. Sarat suggests that because the decision does not seem to advance the fair administration of justice in this case, the court should take the unusual step of refusing to grant the prosecutor's motion to dismiss.

Read More

Criminal Law Opinions

Kelly v. United States

Court: US Supreme Court
Docket: 18-1059
Opinion Date: May 7, 2020
Judge: Elena Kagan
Areas of Law: Criminal Law, Government & Administrative Law, White Collar Crime

During former New Jersey Governor Christie's 2013 reelection campaign, Fort Lee's mayor refused to endorse Christie. Kelly, Christie's Deputy Chief of Staff, Port Authority Deputy Executive Director, Baroni, and another official decided to reduce from three to one the number of lanes reserved at the George Washington Bridge's toll plaza for Fort Lee's commuters. To disguise the political retribution, the lane realignment was said to be for a traffic study. Port Authority traffic engineers were asked to collect some numbers. An extra toll collector was paid overtime. The lane realignment caused four days of gridlock, ending only when the Port Authority's Executive Director learned of the scheme. The Third Circuit affirmed the convictions of Baroni and Kelly for wire fraud, fraud on a federally funded program, and conspiracy to commit those crimes. The Supreme Court reversed. The scheme did not aim to obtain money or property. The wire fraud statute refers to "any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses," 18 U.S.C. 1343. The federal-program fraud statute bars "obtain[ing] by fraud" the "property" (including money) of a federally funded program or entity, section 666(a)(1)(A). The statutes are limited to the protection of property rights and do not authorize federal prosecutors to set standards of good government. The Court rejected arguments that the defendants sought to take control of the Bridge's physical lanes or to deprive the Port Authority of the costs of compensating employees. Their realignment of the access lanes was an exercise of regulatory power; a scheme to alter a regulatory choice is not one to take government property. The time and labor of the employees were an incidental byproduct of that regulatory object. Neither defendant sought to obtain the services that the employees provided.

Read Opinion Are you a lawyer? **Annotate this case**.

Gomes v. Silva

Court: US Court of Appeals for the First Circuit
Docket: 19-1656

Opinion Date: May 1, 2020
Judge: Stahl
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The First Circuit affirmed the judgment of the district court denying Appellant's petition for a writ of habeas corpus, holding that, under the highly deferential standard prescribed by the Antiterrorism and Effective Death Penalty Act for federal habeas review of state criminal convictions, Appellant's claims to habeas relief failed. Appellant was convicted in a Massachusetts superior court of murder in the first degree and related crimes. The Supreme Judicial Court (SJC) affirmed the convictions. Appellant subsequently petitioned the District Court for the District of Massachusetts for a writ of habeas corpus. The district court denied the petition but granted a certificate of appealability. The First Circuit affirmed, holding (1) sufficient evidence supported Appellant's conviction for first-degree murder as a joint venturer, and the SJC's sufficiency determination was not unreasonable; and (2) the SJC reasonably determined that the trial court's admission into evidence of certain items did not constitute error.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Perez-Couvertier

Court: US Court of Appeals for the First Circuit
Docket: 16-2186
Opinion Date: May 7, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The First Circuit affirmed Defendant's conviction of possessing with intent to distribute controlled substances in a protected area and conspiring to distribute controlled substances in a protected area, holding that the district court did not plainly err with respect to any of Defendant's challenges. Specifically, the First Circuit held (1) the district court did not commit plain error in admitting evidence of the conspiracy's activities occurring after he withdrew from the conspiracy or, alternatively, in not instructing the jury to ignore such evidence; (2) the district court did not plainly err in admitting evidence of a drug trafficking organization's violent acts; and (3) the delay between Defendant's indictment and arrest did not violate his Sixth Amendment right to a speedy trial.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Haverkamp

Court: US Court of Appeals for the Second Circuit
Docket: 18-3735
Opinion Date: May 4, 2020
Judge: Barrington D. Parker
Areas of Law: Criminal Law

Defendant pleaded guilty to one count of distribution and receipt of child pornography and one count of possession of child pornography. The district court sentenced him to 121 months of imprisonment, followed by five years of supervised release, and imposed a $200 mandatory special assessment under 18 U.S.C. 3013, as well as a $10,000 assessment under 18 U.S.C. 3014. The Second Circuit held that the district court did not abuse its discretion in sentencing defendant and his sentence was substantively reasonable. The court held that the text of the Justice for Victims of Trafficking Act (JVTA), 18 U.S.C. 3014, taken as a whole and in its context, is straightforwardly meant to be applied on a per-offender, not a per-count, basis. In this case, the district court erroneously applied the special assessment on a per-count, rather than per-offender, basis. Finally, the court held that the computer monitoring condition in question was reasonably related to the nature of defendant's offense. Accordingly, the court affirmed in part, vacated in part, and remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Mladen

Court: US Court of Appeals for the Second Circuit
Docket: 18-0616
Opinion Date: May 6, 2020
Judge: Amalya Lyle Kearse
Areas of Law: Criminal Law, Trusts & Estates

After defendant died while his appeal was pending, counsel moved for

abatement of all incidents of the prosecution, requesting that the appeal be dismissed without a decision on the merits, that defendant's conviction be vacated, and that the matter be remanded to the district court with instructions to dismiss the indictment and order repayment to defendant's estate of the $20,000 fine and $100 special assessment. Because defendant was convicted upon his plea of guilty, and he neither did nor was permitted to challenge on appeal the merits of his conviction, the Second Circuit denied as without merit so much of the motion as seeks (1) vacatur of his conviction, (2) dismissal of the count of the indictment on which he was convicted, and (3) repayment of the mandatory $100 special assessment. The court granted so much of the motion as requests dismissal of this appeal and a remand to the district court for vacatur of the imposed terms of imprisonment and supervised release and for an order requiring that the paid fine of $20,000 be repaid to defendant's estate.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Richardson

Court: US Court of Appeals for the Second Circuit
Docket: 19-412
Opinion Date: May 5, 2020
Judge: Menashi
Areas of Law: Criminal Law

The Second Circuit affirmed defendant's conviction for distribution and possession with intent to distribute a controlled substance. The court held that the district court did not procedurally err by applying the career offender sentencing enhancement pursuant to USSG 4B1.1 because defendant's prior convictions of conspiracy to distribute a controlled substance in violation of 21 U.S.C. 841(a)(1) and 846, and attempted criminal possession of a controlled substance in violation of N.Y. Penal Law 220.16(1), qualify as controlled substance offenses, as defined in USSG 4B1.2(b). The court also held that the district court did not substantively err in sentencing defendant, because it properly considered his criminal history and accounted for his need for mental health and substance abuse treatment.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Rosemond

Court: US Court of Appeals for the Second Circuit
Docket: 18-3561
Opinion Date: May 1, 2020
Judge: Chin
Areas of Law: Criminal Law

The Second Circuit affirmed defendant's conviction for murder-for-hire, conspiracy to commit murder-for-hire, murder through use of a firearm, and possession of a firearm during a murder-for-hire conspiracy. Defendant owned Czar Entertainment, a music management company that represented hip-hop, rap and R&B artists such as Jayceon Taylor, also known as "The Game." Taylor was a member of G-Unit, a rap group run by Curtis Jackson, also known as "50 Cent." Defendant's crimes stemmed from a rivalry with Violator Records, the company that managed G-Unit. The court rejected defendant's contention that his attorney was ineffective because he conceded that defendant paid for the victim to be shot, even though he told counsel not to make this concession. The court held that defendant failed to show that this was objectively unreasonable or that he would have been found not guilty had a different argument been advanced. In this case, there was ample evidence supporting counsel's strategy to concede that defendant ordered a shooting where, among other things, the government's key witness, who participated in the conspiracy and lured the victim to be shot, testified that defendant agreed to pay the shooter. The court also held that the district court did not abuse its broad discretion by admitting prior bad-act evidence under Federal Rule of Evidence 404(b)(1).

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Lacerda

Court: US Court of Appeals for the Third Circuit
Docket: 15-2812
Opinion Date: May 5, 2020
Judge: Porter
Areas of Law: Criminal Law, White Collar Crime

VOG billed itself as an advocacy group helping victims of timeshare fraud get out of their timeshare debts. A jury determined that VOG had actually

defrauded its customers and that three individual defendants (including Lacerda) were each knowing participants in that fraud. Lacerda was sentenced to 324 months' imprisonment for his leading role in the fraudulent enterprise. The Third Circuit affirmed the respective convictions and sentences. The court rejected a claim of impermissible "overview testimony" by an FBI agent; an officer who is familiar with an investigation or was personally involved may tell the story of that investigation—how the investigation began, who was involved, and what techniques were used, and, with a proper foundation, may offer lay opinion testimony and testify about matters within his personal knowledge. The district court did not abuse its discretion when it disqualified defense counsel based on a conflict of interest; when it denied replacement counsel's motion for a continuance; when it excluded from evidence, as hearsay, an email sent by Lacerda to VOG's former CFO; in exercising its sentencing discretion; or by ordering the forfeiture of all VOG's gross proceeds.

Read Opinion Are you a lawyer? **Annotate this case**.

Cucalon v. Barr

Court: US Court of Appeals for the Fourth Circuit
Dockets: 18-1292, 18-2206
Opinion Date: May 7, 2020
Judge: Barbara Milano Keenan
Areas of Law: Criminal Law, Immigration Law

The Fourth Circuit denied petitions for review of the BIA's final order of removal. Applying the modified categorical approach, the court held that defendant's prior conviction for distribution of cocaine under Virginia Code 18.2-248, including distribution of that substance as an accommodation under Virginia Code 18.2-248(D), satisfies the federal definitions of an "aggravated felony" and of a crime "relating to a controlled substance" pursuant to 8 U.S.C. 1227(a)(2)(A)(iii), 1227(a)(2)(B)(i). The court also held that the district court did not abuse its discretion in denying petitioner's motion to reconsider.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Doctor

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-4874
Opinion Date: May 4, 2020
Judge: Roger L. Gregory
Areas of Law: Criminal Law

The Fourth Circuit affirmed the district court's revocation of defendant's supervised release and resulting sentence. The court held that the district court did not clearly err in finding the government proved he committed the assault underlying the supervised release violation; the district court did not commit plain error by adopting the violation report when announcing defendant committed Violation One; and, even if the district court erred in sentencing defendant for a Grade A violation, the error was harmless.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Lewis

Court: US Court of Appeals for the Fourth Circuit
Docket: 19-4028
Opinion Date: May 4, 2020
Judge: Barbara Milano Keenan
Areas of Law: Criminal Law

Defendant was convicted for possessing a firearm as a felon and sentenced to 63 months' imprisonment and a three-year period of supervised release. The district court additionally recommended, without explanation, that defendant receive addiction treatment while incarcerated and ordered, as a special condition of his supervised release, that defendant participate in an addiction treatment program. The Fourth Circuit held that defendant's sentence is procedurally unreasonable because the district court failed to provide an adequate explanation for imposing as a special condition of supervised release the requirement of addiction treatment. The court also held that the district court failed to address defendant's nonfrivolous mitigation arguments. Therefore, the court remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Jordan

Court: US Court of Appeals for the Fifth Circuit
Docket: 19-40499
Opinion Date: May 1, 2020
Judge: Jennifer Walker Elrod
Areas of Law: Criminal Law

The Fifth Circuit affirmed the district court's grant of defendants' motion for a new trial on the basis of prejudicial outside influence on the jury. The court held that the district court did not abuse its broad discretion in granting the motion for a new trial without holding an evidentiary hearing. To the extent there is a bright-line rule applicable to allegations of outside influence on the jury, the court held that it was not applicable to this case. Furthermore, the district court did not abuse its discretion in exercising its prerogative, within broadly defined parameters, to handle the allegation of outside influence in the least disruptive manner possible in this unusual case. Finally, the district court permissibly concluded that the evidence showed a sufficient likelihood of prejudice to shift the burden to the Government, and that the Government did not (and could not) show "no reasonable possibility that the jury's verdict was influenced by" the CSO's comments.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Longoria

Court: US Court of Appeals for the Fifth Circuit
Docket: 19-20201
Opinion Date: May 5, 2020
Judge: Gregg Costa
Areas of Law: Criminal Law

The Fifth Circuit held that the base offense level of 20 was proper for defendant's felon-in-possession crime involving a semiautomatic firearm that is capable of accepting a large capacity magazine. In this case, defendant failed to show that the district court clearly erred in relying on the FBI's agent statement about what was found in the apartment. The court clarified any confusion and held that the 2013 amendment to the commentary on the acceptance-of-responsibility Guideline does not clearly overrule its caselaw allowing the government to withhold the third point for

acceptance of responsibility when it must litigate a suppression motion. The court held that Amendment 775 does not contain the unequivocal override needed to get past the court's precedent. Therefore, the court affirmed defendant's sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. McNabb

Court: US Court of Appeals for the Fifth Circuit
Docket: 19-50265
Opinion Date: May 1, 2020
Judge: Costa
Areas of Law: Criminal Law

The Fifth Circuit affirmed defendant's sentence imposed after he pleaded guilty to possessing a gun after having been convicted of a felony. The court held that defendant is not entitled to relief on his claim that the government breached the plea deal, and thus his appellate waiver remains enforceable. Accordingly, defendant's challenges to his sentence must be dismissed.

Read Opinion Are you a lawyer? **Annotate this case**.

Andrews v. Wayne County

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-1992
Opinion Date: May 4, 2020
Judge: Suhrheinrich
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Canton Police received a 911 call from Andrews, who stated that his fiance, White, had physically attacked him. Officers arrested White. Andrews later took White's medications to the jail; a “KOP” policy allows inmates to keep certain drugs for self-administration. During an intake interview, White admitted to attempting to harm herself or commit suicide in the past but said she was not thinking of harming herself or having suicidal thoughts. An R.N. later evaluated White for nearly two hours, reported White’s chief complaints were “anxiety and depression,” and contacted a pharmacy to verify White’s prescriptions. The R.N. claims White did not exhibit any psychotic behavior,

suicidal ideation, or psychiatric distress but ordered further evaluation. The next day, White was found on the floor with vomit on her face. She stated repeatedly that she took too many pills. The next day, White died in the hospital. The cause of death was Verapamil toxicity. The Sixth Circuit affirmed the rejection of a suit under 42 U.S.C. 1983 on summary judgment. A pretrial detainee does not have an automatic right to a suicide screening. The court rejected an argument that the KOP Policy was deficient because it allows inmates in need of a psychological evaluation to participate before a psychiatrist's assessment of proper housing. The County had no history of suicides relative to the program, so any purported failure to train its employees in suicide risk assessment did not cause White's death.

Read Opinion Are you a lawyer? **Annotate this case**.

Hicks v. Scott

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-3410
Opinion Date: May 1, 2020
Judge: Gibbons
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Cincinnati officers Scott and Moore responded to a reported incident of menacing. Two people alleged that Quandavier had driven by their home that night and threatened to kill them and that Quandavier carried guns. Officer Loreaux identified a vehicle fitting the description. Officers Scott, Moore, Schneider, and Loreaux, standing where the vehicle was parked, heard a voice. Thinking that it was likely Quandavier, they knocked on the exterior door of the residence. It swung open. Three officers entered without a warrant or exigent circumstances. Loreaux remained outside. Neither Scott nor Moore recall announcing their presence or identifying themselves. Inside and upstairs, Scott knocked on a closed door. As it opened, Scott "saw the barrel of a rifle pointed at [her] face." Moore and Schneider also saw Quandavier "nonchalantly" panning the rifle from left to right. Moore reached for its barrel as Scott fired her weapon. Moore did not instruct Quandavier to drop his rifle nor did Scott issue any commands before firing. Quandavier collapsed. The officers immediately radioed for paramedics. Before the officers applied handcuffs or provided first aid, they heard another voice and conducted a sweep. Quandavier died at the scene

without receiving medical attention. In a suit under 42 U.S.C. 1983 for unlawful entry, excessive force, and deliberate indifference to a serious medical need, plus state claims, the district court granted the defendants summary judgment, citing qualified immunity. The Sixth Circuit reversed in part. The district court erred by granting qualified immunity to Scott, Moore, and Schneider on the unlawful entry claim. The court affirmed as to the excessive force, deliberate indifference, and state-law battery claims, and remanded for evaluation of municipal liability and wrongful death claims.

Read Opinion Are you a lawyer? **Annotate this case**.

Moody v. United States

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-5015
Opinion Date: May 6, 2020
Judge: Thapar
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

At Moody's trial, the government produced a video of Moody cooking crack on his stove and waving a handgun while he mused about life in "the game" (drug trafficking). The court ruled that most of the video was admissible. Moody then tried to persuade the jury that the video was filmed more than five years before his indictment, putting it outside the statute of limitations. The jury convicted Moody. Due to prior felony drug convictions, Moody received enhanced, mandatory-minimum life sentences on several counts. He appealed on evidentiary grounds relating to the video. The Sixth Circuit affirmed. Later, Moody raised new claims on collateral review, 28 U.S.C. 2255. The district court found each claim meritless; most were also procedurally defaulted. The court authorized Moody to appeal. The Sixth Circuit dismissed the appeal, stating that none of the claims should have been certified. Reasonable jurists could not doubt that the district court properly denied relief on Moody's claims that he was deprived of his statute-of-limitations defense (violating due process); that the past convictions for his sentencing enhancements were not charged in the indictment or found by the jury; and that his previous lawyers failed to raise the first two claims sooner, violating his right to effective assistance of counsel.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Foreman

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-1827
Opinion Date: May 7, 2020
Judge: Gibbons
Areas of Law: Criminal Law

In 2006, Foreman pled guilty to possession with intent to distribute 50 or more grams of cocaine base, possession with intent to distribute cocaine powder, and possession of a firearm during and in furtherance of a drug trafficking crime. Foreman admitted that he was responsible for approximately 135 grams of crack cocaine and 250 grams of cocaine powder. Foreman had a final Guidelines range of 322-387 months; he was sentenced to 240 months' imprisonment with respect to each drug conviction, to run concurrently, and 60 months' imprisonment for the firearms conviction, to run consecutively. When the First Step Act of 2018 made the Fair Sentencing Act retroactive, Foreman sought relief. The district court held that Foreman was not entitled to a plenary resentencing and declined to revisit his career offender status or hold an in-person hearing, then weighed the new statutory range applicable to Foreman's drug offenses, his recalculated Guidelines range, and the 18 U.S.C. 3553(a) factors, and reduced Foreman's total sentence to 172 months on each drug offense, to run concurrently, plus the mandatory consecutive 60 months on the firearms offense. The Sixth Circuit affirmed. Nothing in the First Step Act entitles a defendant to a plenary resentencing. First Step Act resentencings are not shielded from review for reasonableness; the district court thoroughly explained its rationale, carefully examining Foreman's circumstances, the amended penalty provisions, and the resulting changes to Foreman's Guidelines range.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Smith

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-1724
Opinion Date: May 6, 2020

Judge: Bush
Areas of Law: Criminal Law

In 2006, Smith was convicted of conspiracy to distribute and to possess with intent to distribute 500 grams or more of powder or 50 grams or more of cocaine base (crack cocaine); possession with intent to distribute 50 grams or more of cocaine base (crack cocaine); possession with intent to distribute 500 grams or more of cocaine powder; and being a felon in possession of a firearm. The court imposed a mandatory minimum life sentence. The Fair Sentencing Act subsequently lowered the penalty for cocaine-base offenses, made retroactive through the First Step Act. Smith moved for relief and received a reduced sentence of 360 months, the bottom of the new Guideline range for the counts impacted by the Fair Sentencing Act, to run concurrent to his existing 360-month sentence for his powder cocaine count that was not affected by the Fair Sentencing Act. The Sixth Circuit affirmed, rejecting an argument that the court should have imposed a below-Guideline sentence for all counts. The First Step Act is a limited grant of authority to impose a reduced sentence for certain offenses and does not require a plenary resentencing proceeding. Even assuming the court's obligation to explain its reasons for imposing the modified sentence was akin to that which applies in initial sentencing, the court's use of a modified AO 247 form order to explain its decision was not procedurally unreasonable.

Read Opinion Are you a lawyer? **Annotate this case**.

Kirkman v. Thompson

Court: US Court of Appeals for the Seventh Circuit
Docket: 19-1904
Opinion Date: May 7, 2020
Judge: William Joseph Bauer
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Following a 1992 fight that involved Johnson, Herron, and Walker, two shooters shot the three men. Johnson survived. In the hospital, Johnson described a shooter by the street name "Duke," where Duke lived, and Duke's car. Johnson identified Duke and his accomplice from a photo array. Police pulled over a vehicle matching Johnson's description and arrested

the driver, Kirkman, and the passenger, who matched the general description of the second shooter. Kirkman had a tattoo of Duke on his arm. Police took additional photos and presented a second photo array to Johnson, who identified them as the shooters. At trial, Johnson identified Kirkman and his passenger as the shooters. There was disputed testimony about the cause of the fight. Convicted of murder and aggravated battery with a firearm, Kirkman was sentenced to life in prison. Johnson had a change of heart and submitted an affidavit, identifying Ford and an unknown man as the shooters. At Kirkman's post-conviction hearing, Johnson testified that he and his family had been threatened. Other testimony was inconsistent with Johnson's. Illinois courts denied post-conviction relief, finding that Johnson's recantation lacked credibility. Johnson later pleaded guilty for perjury but failed to specify which statement was false. The Seventh Circuit affirmed the denial of federal habeas relief. Illinois courts found Johnson's recantation lacked credibility. An evidentiary hearing satisfied Kirkman's due process rights. The Illinois trial court's determination defeated Kirkman's innocence and perjured testimony claims.

Read Opinion Are you a lawyer? **Annotate this case**.

Tuduj v. Newbold

Court: US Court of Appeals for the Seventh Circuit
Docket: 19-1699
Opinion Date: May 1, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Illinois prisoner Tuduj, having received extensive dental treatment, filed a "deliberate indifference" suit under 42 U.S.C. 1983 against his dentists and prison officials. The court recruited counsel to assist Tuduj in filing an amended complaint that complied with the Federal Rules of Civil Procedure. Counsel defended against two summary judgment motions, one arguing that Tuduj had not exhausted his administrative remedies and another on the merits While the motions were pending, Tuduj moved "for leave to represent himself," stating that he was "concerned that his counsel has filed a structurally, technically and legally insufficient response doomed to be denied." He asked to file his own brief, except "in the event this Honorable Court deems counsel's response … legally sufficient and Grants same[,]

Plaintiff would be open to continued effective representation." A magistrate denied Tuduj's motion, stating that Tuduj "varie[d] between saying he would like to" represent himself and "indicating that he is happy with counsel's representation as long as he prevails." The district judge granted the motions for summary judgment, citing professional judgment and finding "no competent evidence" of any policy that unlawfully influenced dental-treatment decisions. The Seventh Circuit rejected Tuduj's argument that the court wrongly denied his "unqualified" right to proceed pro se under 28 U.S.C. 1654, the due process clause, the equal protection clause, and the Seventh Amendment. The district court permissibly denied his equivocal request.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Gibson

Court: US Court of Appeals for the Seventh Circuit
Docket: 19-1402
Opinion Date: May 7, 2020
Judge: William Joseph Bauer
Areas of Law: Constitutional Law, Criminal Law

Officer Garrison encountered Gibson, a suspected drug trafficker, walking with a companion. Although initially a consensual encounter, Garrison questioned Gibson and his companion and briefly detained Gibson. After Gibson and his companion departed, Garrison spotted a methamphetamine pipe under his patrol vehicle. Local law enforcement conducted a traffic stop of Gibson's vehicle in the curtilage of his driveway. A drug detection dog signaled the presence of a controlled substance in the vehicle, though nothing was found. Earlier that day, Gibson's wife had met with DEA agents to tell them about methamphetamine inside the home. Police used information Mrs. Gibson had provided to obtain a search warrant. The search of the home uncovered drugs, drug paraphernalia, currency, and AK-47 rifles, which led to Gibson's arrest. Gibson moved to suppress all evidence seized during the search, alleging he was detained without reasonable suspicion, unlawfully frisked, arrested without probable cause, stopped without probable cause or reasonable suspicion, and the traffic stop exceeded a permissible scope. Upon learning of his wife's cooperation, Gibson also argued her statement was insufficiently attenuated to justify the

search warrant. The Seventh Circuit affirmed the denial of the motion. Mrs. Gibson's voluntary statement with DEA agents was independently sufficient to sustain findings of probable cause and sufficiently attenuated from subsequent events to preclude suppression.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Howell

Court: US Court of Appeals for the Seventh Circuit
Docket: 18-3157
Opinion Date: May 4, 2020
Judge: Scudder
Areas of Law: Constitutional Law, Criminal Law

In December 2012, Chicago Police officers responded to an anonymous call reporting a Hispanic man in a black sweater and black hat, carrying a bag, and climbing under a warehouse fence. They found someone who matched the description. After stopping and frisking him, they determined he was not engaged in any crime. Howell, walking toward the police, was white and wearing a black jacket and dark hat. When an officer approached to speak to him, Howell did not answer, looked panicked, and put his hands in his pockets. The officer patted Howell down and found a gun in his jacket. A federal gun charge followed. Howell unsuccessfully moved to suppress the gun. The Seventh Circuit reversed the denial of his suppression motion and vacated his conviction for possessing that gun. The court noted that the facts in the pretrial record differed significantly from those presented at trial, where the arresting officer testified that he decided to proceed with the pat-down only after Howell ignored a directive to remove his hands from his pockets. Viewing the pretrial record as a whole, the police lacked reasonable suspicion to frisk Howell. The court did not reverse Howell's conviction on a second gun charge that resulted from the execution of a warrant to search Howell's apartment three months after the initial stop and the ensuing discovery of more guns and ammunition.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Lewis

Court: US Court of Appeals for the Seventh Circuit
Dockets: 19-1911, 19-1262
Opinion Date: May 7, 2020
Judge: Joel Martin Flaum
Areas of Law: Criminal Law

In 2016-2018, Draheim managed a conspiracy, responsible for at least 38 packages of methamphetamine sent from California to La Crosse, Wisconsin. Draheim supervised at least 11 associates who accepted shipments on her behalf, sent money transfers to California, distributed the meth, rented storage lockers, and collected money owed to her. Draheim provided vehicles. After agents placed a wiretap on her phone and seized several packages of meth en route to Draheim, her California supplier forced Draheim to find a new source. Draheim contacted Lewis, recently out of jail but still involved in the "meth scene." Lewis agreed to purchase meth from a new supplier. During the planned transaction, agents seized the package, which contained 28.6 grams of nearly pure meth. Police subsequently arrested Draheim after they found her daughter dead at home from an overdose; they took Lewis into custody for violating the terms of his state supervision. Both pleaded guilty to meth distribution offenses, 21 U.S.C. 841, 846. Draheim, facing a mandatory-minimum 10-year sentence, unsuccessfully argued that she qualified for "safety-valve relief." The court reasoned that she was the leader of her enterprise. Lewis unsuccessfully contended that he should be sentenced based only on his conviction, not other "relevant conduct." The Seventh Circuit affirmed Draheim's sentence but vacated as to Lewis. The fact that the defendant has engaged in other drug transactions is not, alone, sufficient to justify treating those transactions as relevant conduct for sentencing purposes.

Read Opinion Are you a lawyer? **Annotate this case**.

Bakor v. Barr

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-3011
Opinion Date: May 7, 2020
Judge: Steven M. Colloton
Areas of Law: Criminal Law, Immigration Law

The Eighth Circuit denied a petition for review of the BIA's determination

that defendant committed two crimes involving moral turpitude. The court held that the BIA did not err in determining that petitioner's conviction for the Minnesota crimes of Criminal Sexual Conduct in the Fifth Degree and knowing failure to comply with Minnesota's sex offender registration statute were crimes involving moral turpitude. The court also held that petitioner failed to exhaust his remaining arguments and therefore declined to consider them.

Read Opinion Are you a lawyer? **Annotate this case**.

Smith v. Titus

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-2915
Opinion Date: May 5, 2020
Judge: Steven M. Colloton
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Eighth Circuit affirmed the district court's denial of habeas relief to petitioner based on his claim that the trial court violated his Sixth Amendment right to a public trial when it briefly closed the courtroom to spectators. The district court denied relief based on the ground that the Minnesota Supreme Court’s decision was neither contrary to, nor an unreasonable application of, clearly established federal law. The court agreed and held that it was not objectively unreasonable for the Minnesota Supreme Court to deem it constitutional under the Sixth Amendment for the trial court to explain the parameters of an earlier public order on evidentiary issues in a brief nonpublic proceeding before the jury was sworn.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Becerra

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-2777
Opinion Date: May 7, 2020
Judge: Stras
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's conviction for two counts of being a

felon in possession of a firearm and ammunition. The court held that there was more than enough evidence for defendant's probation officer and other officers to believe defendant had a firearm on him. Therefore, the officers had probable cause to arrest him without a warrant. The court also held that defendant was in custody when he made both statements at issue. In this case, the "request for clarification" of defendant's statement that he had "something" in his car did not require Miranda warnings. Furthermore, because the bulge in defendant's pocket could have been a gun or other weapon that would have posed a danger to the officers and others, they could ask about it without the formality of Miranda warnings. The court joined its sister circuits in declining to recognize the innocent-possessor defense. The court held that the district court did not err in excluding defendant's proposed testimony that he had found the handgun in his car earlier in the day and was about to hand it over to his probation officer. The court reasoned that, even if defendant intended to turn over the gun (or the ammunition) to his probation officer, it is still a crime to knowingly possess it in the first place. Finally, the court held that the district court did not err in denying defendant a sentencing reduction for acceptance of responsibility; the district court considered defendant's mitigation arguments at sentencing; and the district court did not abuse its discretion by imposing a within-Guidelines sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Haynes

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1607
Opinion Date: May 5, 2020
Judge: Raymond W. Gruender
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's conviction and sentence for being a felon in possession of a firearm. The court held that the government did not violate the Speedy Trial Act, and defendant failed to offer any evidence showing that Iowa and federal prosecutors colluded. Furthermore, the district court did not abuse its discretion by failing to hold an evidentiary hearing regarding the existence of collusion. The court also held that the district court did not err in denying the motion to suppress where defendant

was not unlawfully seized. In this case, prior to producing the marijuana cigarette, the officer did not ask defendant any questions but merely ordered him off the bus, particularly as the smell of marijuana alerted the officer that evidence of a more serious crime than failure to use a turn signal might be uncovered during the stop. Finally, the court held that defendant was not unlawfully searched when the officer conducted a pat-down search incident to arrest; the evidence was sufficient to support defendant's conviction; defendant's Rehaif claim failed because there was sufficient evidence that he knew of his prohibited status; and defendant's sentence was not substantively unreasonable nor an abuse of the district court's discretion.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Roberts

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1176
Opinion Date: May 1, 2020
Judge: Steven M. Colloton
Areas of Law: Criminal Law

The Eighth Circuit vacated defendant's sentence imposed after he pleaded guilty to unlawful possession of a firearm as a previously convicted felon. The court held that, although the district court properly applied a four-level increase for possession of a firearm "in connection with another felony offense" under USSG 2K2.1(b)(6)(B), but that a two-level increase for "using a minor to commit a crime" under USSG 3B1.4 should not have applied. In this case, the evidence showed only that defendant engaged in an arm's-length transaction with a minor. The court held that this mere joint participation in an offense as a partner, does not amount to "use" of a minor "to commit the offense" of unlawful possession of a firearm by a felon. Accordingly, the court remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Wright

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1081

Opinion Date: May 5, 2020
Judge: Erickson
Areas of Law: Criminal Law

The Eighth Circuit affirmed the district court's restitution order and certain special conditions of defendant's supervised release imposed after he pleaded guilty to sex trafficking of a child. The court found no error in the district court's restitution amount of $20,000, holding that the evidence supported the amount in light of the aggregate harm to the victim. The court also held that the special conditions -- including a requirement that defendant participate in sex offender treatment including psychological testing and polygraph examinations, a prohibition against contact with any minors without pre-approval, and a requirement that defendant seek prior approval before using temporary commercial lodging, such as a hotel or motel -- where reasonably related to both the offense of conviction and to defendant's history of sexual contact with minor females.

Read Opinion Are you a lawyer? **Annotate this case**.

Benson v. Chappell

Court: US Court of Appeals for the Ninth Circuit
Docket: 13-99004
Opinion Date: May 1, 2020
Judge: Consuelo Maria Callahan
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Ninth Circuit affirmed the district court's denial of petitioner's habeas corpus petition challenging his California conviction and death sentence for murder and other crimes. Petitioner raised two certified claims and two uncertified claims. The panel held that petitioner failed to show that the California Supreme Court's denials of his claims were unreasonable determinations of the facts or contrary to clearly established federal law. In this case, the California Supreme Court reasonably determined that an officer's misstatement during petitioner's interrogation that there was no death penalty in California did not prompt petitioner's confessions. Furthermore, petitioner failed to show that his statements were not knowing, voluntary, and intelligent. Even if petitioner were able to show that trial counsel was ineffective in not fully investigating his abuse as a child or his alleged organic brain injury, the panel held that the state court could

reasonably have determined that any shortcoming in trial counsel's investigation was not prejudicial. Finally, the panel granted a certificate of appealability on petitioner's two uncertified claims and held that the state court reasonably rejected the claims that his trial counsel should have impeached the government's case and the prosecutor withheld material, exculpatory evidence.

Read Opinion Are you a lawyer? **Annotate this case**.

Mero v. Barr

Court: US Court of Appeals for the Ninth Circuit
Docket: 17-70929
Opinion Date: May 1, 2020
Judge: Paul Jeffrey Watford
Areas of Law: Criminal Law, Immigration Law

The Ninth Circuit granted in part a petition for review of the BIA's finding that petitioner was removable based on his conviction for possession of visual presentation depicting sexual conduct of a person under 16 years of age, in violation of Nevada Revised Statutes (N.R.S.) 200.730. Applying the categorical approach, the panel compared the elements of N.R.S. 200.730 with the applicable definition of "sexual abuse of a minor," which requires proof of three elements. The panel held that N.R.S. 200.730 punishes a broader range of conduct because the Nevada statute does not require proof that the offender participated in sexual conduct with a minor. Therefore, petitioner's conviction did not qualify as sexual abuse of a minor. The panel explained that, with a possession-only offense such as N.R.S. 200.730, the minor depicted in the image is not the direct object of the offender's conduct, which is a necessary predicate for the offense to qualify as sexual abuse of a minor.

Read Opinion Are you a lawyer? **Annotate this case**.

Romero-Millan v. Barr

Court: US Court of Appeals for the Ninth Circuit
Dockets: 16-73915, 17-72893, 18-71555
Opinion Date: May 4, 2020

Areas of Law: Criminal Law

The Ninth Circuit certified the following questions of state law to the Arizona Supreme Court: 1. Is Arizona's possession of drug paraphernalia statute, A.R.S. 13-3415, divisible as to drug type? 2. Is Arizona's drug possession statute, A.R.S. 13-3408, divisible as to drug type? 3. Put another way, is jury unanimity (or concurrence) required as to which drug or drugs listed in A.R.S. 13-3401(6), (19), (20), or (23) was involved in an offense under either statute?

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Yang

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-10341
Opinion Date: May 4, 2020
Judge: Piersol
Areas of Law: Criminal Law

The Ninth Circuit affirmed the district court's denial of defendant's motion to suppress after he pleaded guilty to receipt of stolen mail and being a prohibited person in possession of a firearm. Defendant moved to suppress the evidence seized from his residence and the statements he made to law enforcement on the basis that the search warrant obtained by the Postal Inspection Service relied on evidence that was obtained illegally. The panel declined to address the potential Fourth Amendment privacy interests that may be implicated by the warrantless use of this Automatic License Plate Recognition (ALPR) technology, and held that defendant does not have a reasonable expectation of privacy in the historical location data of the Yukon under the facts of this case. The panel found no evidence in the record that Prestige Motors had a policy or practice of allowing lessees to keep cars beyond the rental period and Prestige had made affirmative attempts to repossess the vehicle by activating the GPS unit to locate and disable the vehicle. Therefore, defendant lacked standing to challenge the warrantless search of the database.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Neugin

Court: US Court of Appeals for the Tenth Circuit
Docket: 19-7043
Opinion Date: May 1, 2020
Judge: Scott Milne Matheson, Jr.
Areas of Law: Constitutional Law, Criminal Law

Jack Neugin pled guilty to being a felon in possession of a firearm and ammunition on the condition that he could appeal the district court's denial of his motion to suppress evidence of the ammunition and firearm police found in the bed of his pickup truck. Officers responded to a reported verbal altercation between Neugin and his girlfriend. One of the officers saw ammunition in the back of the truck after he lifted the truck's camper lit do allow the girlfriend to retrieve her belongings. Neugin argued the officers discovered the evidence during an unconstitutional search; the district court concluded the officer was acting "in a lawful position" as "community caretaker," and found no Fourth Amendment violation. The Tenth Circuit reversed, finding that : (1) the officer conducted the without a warrant or probable cause, (2) the community caretaking exception to the warrant requirement does not apply, and (3) the inevitable discovery exception to the exclusionary rule does not apply. The evidence seized should have been suppressed.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Ramon

Court: US Court of Appeals for the Tenth Circuit
Docket: 19-1221
Opinion Date: May 1, 2020
Judge: Gregory Alan Phillips
Areas of Law: Constitutional Law, Criminal Law

In 2016, after serving a federal prison sentence for having possessed a firearm after a felony conviction, Charles Ramon III began serving a mandatory term of supervised release. Before Ramon completed the term, his probation officer filed a petition, soon followed by two superseding petitions, to revoke Ramon’s supervised release. At the revocation hearing, the district court found three violations—two for possessing a controlled

substance and one for again illegally possessing a firearm. Of these, the most serious was Ramon's illegal possession of a firearm—a Grade B violation. For this, the court imposed the statutory maximum sentence of twenty-four months in prison. During the revocation hearing, the government mentioned that it might seek to indict Ramon for illegally possessing a firearm (the conduct in part underlying the revocation). Mindful of this, the district court ordered that Ramon's twenty-four-month sentence run "consecutively to any sentences imposed previously or prospectively in federal or state court." At the hearing, Ramon did not object to the district court's running his sentence consecutively to future federal sentences. On appeal, Ramon argued that the district court exceeded its sentencing authority under 18 U.S.C. 3584(a) by ordering that Ramon's sentence run consecutively to future federal sentences. By the terms of 18 U.S.C. 3584(a), the Tenth Circuit determined the district court did err. But Ramon failed to object to this at trial, and on appeal, failed to show that the error was plain, thus, judgment was affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Richards

Court: US Court of Appeals for the Tenth Circuit
Docket: 19-8044
Opinion Date: May 6, 2020
Judge: Baldock
Areas of Law: Constitutional Law, Criminal Law

In 2018, the Wyoming Division of Criminal Investigation (DCI) obtained a search warrant to review the contents of Defendant–Appellant Joshua Richards' Tumblr account. During the search and subsequent investigation, DCI agents discovered Defendant had re-blogged videos and images of child pornography to his private Tumblr so he could later access and view the materials. Defendant ultimately pleaded guilty to one count of accessing with intent to view child pornography. He was sentenced to twenty-four months' imprisonment followed by five years of supervised release. The district court imposed several special conditions of supervised release, which, as relevant here, related to drugs and alcohol and required Defendant to submit to polygraph testing. On appeal, Defendant argued the district court erred in imposing these special conditions. He also challenged

the length of his prison sentence as substantively unreasonable. The Tenth Circuit determined the alcohol and drug conditions did not directly conflict with the relevant policy statement in the sentencing guidelines, so the district court's decision to impose the conditions was not manifestly unreasonable. And given the circumstances of the case, the Court determined the trial court did not abuse its discretion in imposing Defendant's twenty-four month sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

Andrews v. Warden

Court: US Court of Appeals for the Eleventh Circuit
Docket: 19-12443
Opinion Date: May 5, 2020
Judge: William Holcombe Pryor, Jr.
Areas of Law: Criminal Law

The Eleventh Circuit affirmed the district court's denial of habeas relief under 28 U.S.C. 2241. Plaintiff alleged that President Obama commuted his "total sentence" of imprisonment, which included the 37 months of imprisonment that he served as part of his 2003 sentence. Based on the terms of the commutation order, the Constitution, and Supreme Court precedent, the court could not say that the Bureau erred in excluding the 37-month term of imprisonment from its recalculation.

Read Opinion Are you a lawyer? **Annotate this case**.

Hollis v. United States

Court: US Court of Appeals for the Eleventh Circuit
Docket: 19-11323
Opinion Date: May 6, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Eleventh Circuit affirmed the district court's denial of petitioner's motion to vacate his sentence under 28 U.S.C. 2255. The court held that petitioner cannot prove that his counsel rendered ineffective assistance, because petitioner's prior convictions in Alabama categorically qualify as predicate

offenses under both the Armed Career Criminal Act and the career-offender provision of the Guidelines, and his prior conviction in Georgia qualifies as a predicate offense under the Act. Therefore, counsel did not perform deficiently by failing to raise a meritless objection.

Read Opinion Are you a lawyer? **Annotate this case**.

Knight v. Florida Department of Corrections

Court: US Court of Appeals for the Eleventh Circuit
Docket: 18-12488
Opinion Date: May 1, 2020
Judge: Newsom
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Eleventh Circuit affirmed the district court's denial of a 28 U.S.C. 2254 petition for habeas relief. Petitioner alleged that his counsel rendered ineffective assistance under Strickland v. Washington, 466 U.S. 668 (1984), by failing to adequately investigate and present mitigating evidence during the sentencing phase of his capital-murder trial. The court held that, even assuming that counsel performed deficiently in failing to investigate and present the mitigation evidence that petitioner now raises—thus satisfying the first prong of the two-part Strickland standard that governs ineffective-assistance claims—petitioner failed to carry his burden of demonstrating resulting prejudice.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Evans

Court: US Court of Appeals for the Eleventh Circuit
Docket: 17-15323
Opinion Date: May 6, 2020
Judge: Grant
Areas of Law: Criminal Law

The Eleventh Circuit affirmed defendant's conviction and sentence for being a felon in possession of a firearm. The court held that, given the totality of the circumstances, it was reasonable for officers, mistaking a dog's whimper for a person in distress, to enter defendant's home without a warrant.

Therefore, defendant's challenge to the district court's denial of his motion to suppress evidence failed. The court upheld the district court's imposition of a 22 offense level finding because defendant possessed a semiautomatic firearm capable of accepting a large capacity magazine under USSG 2K2.1(a)(3)(A)(i) (2016). The court also upheld defendant's sentencing enhancement under USSG 2K2.1(b)(4)(B) for possessing a rifle that had an obliterated serial number.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. McLellan

Court: US Court of Appeals for the Eleventh Circuit
Docket: 18-13289
Opinion Date: May 6, 2020
Judge: Boggs
Areas of Law: Criminal Law

The Eleventh Circuit affirmed defendant's conviction for two counts of being a felon in possession of a firearm. The court held that the district court did not abuse its discretion in permitting one of his arresting officers to offer testimony at trial on the correlation between guns and drug activity and to suggest that defendant was selling drugs; the court declined to evaluate the applicability of the Armed Career Criminal Act (ACCA), because the district court would have imposed the same sentence regardless of whether the mandatory minimum applied; and the court rejected defendant's claim under Rehaif v. United States, 139 S. Ct. 2191 (2019), and held that there was no plain error in the district court's failure to instruct the jury of the knowledge-of-status element and any error from the lack of a knowledge-of-status element in defendant's plea colloquy did not affect his substantial rights. Finally, the court remanded for clarification of the judgment to reflect the sentence the district court said it would have imposed if the Armed Career Criminal Act did not apply.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Russell

Court: US Court of Appeals for the Eleventh Circuit

Docket: 18-11202
Opinion Date: May 4, 2020
Judge: Charles R. Wilson
Areas of Law: Criminal Law

Defendant was convicted of possessing a firearm and ammunition as an immigrant illegally or unlawfully in the United States. After defendant appealed his conviction and sentence, the Supreme Court issued its decision in Rehaif v. United States, 588 U.S. ___, 139 S. Ct. 2191 (2019), which reversed a decision from this court and held that under 18 U.S.C. 922(g), the government must prove that a defendant knew "his status as a person barred from possessing a firearm" when he knowingly possessed a firearm. The Eleventh Circuit held that defendant established the necessary prejudice under plain error review and vacated defendant's section 922(g) conviction, remanding for further proceedings. In this case, the district court committed an error that was made plain by the Supreme Court in Rehaif. Furthermore, defendant has sufficiently shown a reasonable probability that but for the error, the outcome of his trial would have been different.

Read Opinion Are you a lawyer? **Annotate this case**.

Welch v. United States

Court: US Court of Appeals for the Eleventh Circuit
Docket: 14-15733
Opinion Date: May 6, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Eleventh Circuit affirmed the district court's denial of petitioner's 28 U.S.C. 2255 motion to vacate his sentence. The court held that defendant's prior 1996 Florida convictions for robbery qualified as violent felonies under the Armed Career Criminal Act's (ACCA) elements clause, and rejected his contention that the court's decision in his direct appeal carved out a narrow exception to pre-1997 Florida robbery convictions obtained in Florida's Fourth District Court of Appeal. The court also held that petitioner's prior Florida felony battery conviction was a violent felony under the ACCA in light of the court's holding in United States v. Vail-Bailon, 868 F.3d 1293 (11th Cir. 2017) (en banc), cert. denied, 138 S. Ct. 2620 (2018).

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Trujillo

Court: Arizona Supreme Court
Docket: CR-18-0531-PR
Opinion Date: May 4, 2020
Judge: Gould
Areas of Law: Constitutional Law, Criminal Law

The Supreme Court held that, for purposes of imposing mandatory sex offender registration under Ariz. Rev. Stat. 13-3821(A)(3), a judge has the authority to make the necessary factual finding that the victim is under the age of eighteen and that Arizona's sex offender registration statutes are civil regulatory statutes, not criminal penalties. Defendant was convicted by a jury of one count of sexual abuse. In reaching its verdict the jury determined that the victim was "fifteen or more years of age." At sentencing, the trial court ordered Defendant to register as a sex offender. Defendant objected, arguing that, pursuant to Apprendi v. New Jersey, 530 U.S. 466 (2000), a jury was required to find whether Defendant was under eighteen pursuant to section 13-3821(A)(3). The trial court denied the objection. The court of appeals affirmed. The Supreme Court affirmed, holding (1) Apprendi does not apply to factual findings that are necessary to impose registration because sex offender registration is a civil regulatory requirement, not a criminal penalty; and (2) the trial judge did not violate Apprendi by determining that the victim was under eighteen.

Read Opinion Are you a lawyer? **Annotate this case**.

Barnett v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 181
Opinion Date: May 7, 2020
Judge: Hudson
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's "motion for credit for time spent in custody," holding that the

circuit court's findings were not clearly erroneous. In his motion, Appellant alleged that he was entitled to 312 days of jail-time credit and that the circuit court should enter a new sentencing order nunc pro tunc that reflected the correct amount of jail-time credit. The circuit court denied the motion. The Supreme Court affirmed, holding that the circuit court's denial of Appellant's motion was not clearly erroneous because Appellant failed to demonstrate a clerical error subject to correction.

Read Opinion Are you a lawyer? **Annotate this case**.

Mason v. Kelley

Court: Arkansas Supreme Court
Citation: 2020 Ark. 182
Opinion Date: May 7, 2020
Judge: Rhonda K. Wood
Areas of Law: Criminal Law

The Supreme Court affirmed the order of the circuit court dismissing Appellant's pro se petition for writ of habeas corpus, holding that Appellant stated no ground on which the writ could issue. Appellant was convicted of aggravated robbery, theft of property, and second-degree battery and sentenced as a habitual offender to an aggregate term of 660 months' imprisonment. The court of appeals affirmed. Appellant later petitioned for writ of habeas corpus, asserting that the trial court misapplied Arkansas's habitual-offender statutes. The circuit court dismissed the petition. The Supreme Court affirmed, holding that the issues Appellant raised in his petition for the writ should have been raised at trial, on direct appeal, or in a petition for postconviction relief.

Read Opinion Are you a lawyer? **Annotate this case**.

Ray v. Kelley

Court: Arkansas Supreme Court
Citation: 2020 Ark. 184
Opinion Date: May 7, 2020
Judge: Wynne
Areas of Law: Criminal Law

The Supreme Court dismissed Appellant's appeal from an order denying his pro se petition for permission to reinvest jurisdiction in the trial court to consider a petition for writ of error coram nobis, holding that the circuit court had no jurisdiction to consider the petition. Appellant entered negotiated guilty pleas to rape and other offenses. Appellant later filed a petition for writ of error coram nobis in the Chicot County Circuit Court, the court where he was incarcerated, setting out two grounds for coram nobis relief. The circuit court denied the petition. The Supreme Court dismissed Appellant's appeal, holding that jurisdiction lay in the trial court where Appellant was convicted, which in this case was the Ashley County Circuit Court. Therefore, the Chicot County Circuit Court was without jurisdiction to address Appellant's coram nobis petition.

Read Opinion Are you a lawyer? **Annotate this case**.

Walker v. Kelley

Court: Arkansas Supreme Court
Citation: 2020 Ark. 183
Opinion Date: May 7, 2020
Judge: Rhonda K. Wood
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's pro se petition for declaratory judgment, holding that Appellant could not use a declaratory-judgment action to collaterally attack his criminal conviction. Appellant was convicted of first-degree murder and second-degree unlawful discharge of a firearm from a vehicle. The court of appeals affirmed. Years later, Appellant filed a petition for declaratory judgment alleging that he was denied due process in his criminal trial when the court admitted the prior testimony of an unavailable witness and that this admission violated the Confrontation Clause. The circuit court denied the petition. The Supreme Court affirmed, holding that a declaratory judgment action provided no relief on these grounds.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Flores

Court: Supreme Court of California
Docket: S116307
Opinion Date: May 4, 2020
Judge: Kruger
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction of three counts of first degree murder and his sentence of death, holding that the three or four minor errors at Defendant's trial were harmless and did not interfere with his due process right to a fair trial. Specifically, the Supreme Court held (1) no error occurred during jury selection; (2) Defendant was not prejudiced by any misstatements by the prosecutor; (3) assuming certain evidence was inadmissible, the court's admonition to the jury and the court's instruction cured the resultant harm; (4) the trial court erred in admitting testimony that the victim was afraid of Defendant, but the error was harmless; and (5) Defendant's remaining allegations of error were without merit.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. Law

Court: California Courts of Appeal
Docket: E072845(Fourth Appellate District)
Opinion Date: May 5, 2020
Judge: Slough
Areas of Law: Constitutional Law, Criminal Law

In 2001, appellant Terrell Law and his codefendant Brett May committed a home invasion robbery, during which one of them shot and killed one of the residents. They were tried jointly in 2006 before two separately empaneled juries who found them both guilty of first degree felony murder with the special circumstance described in Penal Code section 190.2(a)(17(A) and (d). Though Law's jury found he was not the shooter, they nonetheless concluded he was a "major participant" in the underlying robbery and acted "with reckless indifference to human life." In 2018, the Legislature enacted Senate Bill No. 1437 (2017-2018 Reg. Sess.) which, among other things, amended the definition of felony murder in Penal Code section 189. The legislation also added Penal Code section 1170.95, which established a procedure for vacating murder convictions predating the amendment that could not be sustained under the new definition of felony murder. Law

challenged the trial court's summary denial of his section 1170.95 petition to vacate his murder conviction, arguing the trial court erred by reviewing his record of conviction and determining the jury's true finding on the special circumstance rendered him ineligible for relief. The Court of Appeal concluded it was proper for a trial court to review the record of conviction when determining whether a section 1170.95 petitioner had stated a prima facie claim for relief. Additionally, the Court concluded Law "undoubtedly qualifies" as a major participant who acted with reckless indifference to human life, a conclusion that rendered him ineligible for relief under section 1170.95. The Court therefore affirmed the order denying his petition.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. Sanchez

Court: California Courts of Appeal
Docket: E072647(Fourth Appellate District)
Opinion Date: May 7, 2020
Judge: Menetrez
Areas of Law: Constitutional Law, Criminal Law

Victor Sanchez was charged with first degree murder, but pled guilty to voluntary manslaughter. He filed a petition under Penal Code section 1170.95 to vacate that conviction. The trial court denied the petition, concluding that Sanchez was ineligible for relief because he was not convicted of murder. After review, the Court of Appeal joined other courts that held section 1170.95 did not apply to defendants convicted of voluntary manslaughter. The Court also rejected Sanchez's argument that section 1170.95 violated equal protection.

Read Opinion Are you a lawyer? **Annotate this case**.

Galeotti v. International Union of Operating Engineers

Court: California Courts of Appeal
Docket: A157785(First Appellate District)
Opinion Date: May 6, 2020
Judge: Henry E. Needham, Jr.
Areas of Law: Criminal Law, Labor & Employment Law, White Collar Crime

Galeotti, a former Union Local 3 employee, filed a complaint against Local 3 and three of individual union leaders, alleging that the individual defendants required union employees to pay them money to keep their jobs, lied about the reason for collecting the money, and caused Local 3 to terminate Galeotti's employment when he failed to pay the full amount demanded. The trial court dismissed his second amended complaint without leave to amend. The court of appeal reversed in part, reasoning that a threat to terminate employment can provide a basis for an extortion claim and that the allegations of the second amended complaint stated a cause of action for wrongful termination in violation of the public policy underlying the extortion statutes. The complaint stated a cause of action for violations of the Racketeer Influenced and Corrupt Organizations Act (RICO; 18 U.S.C. 1961), based on the predicate acts of extortion, but did not state a cause of action for interference with prospective economic advantage.

Read Opinion Are you a lawyer? **Annotate this case**.

In re I.A.

Court: California Courts of Appeal
Docket: B296549(Second Appellate District)
Opinion Date: May 4, 2020
Judge: Tangeman
Areas of Law: Criminal Law, Juvenile Law

Where a juvenile court vacates its true finding on a generic murder allegation and redesignates it as a finding on an uncharged target offense, and does so before a minor has had the opportunity to contest the court's findings or orders, the minor may challenge the sufficiency of the evidence of the redesignated offense on appeal. The Court of Appeal held that there was insufficient evidence to support the juvenile court's decision sustaining the allegations that I.A. possessed a concealable firearm and committed vandalism. Therefore, the court reversed the juvenile court's findings, vacating the jurisdiction and disposition order and dismissing the Welfare and Institutions Code section 602 petition.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Edwards

Court: California Courts of Appeal
Docket: A158055(First Appellate District)
Opinion Date: May 1, 2020
Judge: Petrou
Areas of Law: Criminal Law

In 2006, Edwards fired an assault weapon into an apartment, killing the victim. Edwards pled guilty to possession of a firearm as a felon and was convicted of second-degree murder and shooting into an inhabited dwelling. Following the enactment of Senate Bill 1437, Edwards filed a Penal Code 1170.95 resentencing petition, checking form boxes indicating that he was convicted under a theory of felony murder or murder under the natural and probable consequences doctrine and that he could not now be convicted of 1st or 2nd-degree murder because of changes to Penal Code 188 and 189. Edwards submitted the jury instructions and the transcript of the prosecutor's closing remarks that Edwards acted with "both express malice, specific intent to kill, as well as implied malice," described as "an intentional act, the natural consequences of which are dangerous to human life, and at the time that the individual acted, they knew of the danger, and they deliberately acted with conscious disregard." The court denied the petition, finding that Edwards was convicted on a valid theory of murder that survived the statutory changes. The court of appeal affirmed. The superior court did not err in considering the record of conviction. Edwards could not meet the statutory prerequisites for even filing a section 1170.95 petition because he was not charged or convicted of second-degree felony murder or murder under the natural or probable consequences doctrine directed at accomplice liability.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Thomkins

Court: California Courts of Appeal
Docket: A141375(First Appellate District)
Opinion Date: May 1, 2020
Judge: Streeter
Areas of Law: Criminal Law

On Easter night in 2011, gunfire erupted at an Oakland bar-restaurant, leaving two people dead and five wounded. Thompkins and Fox were convicted of two counts of first-degree murder for the benefit of a criminal street gang, with firearm discharge enhancements, a multiple-murder special circumstance, and five counts of attempted murder with great bodily injury findings, gang enhancements, and firearm discharge enhancements. Thompkins was convicted as the shooter and Fox as an accomplice. Both were sentenced to life in prison without possibility of parole, plus 224 years to life. After Thompkins was sentenced, Fox stated under oath he was the actual shooter and Thompkins knew nothing about Fox's intentions. Thompkins claimed this new testimony, and his attorney's incompetent reaction entitled him to a new trial and submitted a declaration by another gang member who was present that night. The court of appeal concluded that Thompkins's attorney was not ineffective for failing to bring a motion to recall the sentence followed by a new trial motion because Thompkins failed to show prejudice. The attempted murder convictions and related enhancements must be reversed for both defendants based on the flawed kill zone instruction. Introducing evidence that defendants admitted their gang affiliation at jail intake violated the defendants' privilege against self-incrimination but was harmless. There was some evidentiary error that was harmless due to the wealth of admissible evidence establishing the gang enhancements. Arguments based on the statutory amendments to Penal Code 188 and 189 must be raised in the trial court (section 1170.95). The case must be remanded so the judge may exercise his discretion whether to impose or strike the firearm enhancements on under Penal Code 12022.53.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Torres

Court: California Courts of Appeal
Docket: B295043(Second Appellate District)
Opinion Date: May 4, 2020
Judge: Wiley
Areas of Law: Criminal Law

After the trial court admitted a witness's former testimony, the Court of Appeal applied People v. Roldan (2012) 205 Cal.App.4th 969, 975–985, and reversed. Roldan held that, before invoking the former testimony exception,

prosecutors should react appropriately to the impending deportation risk by following four steps: alert the defense to the risk; videotape the preliminary hearing testimony; use judicial measures to try to delay deportation; and consider an array of other specific measures. In this case, the prosecution conceded that prosecutors were simply unaware of Roldan and did not comply with it. The court held that Roldan controls the court's analysis because the facts about prosecutorial diligence are weaker here than they were in Roldan, where the appellate court held for the defense. In this case, the record before deportation is of prosecutorial inaction where the prosecution's brief in this court admits the investigating officer did not do anything to ensure that the witness would not be deported, nor is there other evidence of prosecutorial efforts to delay the witness's departure or to videotape his testimony at the preliminary hearing.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Triplett

Court: California Courts of Appeal
Docket: B298914(Second Appellate District)
Opinion Date: May 1, 2020
Judge: Frances Rothschild
Areas of Law: Criminal Law

Defendant was convicted of assault with a deadly weapon, carjacking, and attempted murder. In the published portion of the opinion, the Court of Appeal held that the trial court erred by denying defense counsel's request to inform the jurors that they could have testimony of certain witnesses read back to them. The court also held that, under the circumstances in this case, the error was harmless.

Read Opinion Are you a lawyer? **Annotate this case**.

Colorado In Interest of G.S.S.

Court: Colorado Supreme Court
Citation: 2020 CO 32
Opinion Date: May 4, 2020
Judge: Brian D. Boatright

Areas of Law: Constitutional Law, Criminal Law, Juvenile Law

After being charged, fourteen-year-old G.S.S. was detained for more than three months without bail, even though he had not entered a plea and had not been tried on the charges against him. At that point, G.S.S.'s counsel filed a motion to dismiss, arguing that G.S.S.'s "right to a speedy trial" had been violated under section 19-2-509(4)(b), C.R.S. (2019). The trial court agreed and dismissed the case against G.S.S. with prejudice, and the court of appeals affirmed in Colorado in Interest of G.S.S., 2019 COA 4M, __ P.3d __. The Colorado Supreme Court then granted certiorari to determine the proper remedy for a violation of the sixty-day limit in section 19-2-509(4)(b). The Supreme Court determined the remedy for a section 19-2-509(4)(b) violation was for the trial court to immediately hold a bail hearing and order the juvenile's release. Accordingly, the judgment of the court of appeals was reversed.

Read Opinion Are you a lawyer? **Annotate this case**.

Barringer v. Halkitis

Court: Florida Supreme Court
Docket: SC19-1071
Opinion Date: May 7, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court held that Jay Barringer's quo warranto petition filed in this case was a frivolous proceeding brought before the Supreme Court by a state prisoner and sanctioned Barringer by barring him from filing any further pro se requests for relief related to his criminal case. Barringer was convicted of one count of attempted sexual battery of a victim less than twelve years old and sentenced to twenty-five-years' imprisonment. In 2011, Barringer began filing petitions in the Supreme Court. The Court did not grant the relief sought in any of Barringer's filings. In the instant quo warranto petition Barringer challenged his conviction on the ground that the information was defective, a claim Barringer previously raised by way of a habeas petition. The Supreme Court denied the petition and found that Barringer abused the Court's limited judicial resources. The Court sanctioned Barringer by directing the Clerk of Court to reject any future

pleadings or other requests for relief submitted by Barringer that are related to his criminal case, unless such filings are signed by a member of The Florida Bar in good standing.

Read Opinion Are you a lawyer? **Annotate this case**.

Franqui v. State

Court: Florida Supreme Court
Docket: SC19-203
Opinion Date: May 7, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the order of the circuit court denying Appellant's claim of intellectual disability, raised in successive motions for postconviction relief under Fla. R. Crim. P. 3.851, holding that the circuit court did not err in denying relief. Appellant was convicted of first-degree murder and sentenced to death in two separate cases. After the United States Supreme Court decided Hall v. Florida, 572 U.S. 701 (2014), Appellant filed successive motions for postconviction relief in both of his capital cases, asserting that the circuit court's denials of his previous claims of intellectual disability were based on the court's improper interpretation of Florida's intellectual disability statute. The circuit court summarily denied the motions. The Supreme Court reversed and remanded for an evidentiary hearing on the issue of intellectual disability. After a hearing, the circuit court denied the claim. The Supreme Court affirmed, holding (1) the circuit court did not err in denying Appellant's intellectual disability claim; and (2) Appellant was not entitled to relief under Hurst v. Florida, 136 S. Ct. 616 (2016), or Hurst v. State, 202 So. 3d 40 (Fla. 2016).

Read Opinion Are you a lawyer? **Annotate this case**.

Hicks v. State

Court: Florida Supreme Court
Docket: SC19-1978
Opinion Date: May 7, 2020
Judge: Per Curiam

Areas of Law: Criminal Law

The Supreme Court denied the instant mandamus petition filed by Hicks and sanctioned Hicks by barring him from filing any further pro se requests for relief related to his criminal case. Hicks was convicted of one count of lewd and lascivious conduct by a person over eighteen years of age on a victim under sixteen years of age. Since 2016, Hicks filed thirteen pro se requests for relief in the Supreme Court related to his criminal case. The Court did not grant the relief sought in any of Hicks' filings. In the instant petition, Hicks sought a writ of mandamus compelling the circuit court to comply with the requirements of Fla. R. Crim. P. 3.850 by filing a copy of an order denying his second postconviction motion with the clerk of court. The Supreme Court dismissed the petition and found that Hicks abused this Court's limited judicial resources. The Court directed the Clerk of Court to reject any future pleadings or other requests for relief submitted by Hicks that are related to his criminal case, unless such filings are signed by a member of The Florida Bar in good standing.

Read Opinion Are you a lawyer? **Annotate this case**.

Burley v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0356
Opinion Date: May 4, 2020
Judge: Boggs
Areas of Law: Constitutional Law, Criminal Law

In 1992, Douglas Burley pled guilty to malice murder. He moved for an out-of-time appeal in 2019, claiming that his right to appeal was frustrated by his plea counsel's erroneous advice that he could not appeal his conviction because it was the product of a guilty plea. The trial court denied Burley's motion. After review, the Georgia Supreme Court vacated the trial court's judgment and remanded the case with direction to hold a hearing to determine whether ineffective assistance of counsel frustrated Burley's right to appeal.

Read Opinion Are you a lawyer? **Annotate this case**.

Carter v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0022
Opinion Date: May 4, 2020
Judge: David E. Nahmias
Areas of Law: Construction Law, Criminal Law

Brandon Carter was convicted by jury of malice murder and two firearm offenses in connection with the shooting death of Terrance Baker. On appeal, Carter contended the trial court erred by admitting certain hearsay statements into evidence and by violating his constitutional right to be present during his trial. Finding no reversible error, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Clarke v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0258
Opinion Date: May 4, 2020
Judge: Ellington
Areas of Law: Constitutional Law, Criminal Law

Rupert Clark was convicted by jury for the malice murder of his wife, Rosemarie Lebert-Clark. He was also convicted of possession of a firearm during the commission of a felony. On appeal, he argued he received ineffective assistance of trial counsel, and that the trial court erred in admitting certain evidence, violated the continuing witness rule by sending out with the deliberating jury printouts of text messages, and by failing to instruct the jury that a defendant's uncorroborated confession was not alone sufficient to warrant a conviction. Finding no reversible error after reviewing the trial court record, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Collins v. Georgia

Court: Supreme Court of Georgia

Docket: S20A0195
Opinion Date: May 4, 2020
Judge: Harold D. Melton
Areas of Law: Constitutional Law, Criminal Law

Renita Collins was tried for murder along with co-defendant Michael Stallworth. Collins appealed her convictions for murder and possession of a firearm while in commission of a felony in connection with the shooting death of Keith Jacobs. On appeal. Collins contended she was denied a fair trial due to juror misconduct, the trial court abused its discretion by not allowing her to subpoena juror testimony to show that misconduct had occurred, and the trial court abused its discretion when it failed to excuse a prospective juror for cause. Finding no reversible error, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Dawson v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0217
Opinion Date: May 4, 2020
Judge: Warren
Areas of Law: Constitutional Law, Criminal Law

Lavaris Dawson was convicted by jury of felony murder and other crimes in connection with the shooting death of Mamadou Camara. On appeal, Dawson challenged the sufficiency of the evidence supporting his convictions, and argued the trial court erred in admitting Dawson's statements to a detective during an interview because those statements were impermissibly induced by a hope of benefit, and that Dawson was denied his due process right to a timely appeal. After review, the Georgia Supreme Court disagreed and affirmed Dawson's convictions.

Read Opinion Are you a lawyer? **Annotate this case**.

Evans v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0007

Opinion Date: May 4, 2020
Judge: McMillan
Areas of Law: Constitutional Law, Criminal Law

Jimmy Evans was convicted by jury for murder and other crimes relating to the 2006 deaths of Tavoris Calhoun and Dezmon Thomas. On appeal, Evans argued that because he was visibly intoxicated at the time he made statements to law enforcement and consented to a search of his home and person, the statements and consent were involuntarily given and the trial court should have granted his motion for new trial on this ground. Furthermore, Evans argued that his trial counsel was ineffective for failing to file a motion to suppress at trial on the same basis. Because Evans failed to show error or ineffective assistance of counsel, the Georgia Supreme Court affirmed his conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Hill v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0285
Opinion Date: May 4, 2020
Judge: Harold D. Melton
Areas of Law: Constitutional Law, Criminal Law

Esco Hill was convicted by jury of malice murder and other crimes relating to the stabbing death of Alford Morris in 2014. On appeal, Hill argued the trial court committed reversible error by requiring him to be visibly shackled for the duration of his six-day trial. After review of the trial court record, the Georgia Supreme Court concurred this was reversible error, consequently, reversed judgment of conviction. Because the Court concluded the evidence at trial was sufficient to sustain Hill's conviction, the State could re-try him. The Court did not address Hill's remaining enumerations of error, "as they are not likely to recur in the event of a retrial."

Read Opinion Are you a lawyer? **Annotate this case**.

Oliver v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0489
Opinion Date: May 4, 2020
Judge: McMillan
Areas of Law: Constitutional Law, Criminal Law

Jacquan Oliver entered a negotiated plea of guilty to felony murder in connection with the shooting death of Alexander Mixon. He appealed his conviction and sentence, arguing that the trial court abused its discretion in finding a factual basis for his plea, and in determining the plea was voluntarily, knowingly and intelligently made. Finding no merit to these contentions, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Rosser v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0103
Opinion Date: May 4, 2020
Judge: Bethel
Areas of Law: Constitutional Law, Criminal Law

Larry Rosser was convicted by jury of malice murder and other crimes in connection with the death of Alexis Vereen. On appeal, Rosser challenged the sufficiency of the evidence presented against him at trial, and argued the trial court erred by not granting his motion for a mistrial, and by allowing the State to introduce a portion of Rosser's custodial statement to law enforcement. In addition, he argued he received constitutionally ineffective assistance of trial counsel. Finding no reversible error after reviewing the trial court record, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Spencer v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0871
Opinion Date: May 4, 2020
Judge: Keith R. Blackwell

Areas of Law: Constitutional Law, Criminal Law

Christopher Spencer was convicted by jury of murder and other crimes in connection with the fatal shootings of Sylvia Watson and Samuel White. Spencer appealed, claiming only that the evidence was insufficient to support his convictions. Finding no reversible error after reviewing the trial court record, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Styles v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0236
Opinion Date: May 4, 2020
Judge: Ellington
Areas of Law: Constitutional Law, Criminal Law

Derrick Styles was convicted by jury of felony murder and other crimes in connection with the shooting death of Alberto Lumens and the armed robbery fo Juan Lumens Garcia. On appeal, Styles contended the trial court erred in admitting into evidence a recording of an inculpatory telephone conversation between himself and a witness. He also argued his trial counsel was ineffective for failing to object to an allegedly improper comment by the prosecutor during closing argument. Finding no merit to these contentions, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Whitehead v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0171
Opinion Date: May 4, 2020
Judge: Ellington
Areas of Law: Constitutional Law, Criminal Law

Javis Whitehead was convicted by jury of murder and other crimes in connection with the shooting death of Dominique Larry. On appeal, Whitehead challenged the sufficiency of the evidence presented to rebut his

claim of self-defense and to convict him for murder beyond a reasonable doubt. He also argued the trial court erred in denying his motion to suppress his custodial statement, and in refusing to excuse for cause the District Attorney from the panel of prospective jurors prior to the conclusion of voir dire. Finding no merit to these contentions, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Idaho v. Blythe

Court: Idaho Supreme Court - Criminal
Docket: 46992
Opinion Date: May 4, 2020
Judge: Roger S. Burdick
Areas of Law: Constitutional Law, Criminal Law

Nicholas Blythe appealed after he was convicted of possessing a controlled substance. He conditionally pled guilty, reserving the right to challenge his sentence. On appeal, he argued the district court erred in denying his motion to suppress certain evidence found because the evidence presented at trial was found in violation of Blythe's Fourth Amendment rights. After review, the Idaho Supreme Court determined the search at issue took place before an arrest occurred, and because no rationale justifying a search incident to arrest was sufficiently present here, the search of Blythe's shoes was not a valid search incident to arrest. Therefore, the district court erred in holding that the search was reasonable under the Fourth Amendment. Blythe's conviction was vacated, the district court order denying Blythe's motion to suppress was reversed, and the matter remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

Idaho v. Glodowski

Court: Idaho Supreme Court - Criminal
Docket: 47131
Opinion Date: May 6, 2020
Judge: Roger S. Burdick

Areas of Law: Constitutional Law, Criminal Law

David Glodowski appealed after he was convicted for failing to update his sex-offender registration in violation of Idaho Code section 18-8309. He argued the district court erred by ruling that his prior conviction under a Wisconsin statute was "substantially equivalent" to Idaho statutes that required sex-offender registration in Idaho. After review, the Idaho Supreme Court determined the district court improperly allowed the State to seek a redetermination of the "substantially equivalent" element given that the Idaho Bureau of Criminal Identification made a final determination on that element. However, because the State put forth sufficient evidence to prove that element, and the district court's jury instruction accomplished the same purpose, the Supreme Court concluded the error was harmless. Accordingly, the Court found no reversible error in the district court's decision to grant the State's motion and provide the jury instruction. Therefore, judgment of conviction was affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Idaho v. Jones

Court: Idaho Supreme Court - Criminal
Docket: 45905
Opinion Date: May 4, 2020
Judge: Roger S. Burdick
Areas of Law: Constitutional Law, Criminal Law

Timothy Jones was convicted by jury of trafficking heroin and possession of drug paraphernalia. On appeal, he argued the trial court erred in admitting certain evidence regarding his probation status, a knife found in the initial police search of his person, and that the trial court abused its discretion in arriving at his sentence. Finding no reversible error, the Idaho Supreme Court affirmed Jones' conviction and sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Gordon

Court: Iowa Supreme Court

Docket: 18-1099
Opinion Date: May 1, 2020
Judge: Brent R. Appel
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction for assault on a peace officer with a dangerous weapon, a felony, and several misdemeanors, holding that Defendant did not receive ineffective assistance of counsel. After Defendant pleaded guilty, he absconded. He was later returned to custody. On appeal, Defendant argued that he received ineffective assistance of counsel because the plea bargain contained an unlawful term. Specifically, Defendant argued that the plea bargain's provision that he would be released from jail for a forty-eight-hour furlough after pleading guilty was illegal and that his trial counsel committed ineffective assistance in obtaining the illegal benefit for him. The Supreme Court affirmed, holding that where Defendant entered into the plea agreement with the illegally lenient sentence, he could not benefit from that sentence and then attack the plea bargain.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Craig

Court: Kansas Supreme Court
Docket: 119660
Opinion Date: May 1, 2020
Judge: Dan Biles
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's conviction and sentence for first-degree felony murder, holding that there was no error in the proceedings below. A jury found Defendant guilty of both first-degree felony murder and second-degree intentional murder. At sentencing, Defendant moved for a new trial and judgment notwithstanding the verdict, arguing that the jury must have had reasonable doubt on the first-degree felony murder theory because it convicted him of second-degree murder for the same killing. The district court dismissed the second-degree murder conviction and sentenced Defendant for the felony murder over his objection. The Supreme Court affirmed, holding (1) the district court did not err when it sentenced Defendant on felony murder instead of declaring a mistrial because

Defendant did not establish that the jury failed to find each element of the felony murder beyond a reasonable doubt or that the jury's first- and second-degree murder verdicts were so irreconcilable as to require a new trial; and (2) the district court did not err in declining to give an instruction on voluntary intoxication.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Lemmie

Court: Kansas Supreme Court
Docket: 119439
Opinion Date: May 1, 2020
Judge: Carol A. Beier
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's convictions of first-degree felony murder, aggravated robbery, conspiracy to commit aggravated robbery, criminal possession of a firearm, fleeing and eluding, and interference with law enforcement, holding that Defendant's arguments on appeal failed. Specifically, the Supreme Court held (1) any possible violation of Defendant's Fifth Amendment right in the admission of a witness's testimony about Defendant giving the witness phone passcodes was undoubtedly harmless; (2) the district court did not err by admitting hearsay statements as statements of a coconspirator and contemporaneous statements; (3) the State introduced sufficient evidence to convict Defendant of first-degree murder; and (4) the district judge did not abuse its discretion by admitting testimony that Defendant was upset over a meth pipe that went missing.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Mullen

Court: Maine Supreme Judicial Court
Citation: 2020 ME 56
Opinion Date: May 5, 2020
Judge: Connors
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed Defendant's conviction for reckless

conduct and aggravated criminal mischief, holding that the trial court did not abuse its discretion by offering Defendant a continuance of the trial in lieu of excluding his medical records. On appeal, Defendant argued that the trial court abused its discretion by denying his motion to suppress his personal medical records as a sanction for the State's late seizure of the records. The Supreme Judicial Court agreed that the State's conduct undermined the purpose of Maine Rule of Unified Criminal Procedure 18(b) but that the court's offer of a continuance in lieu of the exclusion of the evidence constituted an appropriate response to the State's conduct.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. Billingslea

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12715
Opinion Date: April 30, 2020
Judge: Cypher
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Judicial Court affirmed Defendant's convictions and the decision of the Appeals Court denying Defendant's motion to vacate the entry of his appeal from his convictions in that court and to have the case entered directly in the Supreme Judicial Court, holding that a direct appeal from the third conviction of a habitual offender pursuant to Mass. Gen. Laws ch. 279, 25(b) may be entered in the Appeals Court. Defendant was indicted for serious felonies arising from a brutal attack and rape. In addition to charging the specific felony, each indictment also alleged that the sentence for that felony should be enhanced pursuant to the habitual criminal provision Mass. Gen. Laws ch. 279, 25(a) or the habitual offender provision of section 25(b), or both. After he was convicted, Defendant moved to have the case entered directly in the Supreme Judicial Court. The Appeals Court denied the motion. The Supreme Judicial Court affirmed Defendant's convictions, holding (1) this direct appeal was entitled to the unique review prescribed by Mass Gen. Laws ch. 278, 33E, and the Appeals Court may conduct such section 33E review; (2) Defendant was not impermissibly allowed to waive his right to a jury trial on the sentencing enhancement provisions of the indictments; and (3) Defendant was not entitled to reversal of his convictions on any other ground.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. Martin

Court: Massachusetts Supreme Judicial Court
Docket: SJC-08768
Opinion Date: May 5, 2020
Judge: Ralph D. Gants
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Judicial Court affirmed Defendant's conviction of murder in the first degree and the denial of his motion for a new trial and declined to exercise its authority under Mass. Gen. Laws ch. 278E to reduce Defendant's conviction to murder in the second degree, holding that Defendant was not entitled to relief on any of his allegations of error. Defendant was convicted of murder in the first degree on the theory of felony-murder. Defendant filed a motion for a new trial, which was denied. The Supreme Judicial Court affirmed, holding (1) Defendant's motion for a new trial was correctly denied because Defendant was not prejudiced by counsel's ineffective assistance; (2) this Court declines to extend the reach of the Court's holding in Commonwealth v. Brown, 477 Mass. 805 (2017), to Defendant's case; and (3) trial judge erred when he declined Defendant's request that the jury be instructed on the elements of voluntary and involuntary manslaughter, but the error was not prejudicial in the context of the judge's other instructions.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. Tavares

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12631
Opinion Date: May 6, 2020
Judge: Lowy
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed Defendant's conviction of murder in the first degree on theories of deliberate premeditation and extreme atrocity

or cruelty and declined to exercise its power pursuant to Mass. Gen. Laws ch. 278, 33E to reduce the conviction to manslaughter, holding that there was no reversible error in the proceedings below. Specifically, the Supreme Judicial Court held (1) the trial judge did not err by denying Defendant's requests for a jury instruction pursuant to Commonwealth v. Croft, 345 Mass. 143 (1962); (2) the trial judge did not err by denying Defendant's motions for a required finding of not guilty under Croft because a rational jury could have found that Defendant was guilty of murder in the first degree on both the theories of premeditation and extreme atrocity or cruelty; and (3) there was no basis for reducing Defendant's sentence or ordering a new trial.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Branch

Court: Minnesota Supreme Court
Docket: A18-1055
Opinion Date: May 6, 2020
Judge: Lorie Skjerven Gildea
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's sentences for drive-by shooting at an occupied vehicle and second-degree assault, holding that Minn. Stat. 609.035 did not prohibit the sentences for both offenses when the crimes arose from a single behavioral incident. The district court sentenced Defendant to forty-eight months for drive-by shooting at an occupied vehicle and thirty-six months for second-degree assault and imposed the two sentences to run concurrently. The court of appeals affirmed. The Supreme Court affirmed, holding that, under this Court's analysis in State v. Ferguson, 808 N.W.2d 586 (Minn. 2012), the district court properly imposed multiple sentences in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

Galloway v. Mississippi

Court: Supreme Court of Mississippi
Citation: 2018-CA-01427-SCT

Opinion Date: May 7, 2020
Judge: Beam
Areas of Law: Constitutional Law, Criminal Law

Leslie Galloway appealed the denial of his 2015 petition for post-conviction relief (PCR) pertaining to his 2007 guilty plea to carjacking, a conviction that was used as an aggravating circumstance in Galloway's 2010 capital-murder trial at which Galloway received a death sentence. Galloway claimed in the petition that his defense counsel Wendy Martin had an actual conflict of interest because, before becoming his defense counsel, Martin had served as an assistant district attorney in the same case, unbeknownst to Galloway. The trial court ruled that Galloway's PCR claim was time barred under Mississippi's Uniform Post-Conviction Collateral Relief Act (UPCCRA), having been filed more than seven years after Galloway's conviction for carjacking. The trial court alternatively found no merit to Galloway's PCR claim, time bar notwithstanding. Accordingly, the trial court denied Galloway's PCR petition. The Mississippi Supreme Court agreed with the trial court that Galloway's PCR claim was time barred under the UPCCRA. The Court also agreed there was no merit to Galloway's PCR claim.

Read Opinion Are you a lawyer? **Annotate this case**.

City of Missoula v. Zerbst

Court: Montana Supreme Court
Citation: 2020 MT 108
Opinion Date: May 5, 2020
Judge: Beth Baker
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court reversed Defendant's conviction for sexual assault, holding that the municipal court erred when it instructed the jury on a definition of "consent" from the 2017 sexual assault statute and not the applicable 2015 statute, and the erroneous jury instruction prejudicially affected Defendant's substantial rights. At trial, the court instructed the jury, over Defendant's objection, on the definition of consent contained in recent amendments to the sexual assault statute. On appeal, Defendant argued that the municipal court failed to apply the correct law when instructing the jury on the elements of the claimed offense. The district court denied the

appeal. The Supreme Court reversed, holding (1) the instructions, as a whole, did not fully and fairly instruct the jury on the law applicable to the case; and (2) Defendant's substantial due process right was prejudiced by the erroneous jury instruction.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Degarmo

Court: Nebraska Supreme Court
Citation: 305 Neb. 680
Opinion Date: May 1, 2020
Judge: Stacy
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction of driving under the influence, holding that Defendant consented to a chemical test of his urine and, therefore, the results of the urine test were admissible. A law enforcement officer stopped Defendant for an expired registration. Based on his observations, the officer, a certified drug recognition evaluation expert, administered field sobriety tests. The officer concluded that Defendant was under the influence of marijuana arrested Defendant for driving under the influence and then took him to a detoxification center. Thereafter, a chemical test of Defendant's urine confirmed the presence of marijuana. On appeal, Defendant challenged the admission of the results of the urine test. The Supreme Court affirmed, holding that Defendant voluntarily consented to the warrantless search of his urine, and therefore, the search fell within a recognized exception to the warrant requirement.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Holz

Court: New York Court of Appeals
Citation: 2020 NY Slip Op 02682
Opinion Date: May 7, 2020
Judge: Fahey
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Court of Appeals held that N.Y. Crim. Proc. Law (CPL) 710.70(2) grants a defendant the right to review of a suppression decision when the order related exclusively to a count that was satisfied by a guilty plea but was not one to which the defendant pleaded guilty. Defendant was charged with two counts of burglary in the second degree. The first count related to a laptop computer, and the second count related to jewelry. Defendant moved to suppress the jewelry, but Supreme Court denied the motion. Defendant then pleaded guilty to one count of burglary in the second degree as charged in the count pertaining to the theft of the laptop computer, in satisfaction of the count charging the burglary of jewelry. On appeal, Defendant argued that Supreme Court erred in denying his motion to suppress the jewelry. The Appellate Division affirmed, concluding that it was jurisdictionally precluded from reviewing the suppression order. The Court of Appeals reversed, holding (1) Defendant's right to appellate review of Supreme Court's suppression order was secured by CPL 710.70(2); and (2) because the Appellate Division did not reach the underlying suppression question the case must be remitted to the Appellate Division for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Maffei

Court: New York Court of Appeals
Citation: 2020 NY Slip Op 02680
Opinion Date: May 7, 2020
Judge: DiFiore
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Court of Appeals affirmed the order of the Appellate Division concluding on direct appeal that Defendant was not entitled to relief on his ineffective assistance of counsel claim, holding that Defendant, on this record, did not sustain his burden to establish that counsel was constitutionally ineffective. After a jury trial, Defendant was convicted of second-degree murder. On appeal, Defendant argued that his trial counsel's failure to challenge a prospective juror constituted ineffective assistance of counsel. The Appellate Division affirmed. The Court of Appeals affirmed, holding (1) the record was inadequate to review Defendant's ineffective assistance of counsel claim; and (2) the appropriate procedure for the litigation of Defendant's challenge to his counsel's performance was a N.Y. Crim. Proc.

Law 440.10 motion.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Bailey

Court: North Carolina Supreme Court
Docket: 360A19
Opinion Date: May 1, 2020
Judge: Davis
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the decision of the court of appeals affirming the order of the trial court denying Defendant's motion to suppress evidence seized during the execution of a search warrant, holding that the warrant supported by probable cause. Defendant pled guilty to the offense of trafficking in cocaine while preserving his right to appeal the denial of his motion to suppress. On appeal, Defendant argued that the trial court erred in denying his motion to suppress because the facts contained in the affidavit were insufficient to establish probable cause to search his residence. The court of appeals affirmed. The Supreme Court affirmed, holding that the affidavit contained facts that were sufficient to provide a nexus between the residence and suspected criminal activity, and therefore, the warrant was supported by probable cause.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Ellis

Court: North Carolina Supreme Court
Docket: 340A19
Opinion Date: May 1, 2020
Judge: Robin E. Hudson
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court reversed the decision of the Court of Appeals affirming the trial court's denial of Defendant's motion to suppress evidence, holding that there was no reasonable suspicion to justify the law enforcement officer's stop when Defendant signaled with his middle finger from the passenger side window of a moving vehicle. While assisting a stranded

motorist, the officer turned his attention to another car traveling on the roadway, a white SUV. Defendant had his arm outside the passenger window and gestured with his middle finger, making an up-and-down motion. Believing that Defendant was committing the crime of disorderly conduct, the officer pursued and then stopped the SUV. At trial, Defendant moved to suppress the officer's testimony, arguing that there was no reasonable suspicion to justify the stop. The trial court denied the motion. Defendant pleaded guilty to resisting, delaying, or obstructing a public officer. The court of appeals affirmed the trial court's denial of Defendant's motion to suppress. The Supreme Court reversed, holding that the specific, articulable facts did not establish reasonable suspicion of the crime of disorderly conduct.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Hobbs
Court: North Carolina Supreme Court
Docket: 263PA18
Opinion Date: May 1, 2020
Judge: Earls
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court reversed Defendant's conviction, holding that the trial court clearly erred in ruling that Defendant failed to prove purposeful discrimination with respect to the State's use of peremptory challenges to strike three jurors without considering all of the evidence presented by Defendant. Defendant was found guilty of one count of first-degree murder and other crimes. On appeal, Defendant argued that the trial court erred by failing to grant three objections that he made under Batson v. Kentucky, 476 U.S. 79 (1986). The court of appeals affirmed Defendant's convictions. The Supreme Court reversed, holding (1) the court of appeals erred in its analysis of Defendant's Batson claims with respect to the three jurors; and (2) as to all three jurors, remand was required for reconsideration of whether Defendant proved purposeful discrimination in each case.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Mylett

Court: North Carolina Supreme Court
Docket: 6A19
Opinion Date: May 1, 2020
Judge: Earls
Areas of Law: Criminal Law

The Supreme Court reversed the decision of the court of appeals affirming the trial court's judgment convicting Defendant for conspiracy to commit harassment of a juror, holding that the trial court erred in denying Defendant's motion to dismiss the conspiracy charge for insufficient evidence. Defendant was convicted of conspiracy to commit harassment of a juror because of his actions at a courthouse following his twin brother's conviction for assault on a government official. On appeal, the court of appeals concluded that the trial court did not err in denying Defendant's motion to dismiss the conspiracy charge for insufficient evidence. The Supreme Court reversed, holding that the evidence in Defendant's trial was insufficient to raise anything more than mere conjecture that he had made an agreement with another person to threaten or intimidate a juror.

Read Opinion Are you a lawyer? **Annotate this case**.

Dodge v. North Dakota

Court: North Dakota Supreme Court
Citation: 2020 ND 100
Opinion Date: May 7, 2020
Judge: Gerald W. VandeWalle
Areas of Law: Constitutional Law, Criminal Law

Richard Dodge appealed from a district court order denying his application for post-conviction relief. Dodge was charged with five felonies and a misdemeanor in December 2015. Dodge was appointed counsel. In April 2016, Dodge's counsel moved the court to withdraw because the attorney-client relationship was "irreparably broken and rendered unreasonably difficult." The court granted the motion, and Dodge was appointed substitute counsel in May 2016. In July 2016, Dodge himself filed a "motion to dismiss counsel." The court denied Dodge's motion. Five months after the deadline for motions and plea agreements, Dodge's counsel sought to have Dodge submit to a psychiatric examination. This request was denied, the trial court

found no evidence, and the the court itself made no observations, that Dodge was incompetent to stand trial. After this denial, Dodge himself again moved to dismiss his trial counsel, and due to the allegations Dodge made in his motion, counsel moved to withdraw. The trial court denied both motions, and instead, required the attorney to appear as standby counsel and assist Dodge during trial if requested, but relieved him of any further obligations to consult with Dodge. The case proceeded to trial. At the beginning of trial, the court gave Dodge the option of representing himself or having his attorney represent him. Dodge chose to have his attorney represent him. Because his attorney had not prepared for trial and had no communication with Dodge since he moved to withdraw, Dodge's attorney asked for a brief recess to consult with Dodge. During the recess, a settlement was reached. Dodge agreed to enter Alford pleas on all counts, waived a presentence investigation, and agreed to be sentenced immediately after entering his pleas. Dodge was immediately sentenced following his guilty pleas, and thereafter sought post-conviction relief on grounds he was not competent to enter his pleas, and that he received ineffective assistance of trial counsel. After review, the North Dakota Supreme Court concluded the district court's finding that Dodge was competent when he entered his pleas was not clearly erroneous, and disposed of his claim of ineffective assistance of counsel.

Read Opinion Are you a lawyer? **Annotate this case**.

Hewitt v. NDDOT

Court: North Dakota Supreme Court
Citation: 2020 ND 102
Opinion Date: May 7, 2020
Judge: Lisa K. Fair McEvers
Areas of Law: Criminal Law, Government & Administrative Law

Larry Hewitt appealed a district court judgment affirming the North Dakota Department of Transportation's revocation of his driving privileges. Hewitt claimed the Department's hearing file was improperly admitted at the administrative hearing. After review, the North Dakota Supreme Court affirmed, concluding the hearing file was properly admitted as a self-authenticating copy of an official record.

Read Opinion Are you a lawyer? **Annotate this case**.

Kastet v. NDDOT

Court: North Dakota Supreme Court
Citation: 2020 ND 91
Opinion Date: May 7, 2020
Judge: Daniel J. Crothers
Areas of Law: Criminal Law, Government & Administrative Law

The North Dakota Department of Transportation (Department) appealed the district court's reversing a hearing officer's decision suspending Holden Kastet's driving privileges for 365 days. The Department argued the hearing officer did not abuse his discretion in admitting the chemical breath test, and State Highway Patrol Trooper King scrupulously complied with the approved method for testing Kastet's breath on the Intoxilyzer 8000. After review, the North Dakota Supreme Court concurred with the Department and reversed the district court judgment. The matter was remanded with instructions to reinstate the hearing officer's decision.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Dahl

Court: North Dakota Supreme Court
Citation: 2020 ND 87
Opinion Date: May 7, 2020
Judge: Jerod E. Tufte
Areas of Law: Constitutional Law, Criminal Law

The State of North Dakota appealed a district court order denying its motion to resume prosecution against Matthew Dahl and dismissing the case. In December 2014, the State charged Dahl with two counts of theft. Dahl did not appear on the charges until he was arrested on a bench warrant in February 2017. In mid-April 2017, the State mailed Dahl a pretrial diversion agreement. Dahl signed and returned the notarized agreement dated May 3, 2017. On May 9, 2017, the state's attorney signed and filed the agreement with the district court, and the court approved the agreement the same day. Under the agreement, the State agreed to suspend prosecution for "two

years from the date of execution" conditioned on Dahl's timely payment of restitution. Dahl failed to make minimum monthly restitution payments. On June 6, 2019, the State moved to resume prosecution, alleging Dahl violated the pretrial diversion agreement by his non-payment. The district court held a hearing on the State's motion in August 2019. The court concluded the pretrial agreement was executed when Dahl signed it on May 3, 2017. The court then denied the State's motion to resume prosecution as untimely under N.D.R.Crim.P. 32.2(d)(2), and dismissed the complaint against Dahl. After review, the North Dakota Supreme Court reversed, concluding the district court erred in determining the State's motion was untimely, and remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Foster

Court: North Dakota Supreme Court
Citation: 2020 ND 85
Opinion Date: May 7, 2020
Judge: Jon J. Jensen
Areas of Law: Constitutional Law, Criminal Law

Akeem Foster was convicted by jury of Terrorizing and Carrying a Concealed Weapon. Foster contended on appeal he was denied a fair trial because he was asked during cross-examination if other witnesses were lying and because the prosecutor expressed personal beliefs about the evidence during closing arguments. Foster also argued there was insufficient evidence to convict him of either charge. After review, the North Dakota Supreme Court affirmed Foster's conviction for Carrying a Concealed Weapon, but reversed his conviction for Terrorizing. The Court found Foster was improperly asked to provide an opinion on the veracity and credibility of the State's witnesses. The improper questioning was prejudicial and denied Foster a fair trial on the terrorizing charge.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Kolstad

Court: North Dakota Supreme Court

Citation: 2020 ND 97
Opinion Date: May 7, 2020
Judge: Gerald W. VandeWalle
Areas of Law: Constitutional Law, Criminal Law

In December 2018, Officer Nelson of the University of North Dakota Police Department conducted a traffic stop of Stanley Kolstad for suspicion of driving under the influence. Kolstad performed field sobriety tests and a preliminary breath test (PBT). Prior to performing the PBT, Kolstad informed Nelson that he had asthma. Nelson testified he was unable to obtain a PBT result because Kolstad was filling his cheeks with air while performing the test. Kolstad was arrested for DUI and refusing to submit to a chemical test. Kolstad was transported to the UND police station to be given an Intoxilyzer breath test. Prior to the Intoxilyzer test, Nelson read Kolstad the implied consent advisory. But, because Nelson was not a certified operator of the Intoxilyzer machine, Officer Waltz conducted the test. Prior to the test, Kolstad informed Waltz he had asthma. The Intoxilyzer test results were deficient. Waltz testified Kolstad was not providing enough air for the test machine to provide a valid result. Kolstad was charged with driving under the influence and refusing to submit to a chemical test. Kolstad's counsel made a discovery request to the State seeking copies of any audio or video recordings taken by police officers. Kolstad's counsel also requested the State inform him whether any sound or video recordings taken of Kolstad were subsequently "altered, edited, destroyed, or discarded." The State provided Kolstad's counsel with dash camera footage from Nelson's police car that had been taken at the scene of the arrest, but the State did not provide any body camera footage from either Nelson or Waltz. Upon learning that Waltz's body camera footage was successfully uploaded to UND servers, Kolstad's counsel moved to dismiss the case because the State did not provide any body camera footage in discovery as requested. The district court ultimately dismissed the refusal to submit to a chemical breath test charge as a sanction for failing to provide the body camera footage. The State appealed, arguing the alleged discovery violation did not rise to a constitutional violation of Kolstad's due process rights, and the district court abused its discretion in dismissing the refusal charge. Kolstad argued the district court's order dismissing the refusal charge was not appealable, and if it was, the court did not abuse its discretion in dismissing the charge. The North Dakota Supreme Court concluded there was nothing in the record to indicate the district court adequately considered an

alternative or less severe sanction to dismissal, and by not considering a less severe sanction, the trial court erred. The district court's order dismissing the refusal charge was reversed, and the matter remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Michel

Court: North Dakota Supreme Court
Citation: 2020 ND 101
Opinion Date: May 7, 2020
Judge: Jerod E. Tufte
Areas of Law: Constitutional Law, Criminal Law

Kevin Michel was convicted by jury of knowingly receiving stolen property. Jamestown Police began investigating theft of tires from Northwest Tire in October 2017. About ten months later, Thomas Melland and Andrew Heckelsmiller became suspects in the investigation. Heckelsmiller told police he had sold stolen tires to Michel. In August 2018, Detective LeRoy Gross spoke with Michel about the stolen tires. Michel acknowledged he had bought tires from Heckelsmiller and Melland. Michel also told Detective Gross he stopped buying tires from Heckelsmiller and Melland after seeing a Facebook post from Northwest Tire offering a $500 reward for information regarding stolen tires. Detective Gross told Michel, "There's going to be a lot of restitution these two boys are going to have to come up with unless we can get some tires back." Michel said he had sold several of the tires but still had some of them. Michel turned over seven new tires to Detective Gross. Representatives from Northwest Tire and J&L Service identified the tires as some of those stolen from their shops. During the jury's deliberations, the jury submitted a note with written questions to the court. Michel argued on appeal the district court erred by not specifically answering the jury's questions and instead referring them to the existing jury instructions. After review, the North Dakota Supreme Court affirmed the criminal judgment, except as to the award of restitution. The award was reversed because the district court awarded more than what was required to make the victims whole. The matter was remanded for a redetermination of restitution.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Wayland

Court: North Dakota Supreme Court
Citation: 2020 ND 106
Opinion Date: May 7, 2020
Judge: Jon J. Jensen
Areas of Law: Constitutional Law, Criminal Law

Joey Wayland appealed after he was convicted by jury of Theft of Property and Possession of Drug Paraphernalia. Wayland contended his case should have been dismissed because his right to a speedy trial was violated by a continuance of his trial from March 11, 2019 to April 8, 2019. Wayland also contended the district court violated his right to remain silent by ordering him to submit to a mental health evaluation. Finding no reversible error, the North Dakota Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Schwindt v. Sorel

Court: North Dakota Supreme Court
Citation: 2020 ND 92
Opinion Date: May 7, 2020
Judge: Lisa K. Fair McEvers
Areas of Law: Constitutional Law, Criminal Law, Government & Administrative Law

Gregory Schwindt appealed a district court judgment affirming a Department of Transportation hearing officer's revocation of his driving privileges for 180 days. Schwindt argued North Dakota's implied consent and refusal laws were unconstitutional, the hearing officer erred by considering the results of the horizontal gaze nystagmus (HGN) test, and the hearing officer erred in finding he refused to take a chemical test. After review, the North Dakota Supreme Court concluded the hearing officer's findings of fact were supported by a preponderance of the evidence, the conclusions of law were sustained by the findings of fact, and the decision to revoke Schwindt's driving privileges was in accordance with the law.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. McDougald v. Greene

Court: Supreme Court of Ohio
Citation: 2020-Ohio-2782
Opinion Date: May 6, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court denied a writ of mandamus sought by Relator to compel Respondent, the public-records custodian at the Southern Ohio Correctional Facility (SOCF), to provide Relator with three public records and to pay Relator statutory damages and court costs associated with this litigation, holding that Relator was not entitled to either a writ of mandamus nor statutory damages. When Relator was an inmate at SOCF he submitted a public-records request to Respondent seeking three documents. Respondent provided one of the three documents. Relator then filed a complaint for a writ of mandamus seeking an order compelling Respondent to provide the two documents and to pay statutory damages and court costs associated with this litigation. The Supreme Court denied the writ of mandamus on the merits, holding that Respondent's response to Relator fully satisfied Respondent's obligations under Ohio Rev. Code 149.43, and therefore, Relator was not entitled a writ of mandamus, and there was no basis to award statutory damages.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Parker Bey v. Byrd

Court: Supreme Court of Ohio
Citation: 2020-Ohio-2766
Opinion Date: May 5, 2020
Judge: Maureen O'Connor
Areas of Law: Criminal Law

The Supreme Court affirmed in part and reversed in part the judgment of the court of appeals denying Appellant's complaint for a writ of mandamus to compel the Cuyahoga County Clerk of Courts to produce various court records and denying the clerk's request that Appellant be declared a vexatious litigator, holding that the court of appeals erred in denying Appellant's complaint on the grounds that he did not invoke the Rules of

Superintendence as the basis for his request. Appellant sought copies of journal entries from his criminal case and a copy of the clerk of courts' records-retention schedule. The clerk largely denied the request. Appellant then filed a complaint for a writ of mandamus. The court of appeals denied Appellant's request for mandamus relief, concluding that the clerk had no clear legal duty to provide the requested records. The Supreme Court reversed, holding (1) this action to compel the production of journal entries from a 1995 case was properly brought under the Public Records Act; and (2) this Court declines to impose sanctions on Appellant or to declare him a vexatious litigator.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Dangler

Court: Supreme Court of Ohio
Citation: 2020-Ohio-2765
Opinion Date: May 5, 2020
Judge: DeWine
Areas of Law: Criminal Law

The Supreme Court reversed the judgment of the court of appeals vacating Defendant's conviction and sentence and reinstated the trial court's acceptance of Defendant's plea of no contest to sexual battery, holding that the trial court did not completely fail to comply with Crim.R.11(C)(2)(a), and there was nothing in the record to support a conclusion that Defendant would not have entered his plea had the trial court been more detailed in its explanation. On appeal, Defendant sought to vacate his plea of no contest, arguing that his plea was invalid because the trial court erred by not explaining more fully the obligations and restrictions that went with his status as a sex offender, in violation of Crim. R. 11(C)(2)(a). The court of appeals vacated the conviction without requiring Defendant to show prejudice, concluding that the trial court had completely failed to comply with Crim. R. 11(C)(2)(a). The Supreme Court reversed, holding (1) the trial court did not completely failed to comply with Crim R. 11(C)(2)(a)'s maximum-penalty-advisement requirement; and (2) because Defendant did not establish prejudice, he was not entitled to have his no-contest plea vacated for a failure to comply with Crim.R. 11(C).

Read Opinion Are you a lawyer? **Annotate this case**.

Oregon v. Haji

Court: Oregon Supreme Court
Docket: S066254
Opinion Date: May 7, 2020
Judge: Nakamoto
Areas of Law: Constitutional Law, Criminal Law

After a grand jury issued an indictment charging defendant Hanad Ali Haji with multiple offenses, the district attorney determined that the indictment could be challenged by demurrer because the basis for joining those offenses was not expressly alleged. Instead of seeking another indictment from the grand jury, the district attorney obtained leave from the trial court to amend the indictment by adding allegations specifying the statutory basis for joinder, without adding factual allegations about the crimes. Defendant was convicted on some of the charges at trial, and the Court of Appeals affirmed. The issue this case presented for the Oregon Supreme Court's review centered on whether the district attorney could add allegations specifying the statutory basis for joinder of multiple offenses to an indictment instead of resubmitting the case to the grand jury. The Supreme Court determined that neither the statute permitting joinder of multiple offenses in a single indictment nor Article VII (Amended), section 5(6), of the Oregon Constitution precluded a district attorney, with approval of the trial court, from amending an indictment to add allegations specifying the statutory basis for joinder of multiple offenses. The Supreme Court affirmed the decision of the Court of Appeals, based in part on different reasoning, and affirmed the judgment of the circuit court.

Read Opinion Are you a lawyer? **Annotate this case**.

South Carolina v. Durant

Court: South Carolina Supreme Court
Docket: 27964
Opinion Date: May 6, 2020
Judge: Kaye Gorenflo Hearn
Areas of Law: Constitutional Law, Criminal Law

Appellant Larry Durant was convicted of second-degree criminal sexual conduct (CSC) for sexually abusing a teenage girl in his church office where he served as the pastor. Durant contended the trial court improperly permitted the State to introduce evidence of prior sexual abuse allegations as evidence of a common scheme or plan under Rule 404(b), SCRE, and that the State committed a "Brady" violation by failing to accurately disclose the criminal history of its witness. After review, the South Carolina Supreme Court affirmed the admissibility of the girls' testimony. "[W]hile the State failed to disclose the criminal background information of its witness, we find this information was not material." The Court found Durant exercised his position of trust, authority, and spiritual leadership to hold private prayer meetings with teen girls who had grown up in his church. He told them he was praying for their health and good fortune, and represented that part of this process was touching them sexually and having intercourse. Durant then warned the girls of misfortune if they refused or told anyone. Moreover, he used scripture as a means of grooming the children into performing sex acts. "These facts demonstrate the requisite logical connection between the prior acts of sexual abuse and the one forming the basis of the crime charged." The Court therefore affirmed Durant's conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

South Carolina v. Perry

Court: South Carolina Supreme Court
Docket: 27963
Opinion Date: May 6, 2020
Judge: Few
Areas of Law: Constitutional Law, Criminal Law

Petitioner Wallace Perry was convicted on two counts of criminal sexual conduct (CSC) with a minor in the first degree and two counts of CSC with a minor in the second degree for sexually assaulting two of his biological daughters. Prior to Perry's trial, the State made a motion to admit the testimony of Perry's stepdaughter from an earlier marriage that Perry sexually assaulted her twenty-two to twenty-seven years earlier. The State argued the trial court should not exclude the stepdaughter's testimony under Rule 404(b) of the South Carolina Rules of Evidence because it fit the

"common scheme or plan" exception. Perry objected to this testimony. The trial court initially reserved ruling on the issue, but later indicated it was inclined to allow the stepdaughter to testify. The jury convicted Perry on all counts, and the trial court sentenced him to thirty years in prison. The court of appeals affirmed. The South Carolina Supreme Court determined it was not enough to meet the "logical connection" standard for admission of other crimes under the common scheme or plan exception to Rule 404(b) that the defendant previously committed the same crime. "When evidence of other crimes is admitted based solely on the similarity of a previous crime, the evidence serves only the purpose prohibited by Rule 404(b), and allows the jury to convict the defendant on the improper inference of propensity that because he did it before, he must have done it again. ...The common scheme or plan exception demands more." The Supreme Court held State must show a logical connection between the other crime and the crime charged such that the evidence of other crimes "reasonably tends to prove a material fact in issue." The State must also convince the trial court that the probative force of the evidence when used for this legitimate purpose is not substantially outweighed by the danger of unfair prejudice from the inherent tendency of the evidence to show the defendant's propensity to commit similar crimes. In this case, the State did not meet its burden. Conviction was reversed and the matter remanded for a new trial.

Read Opinion Are you a lawyer? **Annotate this case**.

South Carolina v. Quinn

Court: South Carolina Supreme Court
Docket: 27966
Opinion Date: May 6, 2020
Judge: Kaye Gorenflo Hearn
Areas of Law: Constitutional Law, Criminal Law, White Collar Crime

Respondent Rick Quinn, Jr. was a former member of the South Carolina House of Representatives, representing constituents in Richland and Lexington counties from 1989-2004 and 2010-2017 and serving as House Majority Leader from 1999- 2004. He owned and operated a mail business called Mail Marketing Strategies (MMS) in Columbia, while his father owned and operated a political consulting firm, Richard Quinn & Associates (RQ&A). In 2014, Attorney General Alan Wilson designated First Circuit

Solicitor David Pascoe as special prosecutor to conduct a State grand jury investigation into alleged public corruption committed by current and former members of the South Carolina General Assembly. This case arose from a prior state grand jury investigation of former House Speaker Bobby Harrell, which resulted in six counts of misusing campaign funds, to which he pleaded guilty. During the course of the investigation into Speaker Harrell, SLED uncovered potentially criminal conduct by Representative Jimmy Merrill and Representative Rick Quinn, and a second grand jury investigation was initiated to investigate the conduct of these individuals. The investigation focused on Quinn's practice of using his office as House Majority Leader and leader of the House Republican Caucus to direct mailing and political services to his family's businesses. Quinn only admitted to a limited set of facts supporting the indictment. Believing the plea lacked a sufficient basis, the State moved to vacate Quinn's guilty plea, reconsider the sentence, and for the trial court's recusal. The State appealed the order denying its motions. After review, the South Carolina Supreme Court determined that the State could not appeal the guilty plea, the trial court did not abuse its discretion in sentencing, and there was no evidence of judicial bias or prejudice requiring the court to recuse itself. Therefore, the Court dismissed the State's appeal of the guilty plea, and affirmed as to all other issues.

Read Opinion Are you a lawyer? **Annotate this case**.

Texas v. Arellano

Court: Texas Court of Criminal Appeals
Docket: PD-0287-19
Opinion Date: May 6, 2020
Judge: Slaughter
Areas of Law: Constitutional Law, Criminal Law

After Appellee Cesar Ramiro Arellano was arrested for driving while intoxicated, the arresting officer, Phillip Garcia, prepared a probable cause affidavit to support a search warrant for a blood draw. Officer Garcia submitted his sworn affidavit to the on-duty magistrate. Using a cursive signature, the magistrate signed the blank signature line of a form search warrant authorizing the search and seizure of Appellee's blood. Below the signature line appeared the words, "Magistrate, Victoria County, Texas."

Aside from the cursive signature, the magistrate's name was not typed or handwritten anywhere on the warrant. Upon execution of the search warrant, Appellee was charged with DWI. In the trial court, Appellee filed a motion to suppress all evidence stemming from the blood draw. At the pretrial suppression hearing, Appellee argued that the search warrant to obtain the blood specimen was facially invalid because the magistrate's signature was illegible in violation of the requirements of Code of Criminal Procedure Article 18.04(5). The trial court agreed, the court of appeals concurred, and the evidence was suppressed because of the illegible signature. The Texas Court of Criminal Appeals disagreed with both lower courts, finding the court of appeals erred in holding that reliance on the statutory good-faith exception was automatically precluded based on an illegible magistrate's signature in violation of Code of Criminal Procedure Article 18.04(5). Because the remaining issues in the case were not properly addressed by the court of appeals, judgment was vacated and the matter remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

About Justia Opinion Summaries

Justia Weekly Opinion Summaries is a free service, with 63 different newsletters, each covering a different practice area.

Justia also provides 68 daily jurisdictional newsletters, covering every federal appellate court and the highest courts of all US states.

All daily and weekly Justia newsletters are free. Subscribe or modify your newsletter subscription preferences at daily.justia.com.

You may freely redistribute this email in whole.

About Justia

Justia is an online platform that provides the community with open access to the law, legal information, and lawyers.



Unsubscribe From This Newsletter

or unsubscribe from all Justia newsletters immediately **here.**



Justia | 1380 Pear Ave #2B, Mountain View, CA 94043

From: Criminal Law - Justia Weekly Opinion Summaries
To: Tyson, Christine E (POL)
Subject: Latest 111 Cases This Week: Kelly v. United States (U.S.), Gomes v. Silva (1st Cir.), United States v. Perez-Couvertier (1st Cir.)
Date: Friday, May 8, 2020 9:06:17 AM

If you are unable to see this message, click here to view it in a web browser.

Justia Weekly Opinion Summaries

Criminal Law
May 8, 2020

Table of Contents

Kelly v. United States
Criminal Law, Government & Administrative Law, White Collar Crime
US Supreme Court

Gomes v. Silva
Civil Rights, Constitutional Law, Criminal Law

US Court of Appeals for the First Circuit

United States v. Perez-Couvertier
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the First Circuit

United States v. Haverkamp
Criminal Law
US Court of Appeals for the Second Circuit

United States v. Mladen
Criminal Law, Trusts & Estates
US Court of Appeals for the Second Circuit

United States v. Richardson
Criminal Law
US Court of Appeals for the Second Circuit

United States v. Rosemond
Criminal Law
US Court of Appeals for the Second Circuit

United States v. Lacerda
Criminal Law, White Collar Crime
US Court of Appeals for the Third Circuit

Cucalon v. Barr
Criminal Law, Immigration Law
US Court of Appeals for the Fourth Circuit

United States v. Doctor
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Lewis
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Jordan
Criminal Law
US Court of Appeals for the Fifth Circuit

United States v. Longoria
Criminal Law
US Court of Appeals for the Fifth Circuit

United States v. McNabb
Criminal Law
US Court of Appeals for the Fifth Circuit

Andrews v. Wayne County
Civil Rights, Constitutional Law, Criminal Law

US Court of Appeals for the Sixth Circuit

Hicks v. Scott
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Sixth Circuit

Moody v. United States
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Sixth Circuit

United States v. Foreman
Criminal Law
US Court of Appeals for the Sixth Circuit

United States v. Smith
Criminal Law
US Court of Appeals for the Sixth Circuit

Kirkman v. Thompson
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

Tuduj v. Newbold
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

United States v. Gibson
Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

United States v. Howell
Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

United States v. Lewis
Criminal Law
US Court of Appeals for the Seventh Circuit

Bakor v. Barr
Criminal Law, Immigration Law
US Court of Appeals for the Eighth Circuit

Smith v. Titus
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Becerra
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Haynes
Criminal Law

US Court of Appeals for the Eighth Circuit

United States v. Roberts
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Wright
Criminal Law
US Court of Appeals for the Eighth Circuit

Benson v. Chappell
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Ninth Circuit

Mero v. Barr
Criminal Law, Immigration Law
US Court of Appeals for the Ninth Circuit

Romero-Millan v. Barr
Criminal Law
US Court of Appeals for the Ninth Circuit

United States v. Yang
Criminal Law
US Court of Appeals for the Ninth Circuit

United States v. Neugin
Constitutional Law, Criminal Law
US Court of Appeals for the Tenth Circuit

United States v. Ramon
Constitutional Law, Criminal Law
US Court of Appeals for the Tenth Circuit

United States v. Richards
Constitutional Law, Criminal Law
US Court of Appeals for the Tenth Circuit

Andrews v. Warden
Criminal Law
US Court of Appeals for the Eleventh Circuit

Hollis v. United States
Criminal Law
US Court of Appeals for the Eleventh Circuit

Knight v. Florida Department of Corrections
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Eleventh Circuit

United States v. Evans
Criminal Law

US Court of Appeals for the Eleventh Circuit

United States v. McLellan
Criminal Law
US Court of Appeals for the Eleventh Circuit

United States v. Russell
Criminal Law
US Court of Appeals for the Eleventh Circuit

Welch v. United States
Criminal Law
US Court of Appeals for the Eleventh Circuit

State v. Trujillo
Constitutional Law, Criminal Law
Arizona Supreme Court

Barnett v. State
Criminal Law
Arkansas Supreme Court

Mason v. Kelley
Criminal Law
Arkansas Supreme Court

Ray v. Kelley
Criminal Law
Arkansas Supreme Court

Walker v. Kelley
Criminal Law
Arkansas Supreme Court

People v. Flores
Civil Rights, Constitutional Law, Criminal Law
Supreme Court of California

California v. Law
Constitutional Law, Criminal Law
California Courts of Appeal

California v. Sanchez
Constitutional Law, Criminal Law
California Courts of Appeal

Galeotti v. International Union of Operating Engineers
Criminal Law, Labor & Employment Law, White Collar Crime
California Courts of Appeal

In re I.A.
Criminal Law, Juvenile Law

California Courts of Appeal

People v. Edwards
Criminal Law
California Courts of Appeal

People v. Thomkins
Criminal Law
California Courts of Appeal

People v. Torres
Criminal Law
California Courts of Appeal

People v. Triplett
Criminal Law
California Courts of Appeal

Colorado In Interest of G.S.S.
Constitutional Law, Criminal Law, Juvenile Law
Colorado Supreme Court

Barringer v. Halkitis
Criminal Law
Florida Supreme Court

Franqui v. State
Criminal Law
Florida Supreme Court

Hicks v. State
Criminal Law
Florida Supreme Court

Burley v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Carter v. Georgia
Construction Law, Criminal Law
Supreme Court of Georgia

Clarke v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Collins v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Dawson v. Georgia
Constitutional Law, Criminal Law

Supreme Court of Georgia

Evans v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Hill v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Oliver v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Rosser v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Spencer v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Styles v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Whitehead v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Idaho v. Blythe
Constitutional Law, Criminal Law
Idaho Supreme Court - Criminal

Idaho v. Glodowski
Constitutional Law, Criminal Law
Idaho Supreme Court - Criminal

Idaho v. Jones
Constitutional Law, Criminal Law
Idaho Supreme Court - Criminal

State v. Gordon
Civil Rights, Constitutional Law, Criminal Law
Iowa Supreme Court

State v. Craig
Criminal Law
Kansas Supreme Court

State v. Lemmie
Criminal Law

Kansas Supreme Court

State v. Mullen
Criminal Law
Maine Supreme Judicial Court

Commonwealth v. Billingslea
Civil Rights, Constitutional Law, Criminal Law
Massachusetts Supreme Judicial Court

Commonwealth v. Martin
Civil Rights, Constitutional Law, Criminal Law
Massachusetts Supreme Judicial Court

Commonwealth v. Tavares
Criminal Law
Massachusetts Supreme Judicial Court

State v. Branch
Criminal Law
Minnesota Supreme Court

Galloway v. Mississippi
Constitutional Law, Criminal Law
Supreme Court of Mississippi

City of Missoula v. Zerbst
Civil Rights, Constitutional Law, Criminal Law
Montana Supreme Court

State v. Degarmo
Civil Rights, Constitutional Law, Criminal Law
Nebraska Supreme Court

People v. Holz
Civil Rights, Constitutional Law, Criminal Law
New York Court of Appeals

People v. Maffei
Civil Rights, Constitutional Law, Criminal Law
New York Court of Appeals

State v. Bailey
Civil Rights, Constitutional Law, Criminal Law
North Carolina Supreme Court

State v. Ellis
Civil Rights, Constitutional Law, Criminal Law
North Carolina Supreme Court

State v. Hobbs
Civil Rights, Constitutional Law, Criminal Law

North Carolina Supreme Court

State v. Mylett
Criminal Law
North Carolina Supreme Court

Dodge v. North Dakota
Constitutional Law, Criminal Law
North Dakota Supreme Court

Hewitt v. NDDOT
Criminal Law, Government & Administrative Law
North Dakota Supreme Court

Kastet v. NDDOT
Criminal Law, Government & Administrative Law
North Dakota Supreme Court

North Dakota v. Dahl
Constitutional Law, Criminal Law
North Dakota Supreme Court

North Dakota v. Foster
Constitutional Law, Criminal Law
North Dakota Supreme Court

North Dakota v. Kolstad
Constitutional Law, Criminal Law
North Dakota Supreme Court

North Dakota v. Michel
Constitutional Law, Criminal Law
North Dakota Supreme Court

North Dakota v. Wayland
Constitutional Law, Criminal Law
North Dakota Supreme Court

Schwindt v. Sorel
Constitutional Law, Criminal Law, Government & Administrative Law
North Dakota Supreme Court

State ex rel. McDougald v. Greene
Criminal Law
Supreme Court of Ohio

State ex rel. Parker Bey v. Byrd
Criminal Law
Supreme Court of Ohio

State v. Dangler
Criminal Law

Supreme Court of Ohio

Oregon v. Haji
Constitutional Law, Criminal Law
Oregon Supreme Court

South Carolina v. Durant
Constitutional Law, Criminal Law
South Carolina Supreme Court

South Carolina v. Perry
Constitutional Law, Criminal Law
South Carolina Supreme Court

South Carolina v. Quinn
Constitutional Law, Criminal Law, White Collar Crime
South Carolina Supreme Court

Texas v. Arellano
Constitutional Law, Criminal Law
Texas Court of Criminal Appeals

COVID-19 Updates: Law & Legal Resources Related to Coronavirus

Click here to remove Verdict from subsequent Justia newsletter(s).

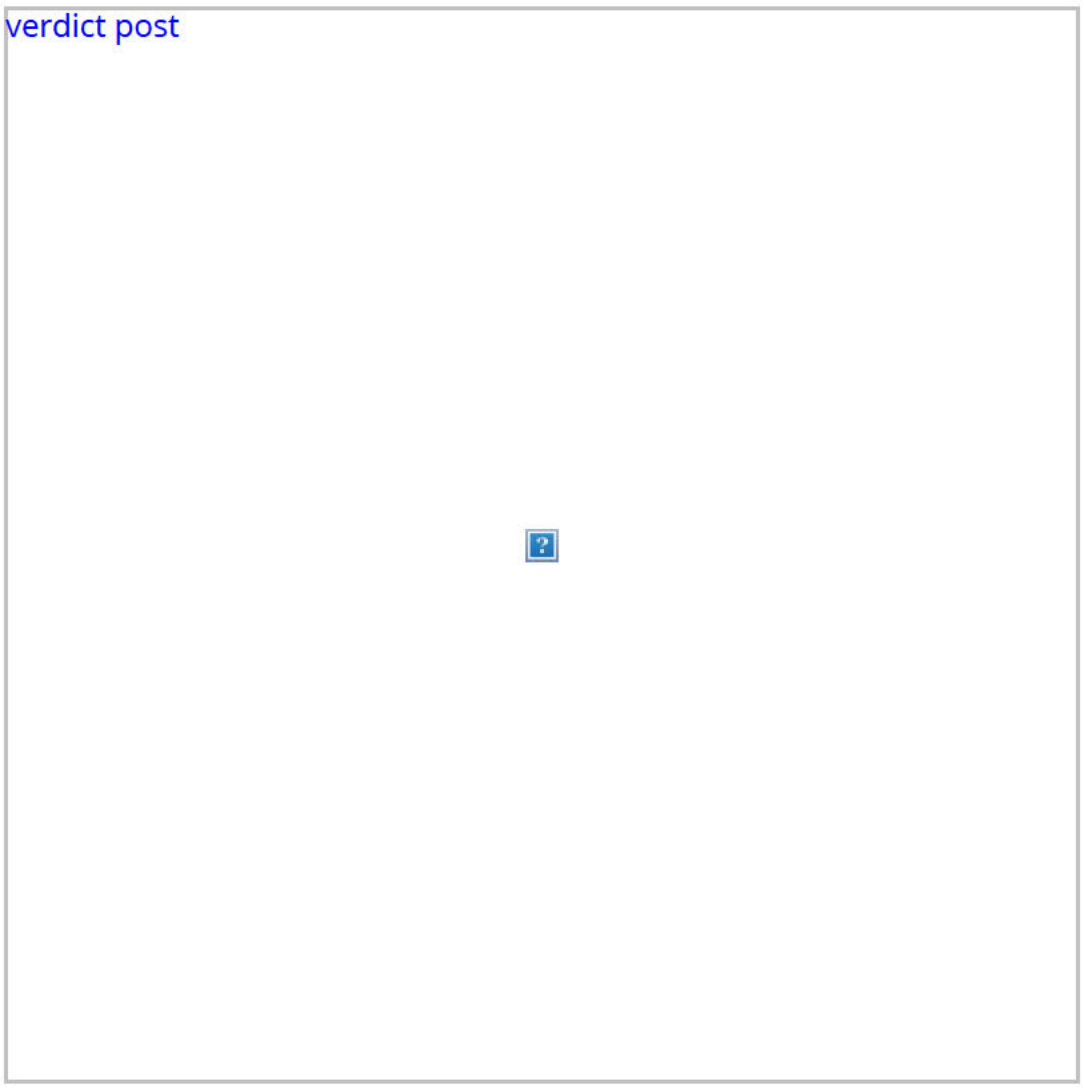
New on Verdict

Legal Analysis and Commentary

Department of Justice Once Again Proves Its Loyalty to the President, Not the Rule of Law

AUSTIN SARAT

verdict post



Austin Sarat—Associate Provost, Associate Dean of the Faculty, and William Nelson Cromwell Professor of Jurisprudence and Political Science at Amherst College—comments on the recent news that the Justice Department will seek dismissal of charges against Michael Flynn. Sarat suggests that because the decision does not seem to advance the fair administration of justice in this case, the court should take the unusual step of refusing to grant the prosecutor's motion to dismiss.

Read More

Criminal Law Opinions

Kelly v. United States

Court: US Supreme Court
Docket: 18-1059
Opinion Date: May 7, 2020
Judge: Elena Kagan
Areas of Law: Criminal Law, Government & Administrative Law, White Collar Crime

During former New Jersey Governor Christie's 2013 reelection campaign, Fort Lee's mayor refused to endorse Christie. Kelly, Christie's Deputy Chief of Staff, Port Authority Deputy Executive Director, Baroni, and another official decided to reduce from three to one the number of lanes reserved at the George Washington Bridge's toll plaza for Fort Lee's commuters. To disguise the political retribution, the lane realignment was said to be for a traffic study. Port Authority traffic engineers were asked to collect some numbers. An extra toll collector was paid overtime. The lane realignment caused four days of gridlock, ending only when the Port Authority's Executive Director learned of the scheme. The Third Circuit affirmed the convictions of Baroni and Kelly for wire fraud, fraud on a federally funded program, and conspiracy to commit those crimes. The Supreme Court reversed. The scheme did not aim to obtain money or property. The wire fraud statute refers to "any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses," 18 U.S.C. 1343. The federal-program fraud statute bars "obtain[ing] by fraud" the "property" (including money) of a federally funded program or entity, section 666(a)(1)(A). The statutes are limited to the protection of property rights and do not authorize federal prosecutors to set standards of good government. The Court rejected arguments that the defendants sought to take control of the Bridge's physical lanes or to deprive the Port Authority of the costs of compensating employees. Their realignment of the access lanes was an exercise of regulatory power; a scheme to alter a regulatory choice is not one to take government property. The time and labor of the employees were an incidental byproduct of that regulatory object. Neither defendant sought to obtain the services that the employees provided.

Read Opinion Are you a lawyer? **Annotate this case**.

Gomes v. Silva

Court: US Court of Appeals for the First Circuit
Docket: 19-1656

Opinion Date: May 1, 2020
Judge: Stahl
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The First Circuit affirmed the judgment of the district court denying Appellant's petition for a writ of habeas corpus, holding that, under the highly deferential standard prescribed by the Antiterrorism and Effective Death Penalty Act for federal habeas review of state criminal convictions, Appellant's claims to habeas relief failed. Appellant was convicted in a Massachusetts superior court of murder in the first degree and related crimes. The Supreme Judicial Court (SJC) affirmed the convictions. Appellant subsequently petitioned the District Court for the District of Massachusetts for a writ of habeas corpus. The district court denied the petition but granted a certificate of appealability. The First Circuit affirmed, holding (1) sufficient evidence supported Appellant's conviction for first-degree murder as a joint venturer, and the SJC's sufficiency determination was not unreasonable; and (2) the SJC reasonably determined that the trial court's admission into evidence of certain items did not constitute error.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Perez-Couvertier

Court: US Court of Appeals for the First Circuit
Docket: 16-2186
Opinion Date: May 7, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The First Circuit affirmed Defendant's conviction of possessing with intent to distribute controlled substances in a protected area and conspiring to distribute controlled substances in a protected area, holding that the district court did not plainly err with respect to any of Defendant's challenges. Specifically, the First Circuit held (1) the district court did not commit plain error in admitting evidence of the conspiracy's activities occurring after he withdrew from the conspiracy or, alternatively, in not instructing the jury to ignore such evidence; (2) the district court did not plainly err in admitting evidence of a drug trafficking organization's violent acts; and (3) the delay between Defendant's indictment and arrest did not violate his Sixth Amendment right to a speedy trial.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Haverkamp

Court: US Court of Appeals for the Second Circuit
Docket: 18-3735
Opinion Date: May 4, 2020
Judge: Barrington D. Parker
Areas of Law: Criminal Law

Defendant pleaded guilty to one count of distribution and receipt of child pornography and one count of possession of child pornography. The district court sentenced him to 121 months of imprisonment, followed by five years of supervised release, and imposed a $200 mandatory special assessment under 18 U.S.C. 3013, as well as a $10,000 assessment under 18 U.S.C. 3014. The Second Circuit held that the district court did not abuse its discretion in sentencing defendant and his sentence was substantively reasonable. The court held that the text of the Justice for Victims of Trafficking Act (JVTA), 18 U.S.C. 3014, taken as a whole and in its context, is straightforwardly meant to be applied on a per-offender, not a per-count, basis. In this case, the district court erroneously applied the special assessment on a per-count, rather than per-offender, basis. Finally, the court held that the computer monitoring condition in question was reasonably related to the nature of defendant's offense. Accordingly, the court affirmed in part, vacated in part, and remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Mladen

Court: US Court of Appeals for the Second Circuit
Docket: 18-0616
Opinion Date: May 6, 2020
Judge: Amalya Lyle Kearse
Areas of Law: Criminal Law, Trusts & Estates

After defendant died while his appeal was pending, counsel moved for

abatement of all incidents of the prosecution, requesting that the appeal be dismissed without a decision on the merits, that defendant's conviction be vacated, and that the matter be remanded to the district court with instructions to dismiss the indictment and order repayment to defendant's estate of the $20,000 fine and $100 special assessment. Because defendant was convicted upon his plea of guilty, and he neither did nor was permitted to challenge on appeal the merits of his conviction, the Second Circuit denied as without merit so much of the motion as seeks (1) vacatur of his conviction, (2) dismissal of the count of the indictment on which he was convicted, and (3) repayment of the mandatory $100 special assessment. The court granted so much of the motion as requests dismissal of this appeal and a remand to the district court for vacatur of the imposed terms of imprisonment and supervised release and for an order requiring that the paid fine of $20,000 be repaid to defendant's estate.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Richardson

Court: US Court of Appeals for the Second Circuit
Docket: 19-412
Opinion Date: May 5, 2020
Judge: Menashi
Areas of Law: Criminal Law

The Second Circuit affirmed defendant's conviction for distribution and possession with intent to distribute a controlled substance. The court held that the district court did not procedurally err by applying the career offender sentencing enhancement pursuant to USSG 4B1.1 because defendant's prior convictions of conspiracy to distribute a controlled substance in violation of 21 U.S.C. 841(a)(1) and 846, and attempted criminal possession of a controlled substance in violation of N.Y. Penal Law 220.16(1), qualify as controlled substance offenses, as defined in USSG 4B1.2(b). The court also held that the district court did not substantively err in sentencing defendant, because it properly considered his criminal history and accounted for his need for mental health and substance abuse treatment.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Rosemond

Court: US Court of Appeals for the Second Circuit
Docket: 18-3561
Opinion Date: May 1, 2020
Judge: Chin
Areas of Law: Criminal Law

The Second Circuit affirmed defendant's conviction for murder-for-hire, conspiracy to commit murder-for-hire, murder through use of a firearm, and possession of a firearm during a murder-for-hire conspiracy. Defendant owned Czar Entertainment, a music management company that represented hip-hop, rap and R&B artists such as Jayceon Taylor, also known as "The Game." Taylor was a member of G-Unit, a rap group run by Curtis Jackson, also known as "50 Cent." Defendant's crimes stemmed from a rivalry with Violator Records, the company that managed G-Unit. The court rejected defendant's contention that his attorney was ineffective because he conceded that defendant paid for the victim to be shot, even though he told counsel not to make this concession. The court held that defendant failed to show that this was objectively unreasonable or that he would have been found not guilty had a different argument been advanced. In this case, there was ample evidence supporting counsel's strategy to concede that defendant ordered a shooting where, among other things, the government's key witness, who participated in the conspiracy and lured the victim to be shot, testified that defendant agreed to pay the shooter. The court also held that the district court did not abuse its broad discretion by admitting prior bad-act evidence under Federal Rule of Evidence 404(b)(1).

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Lacerda

Court: US Court of Appeals for the Third Circuit
Docket: 15-2812
Opinion Date: May 5, 2020
Judge: Porter
Areas of Law: Criminal Law, White Collar Crime

VOG billed itself as an advocacy group helping victims of timeshare fraud get out of their timeshare debts. A jury determined that VOG had actually

defrauded its customers and that three individual defendants (including Lacerda) were each knowing participants in that fraud. Lacerda was sentenced to 324 months' imprisonment for his leading role in the fraudulent enterprise. The Third Circuit affirmed the respective convictions and sentences. The court rejected a claim of impermissible "overview testimony" by an FBI agent; an officer who is familiar with an investigation or was personally involved may tell the story of that investigation—how the investigation began, who was involved, and what techniques were used, and, with a proper foundation, may offer lay opinion testimony and testify about matters within his personal knowledge. The district court did not abuse its discretion when it disqualified defense counsel based on a conflict of interest; when it denied replacement counsel's motion for a continuance; when it excluded from evidence, as hearsay, an email sent by Lacerda to VOG's former CFO; in exercising its sentencing discretion; or by ordering the forfeiture of all VOG's gross proceeds.

Read Opinion Are you a lawyer? **Annotate this case**.

Cucalon v. Barr

Court: US Court of Appeals for the Fourth Circuit
Dockets: 18-1292, 18-2206
Opinion Date: May 7, 2020
Judge: Barbara Milano Keenan
Areas of Law: Criminal Law, Immigration Law

The Fourth Circuit denied petitions for review of the BIA's final order of removal. Applying the modified categorical approach, the court held that defendant's prior conviction for distribution of cocaine under Virginia Code 18.2-248, including distribution of that substance as an accommodation under Virginia Code 18.2-248(D), satisfies the federal definitions of an "aggravated felony" and of a crime "relating to a controlled substance" pursuant to 8 U.S.C. 1227(a)(2)(A)(iii), 1227(a)(2)(B)(i). The court also held that the district court did not abuse its discretion in denying petitioner's motion to reconsider.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Doctor

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-4874
Opinion Date: May 4, 2020
Judge: Roger L. Gregory
Areas of Law: Criminal Law

The Fourth Circuit affirmed the district court's revocation of defendant's supervised release and resulting sentence. The court held that the district court did not clearly err in finding the government proved he committed the assault underlying the supervised release violation; the district court did not commit plain error by adopting the violation report when announcing defendant committed Violation One; and, even if the district court erred in sentencing defendant for a Grade A violation, the error was harmless.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Lewis

Court: US Court of Appeals for the Fourth Circuit
Docket: 19-4028
Opinion Date: May 4, 2020
Judge: Barbara Milano Keenan
Areas of Law: Criminal Law

Defendant was convicted for possessing a firearm as a felon and sentenced to 63 months' imprisonment and a three-year period of supervised release. The district court additionally recommended, without explanation, that defendant receive addiction treatment while incarcerated and ordered, as a special condition of his supervised release, that defendant participate in an addiction treatment program. The Fourth Circuit held that defendant's sentence is procedurally unreasonable because the district court failed to provide an adequate explanation for imposing as a special condition of supervised release the requirement of addiction treatment. The court also held that the district court failed to address defendant's nonfrivolous mitigation arguments. Therefore, the court remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Jordan

Court: US Court of Appeals for the Fifth Circuit
Docket: 19-40499
Opinion Date: May 1, 2020
Judge: Jennifer Walker Elrod
Areas of Law: Criminal Law

The Fifth Circuit affirmed the district court's grant of defendants' motion for a new trial on the basis of prejudicial outside influence on the jury. The court held that the district court did not abuse its broad discretion in granting the motion for a new trial without holding an evidentiary hearing. To the extent there is a bright-line rule applicable to allegations of outside influence on the jury, the court held that it was not applicable to this case. Furthermore, the district court did not abuse its discretion in exercising its prerogative, within broadly defined parameters, to handle the allegation of outside influence in the least disruptive manner possible in this unusual case. Finally, the district court permissibly concluded that the evidence showed a sufficient likelihood of prejudice to shift the burden to the Government, and that the Government did not (and could not) show "no reasonable possibility that the jury's verdict was influenced by" the CSO's comments.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Longoria

Court: US Court of Appeals for the Fifth Circuit
Docket: 19-20201
Opinion Date: May 5, 2020
Judge: Gregg Costa
Areas of Law: Criminal Law

The Fifth Circuit held that the base offense level of 20 was proper for defendant's felon-in-possession crime involving a semiautomatic firearm that is capable of accepting a large capacity magazine. In this case, defendant failed to show that the district court clearly erred in relying on the FBI's agent statement about what was found in the apartment. The court clarified any confusion and held that the 2013 amendment to the commentary on the acceptance-of-responsibility Guideline does not clearly overrule its caselaw allowing the government to withhold the third point for

acceptance of responsibility when it must litigate a suppression motion. The court held that Amendment 775 does not contain the unequivocal override needed to get past the court's precedent. Therefore, the court affirmed defendant's sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. McNabb

Court: US Court of Appeals for the Fifth Circuit
Docket: 19-50265
Opinion Date: May 1, 2020
Judge: Costa
Areas of Law: Criminal Law

The Fifth Circuit affirmed defendant's sentence imposed after he pleaded guilty to possessing a gun after having been convicted of a felony. The court held that defendant is not entitled to relief on his claim that the government breached the plea deal, and thus his appellate waiver remains enforceable. Accordingly, defendant's challenges to his sentence must be dismissed.

Read Opinion Are you a lawyer? **Annotate this case**.

Andrews v. Wayne County

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-1992
Opinion Date: May 4, 2020
Judge: Suhrheinrich
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Canton Police received a 911 call from Andrews, who stated that his fiance, White, had physically attacked him. Officers arrested White. Andrews later took White's medications to the jail; a “KOP” policy allows inmates to keep certain drugs for self-administration. During an intake interview, White admitted to attempting to harm herself or commit suicide in the past but said she was not thinking of harming herself or having suicidal thoughts. An R.N. later evaluated White for nearly two hours, reported White’s chief complaints were “anxiety and depression,” and contacted a pharmacy to verify White’s prescriptions. The R.N. claims White did not exhibit any psychotic behavior,

suicidal ideation, or psychiatric distress but ordered further evaluation. The next day, White was found on the floor with vomit on her face. She stated repeatedly that she took too many pills. The next day, White died in the hospital. The cause of death was Verapamil toxicity. The Sixth Circuit affirmed the rejection of a suit under 42 U.S.C. 1983 on summary judgment. A pretrial detainee does not have an automatic right to a suicide screening. The court rejected an argument that the KOP Policy was deficient because it allows inmates in need of a psychological evaluation to participate before a psychiatrist's assessment of proper housing. The County had no history of suicides relative to the program, so any purported failure to train its employees in suicide risk assessment did not cause White's death.

Read Opinion Are you a lawyer? **Annotate this case**.

Hicks v. Scott

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-3410
Opinion Date: May 1, 2020
Judge: Gibbons
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Cincinnati officers Scott and Moore responded to a reported incident of menacing. Two people alleged that Quandavier had driven by their home that night and threatened to kill them and that Quandavier carried guns. Officer Loreaux identified a vehicle fitting the description. Officers Scott, Moore, Schneider, and Loreaux, standing where the vehicle was parked, heard a voice. Thinking that it was likely Quandavier, they knocked on the exterior door of the residence. It swung open. Three officers entered without a warrant or exigent circumstances. Loreaux remained outside. Neither Scott nor Moore recall announcing their presence or identifying themselves. Inside and upstairs, Scott knocked on a closed door. As it opened, Scott "saw the barrel of a rifle pointed at [her] face." Moore and Schneider also saw Quandavier "nonchalantly" panning the rifle from left to right. Moore reached for its barrel as Scott fired her weapon. Moore did not instruct Quandavier to drop his rifle nor did Scott issue any commands before firing. Quandavier collapsed. The officers immediately radioed for paramedics. Before the officers applied handcuffs or provided first aid, they heard another voice and conducted a sweep. Quandavier died at the scene

without receiving medical attention. In a suit under 42 U.S.C. 1983 for unlawful entry, excessive force, and deliberate indifference to a serious medical need, plus state claims, the district court granted the defendants summary judgment, citing qualified immunity. The Sixth Circuit reversed in part. The district court erred by granting qualified immunity to Scott, Moore, and Schneider on the unlawful entry claim. The court affirmed as to the excessive force, deliberate indifference, and state-law battery claims, and remanded for evaluation of municipal liability and wrongful death claims.

Read Opinion Are you a lawyer? **Annotate this case**.

Moody v. United States

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-5015
Opinion Date: May 6, 2020
Judge: Thapar
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

At Moody's trial, the government produced a video of Moody cooking crack on his stove and waving a handgun while he mused about life in "the game" (drug trafficking). The court ruled that most of the video was admissible. Moody then tried to persuade the jury that the video was filmed more than five years before his indictment, putting it outside the statute of limitations. The jury convicted Moody. Due to prior felony drug convictions, Moody received enhanced, mandatory-minimum life sentences on several counts. He appealed on evidentiary grounds relating to the video. The Sixth Circuit affirmed. Later, Moody raised new claims on collateral review, 28 U.S.C. 2255. The district court found each claim meritless; most were also procedurally defaulted. The court authorized Moody to appeal. The Sixth Circuit dismissed the appeal, stating that none of the claims should have been certified. Reasonable jurists could not doubt that the district court properly denied relief on Moody's claims that he was deprived of his statute-of-limitations defense (violating due process); that the past convictions for his sentencing enhancements were not charged in the indictment or found by the jury; and that his previous lawyers failed to raise the first two claims sooner, violating his right to effective assistance of counsel.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Foreman

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-1827
Opinion Date: May 7, 2020
Judge: Gibbons
Areas of Law: Criminal Law

In 2006, Foreman pled guilty to possession with intent to distribute 50 or more grams of cocaine base, possession with intent to distribute cocaine powder, and possession of a firearm during and in furtherance of a drug trafficking crime. Foreman admitted that he was responsible for approximately 135 grams of crack cocaine and 250 grams of cocaine powder. Foreman had a final Guidelines range of 322-387 months; he was sentenced to 240 months' imprisonment with respect to each drug conviction, to run concurrently, and 60 months' imprisonment for the firearms conviction, to run consecutively. When the First Step Act of 2018 made the Fair Sentencing Act retroactive, Foreman sought relief. The district court held that Foreman was not entitled to a plenary resentencing and declined to revisit his career offender status or hold an in-person hearing, then weighed the new statutory range applicable to Foreman's drug offenses, his recalculated Guidelines range, and the 18 U.S.C. 3553(a) factors, and reduced Foreman's total sentence to 172 months on each drug offense, to run concurrently, plus the mandatory consecutive 60 months on the firearms offense. The Sixth Circuit affirmed. Nothing in the First Step Act entitles a defendant to a plenary resentencing. First Step Act resentencings are not shielded from review for reasonableness; the district court thoroughly explained its rationale, carefully examining Foreman's circumstances, the amended penalty provisions, and the resulting changes to Foreman's Guidelines range.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Smith

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-1724
Opinion Date: May 6, 2020

Judge: Bush
Areas of Law: Criminal Law

In 2006, Smith was convicted of conspiracy to distribute and to possess with intent to distribute 500 grams or more of powder or 50 grams or more of cocaine base (crack cocaine); possession with intent to distribute 50 grams or more of cocaine base (crack cocaine); possession with intent to distribute 500 grams or more of cocaine powder; and being a felon in possession of a firearm. The court imposed a mandatory minimum life sentence. The Fair Sentencing Act subsequently lowered the penalty for cocaine-base offenses, made retroactive through the First Step Act. Smith moved for relief and received a reduced sentence of 360 months, the bottom of the new Guideline range for the counts impacted by the Fair Sentencing Act, to run concurrent to his existing 360-month sentence for his powder cocaine count that was not affected by the Fair Sentencing Act. The Sixth Circuit affirmed, rejecting an argument that the court should have imposed a below-Guideline sentence for all counts. The First Step Act is a limited grant of authority to impose a reduced sentence for certain offenses and does not require a plenary resentencing proceeding. Even assuming the court's obligation to explain its reasons for imposing the modified sentence was akin to that which applies in initial sentencing, the court's use of a modified AO 247 form order to explain its decision was not procedurally unreasonable.

Read Opinion Are you a lawyer? **Annotate this case**.

Kirkman v. Thompson

Court: US Court of Appeals for the Seventh Circuit
Docket: 19-1904
Opinion Date: May 7, 2020
Judge: William Joseph Bauer
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Following a 1992 fight that involved Johnson, Herron, and Walker, two shooters shot the three men. Johnson survived. In the hospital, Johnson described a shooter by the street name "Duke," where Duke lived, and Duke's car. Johnson identified Duke and his accomplice from a photo array. Police pulled over a vehicle matching Johnson's description and arrested

the driver, Kirkman, and the passenger, who matched the general description of the second shooter. Kirkman had a tattoo of Duke on his arm. Police took additional photos and presented a second photo array to Johnson, who identified them as the shooters. At trial, Johnson identified Kirkman and his passenger as the shooters. There was disputed testimony about the cause of the fight. Convicted of murder and aggravated battery with a firearm, Kirkman was sentenced to life in prison. Johnson had a change of heart and submitted an affidavit, identifying Ford and an unknown man as the shooters. At Kirkman's post-conviction hearing, Johnson testified that he and his family had been threatened. Other testimony was inconsistent with Johnson's. Illinois courts denied post-conviction relief, finding that Johnson's recantation lacked credibility. Johnson later pleaded guilty for perjury but failed to specify which statement was false. The Seventh Circuit affirmed the denial of federal habeas relief. Illinois courts found Johnson's recantation lacked credibility. An evidentiary hearing satisfied Kirkman's due process rights. The Illinois trial court's determination defeated Kirkman's innocence and perjured testimony claims.

Read Opinion Are you a lawyer? **Annotate this case**.

Tuduj v. Newbold

Court: US Court of Appeals for the Seventh Circuit
Docket: 19-1699
Opinion Date: May 1, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Illinois prisoner Tuduj, having received extensive dental treatment, filed a "deliberate indifference" suit under 42 U.S.C. 1983 against his dentists and prison officials. The court recruited counsel to assist Tuduj in filing an amended complaint that complied with the Federal Rules of Civil Procedure. Counsel defended against two summary judgment motions, one arguing that Tuduj had not exhausted his administrative remedies and another on the merits While the motions were pending, Tuduj moved "for leave to represent himself," stating that he was "concerned that his counsel has filed a structurally, technically and legally insufficient response doomed to be denied." He asked to file his own brief, except "in the event this Honorable Court deems counsel's response … legally sufficient and Grants same[,]

Plaintiff would be open to continued effective representation." A magistrate denied Tuduj's motion, stating that Tuduj "varie[d] between saying he would like to" represent himself and "indicating that he is happy with counsel's representation as long as he prevails." The district judge granted the motions for summary judgment, citing professional judgment and finding "no competent evidence" of any policy that unlawfully influenced dental-treatment decisions. The Seventh Circuit rejected Tuduj's argument that the court wrongly denied his "unqualified" right to proceed pro se under 28 U.S.C. 1654, the due process clause, the equal protection clause, and the Seventh Amendment. The district court permissibly denied his equivocal request.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Gibson

Court: US Court of Appeals for the Seventh Circuit
Docket: 19-1402
Opinion Date: May 7, 2020
Judge: William Joseph Bauer
Areas of Law: Constitutional Law, Criminal Law

Officer Garrison encountered Gibson, a suspected drug trafficker, walking with a companion. Although initially a consensual encounter, Garrison questioned Gibson and his companion and briefly detained Gibson. After Gibson and his companion departed, Garrison spotted a methamphetamine pipe under his patrol vehicle. Local law enforcement conducted a traffic stop of Gibson's vehicle in the curtilage of his driveway. A drug detection dog signaled the presence of a controlled substance in the vehicle, though nothing was found. Earlier that day, Gibson's wife had met with DEA agents to tell them about methamphetamine inside the home. Police used information Mrs. Gibson had provided to obtain a search warrant. The search of the home uncovered drugs, drug paraphernalia, currency, and AK-47 rifles, which led to Gibson's arrest. Gibson moved to suppress all evidence seized during the search, alleging he was detained without reasonable suspicion, unlawfully frisked, arrested without probable cause, stopped without probable cause or reasonable suspicion, and the traffic stop exceeded a permissible scope. Upon learning of his wife's cooperation, Gibson also argued her statement was insufficiently attenuated to justify the

search warrant. The Seventh Circuit affirmed the denial of the motion. Mrs. Gibson's voluntary statement with DEA agents was independently sufficient to sustain findings of probable cause and sufficiently attenuated from subsequent events to preclude suppression.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Howell

Court: US Court of Appeals for the Seventh Circuit
Docket: 18-3157
Opinion Date: May 4, 2020
Judge: Scudder
Areas of Law: Constitutional Law, Criminal Law

In December 2012, Chicago Police officers responded to an anonymous call reporting a Hispanic man in a black sweater and black hat, carrying a bag, and climbing under a warehouse fence. They found someone who matched the description. After stopping and frisking him, they determined he was not engaged in any crime. Howell, walking toward the police, was white and wearing a black jacket and dark hat. When an officer approached to speak to him, Howell did not answer, looked panicked, and put his hands in his pockets. The officer patted Howell down and found a gun in his jacket. A federal gun charge followed. Howell unsuccessfully moved to suppress the gun. The Seventh Circuit reversed the denial of his suppression motion and vacated his conviction for possessing that gun. The court noted that the facts in the pretrial record differed significantly from those presented at trial, where the arresting officer testified that he decided to proceed with the pat-down only after Howell ignored a directive to remove his hands from his pockets. Viewing the pretrial record as a whole, the police lacked reasonable suspicion to frisk Howell. The court did not reverse Howell's conviction on a second gun charge that resulted from the execution of a warrant to search Howell's apartment three months after the initial stop and the ensuing discovery of more guns and ammunition.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Lewis

Court: US Court of Appeals for the Seventh Circuit
Dockets: 19-1911, 19-1262
Opinion Date: May 7, 2020
Judge: Joel Martin Flaum
Areas of Law: Criminal Law

In 2016-2018, Draheim managed a conspiracy, responsible for at least 38 packages of methamphetamine sent from California to La Crosse, Wisconsin. Draheim supervised at least 11 associates who accepted shipments on her behalf, sent money transfers to California, distributed the meth, rented storage lockers, and collected money owed to her. Draheim provided vehicles. After agents placed a wiretap on her phone and seized several packages of meth en route to Draheim, her California supplier forced Draheim to find a new source. Draheim contacted Lewis, recently out of jail but still involved in the "meth scene." Lewis agreed to purchase meth from a new supplier. During the planned transaction, agents seized the package, which contained 28.6 grams of nearly pure meth. Police subsequently arrested Draheim after they found her daughter dead at home from an overdose; they took Lewis into custody for violating the terms of his state supervision. Both pleaded guilty to meth distribution offenses, 21 U.S.C. 841, 846. Draheim, facing a mandatory-minimum 10-year sentence, unsuccessfully argued that she qualified for "safety-valve relief." The court reasoned that she was the leader of her enterprise. Lewis unsuccessfully contended that he should be sentenced based only on his conviction, not other "relevant conduct." The Seventh Circuit affirmed Draheim's sentence but vacated as to Lewis. The fact that the defendant has engaged in other drug transactions is not, alone, sufficient to justify treating those transactions as relevant conduct for sentencing purposes.

Read Opinion Are you a lawyer? **Annotate this case**.

Bakor v. Barr

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-3011
Opinion Date: May 7, 2020
Judge: Steven M. Colloton
Areas of Law: Criminal Law, Immigration Law

The Eighth Circuit denied a petition for review of the BIA's determination

that defendant committed two crimes involving moral turpitude. The court held that the BIA did not err in determining that petitioner's conviction for the Minnesota crimes of Criminal Sexual Conduct in the Fifth Degree and knowing failure to comply with Minnesota's sex offender registration statute were crimes involving moral turpitude. The court also held that petitioner failed to exhaust his remaining arguments and therefore declined to consider them.

Read Opinion Are you a lawyer? **Annotate this case**.

Smith v. Titus

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-2915
Opinion Date: May 5, 2020
Judge: Steven M. Colloton
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Eighth Circuit affirmed the district court's denial of habeas relief to petitioner based on his claim that the trial court violated his Sixth Amendment right to a public trial when it briefly closed the courtroom to spectators. The district court denied relief based on the ground that the Minnesota Supreme Court’s decision was neither contrary to, nor an unreasonable application of, clearly established federal law. The court agreed and held that it was not objectively unreasonable for the Minnesota Supreme Court to deem it constitutional under the Sixth Amendment for the trial court to explain the parameters of an earlier public order on evidentiary issues in a brief nonpublic proceeding before the jury was sworn.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Becerra

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-2777
Opinion Date: May 7, 2020
Judge: Stras
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's conviction for two counts of being a

felon in possession of a firearm and ammunition. The court held that there was more than enough evidence for defendant's probation officer and other officers to believe defendant had a firearm on him. Therefore, the officers had probable cause to arrest him without a warrant. The court also held that defendant was in custody when he made both statements at issue. In this case, the "request for clarification" of defendant's statement that he had "something" in his car did not require Miranda warnings. Furthermore, because the bulge in defendant's pocket could have been a gun or other weapon that would have posed a danger to the officers and others, they could ask about it without the formality of Miranda warnings. The court joined its sister circuits in declining to recognize the innocent-possessor defense. The court held that the district court did not err in excluding defendant's proposed testimony that he had found the handgun in his car earlier in the day and was about to hand it over to his probation officer. The court reasoned that, even if defendant intended to turn over the gun (or the ammunition) to his probation officer, it is still a crime to knowingly possess it in the first place. Finally, the court held that the district court did not err in denying defendant a sentencing reduction for acceptance of responsibility; the district court considered defendant's mitigation arguments at sentencing; and the district court did not abuse its discretion by imposing a within-Guidelines sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Haynes

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1607
Opinion Date: May 5, 2020
Judge: Raymond W. Gruender
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's conviction and sentence for being a felon in possession of a firearm. The court held that the government did not violate the Speedy Trial Act, and defendant failed to offer any evidence showing that Iowa and federal prosecutors colluded. Furthermore, the district court did not abuse its discretion by failing to hold an evidentiary hearing regarding the existence of collusion. The court also held that the district court did not err in denying the motion to suppress where defendant

was not unlawfully seized. In this case, prior to producing the marijuana cigarette, the officer did not ask defendant any questions but merely ordered him off the bus, particularly as the smell of marijuana alerted the officer that evidence of a more serious crime than failure to use a turn signal might be uncovered during the stop. Finally, the court held that defendant was not unlawfully searched when the officer conducted a pat-down search incident to arrest; the evidence was sufficient to support defendant's conviction; defendant's Rehaif claim failed because there was sufficient evidence that he knew of his prohibited status; and defendant's sentence was not substantively unreasonable nor an abuse of the district court's discretion.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Roberts

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1176
Opinion Date: May 1, 2020
Judge: Steven M. Colloton
Areas of Law: Criminal Law

The Eighth Circuit vacated defendant's sentence imposed after he pleaded guilty to unlawful possession of a firearm as a previously convicted felon. The court held that, although the district court properly applied a four-level increase for possession of a firearm "in connection with another felony offense" under USSG 2K2.1(b)(6)(B), but that a two-level increase for "using a minor to commit a crime" under USSG 3B1.4 should not have applied. In this case, the evidence showed only that defendant engaged in an arm's-length transaction with a minor. The court held that this mere joint participation in an offense as a partner, does not amount to "use" of a minor "to commit the offense" of unlawful possession of a firearm by a felon. Accordingly, the court remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Wright

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1081

Opinion Date: May 5, 2020
Judge: Erickson
Areas of Law: Criminal Law

The Eighth Circuit affirmed the district court's restitution order and certain special conditions of defendant's supervised release imposed after he pleaded guilty to sex trafficking of a child. The court found no error in the district court's restitution amount of $20,000, holding that the evidence supported the amount in light of the aggregate harm to the victim. The court also held that the special conditions -- including a requirement that defendant participate in sex offender treatment including psychological testing and polygraph examinations, a prohibition against contact with any minors without pre-approval, and a requirement that defendant seek prior approval before using temporary commercial lodging, such as a hotel or motel -- where reasonably related to both the offense of conviction and to defendant's history of sexual contact with minor females.

Read Opinion Are you a lawyer? **Annotate this case**.

Benson v. Chappell

Court: US Court of Appeals for the Ninth Circuit
Docket: 13-99004
Opinion Date: May 1, 2020
Judge: Consuelo Maria Callahan
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Ninth Circuit affirmed the district court's denial of petitioner's habeas corpus petition challenging his California conviction and death sentence for murder and other crimes. Petitioner raised two certified claims and two uncertified claims. The panel held that petitioner failed to show that the California Supreme Court's denials of his claims were unreasonable determinations of the facts or contrary to clearly established federal law. In this case, the California Supreme Court reasonably determined that an officer's misstatement during petitioner's interrogation that there was no death penalty in California did not prompt petitioner's confessions. Furthermore, petitioner failed to show that his statements were not knowing, voluntary, and intelligent. Even if petitioner were able to show that trial counsel was ineffective in not fully investigating his abuse as a child or his alleged organic brain injury, the panel held that the state court could

reasonably have determined that any shortcoming in trial counsel's investigation was not prejudicial. Finally, the panel granted a certificate of appealability on petitioner's two uncertified claims and held that the state court reasonably rejected the claims that his trial counsel should have impeached the government's case and the prosecutor withheld material, exculpatory evidence.

Read Opinion Are you a lawyer? **Annotate this case**.

Mero v. Barr

Court: US Court of Appeals for the Ninth Circuit
Docket: 17-70929
Opinion Date: May 1, 2020
Judge: Paul Jeffrey Watford
Areas of Law: Criminal Law, Immigration Law

The Ninth Circuit granted in part a petition for review of the BIA's finding that petitioner was removable based on his conviction for possession of visual presentation depicting sexual conduct of a person under 16 years of age, in violation of Nevada Revised Statutes (N.R.S.) 200.730. Applying the categorical approach, the panel compared the elements of N.R.S. 200.730 with the applicable definition of "sexual abuse of a minor," which requires proof of three elements. The panel held that N.R.S. 200.730 punishes a broader range of conduct because the Nevada statute does not require proof that the offender participated in sexual conduct with a minor. Therefore, petitioner's conviction did not qualify as sexual abuse of a minor. The panel explained that, with a possession-only offense such as N.R.S. 200.730, the minor depicted in the image is not the direct object of the offender's conduct, which is a necessary predicate for the offense to qualify as sexual abuse of a minor.

Read Opinion Are you a lawyer? **Annotate this case**.

Romero-Millan v. Barr

Court: US Court of Appeals for the Ninth Circuit
Dockets: 16-73915, 17-72893, 18-71555
Opinion Date: May 4, 2020

Areas of Law: Criminal Law

The Ninth Circuit certified the following questions of state law to the Arizona Supreme Court: 1. Is Arizona's possession of drug paraphernalia statute, A.R.S. 13-3415, divisible as to drug type? 2. Is Arizona's drug possession statute, A.R.S. 13-3408, divisible as to drug type? 3. Put another way, is jury unanimity (or concurrence) required as to which drug or drugs listed in A.R.S. 13-3401(6), (19), (20), or (23) was involved in an offense under either statute?

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Yang

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-10341
Opinion Date: May 4, 2020
Judge: Piersol
Areas of Law: Criminal Law

The Ninth Circuit affirmed the district court's denial of defendant's motion to suppress after he pleaded guilty to receipt of stolen mail and being a prohibited person in possession of a firearm. Defendant moved to suppress the evidence seized from his residence and the statements he made to law enforcement on the basis that the search warrant obtained by the Postal Inspection Service relied on evidence that was obtained illegally. The panel declined to address the potential Fourth Amendment privacy interests that may be implicated by the warrantless use of this Automatic License Plate Recognition (ALPR) technology, and held that defendant does not have a reasonable expectation of privacy in the historical location data of the Yukon under the facts of this case. The panel found no evidence in the record that Prestige Motors had a policy or practice of allowing lessees to keep cars beyond the rental period and Prestige had made affirmative attempts to repossess the vehicle by activating the GPS unit to locate and disable the vehicle. Therefore, defendant lacked standing to challenge the warrantless search of the database.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Neugin

Court: US Court of Appeals for the Tenth Circuit
Docket: 19-7043
Opinion Date: May 1, 2020
Judge: Scott Milne Matheson, Jr.
Areas of Law: Constitutional Law, Criminal Law

Jack Neugin pled guilty to being a felon in possession of a firearm and ammunition on the condition that he could appeal the district court's denial of his motion to suppress evidence of the ammunition and firearm police found in the bed of his pickup truck. Officers responded to a reported verbal altercation between Neugin and his girlfriend. One of the officers saw ammunition in the back of the truck after he lifted the truck's camper lit do allow the girlfriend to retrieve her belongings. Neugin argued the officers discovered the evidence during an unconstitutional search; the district court concluded the officer was acting "in a lawful position" as "community caretaker," and found no Fourth Amendment violation. The Tenth Circuit reversed, finding that : (1) the officer conducted the without a warrant or probable cause, (2) the community caretaking exception to the warrant requirement does not apply, and (3) the inevitable discovery exception to the exclusionary rule does not apply. The evidence seized should have been suppressed.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Ramon

Court: US Court of Appeals for the Tenth Circuit
Docket: 19-1221
Opinion Date: May 1, 2020
Judge: Gregory Alan Phillips
Areas of Law: Constitutional Law, Criminal Law

In 2016, after serving a federal prison sentence for having possessed a firearm after a felony conviction, Charles Ramon III began serving a mandatory term of supervised release. Before Ramon completed the term, his probation officer filed a petition, soon followed by two superseding petitions, to revoke Ramon’s supervised release. At the revocation hearing, the district court found three violations—two for possessing a controlled

substance and one for again illegally possessing a firearm. Of these, the most serious was Ramon's illegal possession of a firearm—a Grade B violation. For this, the court imposed the statutory maximum sentence of twenty-four months in prison. During the revocation hearing, the government mentioned that it might seek to indict Ramon for illegally possessing a firearm (the conduct in part underlying the revocation). Mindful of this, the district court ordered that Ramon's twenty-four-month sentence run "consecutively to any sentences imposed previously or prospectively in federal or state court." At the hearing, Ramon did not object to the district court's running his sentence consecutively to future federal sentences. On appeal, Ramon argued that the district court exceeded its sentencing authority under 18 U.S.C. 3584(a) by ordering that Ramon's sentence run consecutively to future federal sentences. By the terms of 18 U.S.C. 3584(a), the Tenth Circuit determined the district court did err. But Ramon failed to object to this at trial, and on appeal, failed to show that the error was plain, thus, judgment was affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Richards

Court: US Court of Appeals for the Tenth Circuit
Docket: 19-8044
Opinion Date: May 6, 2020
Judge: Baldock
Areas of Law: Constitutional Law, Criminal Law

In 2018, the Wyoming Division of Criminal Investigation (DCI) obtained a search warrant to review the contents of Defendant–Appellant Joshua Richards' Tumblr account. During the search and subsequent investigation, DCI agents discovered Defendant had re-blogged videos and images of child pornography to his private Tumblr so he could later access and view the materials. Defendant ultimately pleaded guilty to one count of accessing with intent to view child pornography. He was sentenced to twenty-four months' imprisonment followed by five years of supervised release. The district court imposed several special conditions of supervised release, which, as relevant here, related to drugs and alcohol and required Defendant to submit to polygraph testing. On appeal, Defendant argued the district court erred in imposing these special conditions. He also challenged

the length of his prison sentence as substantively unreasonable. The Tenth Circuit determined the alcohol and drug conditions did not directly conflict with the relevant policy statement in the sentencing guidelines, so the district court's decision to impose the conditions was not manifestly unreasonable. And given the circumstances of the case, the Court determined the trial court did not abuse its discretion in imposing Defendant's twenty-four month sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

Andrews v. Warden

Court: US Court of Appeals for the Eleventh Circuit
Docket: 19-12443
Opinion Date: May 5, 2020
Judge: William Holcombe Pryor, Jr.
Areas of Law: Criminal Law

The Eleventh Circuit affirmed the district court's denial of habeas relief under 28 U.S.C. 2241. Plaintiff alleged that President Obama commuted his "total sentence" of imprisonment, which included the 37 months of imprisonment that he served as part of his 2003 sentence. Based on the terms of the commutation order, the Constitution, and Supreme Court precedent, the court could not say that the Bureau erred in excluding the 37-month term of imprisonment from its recalculation.

Read Opinion Are you a lawyer? **Annotate this case**.

Hollis v. United States

Court: US Court of Appeals for the Eleventh Circuit
Docket: 19-11323
Opinion Date: May 6, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Eleventh Circuit affirmed the district court's denial of petitioner's motion to vacate his sentence under 28 U.S.C. 2255. The court held that petitioner cannot prove that his counsel rendered ineffective assistance, because petitioner's prior convictions in Alabama categorically qualify as predicate

offenses under both the Armed Career Criminal Act and the career-offender provision of the Guidelines, and his prior conviction in Georgia qualifies as a predicate offense under the Act. Therefore, counsel did not perform deficiently by failing to raise a meritless objection.

Read Opinion Are you a lawyer? **Annotate this case**.

Knight v. Florida Department of Corrections

Court: US Court of Appeals for the Eleventh Circuit
Docket: 18-12488
Opinion Date: May 1, 2020
Judge: Newsom
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Eleventh Circuit affirmed the district court's denial of a 28 U.S.C. 2254 petition for habeas relief. Petitioner alleged that his counsel rendered ineffective assistance under Strickland v. Washington, 466 U.S. 668 (1984), by failing to adequately investigate and present mitigating evidence during the sentencing phase of his capital-murder trial. The court held that, even assuming that counsel performed deficiently in failing to investigate and present the mitigation evidence that petitioner now raises—thus satisfying the first prong of the two-part Strickland standard that governs ineffective-assistance claims—petitioner failed to carry his burden of demonstrating resulting prejudice.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Evans

Court: US Court of Appeals for the Eleventh Circuit
Docket: 17-15323
Opinion Date: May 6, 2020
Judge: Grant
Areas of Law: Criminal Law

The Eleventh Circuit affirmed defendant's conviction and sentence for being a felon in possession of a firearm. The court held that, given the totality of the circumstances, it was reasonable for officers, mistaking a dog's whimper for a person in distress, to enter defendant's home without a warrant.

Therefore, defendant's challenge to the district court's denial of his motion to suppress evidence failed. The court upheld the district court's imposition of a 22 offense level finding because defendant possessed a semiautomatic firearm capable of accepting a large capacity magazine under USSG 2K2.1(a)(3)(A)(i) (2016). The court also upheld defendant's sentencing enhancement under USSG 2K2.1(b)(4)(B) for possessing a rifle that had an obliterated serial number.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. McLellan

Court: US Court of Appeals for the Eleventh Circuit
Docket: 18-13289
Opinion Date: May 6, 2020
Judge: Boggs
Areas of Law: Criminal Law

The Eleventh Circuit affirmed defendant's conviction for two counts of being a felon in possession of a firearm. The court held that the district court did not abuse its discretion in permitting one of his arresting officers to offer testimony at trial on the correlation between guns and drug activity and to suggest that defendant was selling drugs; the court declined to evaluate the applicability of the Armed Career Criminal Act (ACCA), because the district court would have imposed the same sentence regardless of whether the mandatory minimum applied; and the court rejected defendant's claim under Rehaif v. United States, 139 S. Ct. 2191 (2019), and held that there was no plain error in the district court's failure to instruct the jury of the knowledge-of-status element and any error from the lack of a knowledge-of-status element in defendant's plea colloquy did not affect his substantial rights. Finally, the court remanded for clarification of the judgment to reflect the sentence the district court said it would have imposed if the Armed Career Criminal Act did not apply.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Russell

Court: US Court of Appeals for the Eleventh Circuit

Docket: 18-11202
Opinion Date: May 4, 2020
Judge: Charles R. Wilson
Areas of Law: Criminal Law

Defendant was convicted of possessing a firearm and ammunition as an immigrant illegally or unlawfully in the United States. After defendant appealed his conviction and sentence, the Supreme Court issued its decision in Rehaif v. United States, 588 U.S. ___, 139 S. Ct. 2191 (2019), which reversed a decision from this court and held that under 18 U.S.C. 922(g), the government must prove that a defendant knew "his status as a person barred from possessing a firearm" when he knowingly possessed a firearm. The Eleventh Circuit held that defendant established the necessary prejudice under plain error review and vacated defendant's section 922(g) conviction, remanding for further proceedings. In this case, the district court committed an error that was made plain by the Supreme Court in Rehaif. Furthermore, defendant has sufficiently shown a reasonable probability that but for the error, the outcome of his trial would have been different.

Read Opinion Are you a lawyer? **Annotate this case**.

Welch v. United States

Court: US Court of Appeals for the Eleventh Circuit
Docket: 14-15733
Opinion Date: May 6, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Eleventh Circuit affirmed the district court's denial of petitioner's 28 U.S.C. 2255 motion to vacate his sentence. The court held that defendant's prior 1996 Florida convictions for robbery qualified as violent felonies under the Armed Career Criminal Act's (ACCA) elements clause, and rejected his contention that the court's decision in his direct appeal carved out a narrow exception to pre-1997 Florida robbery convictions obtained in Florida's Fourth District Court of Appeal. The court also held that petitioner's prior Florida felony battery conviction was a violent felony under the ACCA in light of the court's holding in United States v. Vail-Bailon, 868 F.3d 1293 (11th Cir. 2017) (en banc), cert. denied, 138 S. Ct. 2620 (2018).

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Trujillo

Court: Arizona Supreme Court
Docket: CR-18-0531-PR
Opinion Date: May 4, 2020
Judge: Gould
Areas of Law: Constitutional Law, Criminal Law

The Supreme Court held that, for purposes of imposing mandatory sex offender registration under Ariz. Rev. Stat. 13-3821(A)(3), a judge has the authority to make the necessary factual finding that the victim is under the age of eighteen and that Arizona's sex offender registration statutes are civil regulatory statutes, not criminal penalties. Defendant was convicted by a jury of one count of sexual abuse. In reaching its verdict the jury determined that the victim was "fifteen or more years of age." At sentencing, the trial court ordered Defendant to register as a sex offender. Defendant objected, arguing that, pursuant to Apprendi v. New Jersey, 530 U.S. 466 (2000), a jury was required to find whether Defendant was under eighteen pursuant to section 13-3821(A)(3). The trial court denied the objection. The court of appeals affirmed. The Supreme Court affirmed, holding (1) Apprendi does not apply to factual findings that are necessary to impose registration because sex offender registration is a civil regulatory requirement, not a criminal penalty; and (2) the trial judge did not violate Apprendi by determining that the victim was under eighteen.

Read Opinion Are you a lawyer? **Annotate this case**.

Barnett v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 181
Opinion Date: May 7, 2020
Judge: Hudson
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's "motion for credit for time spent in custody," holding that the

circuit court's findings were not clearly erroneous. In his motion, Appellant alleged that he was entitled to 312 days of jail-time credit and that the circuit court should enter a new sentencing order nunc pro tunc that reflected the correct amount of jail-time credit. The circuit court denied the motion. The Supreme Court affirmed, holding that the circuit court's denial of Appellant's motion was not clearly erroneous because Appellant failed to demonstrate a clerical error subject to correction.

Read Opinion Are you a lawyer? **Annotate this case**.

Mason v. Kelley

Court: Arkansas Supreme Court
Citation: 2020 Ark. 182
Opinion Date: May 7, 2020
Judge: Rhonda K. Wood
Areas of Law: Criminal Law

The Supreme Court affirmed the order of the circuit court dismissing Appellant's pro se petition for writ of habeas corpus, holding that Appellant stated no ground on which the writ could issue. Appellant was convicted of aggravated robbery, theft of property, and second-degree battery and sentenced as a habitual offender to an aggregate term of 660 months' imprisonment. The court of appeals affirmed. Appellant later petitioned for writ of habeas corpus, asserting that the trial court misapplied Arkansas's habitual-offender statutes. The circuit court dismissed the petition. The Supreme Court affirmed, holding that the issues Appellant raised in his petition for the writ should have been raised at trial, on direct appeal, or in a petition for postconviction relief.

Read Opinion Are you a lawyer? **Annotate this case**.

Ray v. Kelley

Court: Arkansas Supreme Court
Citation: 2020 Ark. 184
Opinion Date: May 7, 2020
Judge: Wynne
Areas of Law: Criminal Law

The Supreme Court dismissed Appellant's appeal from an order denying his pro se petition for permission to reinvest jurisdiction in the trial court to consider a petition for writ of error coram nobis, holding that the circuit court had no jurisdiction to consider the petition. Appellant entered negotiated guilty pleas to rape and other offenses. Appellant later filed a petition for writ of error coram nobis in the Chicot County Circuit Court, the court where he was incarcerated, setting out two grounds for coram nobis relief. The circuit court denied the petition. The Supreme Court dismissed Appellant's appeal, holding that jurisdiction lay in the trial court where Appellant was convicted, which in this case was the Ashley County Circuit Court. Therefore, the Chicot County Circuit Court was without jurisdiction to address Appellant's coram nobis petition.

Read Opinion Are you a lawyer? **Annotate this case**.

Walker v. Kelley

Court: Arkansas Supreme Court
Citation: 2020 Ark. 183
Opinion Date: May 7, 2020
Judge: Rhonda K. Wood
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's pro se petition for declaratory judgment, holding that Appellant could not use a declaratory-judgment action to collaterally attack his criminal conviction. Appellant was convicted of first-degree murder and second-degree unlawful discharge of a firearm from a vehicle. The court of appeals affirmed. Years later, Appellant filed a petition for declaratory judgment alleging that he was denied due process in his criminal trial when the court admitted the prior testimony of an unavailable witness and that this admission violated the Confrontation Clause. The circuit court denied the petition. The Supreme Court affirmed, holding that a declaratory judgment action provided no relief on these grounds.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Flores

Court: Supreme Court of California
Docket: S116307
Opinion Date: May 4, 2020
Judge: Kruger
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction of three counts of first degree murder and his sentence of death, holding that the three or four minor errors at Defendant's trial were harmless and did not interfere with his due process right to a fair trial. Specifically, the Supreme Court held (1) no error occurred during jury selection; (2) Defendant was not prejudiced by any misstatements by the prosecutor; (3) assuming certain evidence was inadmissible, the court's admonition to the jury and the court's instruction cured the resultant harm; (4) the trial court erred in admitting testimony that the victim was afraid of Defendant, but the error was harmless; and (5) Defendant's remaining allegations of error were without merit.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. Law

Court: California Courts of Appeal
Docket: E072845(Fourth Appellate District)
Opinion Date: May 5, 2020
Judge: Slough
Areas of Law: Constitutional Law, Criminal Law

In 2001, appellant Terrell Law and his codefendant Brett May committed a home invasion robbery, during which one of them shot and killed one of the residents. They were tried jointly in 2006 before two separately empaneled juries who found them both guilty of first degree felony murder with the special circumstance described in Penal Code section 190.2(a)(17(A) and (d). Though Law's jury found he was not the shooter, they nonetheless concluded he was a "major participant" in the underlying robbery and acted "with reckless indifference to human life." In 2018, the Legislature enacted Senate Bill No. 1437 (2017-2018 Reg. Sess.) which, among other things, amended the definition of felony murder in Penal Code section 189. The legislation also added Penal Code section 1170.95, which established a procedure for vacating murder convictions predating the amendment that could not be sustained under the new definition of felony murder. Law

challenged the trial court's summary denial of his section 1170.95 petition to vacate his murder conviction, arguing the trial court erred by reviewing his record of conviction and determining the jury's true finding on the special circumstance rendered him ineligible for relief. The Court of Appeal concluded it was proper for a trial court to review the record of conviction when determining whether a section 1170.95 petitioner had stated a prima facie claim for relief. Additionally, the Court concluded Law "undoubtedly qualifies" as a major participant who acted with reckless indifference to human life, a conclusion that rendered him ineligible for relief under section 1170.95. The Court therefore affirmed the order denying his petition.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. Sanchez

Court: California Courts of Appeal
Docket: E072647(Fourth Appellate District)
Opinion Date: May 7, 2020
Judge: Menetrez
Areas of Law: Constitutional Law, Criminal Law

Victor Sanchez was charged with first degree murder, but pled guilty to voluntary manslaughter. He filed a petition under Penal Code section 1170.95 to vacate that conviction. The trial court denied the petition, concluding that Sanchez was ineligible for relief because he was not convicted of murder. After review, the Court of Appeal joined other courts that held section 1170.95 did not apply to defendants convicted of voluntary manslaughter. The Court also rejected Sanchez's argument that section 1170.95 violated equal protection.

Read Opinion Are you a lawyer? **Annotate this case**.

Galeotti v. International Union of Operating Engineers

Court: California Courts of Appeal
Docket: A157785(First Appellate District)
Opinion Date: May 6, 2020
Judge: Henry E. Needham, Jr.
Areas of Law: Criminal Law, Labor & Employment Law, White Collar Crime

Galeotti, a former Union Local 3 employee, filed a complaint against Local 3 and three of individual union leaders, alleging that the individual defendants required union employees to pay them money to keep their jobs, lied about the reason for collecting the money, and caused Local 3 to terminate Galeotti's employment when he failed to pay the full amount demanded. The trial court dismissed his second amended complaint without leave to amend. The court of appeal reversed in part, reasoning that a threat to terminate employment can provide a basis for an extortion claim and that the allegations of the second amended complaint stated a cause of action for wrongful termination in violation of the public policy underlying the extortion statutes. The complaint stated a cause of action for violations of the Racketeer Influenced and Corrupt Organizations Act (RICO; 18 U.S.C. 1961), based on the predicate acts of extortion, but did not state a cause of action for interference with prospective economic advantage.

Read Opinion Are you a lawyer? **Annotate this case**.

In re I.A.

Court: California Courts of Appeal
Docket: B296549(Second Appellate District)
Opinion Date: May 4, 2020
Judge: Tangeman
Areas of Law: Criminal Law, Juvenile Law

Where a juvenile court vacates its true finding on a generic murder allegation and redesignates it as a finding on an uncharged target offense, and does so before a minor has had the opportunity to contest the court's findings or orders, the minor may challenge the sufficiency of the evidence of the redesignated offense on appeal. The Court of Appeal held that there was insufficient evidence to support the juvenile court's decision sustaining the allegations that I.A. possessed a concealable firearm and committed vandalism. Therefore, the court reversed the juvenile court's findings, vacating the jurisdiction and disposition order and dismissing the Welfare and Institutions Code section 602 petition.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Edwards

Court: California Courts of Appeal
Docket: A158055(First Appellate District)
Opinion Date: May 1, 2020
Judge: Petrou
Areas of Law: Criminal Law

In 2006, Edwards fired an assault weapon into an apartment, killing the victim. Edwards pled guilty to possession of a firearm as a felon and was convicted of second-degree murder and shooting into an inhabited dwelling. Following the enactment of Senate Bill 1437, Edwards filed a Penal Code 1170.95 resentencing petition, checking form boxes indicating that he was convicted under a theory of felony murder or murder under the natural and probable consequences doctrine and that he could not now be convicted of 1st or 2nd-degree murder because of changes to Penal Code 188 and 189. Edwards submitted the jury instructions and the transcript of the prosecutor's closing remarks that Edwards acted with "both express malice, specific intent to kill, as well as implied malice," described as "an intentional act, the natural consequences of which are dangerous to human life, and at the time that the individual acted, they knew of the danger, and they deliberately acted with conscious disregard." The court denied the petition, finding that Edwards was convicted on a valid theory of murder that survived the statutory changes. The court of appeal affirmed. The superior court did not err in considering the record of conviction. Edwards could not meet the statutory prerequisites for even filing a section 1170.95 petition because he was not charged or convicted of second-degree felony murder or murder under the natural or probable consequences doctrine directed at accomplice liability.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Thomkins

Court: California Courts of Appeal
Docket: A141375(First Appellate District)
Opinion Date: May 1, 2020
Judge: Streeter
Areas of Law: Criminal Law

On Easter night in 2011, gunfire erupted at an Oakland bar-restaurant, leaving two people dead and five wounded. Thompkins and Fox were convicted of two counts of first-degree murder for the benefit of a criminal street gang, with firearm discharge enhancements, a multiple-murder special circumstance, and five counts of attempted murder with great bodily injury findings, gang enhancements, and firearm discharge enhancements. Thompkins was convicted as the shooter and Fox as an accomplice. Both were sentenced to life in prison without possibility of parole, plus 224 years to life. After Thompkins was sentenced, Fox stated under oath he was the actual shooter and Thompkins knew nothing about Fox's intentions. Thompkins claimed this new testimony, and his attorney's incompetent reaction entitled him to a new trial and submitted a declaration by another gang member who was present that night. The court of appeal concluded that Thompkins's attorney was not ineffective for failing to bring a motion to recall the sentence followed by a new trial motion because Thompkins failed to show prejudice. The attempted murder convictions and related enhancements must be reversed for both defendants based on the flawed kill zone instruction. Introducing evidence that defendants admitted their gang affiliation at jail intake violated the defendants' privilege against self-incrimination but was harmless. There was some evidentiary error that was harmless due to the wealth of admissible evidence establishing the gang enhancements. Arguments based on the statutory amendments to Penal Code 188 and 189 must be raised in the trial court (section 1170.95). The case must be remanded so the judge may exercise his discretion whether to impose or strike the firearm enhancements on under Penal Code 12022.53.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Torres

Court: California Courts of Appeal
Docket: B295043(Second Appellate District)
Opinion Date: May 4, 2020
Judge: Wiley
Areas of Law: Criminal Law

After the trial court admitted a witness's former testimony, the Court of Appeal applied People v. Roldan (2012) 205 Cal.App.4th 969, 975–985, and reversed. Roldan held that, before invoking the former testimony exception,

prosecutors should react appropriately to the impending deportation risk by following four steps: alert the defense to the risk; videotape the preliminary hearing testimony; use judicial measures to try to delay deportation; and consider an array of other specific measures. In this case, the prosecution conceded that prosecutors were simply unaware of Roldan and did not comply with it. The court held that Roldan controls the court's analysis because the facts about prosecutorial diligence are weaker here than they were in Roldan, where the appellate court held for the defense. In this case, the record before deportation is of prosecutorial inaction where the prosecution's brief in this court admits the investigating officer did not do anything to ensure that the witness would not be deported, nor is there other evidence of prosecutorial efforts to delay the witness's departure or to videotape his testimony at the preliminary hearing.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Triplett

Court: California Courts of Appeal
Docket: B298914(Second Appellate District)
Opinion Date: May 1, 2020
Judge: Frances Rothschild
Areas of Law: Criminal Law

Defendant was convicted of assault with a deadly weapon, carjacking, and attempted murder. In the published portion of the opinion, the Court of Appeal held that the trial court erred by denying defense counsel's request to inform the jurors that they could have testimony of certain witnesses read back to them. The court also held that, under the circumstances in this case, the error was harmless.

Read Opinion Are you a lawyer? **Annotate this case**.

Colorado In Interest of G.S.S.

Court: Colorado Supreme Court
Citation: 2020 CO 32
Opinion Date: May 4, 2020
Judge: Brian D. Boatright

Areas of Law: Constitutional Law, Criminal Law, Juvenile Law

After being charged, fourteen-year-old G.S.S. was detained for more than three months without bail, even though he had not entered a plea and had not been tried on the charges against him. At that point, G.S.S.'s counsel filed a motion to dismiss, arguing that G.S.S.'s "right to a speedy trial" had been violated under section 19-2-509(4)(b), C.R.S. (2019). The trial court agreed and dismissed the case against G.S.S. with prejudice, and the court of appeals affirmed in Colorado in Interest of G.S.S., 2019 COA 4M, __ P.3d __. The Colorado Supreme Court then granted certiorari to determine the proper remedy for a violation of the sixty-day limit in section 19-2-509(4)(b). The Supreme Court determined the remedy for a section 19-2-509(4)(b) violation was for the trial court to immediately hold a bail hearing and order the juvenile's release. Accordingly, the judgment of the court of appeals was reversed.

Read Opinion Are you a lawyer? **Annotate this case**.

Barringer v. Halkitis

Court: Florida Supreme Court
Docket: SC19-1071
Opinion Date: May 7, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court held that Jay Barringer's quo warranto petition filed in this case was a frivolous proceeding brought before the Supreme Court by a state prisoner and sanctioned Barringer by barring him from filing any further pro se requests for relief related to his criminal case. Barringer was convicted of one count of attempted sexual battery of a victim less than twelve years old and sentenced to twenty-five-years' imprisonment. In 2011, Barringer began filing petitions in the Supreme Court. The Court did not grant the relief sought in any of Barringer's filings. In the instant quo warranto petition Barringer challenged his conviction on the ground that the information was defective, a claim Barringer previously raised by way of a habeas petition. The Supreme Court denied the petition and found that Barringer abused the Court's limited judicial resources. The Court sanctioned Barringer by directing the Clerk of Court to reject any future

pleadings or other requests for relief submitted by Barringer that are related to his criminal case, unless such filings are signed by a member of The Florida Bar in good standing.

Read Opinion Are you a lawyer? **Annotate this case**.

Franqui v. State

Court: Florida Supreme Court
Docket: SC19-203
Opinion Date: May 7, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the order of the circuit court denying Appellant's claim of intellectual disability, raised in successive motions for postconviction relief under Fla. R. Crim. P. 3.851, holding that the circuit court did not err in denying relief. Appellant was convicted of first-degree murder and sentenced to death in two separate cases. After the United States Supreme Court decided Hall v. Florida, 572 U.S. 701 (2014), Appellant filed successive motions for postconviction relief in both of his capital cases, asserting that the circuit court's denials of his previous claims of intellectual disability were based on the court's improper interpretation of Florida's intellectual disability statute. The circuit court summarily denied the motions. The Supreme Court reversed and remanded for an evidentiary hearing on the issue of intellectual disability. After a hearing, the circuit court denied the claim. The Supreme Court affirmed, holding (1) the circuit court did not err in denying Appellant's intellectual disability claim; and (2) Appellant was not entitled to relief under Hurst v. Florida, 136 S. Ct. 616 (2016), or Hurst v. State, 202 So. 3d 40 (Fla. 2016).

Read Opinion Are you a lawyer? **Annotate this case**.

Hicks v. State

Court: Florida Supreme Court
Docket: SC19-1978
Opinion Date: May 7, 2020
Judge: Per Curiam

Areas of Law: Criminal Law

The Supreme Court denied the instant mandamus petition filed by Hicks and sanctioned Hicks by barring him from filing any further pro se requests for relief related to his criminal case. Hicks was convicted of one count of lewd and lascivious conduct by a person over eighteen years of age on a victim under sixteen years of age. Since 2016, Hicks filed thirteen pro se requests for relief in the Supreme Court related to his criminal case. The Court did not grant the relief sought in any of Hicks' filings. In the instant petition, Hicks sought a writ of mandamus compelling the circuit court to comply with the requirements of Fla. R. Crim. P. 3.850 by filing a copy of an order denying his second postconviction motion with the clerk of court. The Supreme Court dismissed the petition and found that Hicks abused this Court's limited judicial resources. The Court directed the Clerk of Court to reject any future pleadings or other requests for relief submitted by Hicks that are related to his criminal case, unless such filings are signed by a member of The Florida Bar in good standing.

Read Opinion Are you a lawyer? **Annotate this case**.

Burley v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0356
Opinion Date: May 4, 2020
Judge: Boggs
Areas of Law: Constitutional Law, Criminal Law

In 1992, Douglas Burley pled guilty to malice murder. He moved for an out-of-time appeal in 2019, claiming that his right to appeal was frustrated by his plea counsel's erroneous advice that he could not appeal his conviction because it was the product of a guilty plea. The trial court denied Burley's motion. After review, the Georgia Supreme Court vacated the trial court's judgment and remanded the case with direction to hold a hearing to determine whether ineffective assistance of counsel frustrated Burley's right to appeal.

Read Opinion Are you a lawyer? **Annotate this case**.

Carter v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0022
Opinion Date: May 4, 2020
Judge: David E. Nahmias
Areas of Law: Construction Law, Criminal Law

Brandon Carter was convicted by jury of malice murder and two firearm offenses in connection with the shooting death of Terrance Baker. On appeal, Carter contended the trial court erred by admitting certain hearsay statements into evidence and by violating his constitutional right to be present during his trial. Finding no reversible error, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Clarke v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0258
Opinion Date: May 4, 2020
Judge: Ellington
Areas of Law: Constitutional Law, Criminal Law

Rupert Clark was convicted by jury for the malice murder of his wife, Rosemarie Lebert-Clark. He was also convicted of possession of a firearm during the commission of a felony. On appeal, he argued he received ineffective assistance of trial counsel, and that the trial court erred in admitting certain evidence, violated the continuing witness rule by sending out with the deliberating jury printouts of text messages, and by failing to instruct the jury that a defendant's uncorroborated confession was not alone sufficient to warrant a conviction. Finding no reversible error after reviewing the trial court record, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Collins v. Georgia

Court: Supreme Court of Georgia

Docket: S20A0195
Opinion Date: May 4, 2020
Judge: Harold D. Melton
Areas of Law: Constitutional Law, Criminal Law

Renita Collins was tried for murder along with co-defendant Michael Stallworth. Collins appealed her convictions for murder and possession of a firearm while in commission of a felony in connection with the shooting death of Keith Jacobs. On appeal. Collins contended she was denied a fair trial due to juror misconduct, the trial court abused its discretion by not allowing her to subpoena juror testimony to show that misconduct had occurred, and the trial court abused its discretion when it failed to excuse a prospective juror for cause. Finding no reversible error, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Dawson v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0217
Opinion Date: May 4, 2020
Judge: Warren
Areas of Law: Constitutional Law, Criminal Law

Lavaris Dawson was convicted by jury of felony murder and other crimes in connection with the shooting death of Mamadou Camara. On appeal, Dawson challenged the sufficiency of the evidence supporting his convictions, and argued the trial court erred in admitting Dawson's statements to a detective during an interview because those statements were impermissibly induced by a hope of benefit, and that Dawson was denied his due process right to a timely appeal. After review, the Georgia Supreme Court disagreed and affirmed Dawson's convictions.

Read Opinion Are you a lawyer? **Annotate this case**.

Evans v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0007

Opinion Date: May 4, 2020
Judge: McMillan
Areas of Law: Constitutional Law, Criminal Law

Jimmy Evans was convicted by jury for murder and other crimes relating to the 2006 deaths of Tavoris Calhoun and Dezmon Thomas. On appeal, Evans argued that because he was visibly intoxicated at the time he made statements to law enforcement and consented to a search of his home and person, the statements and consent were involuntarily given and the trial court should have granted his motion for new trial on this ground. Furthermore, Evans argued that his trial counsel was ineffective for failing to file a motion to suppress at trial on the same basis. Because Evans failed to show error or ineffective assistance of counsel, the Georgia Supreme Court affirmed his conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Hill v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0285
Opinion Date: May 4, 2020
Judge: Harold D. Melton
Areas of Law: Constitutional Law, Criminal Law

Esco Hill was convicted by jury of malice murder and other crimes relating to the stabbing death of Alford Morris in 2014. On appeal, Hill argued the trial court committed reversible error by requiring him to be visibly shackled for the duration of his six-day trial. After review of the trial court record, the Georgia Supreme Court concurred this was reversible error, consequently, reversed judgment of conviction. Because the Court concluded the evidence at trial was sufficient to sustain Hill's conviction, the State could re-try him. The Court did not address Hill's remaining enumerations of error, "as they are not likely to recur in the event of a retrial."

Read Opinion Are you a lawyer? **Annotate this case**.

Oliver v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0489
Opinion Date: May 4, 2020
Judge: McMillan
Areas of Law: Constitutional Law, Criminal Law

Jacquan Oliver entered a negotiated plea of guilty to felony murder in connection with the shooting death of Alexander Mixon. He appealed his conviction and sentence, arguing that the trial court abused its discretion in finding a factual basis for his plea, and in determining the plea was voluntarily, knowingly and intelligently made. Finding no merit to these contentions, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Rosser v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0103
Opinion Date: May 4, 2020
Judge: Bethel
Areas of Law: Constitutional Law, Criminal Law

Larry Rosser was convicted by jury of malice murder and other crimes in connection with the death of Alexis Vereen. On appeal, Rosser challenged the sufficiency of the evidence presented against him at trial, and argued the trial court erred by not granting his motion for a mistrial, and by allowing the State to introduce a portion of Rosser's custodial statement to law enforcement. In addition, he argued he received constitutionally ineffective assistance of trial counsel. Finding no reversible error after reviewing the trial court record, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Spencer v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0871
Opinion Date: May 4, 2020
Judge: Keith R. Blackwell

Areas of Law: Constitutional Law, Criminal Law

Christopher Spencer was convicted by jury of murder and other crimes in connection with the fatal shootings of Sylvia Watson and Samuel White. Spencer appealed, claiming only that the evidence was insufficient to support his convictions. Finding no reversible error after reviewing the trial court record, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Styles v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0236
Opinion Date: May 4, 2020
Judge: Ellington
Areas of Law: Constitutional Law, Criminal Law

Derrick Styles was convicted by jury of felony murder and other crimes in connection with the shooting death of Alberto Lumens and the armed robbery fo Juan Lumens Garcia. On appeal, Styles contended the trial court erred in admitting into evidence a recording of an inculpatory telephone conversation between himself and a witness. He also argued his trial counsel was ineffective for failing to object to an allegedly improper comment by the prosecutor during closing argument. Finding no merit to these contentions, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Whitehead v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0171
Opinion Date: May 4, 2020
Judge: Ellington
Areas of Law: Constitutional Law, Criminal Law

Javis Whitehead was convicted by jury of murder and other crimes in connection with the shooting death of Dominique Larry. On appeal, Whitehead challenged the sufficiency of the evidence presented to rebut his

claim of self-defense and to convict him for murder beyond a reasonable doubt. He also argued the trial court erred in denying his motion to suppress his custodial statement, and in refusing to excuse for cause the District Attorney from the panel of prospective jurors prior to the conclusion of voir dire. Finding no merit to these contentions, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Idaho v. Blythe

Court: Idaho Supreme Court - Criminal
Docket: 46992
Opinion Date: May 4, 2020
Judge: Roger S. Burdick
Areas of Law: Constitutional Law, Criminal Law

Nicholas Blythe appealed after he was convicted of possessing a controlled substance. He conditionally pled guilty, reserving the right to challenge his sentence. On appeal, he argued the district court erred in denying his motion to suppress certain evidence found because the evidence presented at trial was found in violation of Blythe's Fourth Amendment rights. After review, the Idaho Supreme Court determined the search at issue took place before an arrest occurred, and because no rationale justifying a search incident to arrest was sufficiently present here, the search of Blythe's shoes was not a valid search incident to arrest. Therefore, the district court erred in holding that the search was reasonable under the Fourth Amendment. Blythe's conviction was vacated, the district court order denying Blythe's motion to suppress was reversed, and the matter remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

Idaho v. Glodowski

Court: Idaho Supreme Court - Criminal
Docket: 47131
Opinion Date: May 6, 2020
Judge: Roger S. Burdick

Areas of Law: Constitutional Law, Criminal Law

David Glodowski appealed after he was convicted for failing to update his sex-offender registration in violation of Idaho Code section 18-8309. He argued the district court erred by ruling that his prior conviction under a Wisconsin statute was "substantially equivalent" to Idaho statutes that required sex-offender registration in Idaho. After review, the Idaho Supreme Court determined the district court improperly allowed the State to seek a redetermination of the "substantially equivalent" element given that the Idaho Bureau of Criminal Identification made a final determination on that element. However, because the State put forth sufficient evidence to prove that element, and the district court's jury instruction accomplished the same purpose, the Supreme Court concluded the error was harmless. Accordingly, the Court found no reversible error in the district court's decision to grant the State's motion and provide the jury instruction. Therefore, judgment of conviction was affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Idaho v. Jones

Court: Idaho Supreme Court - Criminal
Docket: 45905
Opinion Date: May 4, 2020
Judge: Roger S. Burdick
Areas of Law: Constitutional Law, Criminal Law

Timothy Jones was convicted by jury of trafficking heroin and possession of drug paraphernalia. On appeal, he argued the trial court erred in admitting certain evidence regarding his probation status, a knife found in the initial police search of his person, and that the trial court abused its discretion in arriving at his sentence. Finding no reversible error, the Idaho Supreme Court affirmed Jones' conviction and sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Gordon

Court: Iowa Supreme Court

Docket: 18-1099
Opinion Date: May 1, 2020
Judge: Brent R. Appel
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction for assault on a peace officer with a dangerous weapon, a felony, and several misdemeanors, holding that Defendant did not receive ineffective assistance of counsel. After Defendant pleaded guilty, he absconded. He was later returned to custody. On appeal, Defendant argued that he received ineffective assistance of counsel because the plea bargain contained an unlawful term. Specifically, Defendant argued that the plea bargain's provision that he would be released from jail for a forty-eight-hour furlough after pleading guilty was illegal and that his trial counsel committed ineffective assistance in obtaining the illegal benefit for him. The Supreme Court affirmed, holding that where Defendant entered into the plea agreement with the illegally lenient sentence, he could not benefit from that sentence and then attack the plea bargain.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Craig

Court: Kansas Supreme Court
Docket: 119660
Opinion Date: May 1, 2020
Judge: Dan Biles
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's conviction and sentence for first-degree felony murder, holding that there was no error in the proceedings below. A jury found Defendant guilty of both first-degree felony murder and second-degree intentional murder. At sentencing, Defendant moved for a new trial and judgment notwithstanding the verdict, arguing that the jury must have had reasonable doubt on the first-degree felony murder theory because it convicted him of second-degree murder for the same killing. The district court dismissed the second-degree murder conviction and sentenced Defendant for the felony murder over his objection. The Supreme Court affirmed, holding (1) the district court did not err when it sentenced Defendant on felony murder instead of declaring a mistrial because

Defendant did not establish that the jury failed to find each element of the felony murder beyond a reasonable doubt or that the jury's first- and second-degree murder verdicts were so irreconcilable as to require a new trial; and (2) the district court did not err in declining to give an instruction on voluntary intoxication.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Lemmie

Court: Kansas Supreme Court
Docket: 119439
Opinion Date: May 1, 2020
Judge: Carol A. Beier
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's convictions of first-degree felony murder, aggravated robbery, conspiracy to commit aggravated robbery, criminal possession of a firearm, fleeing and eluding, and interference with law enforcement, holding that Defendant's arguments on appeal failed. Specifically, the Supreme Court held (1) any possible violation of Defendant's Fifth Amendment right in the admission of a witness's testimony about Defendant giving the witness phone passcodes was undoubtedly harmless; (2) the district court did not err by admitting hearsay statements as statements of a coconspirator and contemporaneous statements; (3) the State introduced sufficient evidence to convict Defendant of first-degree murder; and (4) the district judge did not abuse its discretion by admitting testimony that Defendant was upset over a meth pipe that went missing.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Mullen

Court: Maine Supreme Judicial Court
Citation: 2020 ME 56
Opinion Date: May 5, 2020
Judge: Connors
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed Defendant's conviction for reckless

conduct and aggravated criminal mischief, holding that the trial court did not abuse its discretion by offering Defendant a continuance of the trial in lieu of excluding his medical records. On appeal, Defendant argued that the trial court abused its discretion by denying his motion to suppress his personal medical records as a sanction for the State's late seizure of the records. The Supreme Judicial Court agreed that the State's conduct undermined the purpose of Maine Rule of Unified Criminal Procedure 18(b) but that the court's offer of a continuance in lieu of the exclusion of the evidence constituted an appropriate response to the State's conduct.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. Billingslea

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12715
Opinion Date: April 30, 2020
Judge: Cypher
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Judicial Court affirmed Defendant's convictions and the decision of the Appeals Court denying Defendant's motion to vacate the entry of his appeal from his convictions in that court and to have the case entered directly in the Supreme Judicial Court, holding that a direct appeal from the third conviction of a habitual offender pursuant to Mass. Gen. Laws ch. 279, 25(b) may be entered in the Appeals Court. Defendant was indicted for serious felonies arising from a brutal attack and rape. In addition to charging the specific felony, each indictment also alleged that the sentence for that felony should be enhanced pursuant to the habitual criminal provision Mass. Gen. Laws ch. 279, 25(a) or the habitual offender provision of section 25(b), or both. After he was convicted, Defendant moved to have the case entered directly in the Supreme Judicial Court. The Appeals Court denied the motion. The Supreme Judicial Court affirmed Defendant's convictions, holding (1) this direct appeal was entitled to the unique review prescribed by Mass Gen. Laws ch. 278, 33E, and the Appeals Court may conduct such section 33E review; (2) Defendant was not impermissibly allowed to waive his right to a jury trial on the sentencing enhancement provisions of the indictments; and (3) Defendant was not entitled to reversal of his convictions on any other ground.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. Martin

Court: Massachusetts Supreme Judicial Court
Docket: SJC-08768
Opinion Date: May 5, 2020
Judge: Ralph D. Gants
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Judicial Court affirmed Defendant's conviction of murder in the first degree and the denial of his motion for a new trial and declined to exercise its authority under Mass. Gen. Laws ch. 278E to reduce Defendant's conviction to murder in the second degree, holding that Defendant was not entitled to relief on any of his allegations of error. Defendant was convicted of murder in the first degree on the theory of felony-murder. Defendant filed a motion for a new trial, which was denied. The Supreme Judicial Court affirmed, holding (1) Defendant's motion for a new trial was correctly denied because Defendant was not prejudiced by counsel's ineffective assistance; (2) this Court declines to extend the reach of the Court's holding in Commonwealth v. Brown, 477 Mass. 805 (2017), to Defendant's case; and (3) trial judge erred when he declined Defendant's request that the jury be instructed on the elements of voluntary and involuntary manslaughter, but the error was not prejudicial in the context of the judge's other instructions.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. Tavares

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12631
Opinion Date: May 6, 2020
Judge: Lowy
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed Defendant's conviction of murder in the first degree on theories of deliberate premeditation and extreme atrocity

or cruelty and declined to exercise its power pursuant to Mass. Gen. Laws ch. 278, 33E to reduce the conviction to manslaughter, holding that there was no reversible error in the proceedings below. Specifically, the Supreme Judicial Court held (1) the trial judge did not err by denying Defendant's requests for a jury instruction pursuant to Commonwealth v. Croft, 345 Mass. 143 (1962); (2) the trial judge did not err by denying Defendant's motions for a required finding of not guilty under Croft because a rational jury could have found that Defendant was guilty of murder in the first degree on both the theories of premeditation and extreme atrocity or cruelty; and (3) there was no basis for reducing Defendant's sentence or ordering a new trial.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Branch

Court: Minnesota Supreme Court
Docket: A18-1055
Opinion Date: May 6, 2020
Judge: Lorie Skjerven Gildea
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's sentences for drive-by shooting at an occupied vehicle and second-degree assault, holding that Minn. Stat. 609.035 did not prohibit the sentences for both offenses when the crimes arose from a single behavioral incident. The district court sentenced Defendant to forty-eight months for drive-by shooting at an occupied vehicle and thirty-six months for second-degree assault and imposed the two sentences to run concurrently. The court of appeals affirmed. The Supreme Court affirmed, holding that, under this Court's analysis in State v. Ferguson, 808 N.W.2d 586 (Minn. 2012), the district court properly imposed multiple sentences in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

Galloway v. Mississippi

Court: Supreme Court of Mississippi
Citation: 2018-CA-01427-SCT

Opinion Date: May 7, 2020
Judge: Beam
Areas of Law: Constitutional Law, Criminal Law

Leslie Galloway appealed the denial of his 2015 petition for post-conviction relief (PCR) pertaining to his 2007 guilty plea to carjacking, a conviction that was used as an aggravating circumstance in Galloway's 2010 capital-murder trial at which Galloway received a death sentence. Galloway claimed in the petition that his defense counsel Wendy Martin had an actual conflict of interest because, before becoming his defense counsel, Martin had served as an assistant district attorney in the same case, unbeknownst to Galloway. The trial court ruled that Galloway's PCR claim was time barred under Mississippi's Uniform Post-Conviction Collateral Relief Act (UPCCRA), having been filed more than seven years after Galloway's conviction for carjacking. The trial court alternatively found no merit to Galloway's PCR claim, time bar notwithstanding. Accordingly, the trial court denied Galloway's PCR petition. The Mississippi Supreme Court agreed with the trial court that Galloway's PCR claim was time barred under the UPCCRA. The Court also agreed there was no merit to Galloway's PCR claim.

Read Opinion Are you a lawyer? **Annotate this case**.

City of Missoula v. Zerbst

Court: Montana Supreme Court
Citation: 2020 MT 108
Opinion Date: May 5, 2020
Judge: Beth Baker
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court reversed Defendant's conviction for sexual assault, holding that the municipal court erred when it instructed the jury on a definition of "consent" from the 2017 sexual assault statute and not the applicable 2015 statute, and the erroneous jury instruction prejudicially affected Defendant's substantial rights. At trial, the court instructed the jury, over Defendant's objection, on the definition of consent contained in recent amendments to the sexual assault statute. On appeal, Defendant argued that the municipal court failed to apply the correct law when instructing the jury on the elements of the claimed offense. The district court denied the

appeal. The Supreme Court reversed, holding (1) the instructions, as a whole, did not fully and fairly instruct the jury on the law applicable to the case; and (2) Defendant's substantial due process right was prejudiced by the erroneous jury instruction.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Degarmo

Court: Nebraska Supreme Court
Citation: 305 Neb. 680
Opinion Date: May 1, 2020
Judge: Stacy
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction of driving under the influence, holding that Defendant consented to a chemical test of his urine and, therefore, the results of the urine test were admissible. A law enforcement officer stopped Defendant for an expired registration. Based on his observations, the officer, a certified drug recognition evaluation expert, administered field sobriety tests. The officer concluded that Defendant was under the influence of marijuana arrested Defendant for driving under the influence and then took him to a detoxification center. Thereafter, a chemical test of Defendant's urine confirmed the presence of marijuana. On appeal, Defendant challenged the admission of the results of the urine test. The Supreme Court affirmed, holding that Defendant voluntarily consented to the warrantless search of his urine, and therefore, the search fell within a recognized exception to the warrant requirement.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Holz

Court: New York Court of Appeals
Citation: 2020 NY Slip Op 02682
Opinion Date: May 7, 2020
Judge: Fahey
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Court of Appeals held that N.Y. Crim. Proc. Law (CPL) 710.70(2) grants a defendant the right to review of a suppression decision when the order related exclusively to a count that was satisfied by a guilty plea but was not one to which the defendant pleaded guilty. Defendant was charged with two counts of burglary in the second degree. The first count related to a laptop computer, and the second count related to jewelry. Defendant moved to suppress the jewelry, but Supreme Court denied the motion. Defendant then pleaded guilty to one count of burglary in the second degree as charged in the count pertaining to the theft of the laptop computer, in satisfaction of the count charging the burglary of jewelry. On appeal, Defendant argued that Supreme Court erred in denying his motion to suppress the jewelry. The Appellate Division affirmed, concluding that it was jurisdictionally precluded from reviewing the suppression order. The Court of Appeals reversed, holding (1) Defendant's right to appellate review of Supreme Court's suppression order was secured by CPL 710.70(2); and (2) because the Appellate Division did not reach the underlying suppression question the case must be remitted to the Appellate Division for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Maffei
Court: New York Court of Appeals
Citation: 2020 NY Slip Op 02680
Opinion Date: May 7, 2020
Judge: DiFiore
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Court of Appeals affirmed the order of the Appellate Division concluding on direct appeal that Defendant was not entitled to relief on his ineffective assistance of counsel claim, holding that Defendant, on this record, did not sustain his burden to establish that counsel was constitutionally ineffective. After a jury trial, Defendant was convicted of second-degree murder. On appeal, Defendant argued that his trial counsel's failure to challenge a prospective juror constituted ineffective assistance of counsel. The Appellate Division affirmed. The Court of Appeals affirmed, holding (1) the record was inadequate to review Defendant's ineffective assistance of counsel claim; and (2) the appropriate procedure for the litigation of Defendant's challenge to his counsel's performance was a N.Y. Crim. Proc.

Law 440.10 motion.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Bailey

Court: North Carolina Supreme Court
Docket: 360A19
Opinion Date: May 1, 2020
Judge: Davis
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the decision of the court of appeals affirming the order of the trial court denying Defendant's motion to suppress evidence seized during the execution of a search warrant, holding that the warrant supported by probable cause. Defendant pled guilty to the offense of trafficking in cocaine while preserving his right to appeal the denial of his motion to suppress. On appeal, Defendant argued that the trial court erred in denying his motion to suppress because the facts contained in the affidavit were insufficient to establish probable cause to search his residence. The court of appeals affirmed. The Supreme Court affirmed, holding that the affidavit contained facts that were sufficient to provide a nexus between the residence and suspected criminal activity, and therefore, the warrant was supported by probable cause.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Ellis

Court: North Carolina Supreme Court
Docket: 340A19
Opinion Date: May 1, 2020
Judge: Robin E. Hudson
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court reversed the decision of the Court of Appeals affirming the trial court's denial of Defendant's motion to suppress evidence, holding that there was no reasonable suspicion to justify the law enforcement officer's stop when Defendant signaled with his middle finger from the passenger side window of a moving vehicle. While assisting a stranded

motorist, the officer turned his attention to another car traveling on the roadway, a white SUV. Defendant had his arm outside the passenger window and gestured with his middle finger, making an up-and-down motion. Believing that Defendant was committing the crime of disorderly conduct, the officer pursued and then stopped the SUV. At trial, Defendant moved to suppress the officer's testimony, arguing that there was no reasonable suspicion to justify the stop. The trial court denied the motion. Defendant pleaded guilty to resisting, delaying, or obstructing a public officer. The court of appeals affirmed the trial court's denial of Defendant's motion to suppress. The Supreme Court reversed, holding that the specific, articulable facts did not establish reasonable suspicion of the crime of disorderly conduct.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Hobbs

Court: North Carolina Supreme Court
Docket: 263PA18
Opinion Date: May 1, 2020
Judge: Earls
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court reversed Defendant's conviction, holding that the trial court clearly erred in ruling that Defendant failed to prove purposeful discrimination with respect to the State's use of peremptory challenges to strike three jurors without considering all of the evidence presented by Defendant. Defendant was found guilty of one count of first-degree murder and other crimes. On appeal, Defendant argued that the trial court erred by failing to grant three objections that he made under Batson v. Kentucky, 476 U.S. 79 (1986). The court of appeals affirmed Defendant's convictions. The Supreme Court reversed, holding (1) the court of appeals erred in its analysis of Defendant's Batson claims with respect to the three jurors; and (2) as to all three jurors, remand was required for reconsideration of whether Defendant proved purposeful discrimination in each case.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Mylett

Court: North Carolina Supreme Court
Docket: 6A19
Opinion Date: May 1, 2020
Judge: Earls
Areas of Law: Criminal Law

The Supreme Court reversed the decision of the court of appeals affirming the trial court's judgment convicting Defendant for conspiracy to commit harassment of a juror, holding that the trial court erred in denying Defendant's motion to dismiss the conspiracy charge for insufficient evidence. Defendant was convicted of conspiracy to commit harassment of a juror because of his actions at a courthouse following his twin brother's conviction for assault on a government official. On appeal, the court of appeals concluded that the trial court did not err in denying Defendant's motion to dismiss the conspiracy charge for insufficient evidence. The Supreme Court reversed, holding that the evidence in Defendant's trial was insufficient to raise anything more than mere conjecture that he had made an agreement with another person to threaten or intimidate a juror.

Read Opinion Are you a lawyer? **Annotate this case**.

Dodge v. North Dakota

Court: North Dakota Supreme Court
Citation: 2020 ND 100
Opinion Date: May 7, 2020
Judge: Gerald W. VandeWalle
Areas of Law: Constitutional Law, Criminal Law

Richard Dodge appealed from a district court order denying his application for post-conviction relief. Dodge was charged with five felonies and a misdemeanor in December 2015. Dodge was appointed counsel. In April 2016, Dodge’s counsel moved the court to withdraw because the attorney-client relationship was “irreparably broken and rendered unreasonably difficult.” The court granted the motion, and Dodge was appointed substitute counsel in May 2016. In July 2016, Dodge himself filed a “motion to dismiss counsel.” The court denied Dodge’s motion. Five months after the deadline for motions and plea agreements, Dodge's counsel sought to have Dodge submit to a psychiatric examination. This request was denied, the trial court

found no evidence, and the the court itself made no observations, that Dodge was incompetent to stand trial. After this denial, Dodge himself again moved to dismiss his trial counsel, and due to the allegations Dodge made in his motion, counsel moved to withdraw. The trial court denied both motions, and instead, required the attorney to appear as standby counsel and assist Dodge during trial if requested, but relieved him of any further obligations to consult with Dodge. The case proceeded to trial. At the beginning of trial, the court gave Dodge the option of representing himself or having his attorney represent him. Dodge chose to have his attorney represent him. Because his attorney had not prepared for trial and had no communication with Dodge since he moved to withdraw, Dodge's attorney asked for a brief recess to consult with Dodge. During the recess, a settlement was reached. Dodge agreed to enter Alford pleas on all counts, waived a presentence investigation, and agreed to be sentenced immediately after entering his pleas. Dodge was immediately sentenced following his guilty pleas, and thereafter sought post-conviction relief on grounds he was not competent to enter his pleas, and that he received ineffective assistance of trial counsel. After review, the North Dakota Supreme Court concluded the district court's finding that Dodge was competent when he entered his pleas was not clearly erroneous, and disposed of his claim of ineffective assistance of counsel.

Read Opinion Are you a lawyer? **Annotate this case**.

Hewitt v. NDDOT

Court: North Dakota Supreme Court
Citation: 2020 ND 102
Opinion Date: May 7, 2020
Judge: Lisa K. Fair McEvers
Areas of Law: Criminal Law, Government & Administrative Law

Larry Hewitt appealed a district court judgment affirming the North Dakota Department of Transportation's revocation of his driving privileges. Hewitt claimed the Department's hearing file was improperly admitted at the administrative hearing. After review, the North Dakota Supreme Court affirmed, concluding the hearing file was properly admitted as a self-authenticating copy of an official record.

Read Opinion Are you a lawyer? **Annotate this case**.

Kastet v. NDDOT

Court: North Dakota Supreme Court
Citation: 2020 ND 91
Opinion Date: May 7, 2020
Judge: Daniel J. Crothers
Areas of Law: Criminal Law, Government & Administrative Law

The North Dakota Department of Transportation (Department) appealed the district court's reversing a hearing officer's decision suspending Holden Kastet's driving privileges for 365 days. The Department argued the hearing officer did not abuse his discretion in admitting the chemical breath test, and State Highway Patrol Trooper King scrupulously complied with the approved method for testing Kastet's breath on the Intoxilyzer 8000. After review, the North Dakota Supreme Court concurred with the Department and reversed the district court judgment. The matter was remanded with instructions to reinstate the hearing officer's decision.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Dahl

Court: North Dakota Supreme Court
Citation: 2020 ND 87
Opinion Date: May 7, 2020
Judge: Jerod E. Tufte
Areas of Law: Constitutional Law, Criminal Law

The State of North Dakota appealed a district court order denying its motion to resume prosecution against Matthew Dahl and dismissing the case. In December 2014, the State charged Dahl with two counts of theft. Dahl did not appear on the charges until he was arrested on a bench warrant in February 2017. In mid-April 2017, the State mailed Dahl a pretrial diversion agreement. Dahl signed and returned the notarized agreement dated May 3, 2017. On May 9, 2017, the state's attorney signed and filed the agreement with the district court, and the court approved the agreement the same day. Under the agreement, the State agreed to suspend prosecution for "two

years from the date of execution" conditioned on Dahl's timely payment of restitution. Dahl failed to make minimum monthly restitution payments. On June 6, 2019, the State moved to resume prosecution, alleging Dahl violated the pretrial diversion agreement by his non-payment. The district court held a hearing on the State's motion in August 2019. The court concluded the pretrial agreement was executed when Dahl signed it on May 3, 2017. The court then denied the State's motion to resume prosecution as untimely under N.D.R.Crim.P. 32.2(d)(2), and dismissed the complaint against Dahl. After review, the North Dakota Supreme Court reversed, concluding the district court erred in determining the State's motion was untimely, and remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Foster

Court: North Dakota Supreme Court
Citation: 2020 ND 85
Opinion Date: May 7, 2020
Judge: Jon J. Jensen
Areas of Law: Constitutional Law, Criminal Law

Akeem Foster was convicted by jury of Terrorizing and Carrying a Concealed Weapon. Foster contended on appeal he was denied a fair trial because he was asked during cross-examination if other witnesses were lying and because the prosecutor expressed personal beliefs about the evidence during closing arguments. Foster also argued there was insufficient evidence to convict him of either charge. After review, the North Dakota Supreme Court affirmed Foster's conviction for Carrying a Concealed Weapon, but reversed his conviction for Terrorizing. The Court found Foster was improperly asked to provide an opinion on the veracity and credibility of the State's witnesses. The improper questioning was prejudicial and denied Foster a fair trial on the terrorizing charge.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Kolstad

Court: North Dakota Supreme Court

Citation: 2020 ND 97
Opinion Date: May 7, 2020
Judge: Gerald W. VandeWalle
Areas of Law: Constitutional Law, Criminal Law

In December 2018, Officer Nelson of the University of North Dakota Police Department conducted a traffic stop of Stanley Kolstad for suspicion of driving under the influence. Kolstad performed field sobriety tests and a preliminary breath test (PBT). Prior to performing the PBT, Kolstad informed Nelson that he had asthma. Nelson testified he was unable to obtain a PBT result because Kolstad was filling his cheeks with air while performing the test. Kolstad was arrested for DUI and refusing to submit to a chemical test. Kolstad was transported to the UND police station to be given an Intoxilyzer breath test. Prior to the Intoxilyzer test, Nelson read Kolstad the implied consent advisory. But, because Nelson was not a certified operator of the Intoxilyzer machine, Officer Waltz conducted the test. Prior to the test, Kolstad informed Waltz he had asthma. The Intoxilyzer test results were deficient. Waltz testified Kolstad was not providing enough air for the test machine to provide a valid result. Kolstad was charged with driving under the influence and refusing to submit to a chemical test. Kolstad's counsel made a discovery request to the State seeking copies of any audio or video recordings taken by police officers. Kolstad's counsel also requested the State inform him whether any sound or video recordings taken of Kolstad were subsequently "altered, edited, destroyed, or discarded." The State provided Kolstad's counsel with dash camera footage from Nelson's police car that had been taken at the scene of the arrest, but the State did not provide any body camera footage from either Nelson or Waltz. Upon learning that Waltz's body camera footage was successfully uploaded to UND servers, Kolstad's counsel moved to dismiss the case because the State did not provide any body camera footage in discovery as requested. The district court ultimately dismissed the refusal to submit to a chemical breath test charge as a sanction for failing to provide the body camera footage. The State appealed, arguing the alleged discovery violation did not rise to a constitutional violation of Kolstad's due process rights, and the district court abused its discretion in dismissing the refusal charge. Kolstad argued the district court's order dismissing the refusal charge was not appealable, and if it was, the court did not abuse its discretion in dismissing the charge. The North Dakota Supreme Court concluded there was nothing in the record to indicate the district court adequately considered an

alternative or less severe sanction to dismissal, and by not considering a less severe sanction, the trial court erred. The district court's order dismissing the refusal charge was reversed, and the matter remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Michel

Court: North Dakota Supreme Court
Citation: 2020 ND 101
Opinion Date: May 7, 2020
Judge: Jerod E. Tufte
Areas of Law: Constitutional Law, Criminal Law

Kevin Michel was convicted by jury of knowingly receiving stolen property. Jamestown Police began investigating theft of tires from Northwest Tire in October 2017. About ten months later, Thomas Melland and Andrew Heckelsmiller became suspects in the investigation. Heckelsmiller told police he had sold stolen tires to Michel. In August 2018, Detective LeRoy Gross spoke with Michel about the stolen tires. Michel acknowledged he had bought tires from Heckelsmiller and Melland. Michel also told Detective Gross he stopped buying tires from Heckelsmiller and Melland after seeing a Facebook post from Northwest Tire offering a $500 reward for information regarding stolen tires. Detective Gross told Michel, "There's going to be a lot of restitution these two boys are going to have to come up with unless we can get some tires back." Michel said he had sold several of the tires but still had some of them. Michel turned over seven new tires to Detective Gross. Representatives from Northwest Tire and J&L Service identified the tires as some of those stolen from their shops. During the jury's deliberations, the jury submitted a note with written questions to the court. Michel argued on appeal the district court erred by not specifically answering the jury's questions and instead referring them to the existing jury instructions. After review, the North Dakota Supreme Court affirmed the criminal judgment, except as to the award of restitution. The award was reversed because the district court awarded more than what was required to make the victims whole. The matter was remanded for a redetermination of restitution.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Wayland

Court: North Dakota Supreme Court
Citation: 2020 ND 106
Opinion Date: May 7, 2020
Judge: Jon J. Jensen
Areas of Law: Constitutional Law, Criminal Law

Joey Wayland appealed after he was convicted by jury of Theft of Property and Possession of Drug Paraphernalia. Wayland contended his case should have been dismissed because his right to a speedy trial was violated by a continuance of his trial from March 11, 2019 to April 8, 2019. Wayland also contended the district court violated his right to remain silent by ordering him to submit to a mental health evaluation. Finding no reversible error, the North Dakota Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Schwindt v. Sorel

Court: North Dakota Supreme Court
Citation: 2020 ND 92
Opinion Date: May 7, 2020
Judge: Lisa K. Fair McEvers
Areas of Law: Constitutional Law, Criminal Law, Government & Administrative Law

Gregory Schwindt appealed a district court judgment affirming a Department of Transportation hearing officer's revocation of his driving privileges for 180 days. Schwindt argued North Dakota's implied consent and refusal laws were unconstitutional, the hearing officer erred by considering the results of the horizontal gaze nystagmus (HGN) test, and the hearing officer erred in finding he refused to take a chemical test. After review, the North Dakota Supreme Court concluded the hearing officer's findings of fact were supported by a preponderance of the evidence, the conclusions of law were sustained by the findings of fact, and the decision to revoke Schwindt's driving privileges was in accordance with the law.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. McDougald v. Greene

Court: Supreme Court of Ohio
Citation: 2020-Ohio-2782
Opinion Date: May 6, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court denied a writ of mandamus sought by Relator to compel Respondent, the public-records custodian at the Southern Ohio Correctional Facility (SOCF), to provide Relator with three public records and to pay Relator statutory damages and court costs associated with this litigation, holding that Relator was not entitled to either a writ of mandamus nor statutory damages. When Relator was an inmate at SOCF he submitted a public-records request to Respondent seeking three documents. Respondent provided one of the three documents. Relator then filed a complaint for a writ of mandamus seeking an order compelling Respondent to provide the two documents and to pay statutory damages and court costs associated with this litigation. The Supreme Court denied the writ of mandamus on the merits, holding that Respondent's response to Relator fully satisfied Respondent's obligations under Ohio Rev. Code 149.43, and therefore, Relator was not entitled a writ of mandamus, and there was no basis to award statutory damages.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Parker Bey v. Byrd

Court: Supreme Court of Ohio
Citation: 2020-Ohio-2766
Opinion Date: May 5, 2020
Judge: Maureen O'Connor
Areas of Law: Criminal Law

The Supreme Court affirmed in part and reversed in part the judgment of the court of appeals denying Appellant's complaint for a writ of mandamus to compel the Cuyahoga County Clerk of Courts to produce various court records and denying the clerk's request that Appellant be declared a vexatious litigator, holding that the court of appeals erred in denying Appellant's complaint on the grounds that he did not invoke the Rules of

Superintendence as the basis for his request. Appellant sought copies of journal entries from his criminal case and a copy of the clerk of courts' records-retention schedule. The clerk largely denied the request. Appellant then filed a complaint for a writ of mandamus. The court of appeals denied Appellant's request for mandamus relief, concluding that the clerk had no clear legal duty to provide the requested records. The Supreme Court reversed, holding (1) this action to compel the production of journal entries from a 1995 case was properly brought under the Public Records Act; and (2) this Court declines to impose sanctions on Appellant or to declare him a vexatious litigator.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Dangler

Court: Supreme Court of Ohio
Citation: 2020-Ohio-2765
Opinion Date: May 5, 2020
Judge: DeWine
Areas of Law: Criminal Law

The Supreme Court reversed the judgment of the court of appeals vacating Defendant's conviction and sentence and reinstated the trial court's acceptance of Defendant's plea of no contest to sexual battery, holding that the trial court did not completely fail to comply with Crim.R.11(C)(2)(a), and there was nothing in the record to support a conclusion that Defendant would not have entered his plea had the trial court been more detailed in its explanation. On appeal, Defendant sought to vacate his plea of no contest, arguing that his plea was invalid because the trial court erred by not explaining more fully the obligations and restrictions that went with his status as a sex offender, in violation of Crim. R. 11(C)(2)(a). The court of appeals vacated the conviction without requiring Defendant to show prejudice, concluding that the trial court had completely failed to comply with Crim. R. 11(C)(2)(a). The Supreme Court reversed, holding (1) the trial court did not completely failed to comply with Crim R. 11(C)(2)(a)'s maximum-penalty-advisement requirement; and (2) because Defendant did not establish prejudice, he was not entitled to have his no-contest plea vacated for a failure to comply with Crim.R. 11(C).

Read Opinion Are you a lawyer? **Annotate this case**.

Oregon v. Haji

Court: Oregon Supreme Court
Docket: S066254
Opinion Date: May 7, 2020
Judge: Nakamoto
Areas of Law: Constitutional Law, Criminal Law

After a grand jury issued an indictment charging defendant Hanad Ali Haji with multiple offenses, the district attorney determined that the indictment could be challenged by demurrer because the basis for joining those offenses was not expressly alleged. Instead of seeking another indictment from the grand jury, the district attorney obtained leave from the trial court to amend the indictment by adding allegations specifying the statutory basis for joinder, without adding factual allegations about the crimes. Defendant was convicted on some of the charges at trial, and the Court of Appeals affirmed. The issue this case presented for the Oregon Supreme Court's review centered on whether the district attorney could add allegations specifying the statutory basis for joinder of multiple offenses to an indictment instead of resubmitting the case to the grand jury. The Supreme Court determined that neither the statute permitting joinder of multiple offenses in a single indictment nor Article VII (Amended), section 5(6), of the Oregon Constitution precluded a district attorney, with approval of the trial court, from amending an indictment to add allegations specifying the statutory basis for joinder of multiple offenses. The Supreme Court affirmed the decision of the Court of Appeals, based in part on different reasoning, and affirmed the judgment of the circuit court.

Read Opinion Are you a lawyer? **Annotate this case**.

South Carolina v. Durant

Court: South Carolina Supreme Court
Docket: 27964
Opinion Date: May 6, 2020
Judge: Kaye Gorenflo Hearn
Areas of Law: Constitutional Law, Criminal Law

Appellant Larry Durant was convicted of second-degree criminal sexual conduct (CSC) for sexually abusing a teenage girl in his church office where he served as the pastor. Durant contended the trial court improperly permitted the State to introduce evidence of prior sexual abuse allegations as evidence of a common scheme or plan under Rule 404(b), SCRE, and that the State committed a "Brady" violation by failing to accurately disclose the criminal history of its witness. After review, the South Carolina Supreme Court affirmed the admissibility of the girls' testimony. "[W]hile the State failed to disclose the criminal background information of its witness, we find this information was not material." The Court found Durant exercised his position of trust, authority, and spiritual leadership to hold private prayer meetings with teen girls who had grown up in his church. He told them he was praying for their health and good fortune, and represented that part of this process was touching them sexually and having intercourse. Durant then warned the girls of misfortune if they refused or told anyone. Moreover, he used scripture as a means of grooming the children into performing sex acts. "These facts demonstrate the requisite logical connection between the prior acts of sexual abuse and the one forming the basis of the crime charged." The Court therefore affirmed Durant's conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

South Carolina v. Perry

Court: South Carolina Supreme Court
Docket: 27963
Opinion Date: May 6, 2020
Judge: Few
Areas of Law: Constitutional Law, Criminal Law

Petitioner Wallace Perry was convicted on two counts of criminal sexual conduct (CSC) with a minor in the first degree and two counts of CSC with a minor in the second degree for sexually assaulting two of his biological daughters. Prior to Perry's trial, the State made a motion to admit the testimony of Perry's stepdaughter from an earlier marriage that Perry sexually assaulted her twenty-two to twenty-seven years earlier. The State argued the trial court should not exclude the stepdaughter's testimony under Rule 404(b) of the South Carolina Rules of Evidence because it fit the

"common scheme or plan" exception. Perry objected to this testimony. The trial court initially reserved ruling on the issue, but later indicated it was inclined to allow the stepdaughter to testify. The jury convicted Perry on all counts, and the trial court sentenced him to thirty years in prison. The court of appeals affirmed. The South Carolina Supreme Court determined it was not enough to meet the "logical connection" standard for admission of other crimes under the common scheme or plan exception to Rule 404(b) that the defendant previously committed the same crime. "When evidence of other crimes is admitted based solely on the similarity of a previous crime, the evidence serves only the purpose prohibited by Rule 404(b), and allows the jury to convict the defendant on the improper inference of propensity that because he did it before, he must have done it again. ...The common scheme or plan exception demands more." The Supreme Court held State must show a logical connection between the other crime and the crime charged such that the evidence of other crimes "reasonably tends to prove a material fact in issue." The State must also convince the trial court that the probative force of the evidence when used for this legitimate purpose is not substantially outweighed by the danger of unfair prejudice from the inherent tendency of the evidence to show the defendant's propensity to commit similar crimes. In this case, the State did not meet its burden. Conviction was reversed and the matter remanded for a new trial.

Read Opinion Are you a lawyer? **Annotate this case**.

South Carolina v. Quinn

Court: South Carolina Supreme Court
Docket: 27966
Opinion Date: May 6, 2020
Judge: Kaye Gorenflo Hearn
Areas of Law: Constitutional Law, Criminal Law, White Collar Crime

Respondent Rick Quinn, Jr. was a former member of the South Carolina House of Representatives, representing constituents in Richland and Lexington counties from 1989-2004 and 2010-2017 and serving as House Majority Leader from 1999- 2004. He owned and operated a mail business called Mail Marketing Strategies (MMS) in Columbia, while his father owned and operated a political consulting firm, Richard Quinn & Associates (RQ&A). In 2014, Attorney General Alan Wilson designated First Circuit

Solicitor David Pascoe as special prosecutor to conduct a State grand jury investigation into alleged public corruption committed by current and former members of the South Carolina General Assembly. This case arose from a prior state grand jury investigation of former House Speaker Bobby Harrell, which resulted in six counts of misusing campaign funds, to which he pleaded guilty. During the course of the investigation into Speaker Harrell, SLED uncovered potentially criminal conduct by Representative Jimmy Merrill and Representative Rick Quinn, and a second grand jury investigation was initiated to investigate the conduct of these individuals. The investigation focused on Quinn's practice of using his office as House Majority Leader and leader of the House Republican Caucus to direct mailing and political services to his family's businesses. Quinn only admitted to a limited set of facts supporting the indictment. Believing the plea lacked a sufficient basis, the State moved to vacate Quinn's guilty plea, reconsider the sentence, and for the trial court's recusal. The State appealed the order denying its motions. After review, the South Carolina Supreme Court determined that the State could not appeal the guilty plea, the trial court did not abuse its discretion in sentencing, and there was no evidence of judicial bias or prejudice requiring the court to recuse itself. Therefore, the Court dismissed the State's appeal of the guilty plea, and affirmed as to all other issues.

Read Opinion Are you a lawyer? **Annotate this case**.

Texas v. Arellano

Court: Texas Court of Criminal Appeals
Docket: PD-0287-19
Opinion Date: May 6, 2020
Judge: Slaughter
Areas of Law: Constitutional Law, Criminal Law

After Appellee Cesar Ramiro Arellano was arrested for driving while intoxicated, the arresting officer, Phillip Garcia, prepared a probable cause affidavit to support a search warrant for a blood draw. Officer Garcia submitted his sworn affidavit to the on-duty magistrate. Using a cursive signature, the magistrate signed the blank signature line of a form search warrant authorizing the search and seizure of Appellee's blood. Below the signature line appeared the words, "Magistrate, Victoria County, Texas."

Aside from the cursive signature, the magistrate's name was not typed or handwritten anywhere on the warrant. Upon execution of the search warrant, Appellee was charged with DWI. In the trial court, Appellee filed a motion to suppress all evidence stemming from the blood draw. At the pretrial suppression hearing, Appellee argued that the search warrant to obtain the blood specimen was facially invalid because the magistrate's signature was illegible in violation of the requirements of Code of Criminal Procedure Article 18.04(5). The trial court agreed, the court of appeals concurred, and the evidence was suppressed because of the illegible signature. The Texas Court of Criminal Appeals disagreed with both lower courts, finding the court of appeals erred in holding that reliance on the statutory good-faith exception was automatically precluded based on an illegible magistrate's signature in violation of Code of Criminal Procedure Article 18.04(5). Because the remaining issues in the case were not properly addressed by the court of appeals, judgment was vacated and the matter remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

About Justia Opinion Summaries

Justia Weekly Opinion Summaries is a free service, with 63 different newsletters, each covering a different practice area.

Justia also provides 68 daily jurisdictional newsletters, covering every federal appellate court and the highest courts of all US states.

All daily and weekly Justia newsletters are free. Subscribe or modify your newsletter subscription preferences at daily.justia.com.

You may freely redistribute this email in whole.

About Justia

Justia is an online platform that provides the community with open access to the law, legal information, and lawyers.



Unsubscribe From This Newsletter

or unsubscribe from all Justia newsletters immediately **here.**



Justia | 1380 Pear Ave #2B, Mountain View, CA 94043

From:	Criminal Law - Justia Weekly Opinion Summaries
To:	Hopkins, Tyler (POL)
Subject:	Latest 111 Cases This Week: Kelly v. United States (U.S.), Gomes v. Silva (1st Cir.), United States v. Perez-Couvertier (1st Cir.)
Date:	Friday, May 8, 2020 9:02:37 AM

If you are unable to see this message, click here to view it in a web browser.

Justia Weekly Opinion Summaries

Criminal Law
May 8, 2020

Table of Contents

Kelly v. United States
Criminal Law, Government & Administrative Law, White Collar Crime
US Supreme Court

Gomes v. Silva
Civil Rights, Constitutional Law, Criminal Law

US Court of Appeals for the First Circuit

United States v. Perez-Couvertier
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the First Circuit

United States v. Haverkamp
Criminal Law
US Court of Appeals for the Second Circuit

United States v. Mladen
Criminal Law, Trusts & Estates
US Court of Appeals for the Second Circuit

United States v. Richardson
Criminal Law
US Court of Appeals for the Second Circuit

United States v. Rosemond
Criminal Law
US Court of Appeals for the Second Circuit

United States v. Lacerda
Criminal Law, White Collar Crime
US Court of Appeals for the Third Circuit

Cucalon v. Barr
Criminal Law, Immigration Law
US Court of Appeals for the Fourth Circuit

United States v. Doctor
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Lewis
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Jordan
Criminal Law
US Court of Appeals for the Fifth Circuit

United States v. Longoria
Criminal Law
US Court of Appeals for the Fifth Circuit

United States v. McNabb
Criminal Law
US Court of Appeals for the Fifth Circuit

Andrews v. Wayne County
Civil Rights, Constitutional Law, Criminal Law

US Court of Appeals for the Sixth Circuit

Hicks v. Scott
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Sixth Circuit

Moody v. United States
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Sixth Circuit

United States v. Foreman
Criminal Law
US Court of Appeals for the Sixth Circuit

United States v. Smith
Criminal Law
US Court of Appeals for the Sixth Circuit

Kirkman v. Thompson
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

Tuduj v. Newbold
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

United States v. Gibson
Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

United States v. Howell
Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

United States v. Lewis
Criminal Law
US Court of Appeals for the Seventh Circuit

Bakor v. Barr
Criminal Law, Immigration Law
US Court of Appeals for the Eighth Circuit

Smith v. Titus
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Becerra
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Haynes
Criminal Law

US Court of Appeals for the Eighth Circuit

United States v. Roberts
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Wright
Criminal Law
US Court of Appeals for the Eighth Circuit

Benson v. Chappell
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Ninth Circuit

Mero v. Barr
Criminal Law, Immigration Law
US Court of Appeals for the Ninth Circuit

Romero-Millan v. Barr
Criminal Law
US Court of Appeals for the Ninth Circuit

United States v. Yang
Criminal Law
US Court of Appeals for the Ninth Circuit

United States v. Neugin
Constitutional Law, Criminal Law
US Court of Appeals for the Tenth Circuit

United States v. Ramon
Constitutional Law, Criminal Law
US Court of Appeals for the Tenth Circuit

United States v. Richards
Constitutional Law, Criminal Law
US Court of Appeals for the Tenth Circuit

Andrews v. Warden
Criminal Law
US Court of Appeals for the Eleventh Circuit

Hollis v. United States
Criminal Law
US Court of Appeals for the Eleventh Circuit

Knight v. Florida Department of Corrections
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Eleventh Circuit

United States v. Evans
Criminal Law

US Court of Appeals for the Eleventh Circuit

United States v. McLellan
Criminal Law
US Court of Appeals for the Eleventh Circuit

United States v. Russell
Criminal Law
US Court of Appeals for the Eleventh Circuit

Welch v. United States
Criminal Law
US Court of Appeals for the Eleventh Circuit

State v. Trujillo
Constitutional Law, Criminal Law
Arizona Supreme Court

Barnett v. State
Criminal Law
Arkansas Supreme Court

Mason v. Kelley
Criminal Law
Arkansas Supreme Court

Ray v. Kelley
Criminal Law
Arkansas Supreme Court

Walker v. Kelley
Criminal Law
Arkansas Supreme Court

People v. Flores
Civil Rights, Constitutional Law, Criminal Law
Supreme Court of California

California v. Law
Constitutional Law, Criminal Law
California Courts of Appeal

California v. Sanchez
Constitutional Law, Criminal Law
California Courts of Appeal

Galeotti v. International Union of Operating Engineers
Criminal Law, Labor & Employment Law, White Collar Crime
California Courts of Appeal

In re I.A.
Criminal Law, Juvenile Law

California Courts of Appeal

People v. Edwards
Criminal Law
California Courts of Appeal

People v. Thomkins
Criminal Law
California Courts of Appeal

People v. Torres
Criminal Law
California Courts of Appeal

People v. Triplett
Criminal Law
California Courts of Appeal

Colorado In Interest of G.S.S.
Constitutional Law, Criminal Law, Juvenile Law
Colorado Supreme Court

Barringer v. Halkitis
Criminal Law
Florida Supreme Court

Franqui v. State
Criminal Law
Florida Supreme Court

Hicks v. State
Criminal Law
Florida Supreme Court

Burley v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Carter v. Georgia
Construction Law, Criminal Law
Supreme Court of Georgia

Clarke v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Collins v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Dawson v. Georgia
Constitutional Law, Criminal Law

Supreme Court of Georgia

Evans v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Hill v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Oliver v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Rosser v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Spencer v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Styles v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Whitehead v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Idaho v. Blythe
Constitutional Law, Criminal Law
Idaho Supreme Court - Criminal

Idaho v. Glodowski
Constitutional Law, Criminal Law
Idaho Supreme Court - Criminal

Idaho v. Jones
Constitutional Law, Criminal Law
Idaho Supreme Court - Criminal

State v. Gordon
Civil Rights, Constitutional Law, Criminal Law
Iowa Supreme Court

State v. Craig
Criminal Law
Kansas Supreme Court

State v. Lemmie
Criminal Law

Kansas Supreme Court

State v. Mullen
Criminal Law
Maine Supreme Judicial Court

Commonwealth v. Billingslea
Civil Rights, Constitutional Law, Criminal Law
Massachusetts Supreme Judicial Court

Commonwealth v. Martin
Civil Rights, Constitutional Law, Criminal Law
Massachusetts Supreme Judicial Court

Commonwealth v. Tavares
Criminal Law
Massachusetts Supreme Judicial Court

State v. Branch
Criminal Law
Minnesota Supreme Court

Galloway v. Mississippi
Constitutional Law, Criminal Law
Supreme Court of Mississippi

City of Missoula v. Zerbst
Civil Rights, Constitutional Law, Criminal Law
Montana Supreme Court

State v. Degarmo
Civil Rights, Constitutional Law, Criminal Law
Nebraska Supreme Court

People v. Holz
Civil Rights, Constitutional Law, Criminal Law
New York Court of Appeals

People v. Maffei
Civil Rights, Constitutional Law, Criminal Law
New York Court of Appeals

State v. Bailey
Civil Rights, Constitutional Law, Criminal Law
North Carolina Supreme Court

State v. Ellis
Civil Rights, Constitutional Law, Criminal Law
North Carolina Supreme Court

State v. Hobbs
Civil Rights, Constitutional Law, Criminal Law

North Carolina Supreme Court

State v. Mylett
Criminal Law
North Carolina Supreme Court

Dodge v. North Dakota
Constitutional Law, Criminal Law
North Dakota Supreme Court

Hewitt v. NDDOT
Criminal Law, Government & Administrative Law
North Dakota Supreme Court

Kastet v. NDDOT
Criminal Law, Government & Administrative Law
North Dakota Supreme Court

North Dakota v. Dahl
Constitutional Law, Criminal Law
North Dakota Supreme Court

North Dakota v. Foster
Constitutional Law, Criminal Law
North Dakota Supreme Court

North Dakota v. Kolstad
Constitutional Law, Criminal Law
North Dakota Supreme Court

North Dakota v. Michel
Constitutional Law, Criminal Law
North Dakota Supreme Court

North Dakota v. Wayland
Constitutional Law, Criminal Law
North Dakota Supreme Court

Schwindt v. Sorel
Constitutional Law, Criminal Law, Government & Administrative Law
North Dakota Supreme Court

State ex rel. McDougald v. Greene
Criminal Law
Supreme Court of Ohio

State ex rel. Parker Bey v. Byrd
Criminal Law
Supreme Court of Ohio

State v. Dangler
Criminal Law

Supreme Court of Ohio

Oregon v. Haji
Constitutional Law, Criminal Law
Oregon Supreme Court

South Carolina v. Durant
Constitutional Law, Criminal Law
South Carolina Supreme Court

South Carolina v. Perry
Constitutional Law, Criminal Law
South Carolina Supreme Court

South Carolina v. Quinn
Constitutional Law, Criminal Law, White Collar Crime
South Carolina Supreme Court

Texas v. Arellano
Constitutional Law, Criminal Law
Texas Court of Criminal Appeals

COVID-19 Updates: Law & Legal Resources Related to Coronavirus

Click here to include Verdict article summaries with your newsletter(s).

Criminal Law Opinions

Kelly v. United States

Court: US Supreme Court
Docket: 18-1059
Opinion Date: May 7, 2020
Judge: Elena Kagan
Areas of Law: Criminal Law, Government & Administrative Law, White Collar Crime

During former New Jersey Governor Christie's 2013 reelection campaign,

Fort Lee's mayor refused to endorse Christie. Kelly, Christie's Deputy Chief of Staff, Port Authority Deputy Executive Director, Baroni, and another official decided to reduce from three to one the number of lanes reserved at the George Washington Bridge's toll plaza for Fort Lee's commuters. To disguise the political retribution, the lane realignment was said to be for a traffic study. Port Authority traffic engineers were asked to collect some numbers. An extra toll collector was paid overtime. The lane realignment caused four days of gridlock, ending only when the Port Authority's Executive Director learned of the scheme. The Third Circuit affirmed the convictions of Baroni and Kelly for wire fraud, fraud on a federally funded program, and conspiracy to commit those crimes. The Supreme Court reversed. The scheme did not aim to obtain money or property. The wire fraud statute refers to "any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses," 18 U.S.C. 1343. The federal-program fraud statute bars "obtain[ing] by fraud" the "property" (including money) of a federally funded program or entity, section 666(a)(1)(A). The statutes are limited to the protection of property rights and do not authorize federal prosecutors to set standards of good government. The Court rejected arguments that the defendants sought to take control of the Bridge's physical lanes or to deprive the Port Authority of the costs of compensating employees. Their realignment of the access lanes was an exercise of regulatory power; a scheme to alter a regulatory choice is not one to take government property. The time and labor of the employees were an incidental byproduct of that regulatory object. Neither defendant sought to obtain the services that the employees provided.

Read Opinion Are you a lawyer? **Annotate this case**.

Gomes v. Silva

Court: US Court of Appeals for the First Circuit
Docket: 19-1656
Opinion Date: May 1, 2020
Judge: Stahl
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The First Circuit affirmed the judgment of the district court denying Appellant's petition for a writ of habeas corpus, holding that, under the highly deferential standard prescribed by the Antiterrorism and Effective

Death Penalty Act for federal habeas review of state criminal convictions, Appellant's claims to habeas relief failed. Appellant was convicted in a Massachusetts superior court of murder in the first degree and related crimes. The Supreme Judicial Court (SJC) affirmed the convictions. Appellant subsequently petitioned the District Court for the District of Massachusetts for a writ of habeas corpus. The district court denied the petition but granted a certificate of appealability. The First Circuit affirmed, holding (1) sufficient evidence supported Appellant's conviction for first-degree murder as a joint venturer, and the SJC's sufficiency determination was not unreasonable; and (2) the SJC reasonably determined that the trial court's admission into evidence of certain items did not constitute error.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Perez-Couvertier

Court: US Court of Appeals for the First Circuit
Docket: 16-2186
Opinion Date: May 7, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The First Circuit affirmed Defendant's conviction of possessing with intent to distribute controlled substances in a protected area and conspiring to distribute controlled substances in a protected area, holding that the district court did not plainly err with respect to any of Defendant's challenges. Specifically, the First Circuit held (1) the district court did not commit plain error in admitting evidence of the conspiracy's activities occurring after he withdrew from the conspiracy or, alternatively, in not instructing the jury to ignore such evidence; (2) the district court did not plainly err in admitting evidence of a drug trafficking organization's violent acts; and (3) the delay between Defendant's indictment and arrest did not violate his Sixth Amendment right to a speedy trial.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Haverkamp

Court: US Court of Appeals for the Second Circuit

Docket: 18-3735
Opinion Date: May 4, 2020
Judge: Barrington D. Parker
Areas of Law: Criminal Law

Defendant pleaded guilty to one count of distribution and receipt of child pornography and one count of possession of child pornography. The district court sentenced him to 121 months of imprisonment, followed by five years of supervised release, and imposed a $200 mandatory special assessment under 18 U.S.C. 3013, as well as a $10,000 assessment under 18 U.S.C. 3014. The Second Circuit held that the district court did not abuse its discretion in sentencing defendant and his sentence was substantively reasonable. The court held that the text of the Justice for Victims of Trafficking Act (JVTA), 18 U.S.C. 3014, taken as a whole and in its context, is straightforwardly meant to be applied on a per-offender, not a per-count, basis. In this case, the district court erroneously applied the special assessment on a per-count, rather than per-offender, basis. Finally, the court held that the computer monitoring condition in question was reasonably related to the nature of defendant's offense. Accordingly, the court affirmed in part, vacated in part, and remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Mladen

Court: US Court of Appeals for the Second Circuit
Docket: 18-0616
Opinion Date: May 6, 2020
Judge: Amalya Lyle Kearse
Areas of Law: Criminal Law, Trusts & Estates

After defendant died while his appeal was pending, counsel moved for abatement of all incidents of the prosecution, requesting that the appeal be dismissed without a decision on the merits, that defendant's conviction be vacated, and that the matter be remanded to the district court with instructions to dismiss the indictment and order repayment to defendant's estate of the $20,000 fine and $100 special assessment. Because defendant was convicted upon his plea of guilty, and he neither did nor was permitted to challenge on appeal the merits of his conviction, the Second

Circuit denied as without merit so much of the motion as seeks (1) vacatur of his conviction, (2) dismissal of the count of the indictment on which he was convicted, and (3) repayment of the mandatory $100 special assessment. The court granted so much of the motion as requests dismissal of this appeal and a remand to the district court for vacatur of the imposed terms of imprisonment and supervised release and for an order requiring that the paid fine of $20,000 be repaid to defendant's estate.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Richardson

Court: US Court of Appeals for the Second Circuit
Docket: 19-412
Opinion Date: May 5, 2020
Judge: Menashi
Areas of Law: Criminal Law

The Second Circuit affirmed defendant's conviction for distribution and possession with intent to distribute a controlled substance. The court held that the district court did not procedurally err by applying the career offender sentencing enhancement pursuant to USSG 4B1.1 because defendant's prior convictions of conspiracy to distribute a controlled substance in violation of 21 U.S.C. 841(a)(1) and 846, and attempted criminal possession of a controlled substance in violation of N.Y. Penal Law 220.16(1), qualify as controlled substance offenses, as defined in USSG 4B1.2(b). The court also held that the district court did not substantively err in sentencing defendant, because it properly considered his criminal history and accounted for his need for mental health and substance abuse treatment.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Rosemond

Court: US Court of Appeals for the Second Circuit
Docket: 18-3561
Opinion Date: May 1, 2020
Judge: Chin
Areas of Law: Criminal Law

The Second Circuit affirmed defendant's conviction for murder-for-hire, conspiracy to commit murder-for-hire, murder through use of a firearm, and possession of a firearm during a murder-for-hire conspiracy. Defendant owned Czar Entertainment, a music management company that represented hip-hop, rap and R&B artists such as Jayceon Taylor, also known as "The Game." Taylor was a member of G-Unit, a rap group run by Curtis Jackson, also known as "50 Cent." Defendant's crimes stemmed from a rivalry with Violator Records, the company that managed G-Unit. The court rejected defendant's contention that his attorney was ineffective because he conceded that defendant paid for the victim to be shot, even though he told counsel not to make this concession. The court held that defendant failed to show that this was objectively unreasonable or that he would have been found not guilty had a different argument been advanced. In this case, there was ample evidence supporting counsel's strategy to concede that defendant ordered a shooting where, among other things, the government's key witness, who participated in the conspiracy and lured the victim to be shot, testified that defendant agreed to pay the shooter. The court also held that the district court did not abuse its broad discretion by admitting prior bad-act evidence under Federal Rule of Evidence 404(b)(1).

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Lacerda

Court: US Court of Appeals for the Third Circuit
Docket: 15-2812
Opinion Date: May 5, 2020
Judge: Porter
Areas of Law: Criminal Law, White Collar Crime

VOG billed itself as an advocacy group helping victims of timeshare fraud get out of their timeshare debts. A jury determined that VOG had actually defrauded its customers and that three individual defendants (including Lacerda) were each knowing participants in that fraud. Lacerda was sentenced to 324 months' imprisonment for his leading role in the fraudulent enterprise. The Third Circuit affirmed the respective convictions and sentences. The court rejected a claim of impermissible "overview testimony" by an FBI agent; an officer who is familiar with an investigation or was personally involved may tell the story of that investigation—how the

investigation began, who was involved, and what techniques were used, and, with a proper foundation, may offer lay opinion testimony and testify about matters within his personal knowledge. The district court did not abuse its discretion when it disqualified defense counsel based on a conflict of interest; when it denied replacement counsel's motion for a continuance; when it excluded from evidence, as hearsay, an email sent by Lacerda to VOG's former CFO; in exercising its sentencing discretion; or by ordering the forfeiture of all VOG's gross proceeds.

Read Opinion Are you a lawyer? **Annotate this case**.

Cucalon v. Barr

Court: US Court of Appeals for the Fourth Circuit
Dockets: 18-1292, 18-2206
Opinion Date: May 7, 2020
Judge: Barbara Milano Keenan
Areas of Law: Criminal Law, Immigration Law

The Fourth Circuit denied petitions for review of the BIA's final order of removal. Applying the modified categorical approach, the court held that defendant's prior conviction for distribution of cocaine under Virginia Code 18.2-248, including distribution of that substance as an accommodation under Virginia Code 18.2-248(D), satisfies the federal definitions of an "aggravated felony" and of a crime "relating to a controlled substance" pursuant to 8 U.S.C. 1227(a)(2)(A)(iii), 1227(a)(2)(B)(i). The court also held that the district court did not abuse its discretion in denying petitioner's motion to reconsider.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Doctor

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-4874
Opinion Date: May 4, 2020
Judge: Roger L. Gregory
Areas of Law: Criminal Law

The Fourth Circuit affirmed the district court's revocation of defendant's

supervised release and resulting sentence. The court held that the district court did not clearly err in finding the government proved he committed the assault underlying the supervised release violation; the district court did not commit plain error by adopting the violation report when announcing defendant committed Violation One; and, even if the district court erred in sentencing defendant for a Grade A violation, the error was harmless.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Lewis

Court: US Court of Appeals for the Fourth Circuit
Docket: 19-4028
Opinion Date: May 4, 2020
Judge: Barbara Milano Keenan
Areas of Law: Criminal Law

Defendant was convicted for possessing a firearm as a felon and sentenced to 63 months' imprisonment and a three-year period of supervised release. The district court additionally recommended, without explanation, that defendant receive addiction treatment while incarcerated and ordered, as a special condition of his supervised release, that defendant participate in an addiction treatment program. The Fourth Circuit held that defendant's sentence is procedurally unreasonable because the district court failed to provide an adequate explanation for imposing as a special condition of supervised release the requirement of addiction treatment. The court also held that the district court failed to address defendant's nonfrivolous mitigation arguments. Therefore, the court remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Jordan

Court: US Court of Appeals for the Fifth Circuit
Docket: 19-40499
Opinion Date: May 1, 2020
Judge: Jennifer Walker Elrod
Areas of Law: Criminal Law

The Fifth Circuit affirmed the district court's grant of defendants' motion for a new trial on the basis of prejudicial outside influence on the jury. The court held that the district court did not abuse its broad discretion in granting the motion for a new trial without holding an evidentiary hearing. To the extent there is a bright-line rule applicable to allegations of outside influence on the jury, the court held that it was not applicable to this case. Furthermore, the district court did not abuse its discretion in exercising its prerogative, within broadly defined parameters, to handle the allegation of outside influence in the least disruptive manner possible in this unusual case. Finally, the district court permissibly concluded that the evidence showed a sufficient likelihood of prejudice to shift the burden to the Government, and that the Government did not (and could not) show "no reasonable possibility that the jury's verdict was influenced by" the CSO's comments.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Longoria

Court: US Court of Appeals for the Fifth Circuit
Docket: 19-20201
Opinion Date: May 5, 2020
Judge: Gregg Costa
Areas of Law: Criminal Law

The Fifth Circuit held that the base offense level of 20 was proper for defendant's felon-in-possession crime involving a semiautomatic firearm that is capable of accepting a large capacity magazine. In this case, defendant failed to show that the district court clearly erred in relying on the FBI's agent statement about what was found in the apartment. The court clarified any confusion and held that the 2013 amendment to the commentary on the acceptance-of-responsibility Guideline does not clearly overrule its caselaw allowing the government to withhold the third point for acceptance of responsibility when it must litigate a suppression motion. The court held that Amendment 775 does not contain the unequivocal override needed to get past the court's precedent. Therefore, the court affirmed defendant's sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. McNabb

Court: US Court of Appeals for the Fifth Circuit
Docket: 19-50265
Opinion Date: May 1, 2020
Judge: Costa
Areas of Law: Criminal Law

The Fifth Circuit affirmed defendant's sentence imposed after he pleaded guilty to possessing a gun after having been convicted of a felony. The court held that defendant is not entitled to relief on his claim that the government breached the plea deal, and thus his appellate waiver remains enforceable. Accordingly, defendant's challenges to his sentence must be dismissed.

Read Opinion Are you a lawyer? **Annotate this case**.

Andrews v. Wayne County

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-1992
Opinion Date: May 4, 2020
Judge: Suhrheinrich
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Canton Police received a 911 call from Andrews, who stated that his fiance, White, had physically attacked him. Officers arrested White. Andrews later took White's medications to the jail; a “KOP” policy allows inmates to keep certain drugs for self-administration. During an intake interview, White admitted to attempting to harm herself or commit suicide in the past but said she was not thinking of harming herself or having suicidal thoughts. An R.N. later evaluated White for nearly two hours, reported White’s chief complaints were “anxiety and depression,” and contacted a pharmacy to verify White’s prescriptions. The R.N. claims White did not exhibit any psychotic behavior, suicidal ideation, or psychiatric distress but ordered further evaluation. The next day, White was found on the floor with vomit on her face. She stated repeatedly that she took too many pills. The next day, White died in the hospital. The cause of death was Verapamil toxicity. The Sixth Circuit affirmed the rejection of a suit under 42 U.S.C. 1983 on summary judgment. A pretrial detainee does not have an automatic right to a suicide screening. The court rejected an argument that the KOP Policy was deficient because

it allows inmates in need of a psychological evaluation to participate before a psychiatrist's assessment of proper housing. The County had no history of suicides relative to the program, so any purported failure to train its employees in suicide risk assessment did not cause White's death.

Read Opinion Are you a lawyer? **Annotate this case**.

Hicks v. Scott

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-3410
Opinion Date: May 1, 2020
Judge: Gibbons
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Cincinnati officers Scott and Moore responded to a reported incident of menacing. Two people alleged that Quandavier had driven by their home that night and threatened to kill them and that Quandavier carried guns. Officer Loreaux identified a vehicle fitting the description. Officers Scott, Moore, Schneider, and Loreaux, standing where the vehicle was parked, heard a voice. Thinking that it was likely Quandavier, they knocked on the exterior door of the residence. It swung open. Three officers entered without a warrant or exigent circumstances. Loreaux remained outside. Neither Scott nor Moore recall announcing their presence or identifying themselves. Inside and upstairs, Scott knocked on a closed door. As it opened, Scott "saw the barrel of a rifle pointed at [her] face." Moore and Schneider also saw Quandavier "nonchalantly" panning the rifle from left to right. Moore reached for its barrel as Scott fired her weapon. Moore did not instruct Quandavier to drop his rifle nor did Scott issue any commands before firing. Quandavier collapsed. The officers immediately radioed for paramedics. Before the officers applied handcuffs or provided first aid, they heard another voice and conducted a sweep. Quandavier died at the scene without receiving medical attention. In a suit under 42 U.S.C. 1983 for unlawful entry, excessive force, and deliberate indifference to a serious medical need, plus state claims, the district court granted the defendants summary judgment, citing qualified immunity. The Sixth Circuit reversed in part. The district court erred by granting qualified immunity to Scott, Moore, and Schneider on the unlawful entry claim. The court affirmed as to the excessive force, deliberate indifference, and state-law battery claims, and

remanded for evaluation of municipal liability and wrongful death claims.

Read Opinion Are you a lawyer? **Annotate this case**.

Moody v. United States

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-5015
Opinion Date: May 6, 2020
Judge: Thapar
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

At Moody's trial, the government produced a video of Moody cooking crack on his stove and waving a handgun while he mused about life in "the game" (drug trafficking). The court ruled that most of the video was admissible. Moody then tried to persuade the jury that the video was filmed more than five years before his indictment, putting it outside the statute of limitations. The jury convicted Moody. Due to prior felony drug convictions, Moody received enhanced, mandatory-minimum life sentences on several counts. He appealed on evidentiary grounds relating to the video. The Sixth Circuit affirmed. Later, Moody raised new claims on collateral review, 28 U.S.C. 2255. The district court found each claim meritless; most were also procedurally defaulted. The court authorized Moody to appeal. The Sixth Circuit dismissed the appeal, stating that none of the claims should have been certified. Reasonable jurists could not doubt that the district court properly denied relief on Moody's claims that he was deprived of his statute-of-limitations defense (violating due process); that the past convictions for his sentencing enhancements were not charged in the indictment or found by the jury; and that his previous lawyers failed to raise the first two claims sooner, violating his right to effective assistance of counsel.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Foreman

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-1827
Opinion Date: May 7, 2020
Judge: Gibbons

Areas of Law: Criminal Law

In 2006, Foreman pled guilty to possession with intent to distribute 50 or more grams of cocaine base, possession with intent to distribute cocaine powder, and possession of a firearm during and in furtherance of a drug trafficking crime. Foreman admitted that he was responsible for approximately 135 grams of crack cocaine and 250 grams of cocaine powder. Foreman had a final Guidelines range of 322-387 months; he was sentenced to 240 months' imprisonment with respect to each drug conviction, to run concurrently, and 60 months' imprisonment for the firearms conviction, to run consecutively. When the First Step Act of 2018 made the Fair Sentencing Act retroactive, Foreman sought relief. The district court held that Foreman was not entitled to a plenary resentencing and declined to revisit his career offender status or hold an in-person hearing, then weighed the new statutory range applicable to Foreman's drug offenses, his recalculated Guidelines range, and the 18 U.S.C. 3553(a) factors, and reduced Foreman's total sentence to 172 months on each drug offense, to run concurrently, plus the mandatory consecutive 60 months on the firearms offense. The Sixth Circuit affirmed. Nothing in the First Step Act entitles a defendant to a plenary resentencing. First Step Act resentencings are not shielded from review for reasonableness; the district court thoroughly explained its rationale, carefully examining Foreman's circumstances, the amended penalty provisions, and the resulting changes to Foreman's Guidelines range.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Smith

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-1724
Opinion Date: May 6, 2020
Judge: Bush
Areas of Law: Criminal Law

In 2006, Smith was convicted of conspiracy to distribute and to possess with intent to distribute 500 grams or more of powder or 50 grams or more of cocaine base (crack cocaine); possession with intent to distribute 50 grams or more of cocaine base (crack cocaine); possession with intent to distribute

500 grams or more of cocaine powder; and being a felon in possession of a firearm. The court imposed a mandatory minimum life sentence. The Fair Sentencing Act subsequently lowered the penalty for cocaine-base offenses, made retroactive through the First Step Act. Smith moved for relief and received a reduced sentence of 360 months, the bottom of the new Guideline range for the counts impacted by the Fair Sentencing Act, to run concurrent to his existing 360-month sentence for his powder cocaine count that was not affected by the Fair Sentencing Act. The Sixth Circuit affirmed, rejecting an argument that the court should have imposed a below-Guideline sentence for all counts. The First Step Act is a limited grant of authority to impose a reduced sentence for certain offenses and does not require a plenary resentencing proceeding. Even assuming the court's obligation to explain its reasons for imposing the modified sentence was akin to that which applies in initial sentencing, the court's use of a modified AO 247 form order to explain its decision was not procedurally unreasonable.

Read Opinion Are you a lawyer? **Annotate this case**.

Kirkman v. Thompson

Court: US Court of Appeals for the Seventh Circuit
Docket: 19-1904
Opinion Date: May 7, 2020
Judge: William Joseph Bauer
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Following a 1992 fight that involved Johnson, Herron, and Walker, two shooters shot the three men. Johnson survived. In the hospital, Johnson described a shooter by the street name "Duke," where Duke lived, and Duke's car. Johnson identified Duke and his accomplice from a photo array. Police pulled over a vehicle matching Johnson's description and arrested the driver, Kirkman, and the passenger, who matched the general description of the second shooter. Kirkman had a tattoo of Duke on his arm. Police took additional photos and presented a second photo array to Johnson, who identified them as the shooters. At trial, Johnson identified Kirkman and his passenger as the shooters. There was disputed testimony about the cause of the fight. Convicted of murder and aggravated battery with a firearm, Kirkman was sentenced to life in prison. Johnson had a

change of heart and submitted an affidavit, identifying Ford and an unknown man as the shooters. At Kirkman's post-conviction hearing, Johnson testified that he and his family had been threatened. Other testimony was inconsistent with Johnson's. Illinois courts denied post-conviction relief, finding that Johnson's recantation lacked credibility. Johnson later pleaded guilty for perjury but failed to specify which statement was false. The Seventh Circuit affirmed the denial of federal habeas relief. Illinois courts found Johnson's recantation lacked credibility. An evidentiary hearing satisfied Kirkman's due process rights. The Illinois trial court's determination defeated Kirkman's innocence and perjured testimony claims.

Read Opinion Are you a lawyer? **Annotate this case**.

Tuduj v. Newbold

Court: US Court of Appeals for the Seventh Circuit
Docket: 19-1699
Opinion Date: May 1, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Illinois prisoner Tuduj, having received extensive dental treatment, filed a "deliberate indifference" suit under 42 U.S.C. 1983 against his dentists and prison officials. The court recruited counsel to assist Tuduj in filing an amended complaint that complied with the Federal Rules of Civil Procedure. Counsel defended against two summary judgment motions, one arguing that Tuduj had not exhausted his administrative remedies and another on the merits While the motions were pending, Tuduj moved "for leave to represent himself," stating that he was "concerned that his counsel has filed a structurally, technically and legally insufficient response doomed to be denied." He asked to file his own brief, except "in the event this Honorable Court deems counsel's response … legally sufficient and Grants same[,] Plaintiff would be open to continued effective representation." A magistrate denied Tuduj's motion, stating that Tuduj "varie[d] between saying he would like to" represent himself and "indicating that he is happy with counsel's representation as long as he prevails." The district judge granted the motions for summary judgment, citing professional judgment and finding "no competent evidence" of any policy that unlawfully influenced dental-treatment decisions. The Seventh Circuit rejected Tuduj's argument

that the court wrongly denied his “unqualified” right to proceed pro se under 28 U.S.C. 1654, the due process clause, the equal protection clause, and the Seventh Amendment. The district court permissibly denied his equivocal request.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Gibson

Court: US Court of Appeals for the Seventh Circuit
Docket: 19-1402
Opinion Date: May 7, 2020
Judge: William Joseph Bauer
Areas of Law: Constitutional Law, Criminal Law

Officer Garrison encountered Gibson, a suspected drug trafficker, walking with a companion. Although initially a consensual encounter, Garrison questioned Gibson and his companion and briefly detained Gibson. After Gibson and his companion departed, Garrison spotted a methamphetamine pipe under his patrol vehicle. Local law enforcement conducted a traffic stop of Gibson’s vehicle in the curtilage of his driveway. A drug detection dog signaled the presence of a controlled substance in the vehicle, though nothing was found. Earlier that day, Gibson’s wife had met with DEA agents to tell them about methamphetamine inside the home. Police used information Mrs. Gibson had provided to obtain a search warrant. The search of the home uncovered drugs, drug paraphernalia, currency, and AK-47 rifles, which led to Gibson’s arrest. Gibson moved to suppress all evidence seized during the search, alleging he was detained without reasonable suspicion, unlawfully frisked, arrested without probable cause, stopped without probable cause or reasonable suspicion, and the traffic stop exceeded a permissible scope. Upon learning of his wife’s cooperation, Gibson also argued her statement was insufficiently attenuated to justify the search warrant. The Seventh Circuit affirmed the denial of the motion. Mrs. Gibson’s voluntary statement with DEA agents was independently sufficient to sustain findings of probable cause and sufficiently attenuated from subsequent events to preclude suppression.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Howell

Court: US Court of Appeals for the Seventh Circuit
Docket: 18-3157
Opinion Date: May 4, 2020
Judge: Scudder
Areas of Law: Constitutional Law, Criminal Law

In December 2012, Chicago Police officers responded to an anonymous call reporting a Hispanic man in a black sweater and black hat, carrying a bag, and climbing under a warehouse fence. They found someone who matched the description. After stopping and frisking him, they determined he was not engaged in any crime. Howell, walking toward the police, was white and wearing a black jacket and dark hat. When an officer approached to speak to him, Howell did not answer, looked panicked, and put his hands in his pockets. The officer patted Howell down and found a gun in his jacket. A federal gun charge followed. Howell unsuccessfully moved to suppress the gun. The Seventh Circuit reversed the denial of his suppression motion and vacated his conviction for possessing that gun. The court noted that the facts in the pretrial record differed significantly from those presented at trial, where the arresting officer testified that he decided to proceed with the pat-down only after Howell ignored a directive to remove his hands from his pockets. Viewing the pretrial record as a whole, the police lacked reasonable suspicion to frisk Howell. The court did not reverse Howell's conviction on a second gun charge that resulted from the execution of a warrant to search Howell's apartment three months after the initial stop and the ensuing discovery of more guns and ammunition.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Lewis

Court: US Court of Appeals for the Seventh Circuit
Dockets: 19-1911, 19-1262
Opinion Date: May 7, 2020
Judge: Joel Martin Flaum
Areas of Law: Criminal Law

In 2016-2018, Draheim managed a conspiracy, responsible for at least 38 packages of methamphetamine sent from California to La Crosse,

Wisconsin. Draheim supervised at least 11 associates who accepted shipments on her behalf, sent money transfers to California, distributed the meth, rented storage lockers, and collected money owed to her. Draheim provided vehicles. After agents placed a wiretap on her phone and seized several packages of meth en route to Draheim, her California supplier forced Draheim to find a new source. Draheim contacted Lewis, recently out of jail but still involved in the "meth scene." Lewis agreed to purchase meth from a new supplier. During the planned transaction, agents seized the package, which contained 28.6 grams of nearly pure meth. Police subsequently arrested Draheim after they found her daughter dead at home from an overdose; they took Lewis into custody for violating the terms of his state supervision. Both pleaded guilty to meth distribution offenses, 21 U.S.C. 841, 846. Draheim, facing a mandatory-minimum 10-year sentence, unsuccessfully argued that she qualified for "safety-valve relief." The court reasoned that she was the leader of her enterprise. Lewis unsuccessfully contended that he should be sentenced based only on his conviction, not other "relevant conduct." The Seventh Circuit affirmed Draheim's sentence but vacated as to Lewis. The fact that the defendant has engaged in other drug transactions is not, alone, sufficient to justify treating those transactions as relevant conduct for sentencing purposes.

Read Opinion Are you a lawyer? **Annotate this case**.

Bakor v. Barr

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-3011
Opinion Date: May 7, 2020
Judge: Steven M. Colloton
Areas of Law: Criminal Law, Immigration Law

The Eighth Circuit denied a petition for review of the BIA's determination that defendant committed two crimes involving moral turpitude. The court held that the BIA did not err in determining that petitioner's conviction for the Minnesota crimes of Criminal Sexual Conduct in the Fifth Degree and knowing failure to comply with Minnesota's sex offender registration statute were crimes involving moral turpitude. The court also held that petitioner failed to exhaust his remaining arguments and therefore declined to consider them.

Read Opinion Are you a lawyer? **Annotate this case**.

Smith v. Titus

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-2915
Opinion Date: May 5, 2020
Judge: Steven M. Colloton
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Eighth Circuit affirmed the district court's denial of habeas relief to petitioner based on his claim that the trial court violated his Sixth Amendment right to a public trial when it briefly closed the courtroom to spectators. The district court denied relief based on the ground that the Minnesota Supreme Court's decision was neither contrary to, nor an unreasonable application of, clearly established federal law. The court agreed and held that it was not objectively unreasonable for the Minnesota Supreme Court to deem it constitutional under the Sixth Amendment for the trial court to explain the parameters of an earlier public order on evidentiary issues in a brief nonpublic proceeding before the jury was sworn.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Becerra

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-2777
Opinion Date: May 7, 2020
Judge: Stras
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's conviction for two counts of being a felon in possession of a firearm and ammunition. The court held that there was more than enough evidence for defendant's probation officer and other officers to believe defendant had a firearm on him. Therefore, the officers had probable cause to arrest him without a warrant. The court also held that defendant was in custody when he made both statements at issue. In this case, the "request for clarification" of defendant's statement that he had "something" in his car did not require Miranda warnings. Furthermore,

because the bulge in defendant's pocket could have been a gun or other weapon that would have posed a danger to the officers and others, they could ask about it without the formality of Miranda warnings. The court joined its sister circuits in declining to recognize the innocent-possessor defense. The court held that the district court did not err in excluding defendant's proposed testimony that he had found the handgun in his car earlier in the day and was about to hand it over to his probation officer. The court reasoned that, even if defendant intended to turn over the gun (or the ammunition) to his probation officer, it is still a crime to knowingly possess it in the first place. Finally, the court held that the district court did not err in denying defendant a sentencing reduction for acceptance of responsibility; the district court considered defendant's mitigation arguments at sentencing; and the district court did not abuse its discretion by imposing a within-Guidelines sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Haynes

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1607
Opinion Date: May 5, 2020
Judge: Raymond W. Gruender
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's conviction and sentence for being a felon in possession of a firearm. The court held that the government did not violate the Speedy Trial Act, and defendant failed to offer any evidence showing that Iowa and federal prosecutors colluded. Furthermore, the district court did not abuse its discretion by failing to hold an evidentiary hearing regarding the existence of collusion. The court also held that the district court did not err in denying the motion to suppress where defendant was not unlawfully seized. In this case, prior to producing the marijuana cigarette, the officer did not ask defendant any questions but merely ordered him off the bus, particularly as the smell of marijuana alerted the officer that evidence of a more serious crime than failure to use a turn signal might be uncovered during the stop. Finally, the court held that defendant was not unlawfully searched when the officer conducted a pat-down search incident to arrest; the evidence was sufficient to support defendant's conviction;

defendant's Rehaif claim failed because there was sufficient evidence that he knew of his prohibited status; and defendant's sentence was not substantively unreasonable nor an abuse of the district court's discretion.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Roberts

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1176
Opinion Date: May 1, 2020
Judge: Steven M. Colloton
Areas of Law: Criminal Law

The Eighth Circuit vacated defendant's sentence imposed after he pleaded guilty to unlawful possession of a firearm as a previously convicted felon. The court held that, although the district court properly applied a four-level increase for possession of a firearm "in connection with another felony offense" under USSG 2K2.1(b)(6)(B), but that a two-level increase for "using a minor to commit a crime" under USSG 3B1.4 should not have applied. In this case, the evidence showed only that defendant engaged in an arm's-length transaction with a minor. The court held that this mere joint participation in an offense as a partner, does not amount to "use" of a minor "to commit the offense" of unlawful possession of a firearm by a felon. Accordingly, the court remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Wright

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1081
Opinion Date: May 5, 2020
Judge: Erickson
Areas of Law: Criminal Law

The Eighth Circuit affirmed the district court's restitution order and certain special conditions of defendant's supervised release imposed after he pleaded guilty to sex trafficking of a child. The court found no error in the district court's restitution amount of $20,000, holding that the evidence

supported the amount in light of the aggregate harm to the victim. The court also held that the special conditions -- including a requirement that defendant participate in sex offender treatment including psychological testing and polygraph examinations, a prohibition against contact with any minors without pre-approval, and a requirement that defendant seek prior approval before using temporary commercial lodging, such as a hotel or motel -- where reasonably related to both the offense of conviction and to defendant's history of sexual contact with minor females.

Read Opinion Are you a lawyer? **Annotate this case**.

Benson v. Chappell

Court: US Court of Appeals for the Ninth Circuit
Docket: 13-99004
Opinion Date: May 1, 2020
Judge: Consuelo Maria Callahan
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Ninth Circuit affirmed the district court's denial of petitioner's habeas corpus petition challenging his California conviction and death sentence for murder and other crimes. Petitioner raised two certified claims and two uncertified claims. The panel held that petitioner failed to show that the California Supreme Court's denials of his claims were unreasonable determinations of the facts or contrary to clearly established federal law. In this case, the California Supreme Court reasonably determined that an officer's misstatement during petitioner's interrogation that there was no death penalty in California did not prompt petitioner's confessions. Furthermore, petitioner failed to show that his statements were not knowing, voluntary, and intelligent. Even if petitioner were able to show that trial counsel was ineffective in not fully investigating his abuse as a child or his alleged organic brain injury, the panel held that the state court could reasonably have determined that any shortcoming in trial counsel's investigation was not prejudicial. Finally, the panel granted a certificate of appealability on petitioner's two uncertified claims and held that the state court reasonably rejected the claims that his trial counsel should have impeached the government's case and the prosecutor withheld material, exculpatory evidence.

Read Opinion Are you a lawyer? **Annotate this case**.

Mero v. Barr

Court: US Court of Appeals for the Ninth Circuit
Docket: 17-70929
Opinion Date: May 1, 2020
Judge: Paul Jeffrey Watford
Areas of Law: Criminal Law, Immigration Law

The Ninth Circuit granted in part a petition for review of the BIA's finding that petitioner was removable based on his conviction for possession of visual presentation depicting sexual conduct of a person under 16 years of age, in violation of Nevada Revised Statutes (N.R.S.) 200.730. Applying the categorical approach, the panel compared the elements of N.R.S. 200.730 with the applicable definition of "sexual abuse of a minor," which requires proof of three elements. The panel held that N.R.S. 200.730 punishes a broader range of conduct because the Nevada statute does not require proof that the offender participated in sexual conduct with a minor. Therefore, petitioner's conviction did not qualify as sexual abuse of a minor. The panel explained that, with a possession-only offense such as N.R.S. 200.730, the minor depicted in the image is not the direct object of the offender's conduct, which is a necessary predicate for the offense to qualify as sexual abuse of a minor.

Read Opinion Are you a lawyer? **Annotate this case**.

Romero-Millan v. Barr

Court: US Court of Appeals for the Ninth Circuit
Dockets: 16-73915, 17-72893, 18-71555
Opinion Date: May 4, 2020
Areas of Law: Criminal Law

The Ninth Circuit certified the following questions of state law to the Arizona Supreme Court: 1. Is Arizona's possession of drug paraphernalia statute, A.R.S. 13-3415, divisible as to drug type? 2. Is Arizona's drug possession statute, A.R.S. 13-3408, divisible as to drug type? 3. Put another way, is jury unanimity (or concurrence) required as to which drug or drugs listed in

A.R.S. 13-3401(6), (19), (20), or (23) was involved in an offense under either statute?

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Yang

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-10341
Opinion Date: May 4, 2020
Judge: Piersol
Areas of Law: Criminal Law

The Ninth Circuit affirmed the district court's denial of defendant's motion to suppress after he pleaded guilty to receipt of stolen mail and being a prohibited person in possession of a firearm. Defendant moved to suppress the evidence seized from his residence and the statements he made to law enforcement on the basis that the search warrant obtained by the Postal Inspection Service relied on evidence that was obtained illegally. The panel declined to address the potential Fourth Amendment privacy interests that may be implicated by the warrantless use of this Automatic License Plate Recognition (ALPR) technology, and held that defendant does not have a reasonable expectation of privacy in the historical location data of the Yukon under the facts of this case. The panel found no evidence in the record that Prestige Motors had a policy or practice of allowing lessees to keep cars beyond the rental period and Prestige had made affirmative attempts to repossess the vehicle by activating the GPS unit to locate and disable the vehicle. Therefore, defendant lacked standing to challenge the warrantless search of the database.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Neugin

Court: US Court of Appeals for the Tenth Circuit
Docket: 19-7043
Opinion Date: May 1, 2020
Judge: Scott Milne Matheson, Jr.
Areas of Law: Constitutional Law, Criminal Law

Jack Neugin pled guilty to being a felon in possession of a firearm and ammunition on the condition that he could appeal the district court's denial of his motion to suppress evidence of the ammunition and firearm police found in the bed of his pickup truck. Officers responded to a reported verbal altercation between Neugin and his girlfriend. One of the officers saw ammunition in the back of the truck after he lifted the truck's camper lit do allow the girlfriend to retrieve her belongings. Neugin argued the officers discovered the evidence during an unconstitutional search; the district court concluded the officer was acting "in a lawful position" as "community caretaker," and found no Fourth Amendment violation. The Tenth Circuit reversed, finding that : (1) the officer conducted the without a warrant or probable cause, (2) the community caretaking exception to the warrant requirement does not apply, and (3) the inevitable discovery exception to the exclusionary rule does not apply. The evidence seized should have been suppressed.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Ramon

Court: US Court of Appeals for the Tenth Circuit
Docket: 19-1221
Opinion Date: May 1, 2020
Judge: Gregory Alan Phillips
Areas of Law: Constitutional Law, Criminal Law

In 2016, after serving a federal prison sentence for having possessed a firearm after a felony conviction, Charles Ramon III began serving a mandatory term of supervised release. Before Ramon completed the term, his probation officer filed a petition, soon followed by two superseding petitions, to revoke Ramon's supervised release. At the revocation hearing, the district court found three violations—two for possessing a controlled substance and one for again illegally possessing a firearm. Of these, the most serious was Ramon's illegal possession of a firearm—a Grade B violation. For this, the court imposed the statutory maximum sentence of twenty-four months in prison. During the revocation hearing, the government mentioned that it might seek to indict Ramon for illegally possessing a firearm (the conduct in part underlying the revocation). Mindful of this, the district court ordered that Ramon's twenty-four-month sentence run

"consecutively to any sentences imposed previously or prospectively in federal or state court." At the hearing, Ramon did not object to the district court's running his sentence consecutively to future federal sentences. On appeal, Ramon argued that the district court exceeded its sentencing authority under 18 U.S.C. 3584(a) by ordering that Ramon's sentence run consecutively to future federal sentences. By the terms of 18 U.S.C. 3584(a), the Tenth Circuit determined the district court did err. But Ramon failed to object to this at trial, and on appeal, failed to show that the error was plain, thus, judgment was affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Richards

Court: US Court of Appeals for the Tenth Circuit
Docket: 19-8044
Opinion Date: May 6, 2020
Judge: Baldock
Areas of Law: Constitutional Law, Criminal Law

In 2018, the Wyoming Division of Criminal Investigation (DCI) obtained a search warrant to review the contents of Defendant–Appellant Joshua Richards' Tumblr account. During the search and subsequent investigation, DCI agents discovered Defendant had re-blogged videos and images of child pornography to his private Tumblr so he could later access and view the materials. Defendant ultimately pleaded guilty to one count of accessing with intent to view child pornography. He was sentenced to twenty-four months' imprisonment followed by five years of supervised release. The district court imposed several special conditions of supervised release, which, as relevant here, related to drugs and alcohol and required Defendant to submit to polygraph testing. On appeal, Defendant argued the district court erred in imposing these special conditions. He also challenged the length of his prison sentence as substantively unreasonable. The Tenth Circuit determined the alcohol and drug conditions did not directly conflict with the relevant policy statement in the sentencing guidelines, so the district court's decision to impose the conditions was not manifestly unreasonable. And given the circumstances of the case, the Court determined the trial court did not abuse its discretion in imposing Defendant's twenty-four month sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

Andrews v. Warden

Court: US Court of Appeals for the Eleventh Circuit
Docket: 19-12443
Opinion Date: May 5, 2020
Judge: William Holcombe Pryor, Jr.
Areas of Law: Criminal Law

The Eleventh Circuit affirmed the district court's denial of habeas relief under 28 U.S.C. 2241. Plaintiff alleged that President Obama commuted his "total sentence" of imprisonment, which included the 37 months of imprisonment that he served as part of his 2003 sentence. Based on the terms of the commutation order, the Constitution, and Supreme Court precedent, the court could not say that the Bureau erred in excluding the 37-month term of imprisonment from its recalculation.

Read Opinion Are you a lawyer? **Annotate this case**.

Hollis v. United States

Court: US Court of Appeals for the Eleventh Circuit
Docket: 19-11323
Opinion Date: May 6, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Eleventh Circuit affirmed the district court's denial of petitioner's motion to vacate his sentence under 28 U.S.C. 2255. The court held that petitioner cannot prove that his counsel rendered ineffective assistance, because petitioner's prior convictions in Alabama categorically qualify as predicate offenses under both the Armed Career Criminal Act and the career-offender provision of the Guidelines, and his prior conviction in Georgia qualifies as a predicate offense under the Act. Therefore, counsel did not perform deficiently by failing to raise a meritless objection.

Read Opinion Are you a lawyer? **Annotate this case**.

Knight v. Florida Department of Corrections

Court: US Court of Appeals for the Eleventh Circuit
Docket: 18-12488
Opinion Date: May 1, 2020
Judge: Newsom
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Eleventh Circuit affirmed the district court's denial of a 28 U.S.C. 2254 petition for habeas relief. Petitioner alleged that his counsel rendered ineffective assistance under Strickland v. Washington, 466 U.S. 668 (1984), by failing to adequately investigate and present mitigating evidence during the sentencing phase of his capital-murder trial. The court held that, even assuming that counsel performed deficiently in failing to investigate and present the mitigation evidence that petitioner now raises—thus satisfying the first prong of the two-part Strickland standard that governs ineffective-assistance claims—petitioner failed to carry his burden of demonstrating resulting prejudice.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Evans

Court: US Court of Appeals for the Eleventh Circuit
Docket: 17-15323
Opinion Date: May 6, 2020
Judge: Grant
Areas of Law: Criminal Law

The Eleventh Circuit affirmed defendant's conviction and sentence for being a felon in possession of a firearm. The court held that, given the totality of the circumstances, it was reasonable for officers, mistaking a dog's whimper for a person in distress, to enter defendant's home without a warrant. Therefore, defendant's challenge to the district court's denial of his motion to suppress evidence failed. The court upheld the district court's imposition of a 22 offense level finding because defendant possessed a semiautomatic firearm capable of accepting a large capacity magazine under USSG 2K2.1(a)(3)(A)(i) (2016). The court also upheld defendant's sentencing enhancement under USSG 2K2.1(b)(4)(B) for possessing a rifle that had an

obliterated serial number.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. McLellan

Court: US Court of Appeals for the Eleventh Circuit
Docket: 18-13289
Opinion Date: May 6, 2020
Judge: Boggs
Areas of Law: Criminal Law

The Eleventh Circuit affirmed defendant's conviction for two counts of being a felon in possession of a firearm. The court held that the district court did not abuse its discretion in permitting one of his arresting officers to offer testimony at trial on the correlation between guns and drug activity and to suggest that defendant was selling drugs; the court declined to evaluate the applicability of the Armed Career Criminal Act (ACCA), because the district court would have imposed the same sentence regardless of whether the mandatory minimum applied; and the court rejected defendant's claim under Rehaif v. United States, 139 S. Ct. 2191 (2019), and held that there was no plain error in the district court's failure to instruct the jury of the knowledge-of-status element and any error from the lack of a knowledge-of-status element in defendant's plea colloquy did not affect his substantial rights. Finally, the court remanded for clarification of the judgment to reflect the sentence the district court said it would have imposed if the Armed Career Criminal Act did not apply.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Russell

Court: US Court of Appeals for the Eleventh Circuit
Docket: 18-11202
Opinion Date: May 4, 2020
Judge: Charles R. Wilson
Areas of Law: Criminal Law

Defendant was convicted of possessing a firearm and ammunition as an immigrant illegally or unlawfully in the United States. After defendant

appealed his conviction and sentence, the Supreme Court issued its decision in Rehaif v. United States, 588 U.S. ___, 139 S. Ct. 2191 (2019), which reversed a decision from this court and held that under 18 U.S.C. 922(g), the government must prove that a defendant knew "his status as a person barred from possessing a firearm" when he knowingly possessed a firearm. The Eleventh Circuit held that defendant established the necessary prejudice under plain error review and vacated defendant's section 922(g) conviction, remanding for further proceedings. In this case, the district court committed an error that was made plain by the Supreme Court in Rehaif. Furthermore, defendant has sufficiently shown a reasonable probability that but for the error, the outcome of his trial would have been different.

Read Opinion Are you a lawyer? **Annotate this case**.

Welch v. United States

Court: US Court of Appeals for the Eleventh Circuit
Docket: 14-15733
Opinion Date: May 6, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Eleventh Circuit affirmed the district court's denial of petitioner's 28 U.S.C. 2255 motion to vacate his sentence. The court held that defendant's prior 1996 Florida convictions for robbery qualified as violent felonies under the Armed Career Criminal Act's (ACCA) elements clause, and rejected his contention that the court's decision in his direct appeal carved out a narrow exception to pre-1997 Florida robbery convictions obtained in Florida's Fourth District Court of Appeal. The court also held that petitioner's prior Florida felony battery conviction was a violent felony under the ACCA in light of the court's holding in United States v. Vail-Bailon, 868 F.3d 1293 (11th Cir. 2017) (en banc), cert. denied, 138 S. Ct. 2620 (2018).

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Trujillo

Court: Arizona Supreme Court
Docket: CR-18-0531-PR

Opinion Date: May 4, 2020
Judge: Gould
Areas of Law: Constitutional Law, Criminal Law

The Supreme Court held that, for purposes of imposing mandatory sex offender registration under Ariz. Rev. Stat. 13-3821(A)(3), a judge has the authority to make the necessary factual finding that the victim is under the age of eighteen and that Arizona's sex offender registration statutes are civil regulatory statutes, not criminal penalties. Defendant was convicted by a jury of one count of sexual abuse. In reaching its verdict the jury determined that the victim was "fifteen or more years of age." At sentencing, the trial court ordered Defendant to register as a sex offender. Defendant objected, arguing that, pursuant to Apprendi v. New Jersey, 530 U.S. 466 (2000), a jury was required to find whether Defendant was under eighteen pursuant to section 13-3821(A)(3). The trial court denied the objection. The court of appeals affirmed. The Supreme Court affirmed, holding (1) Apprendi does not apply to factual findings that are necessary to impose registration because sex offender registration is a civil regulatory requirement, not a criminal penalty; and (2) the trial judge did not violate Apprendi by determining that the victim was under eighteen.

Read Opinion Are you a lawyer? **Annotate this case**.

Barnett v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 181
Opinion Date: May 7, 2020
Judge: Hudson
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's "motion for credit for time spent in custody," holding that the circuit court's findings were not clearly erroneous. In his motion, Appellant alleged that he was entitled to 312 days of jail-time credit and that the circuit court should enter a new sentencing order nunc pro tunc that reflected the correct amount of jail-time credit. The circuit court denied the motion. The Supreme Court affirmed, holding that the circuit court's denial of Appellant's motion was not clearly erroneous because Appellant failed to demonstrate a clerical error subject to correction.

Read Opinion Are you a lawyer? **Annotate this case**.

Mason v. Kelley

Court: Arkansas Supreme Court
Citation: 2020 Ark. 182
Opinion Date: May 7, 2020
Judge: Rhonda K. Wood
Areas of Law: Criminal Law

The Supreme Court affirmed the order of the circuit court dismissing Appellant's pro se petition for writ of habeas corpus, holding that Appellant stated no ground on which the writ could issue. Appellant was convicted of aggravated robbery, theft of property, and second-degree battery and sentenced as a habitual offender to an aggregate term of 660 months' imprisonment. The court of appeals affirmed. Appellant later petitioned for writ of habeas corpus, asserting that the trial court misapplied Arkansas's habitual-offender statutes. The circuit court dismissed the petition. The Supreme Court affirmed, holding that the issues Appellant raised in his petition for the writ should have been raised at trial, on direct appeal, or in a petition for postconviction relief.

Read Opinion Are you a lawyer? **Annotate this case**.

Ray v. Kelley

Court: Arkansas Supreme Court
Citation: 2020 Ark. 184
Opinion Date: May 7, 2020
Judge: Wynne
Areas of Law: Criminal Law

The Supreme Court dismissed Appellant's appeal from an order denying his pro se petition for permission to reinvest jurisdiction in the trial court to consider a petition for writ of error coram nobis, holding that the circuit court had no jurisdiction to consider the petition. Appellant entered negotiated guilty pleas to rape and other offenses. Appellant later filed a petition for writ of error coram nobis in the Chicot County Circuit Court, the court where he

was incarcerated, setting out two grounds for coram nobis relief. The circuit court denied the petition. The Supreme Court dismissed Appellant's appeal, holding that jurisdiction lay in the trial court where Appellant was convicted, which in this case was the Ashley County Circuit Court. Therefore, the Chicot County Circuit Court was without jurisdiction to address Appellant's coram nobis petition.

Read Opinion Are you a lawyer? **Annotate this case**.

Walker v. Kelley

Court: Arkansas Supreme Court
Citation: 2020 Ark. 183
Opinion Date: May 7, 2020
Judge: Rhonda K. Wood
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's pro se petition for declaratory judgment, holding that Appellant could not use a declaratory-judgment action to collaterally attack his criminal conviction. Appellant was convicted of first-degree murder and second-degree unlawful discharge of a firearm from a vehicle. The court of appeals affirmed. Years later, Appellant filed a petition for declaratory judgment alleging that he was denied due process in his criminal trial when the court admitted the prior testimony of an unavailable witness and that this admission violated the Confrontation Clause. The circuit court denied the petition. The Supreme Court affirmed, holding that a declaratory judgment action provided no relief on these grounds.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Flores

Court: Supreme Court of California
Docket: S116307
Opinion Date: May 4, 2020
Judge: Kruger
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction of three counts of first

degree murder and his sentence of death, holding that the three or four minor errors at Defendant's trial were harmless and did not interfere with his due process right to a fair trial. Specifically, the Supreme Court held (1) no error occurred during jury selection; (2) Defendant was not prejudiced by any misstatements by the prosecutor; (3) assuming certain evidence was inadmissible, the court's admonition to the jury and the court's instruction cured the resultant harm; (4) the trial court erred in admitting testimony that the victim was afraid of Defendant, but the error was harmless; and (5) Defendant's remaining allegations of error were without merit.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. Law

Court: California Courts of Appeal
Docket: E072845(Fourth Appellate District)
Opinion Date: May 5, 2020
Judge: Slough
Areas of Law: Constitutional Law, Criminal Law

In 2001, appellant Terrell Law and his codefendant Brett May committed a home invasion robbery, during which one of them shot and killed one of the residents. They were tried jointly in 2006 before two separately empaneled juries who found them both guilty of first degree felony murder with the special circumstance described in Penal Code section 190.2(a)(17(A) and (d). Though Law's jury found he was not the shooter, they nonetheless concluded he was a "major participant" in the underlying robbery and acted "with reckless indifference to human life." In 2018, the Legislature enacted Senate Bill No. 1437 (2017-2018 Reg. Sess.) which, among other things, amended the definition of felony murder in Penal Code section 189. The legislation also added Penal Code section 1170.95, which established a procedure for vacating murder convictions predating the amendment that could not be sustained under the new definition of felony murder. Law challenged the trial court's summary denial of his section 1170.95 petition to vacate his murder conviction, arguing the trial court erred by reviewing his record of conviction and determining the jury's true finding on the special circumstance rendered him ineligible for relief. The Court of Appeal concluded it was proper for a trial court to review the record of conviction when determining whether a section 1170.95 petitioner had stated a prima

facie claim for relief. Additionally, the Court concluded Law "undoubtedly qualifies" as a major participant who acted with reckless indifference to human life, a conclusion that rendered him ineligible for relief under section 1170.95. The Court therefore affirmed the order denying his petition.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. Sanchez

Court: California Courts of Appeal
Docket: E072647(Fourth Appellate District)
Opinion Date: May 7, 2020
Judge: Menetrez
Areas of Law: Constitutional Law, Criminal Law

Victor Sanchez was charged with first degree murder, but pled guilty to voluntary manslaughter. He filed a petition under Penal Code section 1170.95 to vacate that conviction. The trial court denied the petition, concluding that Sanchez was ineligible for relief because he was not convicted of murder. After review, the Court of Appeal joined other courts that held section 1170.95 did not apply to defendants convicted of voluntary manslaughter. The Court also rejected Sanchez's argument that section 1170.95 violated equal protection.

Read Opinion Are you a lawyer? **Annotate this case**.

Galeotti v. International Union of Operating Engineers

Court: California Courts of Appeal
Docket: A157785(First Appellate District)
Opinion Date: May 6, 2020
Judge: Henry E. Needham, Jr.
Areas of Law: Criminal Law, Labor & Employment Law, White Collar Crime

Galeotti, a former Union Local 3 employee, filed a complaint against Local 3 and three of individual union leaders, alleging that the individual defendants required union employees to pay them money to keep their jobs, lied about the reason for collecting the money, and caused Local 3 to terminate Galeotti's employment when he failed to pay the full amount demanded. The trial court dismissed his second amended complaint without leave to amend.

The court of appeal reversed in part, reasoning that a threat to terminate employment can provide a basis for an extortion claim and that the allegations of the second amended complaint stated a cause of action for wrongful termination in violation of the public policy underlying the extortion statutes. The complaint stated a cause of action for violations of the Racketeer Influenced and Corrupt Organizations Act (RICO; 18 U.S.C. 1961), based on the predicate acts of extortion, but did not state a cause of action for interference with prospective economic advantage.

Read Opinion Are you a lawyer? **Annotate this case**.

In re I.A.

Court: California Courts of Appeal
Docket: B296549(Second Appellate District)
Opinion Date: May 4, 2020
Judge: Tangeman
Areas of Law: Criminal Law, Juvenile Law

Where a juvenile court vacates its true finding on a generic murder allegation and redesignates it as a finding on an uncharged target offense, and does so before a minor has had the opportunity to contest the court's findings or orders, the minor may challenge the sufficiency of the evidence of the redesignated offense on appeal. The Court of Appeal held that there was insufficient evidence to support the juvenile court's decision sustaining the allegations that I.A. possessed a concealable firearm and committed vandalism. Therefore, the court reversed the juvenile court's findings, vacating the jurisdiction and disposition order and dismissing the Welfare and Institutions Code section 602 petition.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Edwards

Court: California Courts of Appeal
Docket: A158055(First Appellate District)
Opinion Date: May 1, 2020
Judge: Petrou
Areas of Law: Criminal Law

In 2006, Edwards fired an assault weapon into an apartment, killing the victim. Edwards pled guilty to possession of a firearm as a felon and was convicted of second-degree murder and shooting into an inhabited dwelling. Following the enactment of Senate Bill 1437, Edwards filed a Penal Code 1170.95 resentencing petition, checking form boxes indicating that he was convicted under a theory of felony murder or murder under the natural and probable consequences doctrine and that he could not now be convicted of 1st or 2nd-degree murder because of changes to Penal Code 188 and 189. Edwards submitted the jury instructions and the transcript of the prosecutor's closing remarks that Edwards acted with "both express malice, specific intent to kill, as well as implied malice," described as "an intentional act, the natural consequences of which are dangerous to human life, and at the time that the individual acted, they knew of the danger, and they deliberately acted with conscious disregard." The court denied the petition, finding that Edwards was convicted on a valid theory of murder that survived the statutory changes. The court of appeal affirmed. The superior court did not err in considering the record of conviction. Edwards could not meet the statutory prerequisites for even filing a section 1170.95 petition because he was not charged or convicted of second-degree felony murder or murder under the natural or probable consequences doctrine directed at accomplice liability.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Thomkins

Court: California Courts of Appeal
Docket: A141375(First Appellate District)
Opinion Date: May 1, 2020
Judge: Streeter
Areas of Law: Criminal Law

On Easter night in 2011, gunfire erupted at an Oakland bar-restaurant, leaving two people dead and five wounded. Thompkins and Fox were convicted of two counts of first-degree murder for the benefit of a criminal street gang, with firearm discharge enhancements, a multiple-murder special circumstance, and five counts of attempted murder with great bodily injury findings, gang enhancements, and firearm discharge enhancements.

Thompkins was convicted as the shooter and Fox as an accomplice. Both were sentenced to life in prison without possibility of parole, plus 224 years to life. After Thompkins was sentenced, Fox stated under oath he was the actual shooter and Thompkins knew nothing about Fox's intentions. Thompkins claimed this new testimony, and his attorney's incompetent reaction entitled him to a new trial and submitted a declaration by another gang member who was present that night. The court of appeal concluded that Thompkins's attorney was not ineffective for failing to bring a motion to recall the sentence followed by a new trial motion because Thompkins failed to show prejudice. The attempted murder convictions and related enhancements must be reversed for both defendants based on the flawed kill zone instruction. Introducing evidence that defendants admitted their gang affiliation at jail intake violated the defendants' privilege against self-incrimination but was harmless. There was some evidentiary error that was harmless due to the wealth of admissible evidence establishing the gang enhancements. Arguments based on the statutory amendments to Penal Code 188 and 189 must be raised in the trial court (section 1170.95). The case must be remanded so the judge may exercise his discretion whether to impose or strike the firearm enhancements on under Penal Code 12022.53.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Torres

Court: California Courts of Appeal
Docket: B295043(Second Appellate District)
Opinion Date: May 4, 2020
Judge: Wiley
Areas of Law: Criminal Law

After the trial court admitted a witness's former testimony, the Court of Appeal applied People v. Roldan (2012) 205 Cal.App.4th 969, 975–985, and reversed. Roldan held that, before invoking the former testimony exception, prosecutors should react appropriately to the impending deportation risk by following four steps: alert the defense to the risk; videotape the preliminary hearing testimony; use judicial measures to try to delay deportation; and consider an array of other specific measures. In this case, the prosecution conceded that prosecutors were simply unaware of Roldan and did not comply with it. The court held that Roldan controls the court's analysis

because the facts about prosecutorial diligence are weaker here than they were in Roldan, where the appellate court held for the defense. In this case, the record before deportation is of prosecutorial inaction where the prosecution's brief in this court admits the investigating officer did not do anything to ensure that the witness would not be deported, nor is there other evidence of prosecutorial efforts to delay the witness's departure or to videotape his testimony at the preliminary hearing.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Triplett

Court: California Courts of Appeal
Docket: B298914(Second Appellate District)
Opinion Date: May 1, 2020
Judge: Frances Rothschild
Areas of Law: Criminal Law

Defendant was convicted of assault with a deadly weapon, carjacking, and attempted murder. In the published portion of the opinion, the Court of Appeal held that the trial court erred by denying defense counsel's request to inform the jurors that they could have testimony of certain witnesses read back to them. The court also held that, under the circumstances in this case, the error was harmless.

Read Opinion Are you a lawyer? **Annotate this case**.

Colorado In Interest of G.S.S.

Court: Colorado Supreme Court
Citation: 2020 CO 32
Opinion Date: May 4, 2020
Judge: Brian D. Boatright
Areas of Law: Constitutional Law, Criminal Law, Juvenile Law

After being charged, fourteen-year-old G.S.S. was detained for more than three months without bail, even though he had not entered a plea and had not been tried on the charges against him. At that point, G.S.S.'s counsel filed a motion to dismiss, arguing that G.S.S.'s "right to a speedy trial" had been violated under section 19-2-509(4)(b), C.R.S. (2019). The trial court

agreed and dismissed the case against G.S.S. with prejudice, and the court of appeals affirmed in Colorado in Interest of G.S.S., 2019 COA 4M, __ P.3d __. The Colorado Supreme Court then granted certiorari to determine the proper remedy for a violation of the sixty-day limit in section 19-2-509(4)(b). The Supreme Court determined the remedy for a section 19-2-509(4)(b) violation was for the trial court to immediately hold a bail hearing and order the juvenile's release. Accordingly, the judgment of the court of appeals was reversed.

Read Opinion Are you a lawyer? **Annotate this case**.

Barringer v. Halkitis

Court: Florida Supreme Court
Docket: SC19-1071
Opinion Date: May 7, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court held that Jay Barringer's quo warranto petition filed in this case was a frivolous proceeding brought before the Supreme Court by a state prisoner and sanctioned Barringer by barring him from filing any further pro se requests for relief related to his criminal case. Barringer was convicted of one count of attempted sexual battery of a victim less than twelve years old and sentenced to twenty-five-years' imprisonment. In 2011, Barringer began filing petitions in the Supreme Court. The Court did not grant the relief sought in any of Barringer's filings. In the instant quo warranto petition Barringer challenged his conviction on the ground that the information was defective, a claim Barringer previously raised by way of a habeas petition. The Supreme Court denied the petition and found that Barringer abused the Court's limited judicial resources. The Court sanctioned Barringer by directing the Clerk of Court to reject any future pleadings or other requests for relief submitted by Barringer that are related to his criminal case, unless such filings are signed by a member of The Florida Bar in good standing.

Read Opinion Are you a lawyer? **Annotate this case**.

Franqui v. State

Court: Florida Supreme Court
Docket: SC19-203
Opinion Date: May 7, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the order of the circuit court denying Appellant's claim of intellectual disability, raised in successive motions for postconviction relief under Fla. R. Crim. P. 3.851, holding that the circuit court did not err in denying relief. Appellant was convicted of first-degree murder and sentenced to death in two separate cases. After the United States Supreme Court decided Hall v. Florida, 572 U.S. 701 (2014), Appellant filed successive motions for postconviction relief in both of his capital cases, asserting that the circuit court's denials of his previous claims of intellectual disability were based on the court's improper interpretation of Florida's intellectual disability statute. The circuit court summarily denied the motions. The Supreme Court reversed and remanded for an evidentiary hearing on the issue of intellectual disability. After a hearing, the circuit court denied the claim. The Supreme Court affirmed, holding (1) the circuit court did not err in denying Appellant's intellectual disability claim; and (2) Appellant was not entitled to relief under Hurst v. Florida, 136 S. Ct. 616 (2016), or Hurst v. State, 202 So. 3d 40 (Fla. 2016).

Read Opinion Are you a lawyer? **Annotate this case**.

Hicks v. State

Court: Florida Supreme Court
Docket: SC19-1978
Opinion Date: May 7, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court denied the instant mandamus petition filed by Hicks and sanctioned Hicks by barring him from filing any further pro se requests for relief related to his criminal case. Hicks was convicted of one count of lewd and lascivious conduct by a person over eighteen years of age on a victim under sixteen years of age. Since 2016, Hicks filed thirteen pro se requests for relief in the Supreme Court related to his criminal case. The

Court did not grant the relief sought in any of Hicks' filings. In the instant petition, Hicks sought a writ of mandamus compelling the circuit court to comply with the requirements of Fla. R. Crim. P. 3.850 by filing a copy of an order denying his second postconviction motion with the clerk of court. The Supreme Court dismissed the petition and found that Hicks abused this Court's limited judicial resources. The Court directed the Clerk of Court to reject any future pleadings or other requests for relief submitted by Hicks that are related to his criminal case, unless such filings are signed by a member of The Florida Bar in good standing.

Read Opinion Are you a lawyer? **Annotate this case**.

Burley v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0356
Opinion Date: May 4, 2020
Judge: Boggs
Areas of Law: Constitutional Law, Criminal Law

In 1992, Douglas Burley pled guilty to malice murder. He moved for an out-of-time appeal in 2019, claiming that his right to appeal was frustrated by his plea counsel's erroneous advice that he could not appeal his conviction because it was the product of a guilty plea. The trial court denied Burley's motion. After review, the Georgia Supreme Court vacated the trial court's judgment and remanded the case with direction to hold a hearing to determine whether ineffective assistance of counsel frustrated Burley's right to appeal.

Read Opinion Are you a lawyer? **Annotate this case**.

Carter v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0022
Opinion Date: May 4, 2020
Judge: David E. Nahmias
Areas of Law: Construction Law, Criminal Law

Brandon Carter was convicted by jury of malice murder and two firearm offenses in connection with the shooting death of Terrance Baker. On appeal, Carter contended the trial court erred by admitting certain hearsay statements into evidence and by violating his constitutional right to be present during his trial. Finding no reversible error, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Clarke v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0258
Opinion Date: May 4, 2020
Judge: Ellington
Areas of Law: Constitutional Law, Criminal Law

Rupert Clark was convicted by jury for the malice murder of his wife, Rosemarie Lebert-Clark. He was also convicted of possession of a firearm during the commission of a felony. On appeal, he argued he received ineffective assistance of trial counsel, and that the trial court erred in admitting certain evidence, violated the continuing witness rule by sending out with the deliberating jury printouts of text messages, and by failing to instruct the jury that a defendant's uncorroborated confession was not alone sufficient to warrant a conviction. Finding no reversible error after reviewing the trial court record, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Collins v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0195
Opinion Date: May 4, 2020
Judge: Harold D. Melton
Areas of Law: Constitutional Law, Criminal Law

Renita Collins was tried for murder along with co-defendant Michael Stallworth. Collins appealed her convictions for murder and possession of a firearm while in commission of a felony in connection with the shooting

death of Keith Jacobs. On appeal. Collins contended she was denied a fair trial due to juror misconduct, the trial court abused its discretion by not allowing her to subpoena juror testimony to show that misconduct had occurred, and the trial court abused its discretion when it failed to excuse a prospective juror for cause. Finding no reversible error, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Dawson v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0217
Opinion Date: May 4, 2020
Judge: Warren
Areas of Law: Constitutional Law, Criminal Law

Lavaris Dawson was convicted by jury of felony murder and other crimes in connection with the shooting death of Mamadou Camara. On appeal, Dawson challenged the sufficiency of the evidence supporting his convictions, and argued the trial court erred in admitting Dawson's statements to a detective during an interview because those statements were impermissibly induced by a hope of benefit, and that Dawson was denied his due process right to a timely appeal. After review, the Georgia Supreme Court disagreed and affirmed Dawson's convictions.

Read Opinion Are you a lawyer? **Annotate this case**.

Evans v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0007
Opinion Date: May 4, 2020
Judge: McMillan
Areas of Law: Constitutional Law, Criminal Law

Jimmy Evans was convicted by jury for murder and other crimes relating to the 2006 deaths of Tavoris Calhoun and Dezmon Thomas. On appeal, Evans argued that because he was visibly intoxicated at the time he made statements to law enforcement and consented to a search of his home and

person, the statements and consent were involuntarily given and the trial court should have granted his motion for new trial on this ground. Furthermore, Evans argued that his trial counsel was ineffective for failing to file a motion to suppress at trial on the same basis. Because Evans failed to show error or ineffective assistance of counsel, the Georgia Supreme Court affirmed his conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Hill v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0285
Opinion Date: May 4, 2020
Judge: Harold D. Melton
Areas of Law: Constitutional Law, Criminal Law

Esco Hill was convicted by jury of malice murder and other crimes relating to the stabbing death of Alford Morris in 2014. On appeal, Hill argued the trial court committed reversible error by requiring him to be visibly shackled for the duration of his six-day trial. After review of the trial court record, the Georgia Supreme Court concurred this was reversible error, consequently, reversed judgment of conviction. Because the Court concluded the evidence at trial was sufficient to sustain Hill's conviction, the State could re-try him. The Court did not address Hill's remaining enumerations of error, "as they are not likely to recur in the event of a retrial."

Read Opinion Are you a lawyer? **Annotate this case**.

Oliver v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0489
Opinion Date: May 4, 2020
Judge: McMillan
Areas of Law: Constitutional Law, Criminal Law

Jacquan Oliver entered a negotiated plea of guilty to felony murder in connection with the shooting death of Alexander Mixon. He appealed his

conviction and sentence, arguing that the trial court abused its discretion in finding a factual basis for his plea, and in determining the plea was voluntarily, knowingly and intelligently made. Finding no merit to these contentions, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Rosser v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0103
Opinion Date: May 4, 2020
Judge: Bethel
Areas of Law: Constitutional Law, Criminal Law

Larry Rosser was convicted by jury of malice murder and other crimes in connection with the death of Alexis Vereen. On appeal, Rosser challenged the sufficiency of the evidence presented against him at trial, and argued the trial court erred by not granting his motion for a mistrial, and by allowing the State to introduce a portion of Rosser's custodial statement to law enforcement. In addition, he argued he received constitutionally ineffective assistance of trial counsel. Finding no reversible error after reviewing the trial court record, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Spencer v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0871
Opinion Date: May 4, 2020
Judge: Keith R. Blackwell
Areas of Law: Constitutional Law, Criminal Law

Christopher Spencer was convicted by jury of murder and other crimes in connection with the fatal shootings of Sylvia Watson and Samuel White. Spencer appealed, claiming only that the evidence was insufficient to support his convictions. Finding no reversible error after reviewing the trial court record, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Styles v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0236
Opinion Date: May 4, 2020
Judge: Ellington
Areas of Law: Constitutional Law, Criminal Law

Derrick Styles was convicted by jury of felony murder and other crimes in connection with the shooting death of Alberto Lumens and the armed robbery fo Juan Lumens Garcia. On appeal, Styles contended the trial court erred in admitting into evidence a recording of an inculpatory telephone conversation between himself and a witness. He also argued his trial counsel was ineffective for failing to object to an allegedly improper comment by the prosecutor during closing argument. Finding no merit to these contentions, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Whitehead v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0171
Opinion Date: May 4, 2020
Judge: Ellington
Areas of Law: Constitutional Law, Criminal Law

Javis Whitehead was convicted by jury of murder and other crimes in connection with the shooting death of Dominique Larry. On appeal, Whitehead challenged the sufficiency of the evidence presented to rebut his claim of self-defense and to convict him for murder beyond a reasonable doubt. He also argued the trial court erred in denying his motion to suppress his custodial statement, and in refusing to excuse for cause the District Attorney from the panel of prospective jurors prior to the conclusion of voir dire. Finding no merit to these contentions, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Idaho v. Blythe

Court: Idaho Supreme Court - Criminal
Docket: 46992
Opinion Date: May 4, 2020
Judge: Roger S. Burdick
Areas of Law: Constitutional Law, Criminal Law

Nicholas Blythe appealed after he was convicted of possessing a controlled substance. He conditionally pled guilty, reserving the right to challenge his sentence. On appeal, he argued the district court erred in denying his motion to suppress certain evidence found because the evidence presented at trial was found in violation of Blythe's Fourth Amendment rights. After review, the Idaho Supreme Court determined the search at issue took place before an arrest occurred, and because no rationale justifying a search incident to arrest was sufficiently present here, the search of Blythe's shoes was not a valid search incident to arrest. Therefore, the district court erred in holding that the search was reasonable under the Fourth Amendment. Blythe's conviction was vacated, the district court order denying Blythe's motion to suppress was reversed, and the matter remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

Idaho v. Glodowski

Court: Idaho Supreme Court - Criminal
Docket: 47131
Opinion Date: May 6, 2020
Judge: Roger S. Burdick
Areas of Law: Constitutional Law, Criminal Law

David Glodowski appealed after he was convicted for failing to update his sex-offender registration in violation of Idaho Code section 18-8309. He argued the district court erred by ruling that his prior conviction under a Wisconsin statute was "substantially equivalent" to Idaho statutes that required sex-offender registration in Idaho. After review, the Idaho Supreme Court determined the district court improperly allowed the State to seek a

redetermination of the “substantially equivalent” element given that the Idaho Bureau of Criminal Identification made a final determination on that element. However, because the State put forth sufficient evidence to prove that element, and the district court’s jury instruction accomplished the same purpose, the Supreme Court concluded the error was harmless. Accordingly, the Court found no reversible error in the district court’s decision to grant the State’s motion and provide the jury instruction. Therefore, judgment of conviction was affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Idaho v. Jones

Court: Idaho Supreme Court - Criminal
Docket: 45905
Opinion Date: May 4, 2020
Judge: Roger S. Burdick
Areas of Law: Constitutional Law, Criminal Law

Timothy Jones was convicted by jury of trafficking heroin and possession of drug paraphernalia. On appeal, he argued the trial court erred in admitting certain evidence regarding his probation status, a knife found in the initial police search of his person, and that the trial court abused its discretion in arriving at his sentence. Finding no reversible error, the Idaho Supreme Court affirmed Jones' conviction and sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Gordon

Court: Iowa Supreme Court
Docket: 18-1099
Opinion Date: May 1, 2020
Judge: Brent R. Appel
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction for assault on a peace officer with a dangerous weapon, a felony, and several misdemeanors, holding that Defendant did not receive ineffective assistance of counsel. After Defendant pleaded guilty, he absconded. He was later returned to

custody. On appeal, Defendant argued that he received ineffective assistance of counsel because the plea bargain contained an unlawful term. Specifically, Defendant argued that the plea bargain's provision that he would be released from jail for a forty-eight-hour furlough after pleading guilty was illegal and that his trial counsel committed ineffective assistance in obtaining the illegal benefit for him. The Supreme Court affirmed, holding that where Defendant entered into the plea agreement with the illegally lenient sentence, he could not benefit from that sentence and then attack the plea bargain.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Craig

Court: Kansas Supreme Court
Docket: 119660
Opinion Date: May 1, 2020
Judge: Dan Biles
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's conviction and sentence for first-degree felony murder, holding that there was no error in the proceedings below. A jury found Defendant guilty of both first-degree felony murder and second-degree intentional murder. At sentencing, Defendant moved for a new trial and judgment notwithstanding the verdict, arguing that the jury must have had reasonable doubt on the first-degree felony murder theory because it convicted him of second-degree murder for the same killing. The district court dismissed the second-degree murder conviction and sentenced Defendant for the felony murder over his objection. The Supreme Court affirmed, holding (1) the district court did not err when it sentenced Defendant on felony murder instead of declaring a mistrial because Defendant did not establish that the jury failed to find each element of the felony murder beyond a reasonable doubt or that the jury's first- and second-degree murder verdicts were so irreconcilable as to require a new trial; and (2) the district court did not err in declining to give an instruction on voluntary intoxication.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Lemmie

Court: Kansas Supreme Court
Docket: 119439
Opinion Date: May 1, 2020
Judge: Carol A. Beier
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's convictions of first-degree felony murder, aggravated robbery, conspiracy to commit aggravated robbery, criminal possession of a firearm, fleeing and eluding, and interference with law enforcement, holding that Defendant's arguments on appeal failed. Specifically, the Supreme Court held (1) any possible violation of Defendant's Fifth Amendment right in the admission of a witness's testimony about Defendant giving the witness phone passcodes was undoubtedly harmless; (2) the district court did not err by admitting hearsay statements as statements of a coconspirator and contemporaneous statements; (3) the State introduced sufficient evidence to convict Defendant of first-degree murder; and (4) the district judge did not abuse its discretion by admitting testimony that Defendant was upset over a meth pipe that went missing.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Mullen

Court: Maine Supreme Judicial Court
Citation: 2020 ME 56
Opinion Date: May 5, 2020
Judge: Connors
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed Defendant's conviction for reckless conduct and aggravated criminal mischief, holding that the trial court did not abuse its discretion by offering Defendant a continuance of the trial in lieu of excluding his medical records. On appeal, Defendant argued that the trial court abused its discretion by denying his motion to suppress his personal medical records as a sanction for the State's late seizure of the records. The Supreme Judicial Court agreed that the State's conduct undermined the purpose of Maine Rule of Unified Criminal Procedure 18(b) but that the court's offer of a continuance in lieu of the exclusion of the evidence

constituted an appropriate response to the State's conduct.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. Billingslea

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12715
Opinion Date: April 30, 2020
Judge: Cypher
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Judicial Court affirmed Defendant's convictions and the decision of the Appeals Court denying Defendant's motion to vacate the entry of his appeal from his convictions in that court and to have the case entered directly in the Supreme Judicial Court, holding that a direct appeal from the third conviction of a habitual offender pursuant to Mass. Gen. Laws ch. 279, 25(b) may be entered in the Appeals Court. Defendant was indicted for serious felonies arising from a brutal attack and rape. In addition to charging the specific felony, each indictment also alleged that the sentence for that felony should be enhanced pursuant to the habitual criminal provision Mass. Gen. Laws ch. 279, 25(a) or the habitual offender provision of section 25(b), or both. After he was convicted, Defendant moved to have the case entered directly in the Supreme Judicial Court. The Appeals Court denied the motion. The Supreme Judicial Court affirmed Defendant's convictions, holding (1) this direct appeal was entitled to the unique review prescribed by Mass Gen. Laws ch. 278, 33E, and the Appeals Court may conduct such section 33E review; (2) Defendant was not impermissibly allowed to waive his right to a jury trial on the sentencing enhancement provisions of the indictments; and (3) Defendant was not entitled to reversal of his convictions on any other ground.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. Martin

Court: Massachusetts Supreme Judicial Court
Docket: SJC-08768
Opinion Date: May 5, 2020

Judge: Ralph D. Gants
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Judicial Court affirmed Defendant's conviction of murder in the first degree and the denial of his motion for a new trial and declined to exercise its authority under Mass. Gen. Laws ch. 278E to reduce Defendant's conviction to murder in the second degree, holding that Defendant was not entitled to relief on any of his allegations of error. Defendant was convicted of murder in the first degree on the theory of felony-murder. Defendant filed a motion for a new trial, which was denied. The Supreme Judicial Court affirmed, holding (1) Defendant's motion for a new trial was correctly denied because Defendant was not prejudiced by counsel's ineffective assistance; (2) this Court declines to extend the reach of the Court's holding in Commonwealth v. Brown, 477 Mass. 805 (2017), to Defendant's case; and (3) trial judge erred when he declined Defendant's request that the jury be instructed on the elements of voluntary and involuntary manslaughter, but the error was not prejudicial in the context of the judge's other instructions.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. Tavares

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12631
Opinion Date: May 6, 2020
Judge: Lowy
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed Defendant's conviction of murder in the first degree on theories of deliberate premeditation and extreme atrocity or cruelty and declined to exercise its power pursuant to Mass. Gen. Laws ch. 278, 33E to reduce the conviction to manslaughter, holding that there was no reversible error in the proceedings below. Specifically, the Supreme Judicial Court held (1) the trial judge did not err by denying Defendant's requests for a jury instruction pursuant to Commonwealth v. Croft, 345 Mass. 143 (1962); (2) the trial judge did not err by denying Defendant's motions for a required finding of not guilty under Croft because a rational jury could have found that Defendant was guilty of murder in the first degree

on both the theories of premeditation and extreme atrocity or cruelty; and (3) there was no basis for reducing Defendant's sentence or ordering a new trial.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Branch

Court: Minnesota Supreme Court
Docket: A18-1055
Opinion Date: May 6, 2020
Judge: Lorie Skjerven Gildea
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's sentences for drive-by shooting at an occupied vehicle and second-degree assault, holding that Minn. Stat. 609.035 did not prohibit the sentences for both offenses when the crimes arose from a single behavioral incident. The district court sentenced Defendant to forty-eight months for drive-by shooting at an occupied vehicle and thirty-six months for second-degree assault and imposed the two sentences to run concurrently. The court of appeals affirmed. The Supreme Court affirmed, holding that, under this Court's analysis in State v. Ferguson, 808 N.W.2d 586 (Minn. 2012), the district court properly imposed multiple sentences in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

Galloway v. Mississippi

Court: Supreme Court of Mississippi
Citation: 2018-CA-01427-SCT
Opinion Date: May 7, 2020
Judge: Beam
Areas of Law: Constitutional Law, Criminal Law

Leslie Galloway appealed the denial of his 2015 petition for post-conviction relief (PCR) pertaining to his 2007 guilty plea to carjacking, a conviction that was used as an aggravating circumstance in Galloway's 2010 capital-murder trial at which Galloway received a death sentence. Galloway claimed in the petition that his defense counsel Wendy Martin had an actual

conflict of interest because, before becoming his defense counsel, Martin had served as an assistant district attorney in the same case, unbeknownst to Galloway. The trial court ruled that Galloway's PCR claim was time barred under Mississippi's Uniform Post-Conviction Collateral Relief Act (UPCCRA), having been filed more than seven years after Galloway's conviction for carjacking. The trial court alternatively found no merit to Galloway's PCR claim, time bar notwithstanding. Accordingly, the trial court denied Galloway's PCR petition. The Mississippi Supreme Court agreed with the trial court that Galloway's PCR claim was time barred under the UPCCRA. The Court also agreed there was no merit to Galloway's PCR claim.

Read Opinion Are you a lawyer? **Annotate this case**.

City of Missoula v. Zerbst

Court: Montana Supreme Court
Citation: 2020 MT 108
Opinion Date: May 5, 2020
Judge: Beth Baker
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court reversed Defendant's conviction for sexual assault, holding that the municipal court erred when it instructed the jury on a definition of "consent" from the 2017 sexual assault statute and not the applicable 2015 statute, and the erroneous jury instruction prejudicially affected Defendant's substantial rights. At trial, the court instructed the jury, over Defendant's objection, on the definition of consent contained in recent amendments to the sexual assault statute. On appeal, Defendant argued that the municipal court failed to apply the correct law when instructing the jury on the elements of the claimed offense. The district court denied the appeal. The Supreme Court reversed, holding (1) the instructions, as a whole, did not fully and fairly instruct the jury on the law applicable to the case; and (2) Defendant's substantial due process right was prejudiced by the erroneous jury instruction.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Degarmo

Court: Nebraska Supreme Court
Citation: 305 Neb. 680
Opinion Date: May 1, 2020
Judge: Stacy
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction of driving under the influence, holding that Defendant consented to a chemical test of his urine and, therefore, the results of the urine test were admissible. A law enforcement officer stopped Defendant for an expired registration. Based on his observations, the officer, a certified drug recognition evaluation expert, administered field sobriety tests. The officer concluded that Defendant was under the influence of marijuana arrested Defendant for driving under the influence and then took him to a detoxification center. Thereafter, a chemical test of Defendant's urine confirmed the presence of marijuana. On appeal, Defendant challenged the admission of the results of the urine test. The Supreme Court affirmed, holding that Defendant voluntarily consented to the warrantless search of his urine, and therefore, the search fell within a recognized exception to the warrant requirement.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Holz

Court: New York Court of Appeals
Citation: 2020 NY Slip Op 02682
Opinion Date: May 7, 2020
Judge: Fahey
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Court of Appeals held that N.Y. Crim. Proc. Law (CPL) 710.70(2) grants a defendant the right to review of a suppression decision when the order related exclusively to a count that was satisfied by a guilty plea but was not one to which the defendant pleaded guilty. Defendant was charged with two counts of burglary in the second degree. The first count related to a laptop computer, and the second count related to jewelry. Defendant moved to suppress the jewelry, but Supreme Court denied the motion. Defendant then pleaded guilty to one count of burglary in the second degree as charged in the count pertaining to the theft of the laptop computer, in satisfaction of the

count charging the burglary of jewelry. On appeal, Defendant argued that Supreme Court erred in denying his motion to suppress the jewelry. The Appellate Division affirmed, concluding that it was jurisdictionally precluded from reviewing the suppression order. The Court of Appeals reversed, holding (1) Defendant's right to appellate review of Supreme Court's suppression order was secured by CPL 710.70(2); and (2) because the Appellate Division did not reach the underlying suppression question the case must be remitted to the Appellate Division for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Maffei

Court: New York Court of Appeals
Citation: 2020 NY Slip Op 02680
Opinion Date: May 7, 2020
Judge: DiFiore
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Court of Appeals affirmed the order of the Appellate Division concluding on direct appeal that Defendant was not entitled to relief on his ineffective assistance of counsel claim, holding that Defendant, on this record, did not sustain his burden to establish that counsel was constitutionally ineffective. After a jury trial, Defendant was convicted of second-degree murder. On appeal, Defendant argued that his trial counsel's failure to challenge a prospective juror constituted ineffective assistance of counsel. The Appellate Division affirmed. The Court of Appeals affirmed, holding (1) the record was inadequate to review Defendant's ineffective assistance of counsel claim; and (2) the appropriate procedure for the litigation of Defendant's challenge to his counsel's performance was a N.Y. Crim. Proc. Law 440.10 motion.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Bailey

Court: North Carolina Supreme Court
Docket: 360A19
Opinion Date: May 1, 2020

Judge: Davis
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the decision of the court of appeals affirming the order of the trial court denying Defendant's motion to suppress evidence seized during the execution of a search warrant, holding that the warrant supported by probable cause. Defendant pled guilty to the offense of trafficking in cocaine while preserving his right to appeal the denial of his motion to suppress. On appeal, Defendant argued that the trial court erred in denying his motion to suppress because the facts contained in the affidavit were insufficient to establish probable cause to search his residence. The court of appeals affirmed. The Supreme Court affirmed, holding that the affidavit contained facts that were sufficient to provide a nexus between the residence and suspected criminal activity, and therefore, the warrant was supported by probable cause.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Ellis

Court: North Carolina Supreme Court
Docket: 340A19
Opinion Date: May 1, 2020
Judge: Robin E. Hudson
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court reversed the decision of the Court of Appeals affirming the trial court's denial of Defendant's motion to suppress evidence, holding that there was no reasonable suspicion to justify the law enforcement officer's stop when Defendant signaled with his middle finger from the passenger side window of a moving vehicle. While assisting a stranded motorist, the officer turned his attention to another car traveling on the roadway, a white SUV. Defendant had his arm outside the passenger window and gestured with his middle finger, making an up-and-down motion. Believing that Defendant was committing the crime of disorderly conduct, the officer pursued and then stopped the SUV. At trial, Defendant moved to suppress the officer's testimony, arguing that there was no reasonable suspicion to justify the stop. The trial court denied the motion. Defendant pleaded guilty to resisting, delaying, or obstructing a public

officer. The court of appeals affirmed the trial court's denial of Defendant's motion to suppress. The Supreme Court reversed, holding that the specific, articulable facts did not establish reasonable suspicion of the crime of disorderly conduct.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Hobbs

Court: North Carolina Supreme Court
Docket: 263PA18
Opinion Date: May 1, 2020
Judge: Earls
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court reversed Defendant's conviction, holding that the trial court clearly erred in ruling that Defendant failed to prove purposeful discrimination with respect to the State's use of peremptory challenges to strike three jurors without considering all of the evidence presented by Defendant. Defendant was found guilty of one count of first-degree murder and other crimes. On appeal, Defendant argued that the trial court erred by failing to grant three objections that he made under Batson v. Kentucky, 476 U.S. 79 (1986). The court of appeals affirmed Defendant's convictions. The Supreme Court reversed, holding (1) the court of appeals erred in its analysis of Defendant's Batson claims with respect to the three jurors; and (2) as to all three jurors, remand was required for reconsideration of whether Defendant proved purposeful discrimination in each case.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Mylett

Court: North Carolina Supreme Court
Docket: 6A19
Opinion Date: May 1, 2020
Judge: Earls
Areas of Law: Criminal Law

The Supreme Court reversed the decision of the court of appeals affirming the trial court's judgment convicting Defendant for conspiracy to commit

harassment of a juror, holding that the trial court erred in denying Defendant's motion to dismiss the conspiracy charge for insufficient evidence. Defendant was convicted of conspiracy to commit harassment of a juror because of his actions at a courthouse following his twin brother's conviction for assault on a government official. On appeal, the court of appeals concluded that the trial court did not err in denying Defendant's motion to dismiss the conspiracy charge for insufficient evidence. The Supreme Court reversed, holding that the evidence in Defendant's trial was insufficient to raise anything more than mere conjecture that he had made an agreement with another person to threaten or intimidate a juror.

Read Opinion Are you a lawyer? **Annotate this case**.

Dodge v. North Dakota

Court: North Dakota Supreme Court
Citation: 2020 ND 100
Opinion Date: May 7, 2020
Judge: Gerald W. VandeWalle
Areas of Law: Constitutional Law, Criminal Law

Richard Dodge appealed from a district court order denying his application for post-conviction relief. Dodge was charged with five felonies and a misdemeanor in December 2015. Dodge was appointed counsel. In April 2016, Dodge's counsel moved the court to withdraw because the attorney-client relationship was "irreparably broken and rendered unreasonably difficult." The court granted the motion, and Dodge was appointed substitute counsel in May 2016. In July 2016, Dodge himself filed a "motion to dismiss counsel." The court denied Dodge's motion. Five months after the deadline for motions and plea agreements, Dodge's counsel sought to have Dodge submit to a psychiatric examination. This request was denied, the trial court found no evidence, and the the court itself made no observations, that Dodge was incompetent to stand trial. After this denial, Dodge himself again moved to dismiss his trial counsel, and due to the allegations Dodge made in his motion, counsel moved to withdraw. The trial court denied both motions, and instead, required the attorney to appear as standby counsel and assist Dodge during trial if requested, but relieved him of any further obligations to consult with Dodge. The case proceeded to trial. At the beginning of trial, the court gave Dodge the option of representing himself or

having his attorney represent him. Dodge chose to have his attorney represent him. Because his attorney had not prepared for trial and had no communication with Dodge since he moved to withdraw, Dodge's attorney asked for a brief recess to consult with Dodge. During the recess, a settlement was reached. Dodge agreed to enter Alford pleas on all counts, waived a presentence investigation, and agreed to be sentenced immediately after entering his pleas. Dodge was immediately sentenced following his guilty pleas, and thereafter sought post-conviction relief on grounds he was not competent to enter his pleas, and that he received ineffective assistance of trial counsel. After review, the North Dakota Supreme Court concluded the district court's finding that Dodge was competent when he entered his pleas was not clearly erroneous, and disposed of his claim of ineffective assistance of counsel.

Read Opinion Are you a lawyer? **Annotate this case**.

Hewitt v. NDDOT

Court: North Dakota Supreme Court
Citation: 2020 ND 102
Opinion Date: May 7, 2020
Judge: Lisa K. Fair McEvers
Areas of Law: Criminal Law, Government & Administrative Law

Larry Hewitt appealed a district court judgment affirming the North Dakota Department of Transportation's revocation of his driving privileges. Hewitt claimed the Department's hearing file was improperly admitted at the administrative hearing. After review, the North Dakota Supreme Court affirmed, concluding the hearing file was properly admitted as a self-authenticating copy of an official record.

Read Opinion Are you a lawyer? **Annotate this case**.

Kastet v. NDDOT

Court: North Dakota Supreme Court
Citation: 2020 ND 91
Opinion Date: May 7, 2020
Judge: Daniel J. Crothers

Areas of Law: Criminal Law, Government & Administrative Law

The North Dakota Department of Transportation (Department) appealed the district court's reversing a hearing officer's decision suspending Holden Kastet's driving privileges for 365 days. The Department argued the hearing officer did not abuse his discretion in admitting the chemical breath test, and State Highway Patrol Trooper King scrupulously complied with the approved method for testing Kastet's breath on the Intoxilyzer 8000. After review, the North Dakota Supreme Court concurred with the Department and reversed the district court judgment. The matter was remanded with instructions to reinstate the hearing officer's decision.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Dahl

Court: North Dakota Supreme Court
Citation: 2020 ND 87
Opinion Date: May 7, 2020
Judge: Jerod E. Tufte
Areas of Law: Constitutional Law, Criminal Law

The State of North Dakota appealed a district court order denying its motion to resume prosecution against Matthew Dahl and dismissing the case. In December 2014, the State charged Dahl with two counts of theft. Dahl did not appear on the charges until he was arrested on a bench warrant in February 2017. In mid-April 2017, the State mailed Dahl a pretrial diversion agreement. Dahl signed and returned the notarized agreement dated May 3, 2017. On May 9, 2017, the state's attorney signed and filed the agreement with the district court, and the court approved the agreement the same day. Under the agreement, the State agreed to suspend prosecution for "two years from the date of execution" conditioned on Dahl's timely payment of restitution. Dahl failed to make minimum monthly restitution payments. On June 6, 2019, the State moved to resume prosecution, alleging Dahl violated the pretrial diversion agreement by his non-payment. The district court held a hearing on the State's motion in August 2019. The court concluded the pretrial agreement was executed when Dahl signed it on May 3, 2017. The court then denied the State's motion to resume prosecution as untimely under N.D.R.Crim.P. 32.2(d)(2), and dismissed the complaint

against Dahl. After review, the North Dakota Supreme Court reversed, concluding the district court erred in determining the State's motion was untimely, and remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Foster

Court: North Dakota Supreme Court
Citation: 2020 ND 85
Opinion Date: May 7, 2020
Judge: Jon J. Jensen
Areas of Law: Constitutional Law, Criminal Law

Akeem Foster was convicted by jury of Terrorizing and Carrying a Concealed Weapon. Foster contended on appeal he was denied a fair trial because he was asked during cross-examination if other witnesses were lying and because the prosecutor expressed personal beliefs about the evidence during closing arguments. Foster also argued there was insufficient evidence to convict him of either charge. After review, the North Dakota Supreme Court affirmed Foster's conviction for Carrying a Concealed Weapon, but reversed his conviction for Terrorizing. The Court found Foster was improperly asked to provide an opinion on the veracity and credibility of the State's witnesses. The improper questioning was prejudicial and denied Foster a fair trial on the terrorizing charge.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Kolstad

Court: North Dakota Supreme Court
Citation: 2020 ND 97
Opinion Date: May 7, 2020
Judge: Gerald W. VandeWalle
Areas of Law: Constitutional Law, Criminal Law

In December 2018, Officer Nelson of the University of North Dakota Police Department conducted a traffic stop of Stanley Kolstad for suspicion of driving under the influence. Kolstad performed field sobriety tests and a preliminary breath test (PBT). Prior to performing the PBT, Kolstad informed

Nelson that he had asthma. Nelson testified he was unable to obtain a PBT result because Kolstad was filling his cheeks with air while performing the test. Kolstad was arrested for DUI and refusing to submit to a chemical test. Kolstad was transported to the UND police station to be given an Intoxilyzer breath test. Prior to the Intoxilyzer test, Nelson read Kolstad the implied consent advisory. But, because Nelson was not a certified operator of the Intoxilyzer machine, Officer Waltz conducted the test. Prior to the test, Kolstad informed Waltz he had asthma. The Intoxilyzer test results were deficient. Waltz testified Kolstad was not providing enough air for the test machine to provide a valid result. Kolstad was charged with driving under the influence and refusing to submit to a chemical test. Kolstad's counsel made a discovery request to the State seeking copies of any audio or video recordings taken by police officers. Kolstad's counsel also requested the State inform him whether any sound or video recordings taken of Kolstad were subsequently "altered, edited, destroyed, or discarded." The State provided Kolstad's counsel with dash camera footage from Nelson's police car that had been taken at the scene of the arrest, but the State did not provide any body camera footage from either Nelson or Waltz. Upon learning that Waltz's body camera footage was successfully uploaded to UND servers, Kolstad's counsel moved to dismiss the case because the State did not provide any body camera footage in discovery as requested. The district court ultimately dismissed the refusal to submit to a chemical breath test charge as a sanction for failing to provide the body camera footage. The State appealed, arguing the alleged discovery violation did not rise to a constitutional violation of Kolstad's due process rights, and the district court abused its discretion in dismissing the refusal charge. Kolstad argued the district court's order dismissing the refusal charge was not appealable, and if it was, the court did not abuse its discretion in dismissing the charge. The North Dakota Supreme Court concluded there was nothing in the record to indicate the district court adequately considered an alternative or less severe sanction to dismissal, and by not considering a less severe sanction, the trial court erred. The district court's order dismissing the refusal charge was reversed, and the matter remanded for further proceedings.

Read Opinion

Are you a lawyer? **Annotate this case**.

North Dakota v. Michel

Court: North Dakota Supreme Court
Citation: 2020 ND 101
Opinion Date: May 7, 2020
Judge: Jerod E. Tufte
Areas of Law: Constitutional Law, Criminal Law

Kevin Michel was convicted by jury of knowingly receiving stolen property. Jamestown Police began investigating theft of tires from Northwest Tire in October 2017. About ten months later, Thomas Melland and Andrew Heckelsmiller became suspects in the investigation. Heckelsmiller told police he had sold stolen tires to Michel. In August 2018, Detective LeRoy Gross spoke with Michel about the stolen tires. Michel acknowledged he had bought tires from Heckelsmiller and Melland. Michel also told Detective Gross he stopped buying tires from Heckelsmiller and Melland after seeing a Facebook post from Northwest Tire offering a $500 reward for information regarding stolen tires. Detective Gross told Michel, "There's going to be a lot of restitution these two boys are going to have to come up with unless we can get some tires back." Michel said he had sold several of the tires but still had some of them. Michel turned over seven new tires to Detective Gross. Representatives from Northwest Tire and J&L Service identified the tires as some of those stolen from their shops. During the jury's deliberations, the jury submitted a note with written questions to the court. Michel argued on appeal the district court erred by not specifically answering the jury's questions and instead referring them to the existing jury instructions. After review, the North Dakota Supreme Court affirmed the criminal judgment, except as to the award of restitution. The award was reversed because the district court awarded more than what was required to make the victims whole. The matter was remanded for a redetermination of restitution.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Wayland

Court: North Dakota Supreme Court
Citation: 2020 ND 106
Opinion Date: May 7, 2020
Judge: Jon J. Jensen
Areas of Law: Constitutional Law, Criminal Law

Joey Wayland appealed after he was convicted by jury of Theft of Property and Possession of Drug Paraphernalia. Wayland contended his case should have been dismissed because his right to a speedy trial was violated by a continuance of his trial from March 11, 2019 to April 8, 2019. Wayland also contended the district court violated his right to remain silent by ordering him to submit to a mental health evaluation. Finding no reversible error, the North Dakota Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Schwindt v. Sorel

Court: North Dakota Supreme Court
Citation: 2020 ND 92
Opinion Date: May 7, 2020
Judge: Lisa K. Fair McEvers
Areas of Law: Constitutional Law, Criminal Law, Government & Administrative Law

Gregory Schwindt appealed a district court judgment affirming a Department of Transportation hearing officer's revocation of his driving privileges for 180 days. Schwindt argued North Dakota's implied consent and refusal laws were unconstitutional, the hearing officer erred by considering the results of the horizontal gaze nystagmus (HGN) test, and the hearing officer erred in finding he refused to take a chemical test. After review, the North Dakota Supreme Court concluded the hearing officer's findings of fact were supported by a preponderance of the evidence, the conclusions of law were sustained by the findings of fact, and the decision to revoke Schwindt's driving privileges was in accordance with the law.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. McDougald v. Greene

Court: Supreme Court of Ohio
Citation: 2020-Ohio-2782
Opinion Date: May 6, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court denied a writ of mandamus sought by Relator to

compel Respondent, the public-records custodian at the Southern Ohio Correctional Facility (SOCF), to provide Relator with three public records and to pay Relator statutory damages and court costs associated with this litigation, holding that Relator was not entitled to either a writ of mandamus nor statutory damages. When Relator was an inmate at SOCF he submitted a public-records request to Respondent seeking three documents. Respondent provided one of the three documents. Relator then filed a complaint for a writ of mandamus seeking an order compelling Respondent to provide the two documents and to pay statutory damages and court costs associated with this litigation. The Supreme Court denied the writ of mandamus on the merits, holding that Respondent's response to Relator fully satisfied Respondent's obligations under Ohio Rev. Code 149.43, and therefore, Relator was not entitled a writ of mandamus, and there was no basis to award statutory damages.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Parker Bey v. Byrd

Court: Supreme Court of Ohio
Citation: 2020-Ohio-2766
Opinion Date: May 5, 2020
Judge: Maureen O'Connor
Areas of Law: Criminal Law

The Supreme Court affirmed in part and reversed in part the judgment of the court of appeals denying Appellant's complaint for a writ of mandamus to compel the Cuyahoga County Clerk of Courts to produce various court records and denying the clerk's request that Appellant be declared a vexatious litigator, holding that the court of appeals erred in denying Appellant's complaint on the grounds that he did not invoke the Rules of Superintendence as the basis for his request. Appellant sought copies of journal entries from his criminal case and a copy of the clerk of courts' records-retention schedule. The clerk largely denied the request. Appellant then filed a complaint for a writ of mandamus. The court of appeals denied Appellant's request for mandamus relief, concluding that the clerk had no clear legal duty to provide the requested records. The Supreme Court reversed, holding (1) this action to compel the production of journal entries from a 1995 case was properly brought under the Public Records Act; and

(2) this Court declines to impose sanctions on Appellant or to declare him a vexatious litigator.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Dangler

Court: Supreme Court of Ohio
Citation: 2020-Ohio-2765
Opinion Date: May 5, 2020
Judge: DeWine
Areas of Law: Criminal Law

The Supreme Court reversed the judgment of the court of appeals vacating Defendant's conviction and sentence and reinstated the trial court's acceptance of Defendant's plea of no contest to sexual battery, holding that the trial court did not completely fail to comply with Crim.R.11(C)(2)(a), and there was nothing in the record to support a conclusion that Defendant would not have entered his plea had the trial court been more detailed in its explanation. On appeal, Defendant sought to vacate his plea of no contest, arguing that his plea was invalid because the trial court erred by not explaining more fully the obligations and restrictions that went with his status as a sex offender, in violation of Crim. R. 11(C)(2)(a). The court of appeals vacated the conviction without requiring Defendant to show prejudice, concluding that the trial court had completely failed to comply with Crim. R. 11(C)(2)(a). The Supreme Court reversed, holding (1) the trial court did not completely failed to comply with Crim R. 11(C)(2)(a)'s maximum-penalty-advisement requirement; and (2) because Defendant did not establish prejudice, he was not entitled to have his no-contest plea vacated for a failure to comply with Crim.R. 11(C).

Read Opinion Are you a lawyer? **Annotate this case**.

Oregon v. Haji

Court: Oregon Supreme Court
Docket: S066254
Opinion Date: May 7, 2020
Judge: Nakamoto

Areas of Law: Constitutional Law, Criminal Law

After a grand jury issued an indictment charging defendant Hanad Ali Haji with multiple offenses, the district attorney determined that the indictment could be challenged by demurrer because the basis for joining those offenses was not expressly alleged. Instead of seeking another indictment from the grand jury, the district attorney obtained leave from the trial court to amend the indictment by adding allegations specifying the statutory basis for joinder, without adding factual allegations about the crimes. Defendant was convicted on some of the charges at trial, and the Court of Appeals affirmed. The issue this case presented for the Oregon Supreme Court's review centered on whether the district attorney could add allegations specifying the statutory basis for joinder of multiple offenses to an indictment instead of resubmitting the case to the grand jury. The Supreme Court determined that neither the statute permitting joinder of multiple offenses in a single indictment nor Article VII (Amended), section 5(6), of the Oregon Constitution precluded a district attorney, with approval of the trial court, from amending an indictment to add allegations specifying the statutory basis for joinder of multiple offenses. The Supreme Court affirmed the decision of the Court of Appeals, based in part on different reasoning, and affirmed the judgment of the circuit court.

Read Opinion Are you a lawyer? **Annotate this case**.

South Carolina v. Durant

Court: South Carolina Supreme Court
Docket: 27964
Opinion Date: May 6, 2020
Judge: Kaye Gorenflo Hearn
Areas of Law: Constitutional Law, Criminal Law

Appellant Larry Durant was convicted of second-degree criminal sexual conduct (CSC) for sexually abusing a teenage girl in his church office where he served as the pastor. Durant contended the trial court improperly permitted the State to introduce evidence of prior sexual abuse allegations as evidence of a common scheme or plan under Rule 404(b), SCRE, and that the State committed a "Brady" violation by failing to accurately disclose the criminal history of its witness. After review, the South Carolina Supreme

Court affirmed the admissibility of the girls' testimony. "[W]hile the State failed to disclose the criminal background information of its witness, we find this information was not material." The Court found Durant exercised his position of trust, authority, and spiritual leadership to hold private prayer meetings with teen girls who had grown up in his church. He told them he was praying for their health and good fortune, and represented that part of this process was touching them sexually and having intercourse. Durant then warned the girls of misfortune if they refused or told anyone. Moreover, he used scripture as a means of grooming the children into performing sex acts. "These facts demonstrate the requisite logical connection between the prior acts of sexual abuse and the one forming the basis of the crime charged." The Court therefore affirmed Durant's conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

South Carolina v. Perry

Court: South Carolina Supreme Court
Docket: 27963
Opinion Date: May 6, 2020
Judge: Few
Areas of Law: Constitutional Law, Criminal Law

Petitioner Wallace Perry was convicted on two counts of criminal sexual conduct (CSC) with a minor in the first degree and two counts of CSC with a minor in the second degree for sexually assaulting two of his biological daughters. Prior to Perry's trial, the State made a motion to admit the testimony of Perry's stepdaughter from an earlier marriage that Perry sexually assaulted her twenty-two to twenty-seven years earlier. The State argued the trial court should not exclude the stepdaughter's testimony under Rule 404(b) of the South Carolina Rules of Evidence because it fit the "common scheme or plan" exception. Perry objected to this testimony. The trial court initially reserved ruling on the issue, but later indicated it was inclined to allow the stepdaughter to testify. The jury convicted Perry on all counts, and the trial court sentenced him to thirty years in prison. The court of appeals affirmed. The South Carolina Supreme Court determined it was not enough to meet the "logical connection" standard for admission of other crimes under the common scheme or plan exception to Rule 404(b) that the defendant previously committed the same crime. "When evidence of other

crimes is admitted based solely on the similarity of a previous crime, the evidence serves only the purpose prohibited by Rule 404(b), and allows the jury to convict the defendant on the improper inference of propensity that because he did it before, he must have done it again. ...The common scheme or plan exception demands more." The Supreme Court held State must show a logical connection between the other crime and the crime charged such that the evidence of other crimes "reasonably tends to prove a material fact in issue." The State must also convince the trial court that the probative force of the evidence when used for this legitimate purpose is not substantially outweighed by the danger of unfair prejudice from the inherent tendency of the evidence to show the defendant's propensity to commit similar crimes. In this case, the State did not meet its burden. Conviction was reversed and the matter remanded for a new trial.

Read Opinion Are you a lawyer? **Annotate this case**.

South Carolina v. Quinn

Court: South Carolina Supreme Court
Docket: 27966
Opinion Date: May 6, 2020
Judge: Kaye Gorenflo Hearn
Areas of Law: Constitutional Law, Criminal Law, White Collar Crime

Respondent Rick Quinn, Jr. was a former member of the South Carolina House of Representatives, representing constituents in Richland and Lexington counties from 1989-2004 and 2010-2017 and serving as House Majority Leader from 1999- 2004. He owned and operated a mail business called Mail Marketing Strategies (MMS) in Columbia, while his father owned and operated a political consulting firm, Richard Quinn & Associates (RQ&A). In 2014, Attorney General Alan Wilson designated First Circuit Solicitor David Pascoe as special prosecutor to conduct a State grand jury investigation into alleged public corruption committed by current and former members of the South Carolina General Assembly. This case arose from a prior state grand jury investigation of former House Speaker Bobby Harrell, which resulted in six counts of misusing campaign funds, to which he pleaded guilty. During the course of the investigation into Speaker Harrell, SLED uncovered potentially criminal conduct by Representative Jimmy Merrill and Representative Rick Quinn, and a second grand jury

investigation was initiated to investigate the conduct of these individuals. The investigation focused on Quinn's practice of using his office as House Majority Leader and leader of the House Republican Caucus to direct mailing and political services to his family's businesses. Quinn only admitted to a limited set of facts supporting the indictment. Believing the plea lacked a sufficient basis, the State moved to vacate Quinn's guilty plea, reconsider the sentence, and for the trial court's recusal. The State appealed the order denying its motions. After review, the South Carolina Supreme Court determined that the State could not appeal the guilty plea, the trial court did not abuse its discretion in sentencing, and there was no evidence of judicial bias or prejudice requiring the court to recuse itself. Therefore, the Court dismissed the State's appeal of the guilty plea, and affirmed as to all other issues.

Read Opinion Are you a lawyer? **Annotate this case**.

Texas v. Arellano

Court: Texas Court of Criminal Appeals
Docket: PD-0287-19
Opinion Date: May 6, 2020
Judge: Slaughter
Areas of Law: Constitutional Law, Criminal Law

After Appellee Cesar Ramiro Arellano was arrested for driving while intoxicated, the arresting officer, Phillip Garcia, prepared a probable cause affidavit to support a search warrant for a blood draw. Officer Garcia submitted his sworn affidavit to the on-duty magistrate. Using a cursive signature, the magistrate signed the blank signature line of a form search warrant authorizing the search and seizure of Appellee's blood. Below the signature line appeared the words, "Magistrate, Victoria County, Texas." Aside from the cursive signature, the magistrate's name was not typed or handwritten anywhere on the warrant. Upon execution of the search warrant, Appellee was charged with DWI. In the trial court, Appellee filed a motion to suppress all evidence stemming from the blood draw. At the pretrial suppression hearing, Appellee argued that the search warrant to obtain the blood specimen was facially invalid because the magistrate's signature was illegible in violation of the requirements of Code of Criminal Procedure Article 18.04(5). The trial court agreed, the court of appeals

concurred, and the evidence was suppressed because of the illegible signature. The Texas Court of Criminal Appeals disagreed with both lower courts, finding the court of appeals erred in holding that reliance on the statutory good-faith exception was automatically precluded based on an illegible magistrate's signature in violation of Code of Criminal Procedure Article 18.04(5). Because the remaining issues in the case were not properly addressed by the court of appeals, judgment was vacated and the matter remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

About Justia Opinion Summaries

Justia Weekly Opinion Summaries is a free service, with 63 different newsletters, each covering a different practice area.

Justia also provides 68 daily jurisdictional newsletters, covering every federal appellate court and the highest courts of all US states.

All daily and weekly Justia newsletters are free. Subscribe or modify your newsletter subscription preferences at daily.justia.com.

You may freely redistribute this email in whole.

About Justia

Justia is an online platform that provides the community with open access to the law, legal information, and lawyers.

Contact Us | Privacy Policy

Unsubscribe From This Newsletter
or unsubscribe from all Justia newsletters immediately **here.**

Justia | 1380 Pear Ave #2B, Mountain View, CA 94043

From:	Criminal Law - Justia Weekly Opinion Summaries
To:	Kennedy, Kevin (POL)
Subject:	Latest 111 Cases This Week: Kelly v. United States (U.S.), Gomes v. Silva (1st Cir.), United States v. Perez-Couvertier (1st Cir.)
Date:	Friday, May 8, 2020 9:02:29 AM

If you are unable to see this message, click here to view it in a web browser.

Justia Weekly Opinion Summaries

Criminal Law
May 8, 2020

Table of Contents

Kelly v. United States
Criminal Law, Government & Administrative Law, White Collar Crime
US Supreme Court

Gomes v. Silva
Civil Rights, Constitutional Law, Criminal Law

US Court of Appeals for the First Circuit

United States v. Perez-Couvertier
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the First Circuit

United States v. Haverkamp
Criminal Law
US Court of Appeals for the Second Circuit

United States v. Mladen
Criminal Law, Trusts & Estates
US Court of Appeals for the Second Circuit

United States v. Richardson
Criminal Law
US Court of Appeals for the Second Circuit

United States v. Rosemond
Criminal Law
US Court of Appeals for the Second Circuit

United States v. Lacerda
Criminal Law, White Collar Crime
US Court of Appeals for the Third Circuit

Cucalon v. Barr
Criminal Law, Immigration Law
US Court of Appeals for the Fourth Circuit

United States v. Doctor
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Lewis
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Jordan
Criminal Law
US Court of Appeals for the Fifth Circuit

United States v. Longoria
Criminal Law
US Court of Appeals for the Fifth Circuit

United States v. McNabb
Criminal Law
US Court of Appeals for the Fifth Circuit

Andrews v. Wayne County
Civil Rights, Constitutional Law, Criminal Law

US Court of Appeals for the Sixth Circuit

Hicks v. Scott
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Sixth Circuit

Moody v. United States
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Sixth Circuit

United States v. Foreman
Criminal Law
US Court of Appeals for the Sixth Circuit

United States v. Smith
Criminal Law
US Court of Appeals for the Sixth Circuit

Kirkman v. Thompson
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

Tuduj v. Newbold
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

United States v. Gibson
Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

United States v. Howell
Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

United States v. Lewis
Criminal Law
US Court of Appeals for the Seventh Circuit

Bakor v. Barr
Criminal Law, Immigration Law
US Court of Appeals for the Eighth Circuit

Smith v. Titus
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Becerra
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Haynes
Criminal Law

US Court of Appeals for the Eighth Circuit

United States v. Roberts
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Wright
Criminal Law
US Court of Appeals for the Eighth Circuit

Benson v. Chappell
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Ninth Circuit

Mero v. Barr
Criminal Law, Immigration Law
US Court of Appeals for the Ninth Circuit

Romero-Millan v. Barr
Criminal Law
US Court of Appeals for the Ninth Circuit

United States v. Yang
Criminal Law
US Court of Appeals for the Ninth Circuit

United States v. Neugin
Constitutional Law, Criminal Law
US Court of Appeals for the Tenth Circuit

United States v. Ramon
Constitutional Law, Criminal Law
US Court of Appeals for the Tenth Circuit

United States v. Richards
Constitutional Law, Criminal Law
US Court of Appeals for the Tenth Circuit

Andrews v. Warden
Criminal Law
US Court of Appeals for the Eleventh Circuit

Hollis v. United States
Criminal Law
US Court of Appeals for the Eleventh Circuit

Knight v. Florida Department of Corrections
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Eleventh Circuit

United States v. Evans
Criminal Law

US Court of Appeals for the Eleventh Circuit

United States v. McLellan
Criminal Law
US Court of Appeals for the Eleventh Circuit

United States v. Russell
Criminal Law
US Court of Appeals for the Eleventh Circuit

Welch v. United States
Criminal Law
US Court of Appeals for the Eleventh Circuit

State v. Trujillo
Constitutional Law, Criminal Law
Arizona Supreme Court

Barnett v. State
Criminal Law
Arkansas Supreme Court

Mason v. Kelley
Criminal Law
Arkansas Supreme Court

Ray v. Kelley
Criminal Law
Arkansas Supreme Court

Walker v. Kelley
Criminal Law
Arkansas Supreme Court

People v. Flores
Civil Rights, Constitutional Law, Criminal Law
Supreme Court of California

California v. Law
Constitutional Law, Criminal Law
California Courts of Appeal

California v. Sanchez
Constitutional Law, Criminal Law
California Courts of Appeal

Galeotti v. International Union of Operating Engineers
Criminal Law, Labor & Employment Law, White Collar Crime
California Courts of Appeal

In re I.A.
Criminal Law, Juvenile Law

California Courts of Appeal

People v. Edwards
Criminal Law
California Courts of Appeal

People v. Thomkins
Criminal Law
California Courts of Appeal

People v. Torres
Criminal Law
California Courts of Appeal

People v. Triplett
Criminal Law
California Courts of Appeal

Colorado In Interest of G.S.S.
Constitutional Law, Criminal Law, Juvenile Law
Colorado Supreme Court

Barringer v. Halkitis
Criminal Law
Florida Supreme Court

Franqui v. State
Criminal Law
Florida Supreme Court

Hicks v. State
Criminal Law
Florida Supreme Court

Burley v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Carter v. Georgia
Construction Law, Criminal Law
Supreme Court of Georgia

Clarke v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Collins v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Dawson v. Georgia
Constitutional Law, Criminal Law

Supreme Court of Georgia

Evans v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Hill v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Oliver v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Rosser v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Spencer v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Styles v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Whitehead v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Idaho v. Blythe
Constitutional Law, Criminal Law
Idaho Supreme Court - Criminal

Idaho v. Glodowski
Constitutional Law, Criminal Law
Idaho Supreme Court - Criminal

Idaho v. Jones
Constitutional Law, Criminal Law
Idaho Supreme Court - Criminal

State v. Gordon
Civil Rights, Constitutional Law, Criminal Law
Iowa Supreme Court

State v. Craig
Criminal Law
Kansas Supreme Court

State v. Lemmie
Criminal Law

Kansas Supreme Court

State v. Mullen
Criminal Law
Maine Supreme Judicial Court

Commonwealth v. Billingslea
Civil Rights, Constitutional Law, Criminal Law
Massachusetts Supreme Judicial Court

Commonwealth v. Martin
Civil Rights, Constitutional Law, Criminal Law
Massachusetts Supreme Judicial Court

Commonwealth v. Tavares
Criminal Law
Massachusetts Supreme Judicial Court

State v. Branch
Criminal Law
Minnesota Supreme Court

Galloway v. Mississippi
Constitutional Law, Criminal Law
Supreme Court of Mississippi

City of Missoula v. Zerbst
Civil Rights, Constitutional Law, Criminal Law
Montana Supreme Court

State v. Degarmo
Civil Rights, Constitutional Law, Criminal Law
Nebraska Supreme Court

People v. Holz
Civil Rights, Constitutional Law, Criminal Law
New York Court of Appeals

People v. Maffei
Civil Rights, Constitutional Law, Criminal Law
New York Court of Appeals

State v. Bailey
Civil Rights, Constitutional Law, Criminal Law
North Carolina Supreme Court

State v. Ellis
Civil Rights, Constitutional Law, Criminal Law
North Carolina Supreme Court

State v. Hobbs
Civil Rights, Constitutional Law, Criminal Law

North Carolina Supreme Court

State v. Mylett
Criminal Law
North Carolina Supreme Court

Dodge v. North Dakota
Constitutional Law, Criminal Law
North Dakota Supreme Court

Hewitt v. NDDOT
Criminal Law, Government & Administrative Law
North Dakota Supreme Court

Kastet v. NDDOT
Criminal Law, Government & Administrative Law
North Dakota Supreme Court

North Dakota v. Dahl
Constitutional Law, Criminal Law
North Dakota Supreme Court

North Dakota v. Foster
Constitutional Law, Criminal Law
North Dakota Supreme Court

North Dakota v. Kolstad
Constitutional Law, Criminal Law
North Dakota Supreme Court

North Dakota v. Michel
Constitutional Law, Criminal Law
North Dakota Supreme Court

North Dakota v. Wayland
Constitutional Law, Criminal Law
North Dakota Supreme Court

Schwindt v. Sorel
Constitutional Law, Criminal Law, Government & Administrative Law
North Dakota Supreme Court

State ex rel. McDougald v. Greene
Criminal Law
Supreme Court of Ohio

State ex rel. Parker Bey v. Byrd
Criminal Law
Supreme Court of Ohio

State v. Dangler
Criminal Law

Supreme Court of Ohio

Oregon v. Haji
Constitutional Law, Criminal Law
Oregon Supreme Court

South Carolina v. Durant
Constitutional Law, Criminal Law
South Carolina Supreme Court

South Carolina v. Perry
Constitutional Law, Criminal Law
South Carolina Supreme Court

South Carolina v. Quinn
Constitutional Law, Criminal Law, White Collar Crime
South Carolina Supreme Court

Texas v. Arellano
Constitutional Law, Criminal Law
Texas Court of Criminal Appeals

COVID-19 Updates: Law & Legal Resources Related to Coronavirus

Click here to include Verdict article summaries with your newsletter(s).

Criminal Law Opinions

Kelly v. United States

Court: US Supreme Court
Docket: 18-1059
Opinion Date: May 7, 2020
Judge: Elena Kagan
Areas of Law: Criminal Law, Government & Administrative Law, White Collar Crime

During former New Jersey Governor Christie's 2013 reelection campaign,

Fort Lee's mayor refused to endorse Christie. Kelly, Christie's Deputy Chief of Staff, Port Authority Deputy Executive Director, Baroni, and another official decided to reduce from three to one the number of lanes reserved at the George Washington Bridge's toll plaza for Fort Lee's commuters. To disguise the political retribution, the lane realignment was said to be for a traffic study. Port Authority traffic engineers were asked to collect some numbers. An extra toll collector was paid overtime. The lane realignment caused four days of gridlock, ending only when the Port Authority's Executive Director learned of the scheme. The Third Circuit affirmed the convictions of Baroni and Kelly for wire fraud, fraud on a federally funded program, and conspiracy to commit those crimes. The Supreme Court reversed. The scheme did not aim to obtain money or property. The wire fraud statute refers to "any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses," 18 U.S.C. 1343. The federal-program fraud statute bars "obtain[ing] by fraud" the "property" (including money) of a federally funded program or entity, section 666(a)(1)(A). The statutes are limited to the protection of property rights and do not authorize federal prosecutors to set standards of good government. The Court rejected arguments that the defendants sought to take control of the Bridge's physical lanes or to deprive the Port Authority of the costs of compensating employees. Their realignment of the access lanes was an exercise of regulatory power; a scheme to alter a regulatory choice is not one to take government property. The time and labor of the employees were an incidental byproduct of that regulatory object. Neither defendant sought to obtain the services that the employees provided.

Read Opinion Are you a lawyer? **Annotate this case**.

Gomes v. Silva

Court: US Court of Appeals for the First Circuit
Docket: 19-1656
Opinion Date: May 1, 2020
Judge: Stahl
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The First Circuit affirmed the judgment of the district court denying Appellant's petition for a writ of habeas corpus, holding that, under the highly deferential standard prescribed by the Antiterrorism and Effective

Death Penalty Act for federal habeas review of state criminal convictions, Appellant's claims to habeas relief failed. Appellant was convicted in a Massachusetts superior court of murder in the first degree and related crimes. The Supreme Judicial Court (SJC) affirmed the convictions. Appellant subsequently petitioned the District Court for the District of Massachusetts for a writ of habeas corpus. The district court denied the petition but granted a certificate of appealability. The First Circuit affirmed, holding (1) sufficient evidence supported Appellant's conviction for first-degree murder as a joint venturer, and the SJC's sufficiency determination was not unreasonable; and (2) the SJC reasonably determined that the trial court's admission into evidence of certain items did not constitute error.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Perez-Couvertier

Court: US Court of Appeals for the First Circuit
Docket: 16-2186
Opinion Date: May 7, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The First Circuit affirmed Defendant's conviction of possessing with intent to distribute controlled substances in a protected area and conspiring to distribute controlled substances in a protected area, holding that the district court did not plainly err with respect to any of Defendant's challenges. Specifically, the First Circuit held (1) the district court did not commit plain error in admitting evidence of the conspiracy's activities occurring after he withdrew from the conspiracy or, alternatively, in not instructing the jury to ignore such evidence; (2) the district court did not plainly err in admitting evidence of a drug trafficking organization's violent acts; and (3) the delay between Defendant's indictment and arrest did not violate his Sixth Amendment right to a speedy trial.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Haverkamp

Court: US Court of Appeals for the Second Circuit

Docket: 18-3735
Opinion Date: May 4, 2020
Judge: Barrington D. Parker
Areas of Law: Criminal Law

Defendant pleaded guilty to one count of distribution and receipt of child pornography and one count of possession of child pornography. The district court sentenced him to 121 months of imprisonment, followed by five years of supervised release, and imposed a $200 mandatory special assessment under 18 U.S.C. 3013, as well as a $10,000 assessment under 18 U.S.C. 3014. The Second Circuit held that the district court did not abuse its discretion in sentencing defendant and his sentence was substantively reasonable. The court held that the text of the Justice for Victims of Trafficking Act (JVTA), 18 U.S.C. 3014, taken as a whole and in its context, is straightforwardly meant to be applied on a per-offender, not a per-count, basis. In this case, the district court erroneously applied the special assessment on a per-count, rather than per-offender, basis. Finally, the court held that the computer monitoring condition in question was reasonably related to the nature of defendant's offense. Accordingly, the court affirmed in part, vacated in part, and remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Mladen

Court: US Court of Appeals for the Second Circuit
Docket: 18-0616
Opinion Date: May 6, 2020
Judge: Amalya Lyle Kearse
Areas of Law: Criminal Law, Trusts & Estates

After defendant died while his appeal was pending, counsel moved for abatement of all incidents of the prosecution, requesting that the appeal be dismissed without a decision on the merits, that defendant's conviction be vacated, and that the matter be remanded to the district court with instructions to dismiss the indictment and order repayment to defendant's estate of the $20,000 fine and $100 special assessment. Because defendant was convicted upon his plea of guilty, and he neither did nor was permitted to challenge on appeal the merits of his conviction, the Second

Circuit denied as without merit so much of the motion as seeks (1) vacatur of his conviction, (2) dismissal of the count of the indictment on which he was convicted, and (3) repayment of the mandatory $100 special assessment. The court granted so much of the motion as requests dismissal of this appeal and a remand to the district court for vacatur of the imposed terms of imprisonment and supervised release and for an order requiring that the paid fine of $20,000 be repaid to defendant's estate.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Richardson

Court: US Court of Appeals for the Second Circuit
Docket: 19-412
Opinion Date: May 5, 2020
Judge: Menashi
Areas of Law: Criminal Law

The Second Circuit affirmed defendant's conviction for distribution and possession with intent to distribute a controlled substance. The court held that the district court did not procedurally err by applying the career offender sentencing enhancement pursuant to USSG 4B1.1 because defendant's prior convictions of conspiracy to distribute a controlled substance in violation of 21 U.S.C. 841(a)(1) and 846, and attempted criminal possession of a controlled substance in violation of N.Y. Penal Law 220.16(1), qualify as controlled substance offenses, as defined in USSG 4B1.2(b). The court also held that the district court did not substantively err in sentencing defendant, because it properly considered his criminal history and accounted for his need for mental health and substance abuse treatment.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Rosemond

Court: US Court of Appeals for the Second Circuit
Docket: 18-3561
Opinion Date: May 1, 2020
Judge: Chin
Areas of Law: Criminal Law

The Second Circuit affirmed defendant's conviction for murder-for-hire, conspiracy to commit murder-for-hire, murder through use of a firearm, and possession of a firearm during a murder-for-hire conspiracy. Defendant owned Czar Entertainment, a music management company that represented hip-hop, rap and R&B artists such as Jayceon Taylor, also known as "The Game." Taylor was a member of G-Unit, a rap group run by Curtis Jackson, also known as "50 Cent." Defendant's crimes stemmed from a rivalry with Violator Records, the company that managed G-Unit. The court rejected defendant's contention that his attorney was ineffective because he conceded that defendant paid for the victim to be shot, even though he told counsel not to make this concession. The court held that defendant failed to show that this was objectively unreasonable or that he would have been found not guilty had a different argument been advanced. In this case, there was ample evidence supporting counsel's strategy to concede that defendant ordered a shooting where, among other things, the government's key witness, who participated in the conspiracy and lured the victim to be shot, testified that defendant agreed to pay the shooter. The court also held that the district court did not abuse its broad discretion by admitting prior bad-act evidence under Federal Rule of Evidence 404(b)(1).

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Lacerda

Court: US Court of Appeals for the Third Circuit
Docket: 15-2812
Opinion Date: May 5, 2020
Judge: Porter
Areas of Law: Criminal Law, White Collar Crime

VOG billed itself as an advocacy group helping victims of timeshare fraud get out of their timeshare debts. A jury determined that VOG had actually defrauded its customers and that three individual defendants (including Lacerda) were each knowing participants in that fraud. Lacerda was sentenced to 324 months' imprisonment for his leading role in the fraudulent enterprise. The Third Circuit affirmed the respective convictions and sentences. The court rejected a claim of impermissible "overview testimony" by an FBI agent; an officer who is familiar with an investigation or was personally involved may tell the story of that investigation—how the

investigation began, who was involved, and what techniques were used, and, with a proper foundation, may offer lay opinion testimony and testify about matters within his personal knowledge. The district court did not abuse its discretion when it disqualified defense counsel based on a conflict of interest; when it denied replacement counsel's motion for a continuance; when it excluded from evidence, as hearsay, an email sent by Lacerda to VOG's former CFO; in exercising its sentencing discretion; or by ordering the forfeiture of all VOG's gross proceeds.

Read Opinion Are you a lawyer? **Annotate this case**.

Cucalon v. Barr

Court: US Court of Appeals for the Fourth Circuit
Dockets: 18-1292, 18-2206
Opinion Date: May 7, 2020
Judge: Barbara Milano Keenan
Areas of Law: Criminal Law, Immigration Law

The Fourth Circuit denied petitions for review of the BIA's final order of removal. Applying the modified categorical approach, the court held that defendant's prior conviction for distribution of cocaine under Virginia Code 18.2-248, including distribution of that substance as an accommodation under Virginia Code 18.2-248(D), satisfies the federal definitions of an "aggravated felony" and of a crime "relating to a controlled substance" pursuant to 8 U.S.C. 1227(a)(2)(A)(iii), 1227(a)(2)(B)(i). The court also held that the district court did not abuse its discretion in denying petitioner's motion to reconsider.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Doctor

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-4874
Opinion Date: May 4, 2020
Judge: Roger L. Gregory
Areas of Law: Criminal Law

The Fourth Circuit affirmed the district court's revocation of defendant's

supervised release and resulting sentence. The court held that the district court did not clearly err in finding the government proved he committed the assault underlying the supervised release violation; the district court did not commit plain error by adopting the violation report when announcing defendant committed Violation One; and, even if the district court erred in sentencing defendant for a Grade A violation, the error was harmless.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Lewis

Court: US Court of Appeals for the Fourth Circuit
Docket: 19-4028
Opinion Date: May 4, 2020
Judge: Barbara Milano Keenan
Areas of Law: Criminal Law

Defendant was convicted for possessing a firearm as a felon and sentenced to 63 months' imprisonment and a three-year period of supervised release. The district court additionally recommended, without explanation, that defendant receive addiction treatment while incarcerated and ordered, as a special condition of his supervised release, that defendant participate in an addiction treatment program. The Fourth Circuit held that defendant's sentence is procedurally unreasonable because the district court failed to provide an adequate explanation for imposing as a special condition of supervised release the requirement of addiction treatment. The court also held that the district court failed to address defendant's nonfrivolous mitigation arguments. Therefore, the court remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Jordan

Court: US Court of Appeals for the Fifth Circuit
Docket: 19-40499
Opinion Date: May 1, 2020
Judge: Jennifer Walker Elrod
Areas of Law: Criminal Law

The Fifth Circuit affirmed the district court's grant of defendants' motion for a new trial on the basis of prejudicial outside influence on the jury. The court held that the district court did not abuse its broad discretion in granting the motion for a new trial without holding an evidentiary hearing. To the extent there is a bright-line rule applicable to allegations of outside influence on the jury, the court held that it was not applicable to this case. Furthermore, the district court did not abuse its discretion in exercising its prerogative, within broadly defined parameters, to handle the allegation of outside influence in the least disruptive manner possible in this unusual case. Finally, the district court permissibly concluded that the evidence showed a sufficient likelihood of prejudice to shift the burden to the Government, and that the Government did not (and could not) show "no reasonable possibility that the jury's verdict was influenced by" the CSO's comments.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Longoria

Court: US Court of Appeals for the Fifth Circuit
Docket: 19-20201
Opinion Date: May 5, 2020
Judge: Gregg Costa
Areas of Law: Criminal Law

The Fifth Circuit held that the base offense level of 20 was proper for defendant's felon-in-possession crime involving a semiautomatic firearm that is capable of accepting a large capacity magazine. In this case, defendant failed to show that the district court clearly erred in relying on the FBI's agent statement about what was found in the apartment. The court clarified any confusion and held that the 2013 amendment to the commentary on the acceptance-of-responsibility Guideline does not clearly overrule its caselaw allowing the government to withhold the third point for acceptance of responsibility when it must litigate a suppression motion. The court held that Amendment 775 does not contain the unequivocal override needed to get past the court's precedent. Therefore, the court affirmed defendant's sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. McNabb

Court: US Court of Appeals for the Fifth Circuit
Docket: 19-50265
Opinion Date: May 1, 2020
Judge: Costa
Areas of Law: Criminal Law

The Fifth Circuit affirmed defendant's sentence imposed after he pleaded guilty to possessing a gun after having been convicted of a felony. The court held that defendant is not entitled to relief on his claim that the government breached the plea deal, and thus his appellate waiver remains enforceable. Accordingly, defendant's challenges to his sentence must be dismissed.

Read Opinion Are you a lawyer? **Annotate this case**.

Andrews v. Wayne County

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-1992
Opinion Date: May 4, 2020
Judge: Suhrheinrich
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Canton Police received a 911 call from Andrews, who stated that his fiance, White, had physically attacked him. Officers arrested White. Andrews later took White's medications to the jail; a “KOP” policy allows inmates to keep certain drugs for self-administration. During an intake interview, White admitted to attempting to harm herself or commit suicide in the past but said she was not thinking of harming herself or having suicidal thoughts. An R.N. later evaluated White for nearly two hours, reported White’s chief complaints were “anxiety and depression,” and contacted a pharmacy to verify White’s prescriptions. The R.N. claims White did not exhibit any psychotic behavior, suicidal ideation, or psychiatric distress but ordered further evaluation. The next day, White was found on the floor with vomit on her face. She stated repeatedly that she took too many pills. The next day, White died in the hospital. The cause of death was Verapamil toxicity. The Sixth Circuit affirmed the rejection of a suit under 42 U.S.C. 1983 on summary judgment. A pretrial detainee does not have an automatic right to a suicide screening. The court rejected an argument that the KOP Policy was deficient because

it allows inmates in need of a psychological evaluation to participate before a psychiatrist's assessment of proper housing. The County had no history of suicides relative to the program, so any purported failure to train its employees in suicide risk assessment did not cause White's death.

Read Opinion Are you a lawyer? **Annotate this case**.

Hicks v. Scott

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-3410
Opinion Date: May 1, 2020
Judge: Gibbons
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Cincinnati officers Scott and Moore responded to a reported incident of menacing. Two people alleged that Quandavier had driven by their home that night and threatened to kill them and that Quandavier carried guns. Officer Loreaux identified a vehicle fitting the description. Officers Scott, Moore, Schneider, and Loreaux, standing where the vehicle was parked, heard a voice. Thinking that it was likely Quandavier, they knocked on the exterior door of the residence. It swung open. Three officers entered without a warrant or exigent circumstances. Loreaux remained outside. Neither Scott nor Moore recall announcing their presence or identifying themselves. Inside and upstairs, Scott knocked on a closed door. As it opened, Scott "saw the barrel of a rifle pointed at [her] face." Moore and Schneider also saw Quandavier "nonchalantly" panning the rifle from left to right. Moore reached for its barrel as Scott fired her weapon. Moore did not instruct Quandavier to drop his rifle nor did Scott issue any commands before firing. Quandavier collapsed. The officers immediately radioed for paramedics. Before the officers applied handcuffs or provided first aid, they heard another voice and conducted a sweep. Quandavier died at the scene without receiving medical attention. In a suit under 42 U.S.C. 1983 for unlawful entry, excessive force, and deliberate indifference to a serious medical need, plus state claims, the district court granted the defendants summary judgment, citing qualified immunity. The Sixth Circuit reversed in part. The district court erred by granting qualified immunity to Scott, Moore, and Schneider on the unlawful entry claim. The court affirmed as to the excessive force, deliberate indifference, and state-law battery claims, and

remanded for evaluation of municipal liability and wrongful death claims.

Read Opinion Are you a lawyer? **Annotate this case**.

Moody v. United States

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-5015
Opinion Date: May 6, 2020
Judge: Thapar
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

At Moody's trial, the government produced a video of Moody cooking crack on his stove and waving a handgun while he mused about life in "the game" (drug trafficking). The court ruled that most of the video was admissible. Moody then tried to persuade the jury that the video was filmed more than five years before his indictment, putting it outside the statute of limitations. The jury convicted Moody. Due to prior felony drug convictions, Moody received enhanced, mandatory-minimum life sentences on several counts. He appealed on evidentiary grounds relating to the video. The Sixth Circuit affirmed. Later, Moody raised new claims on collateral review, 28 U.S.C. 2255. The district court found each claim meritless; most were also procedurally defaulted. The court authorized Moody to appeal. The Sixth Circuit dismissed the appeal, stating that none of the claims should have been certified. Reasonable jurists could not doubt that the district court properly denied relief on Moody's claims that he was deprived of his statute-of-limitations defense (violating due process); that the past convictions for his sentencing enhancements were not charged in the indictment or found by the jury; and that his previous lawyers failed to raise the first two claims sooner, violating his right to effective assistance of counsel.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Foreman

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-1827
Opinion Date: May 7, 2020
Judge: Gibbons

Areas of Law: Criminal Law

In 2006, Foreman pled guilty to possession with intent to distribute 50 or more grams of cocaine base, possession with intent to distribute cocaine powder, and possession of a firearm during and in furtherance of a drug trafficking crime. Foreman admitted that he was responsible for approximately 135 grams of crack cocaine and 250 grams of cocaine powder. Foreman had a final Guidelines range of 322-387 months; he was sentenced to 240 months' imprisonment with respect to each drug conviction, to run concurrently, and 60 months' imprisonment for the firearms conviction, to run consecutively. When the First Step Act of 2018 made the Fair Sentencing Act retroactive, Foreman sought relief. The district court held that Foreman was not entitled to a plenary resentencing and declined to revisit his career offender status or hold an in-person hearing, then weighed the new statutory range applicable to Foreman's drug offenses, his recalculated Guidelines range, and the 18 U.S.C. 3553(a) factors, and reduced Foreman's total sentence to 172 months on each drug offense, to run concurrently, plus the mandatory consecutive 60 months on the firearms offense. The Sixth Circuit affirmed. Nothing in the First Step Act entitles a defendant to a plenary resentencing. First Step Act resentencings are not shielded from review for reasonableness; the district court thoroughly explained its rationale, carefully examining Foreman's circumstances, the amended penalty provisions, and the resulting changes to Foreman's Guidelines range.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Smith

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-1724
Opinion Date: May 6, 2020
Judge: Bush
Areas of Law: Criminal Law

In 2006, Smith was convicted of conspiracy to distribute and to possess with intent to distribute 500 grams or more of powder or 50 grams or more of cocaine base (crack cocaine); possession with intent to distribute 50 grams or more of cocaine base (crack cocaine); possession with intent to distribute

500 grams or more of cocaine powder; and being a felon in possession of a firearm. The court imposed a mandatory minimum life sentence. The Fair Sentencing Act subsequently lowered the penalty for cocaine-base offenses, made retroactive through the First Step Act. Smith moved for relief and received a reduced sentence of 360 months, the bottom of the new Guideline range for the counts impacted by the Fair Sentencing Act, to run concurrent to his existing 360-month sentence for his powder cocaine count that was not affected by the Fair Sentencing Act. The Sixth Circuit affirmed, rejecting an argument that the court should have imposed a below-Guideline sentence for all counts. The First Step Act is a limited grant of authority to impose a reduced sentence for certain offenses and does not require a plenary resentencing proceeding. Even assuming the court's obligation to explain its reasons for imposing the modified sentence was akin to that which applies in initial sentencing, the court's use of a modified AO 247 form order to explain its decision was not procedurally unreasonable.

Read Opinion Are you a lawyer? **Annotate this case**.

Kirkman v. Thompson

Court: US Court of Appeals for the Seventh Circuit
Docket: 19-1904
Opinion Date: May 7, 2020
Judge: William Joseph Bauer
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Following a 1992 fight that involved Johnson, Herron, and Walker, two shooters shot the three men. Johnson survived. In the hospital, Johnson described a shooter by the street name "Duke," where Duke lived, and Duke's car. Johnson identified Duke and his accomplice from a photo array. Police pulled over a vehicle matching Johnson's description and arrested the driver, Kirkman, and the passenger, who matched the general description of the second shooter. Kirkman had a tattoo of Duke on his arm. Police took additional photos and presented a second photo array to Johnson, who identified them as the shooters. At trial, Johnson identified Kirkman and his passenger as the shooters. There was disputed testimony about the cause of the fight. Convicted of murder and aggravated battery with a firearm, Kirkman was sentenced to life in prison. Johnson had a

change of heart and submitted an affidavit, identifying Ford and an unknown man as the shooters. At Kirkman's post-conviction hearing, Johnson testified that he and his family had been threatened. Other testimony was inconsistent with Johnson's. Illinois courts denied post-conviction relief, finding that Johnson's recantation lacked credibility. Johnson later pleaded guilty for perjury but failed to specify which statement was false. The Seventh Circuit affirmed the denial of federal habeas relief. Illinois courts found Johnson's recantation lacked credibility. An evidentiary hearing satisfied Kirkman's due process rights. The Illinois trial court's determination defeated Kirkman's innocence and perjured testimony claims.

Read Opinion Are you a lawyer? **Annotate this case**.

Tuduj v. Newbold

Court: US Court of Appeals for the Seventh Circuit
Docket: 19-1699
Opinion Date: May 1, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Illinois prisoner Tuduj, having received extensive dental treatment, filed a "deliberate indifference" suit under 42 U.S.C. 1983 against his dentists and prison officials. The court recruited counsel to assist Tuduj in filing an amended complaint that complied with the Federal Rules of Civil Procedure. Counsel defended against two summary judgment motions, one arguing that Tuduj had not exhausted his administrative remedies and another on the merits While the motions were pending, Tuduj moved "for leave to represent himself," stating that he was "concerned that his counsel has filed a structurally, technically and legally insufficient response doomed to be denied." He asked to file his own brief, except "in the event this Honorable Court deems counsel's response … legally sufficient and Grants same[,] Plaintiff would be open to continued effective representation." A magistrate denied Tuduj's motion, stating that Tuduj "varie[d] between saying he would like to" represent himself and "indicating that he is happy with counsel's representation as long as he prevails." The district judge granted the motions for summary judgment, citing professional judgment and finding "no competent evidence" of any policy that unlawfully influenced dental-treatment decisions. The Seventh Circuit rejected Tuduj's argument

that the court wrongly denied his “unqualified” right to proceed pro se under 28 U.S.C. 1654, the due process clause, the equal protection clause, and the Seventh Amendment. The district court permissibly denied his equivocal request.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Gibson

Court: US Court of Appeals for the Seventh Circuit
Docket: 19-1402
Opinion Date: May 7, 2020
Judge: William Joseph Bauer
Areas of Law: Constitutional Law, Criminal Law

Officer Garrison encountered Gibson, a suspected drug trafficker, walking with a companion. Although initially a consensual encounter, Garrison questioned Gibson and his companion and briefly detained Gibson. After Gibson and his companion departed, Garrison spotted a methamphetamine pipe under his patrol vehicle. Local law enforcement conducted a traffic stop of Gibson’s vehicle in the curtilage of his driveway. A drug detection dog signaled the presence of a controlled substance in the vehicle, though nothing was found. Earlier that day, Gibson’s wife had met with DEA agents to tell them about methamphetamine inside the home. Police used information Mrs. Gibson had provided to obtain a search warrant. The search of the home uncovered drugs, drug paraphernalia, currency, and AK-47 rifles, which led to Gibson’s arrest. Gibson moved to suppress all evidence seized during the search, alleging he was detained without reasonable suspicion, unlawfully frisked, arrested without probable cause, stopped without probable cause or reasonable suspicion, and the traffic stop exceeded a permissible scope. Upon learning of his wife’s cooperation, Gibson also argued her statement was insufficiently attenuated to justify the search warrant. The Seventh Circuit affirmed the denial of the motion. Mrs. Gibson’s voluntary statement with DEA agents was independently sufficient to sustain findings of probable cause and sufficiently attenuated from subsequent events to preclude suppression.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Howell

Court: US Court of Appeals for the Seventh Circuit
Docket: 18-3157
Opinion Date: May 4, 2020
Judge: Scudder
Areas of Law: Constitutional Law, Criminal Law

In December 2012, Chicago Police officers responded to an anonymous call reporting a Hispanic man in a black sweater and black hat, carrying a bag, and climbing under a warehouse fence. They found someone who matched the description. After stopping and frisking him, they determined he was not engaged in any crime. Howell, walking toward the police, was white and wearing a black jacket and dark hat. When an officer approached to speak to him, Howell did not answer, looked panicked, and put his hands in his pockets. The officer patted Howell down and found a gun in his jacket. A federal gun charge followed. Howell unsuccessfully moved to suppress the gun. The Seventh Circuit reversed the denial of his suppression motion and vacated his conviction for possessing that gun. The court noted that the facts in the pretrial record differed significantly from those presented at trial, where the arresting officer testified that he decided to proceed with the pat-down only after Howell ignored a directive to remove his hands from his pockets. Viewing the pretrial record as a whole, the police lacked reasonable suspicion to frisk Howell. The court did not reverse Howell's conviction on a second gun charge that resulted from the execution of a warrant to search Howell's apartment three months after the initial stop and the ensuing discovery of more guns and ammunition.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Lewis

Court: US Court of Appeals for the Seventh Circuit
Dockets: 19-1911, 19-1262
Opinion Date: May 7, 2020
Judge: Joel Martin Flaum
Areas of Law: Criminal Law

In 2016-2018, Draheim managed a conspiracy, responsible for at least 38 packages of methamphetamine sent from California to La Crosse,

Wisconsin. Draheim supervised at least 11 associates who accepted shipments on her behalf, sent money transfers to California, distributed the meth, rented storage lockers, and collected money owed to her. Draheim provided vehicles. After agents placed a wiretap on her phone and seized several packages of meth en route to Draheim, her California supplier forced Draheim to find a new source. Draheim contacted Lewis, recently out of jail but still involved in the "meth scene." Lewis agreed to purchase meth from a new supplier. During the planned transaction, agents seized the package, which contained 28.6 grams of nearly pure meth. Police subsequently arrested Draheim after they found her daughter dead at home from an overdose; they took Lewis into custody for violating the terms of his state supervision. Both pleaded guilty to meth distribution offenses, 21 U.S.C. 841, 846. Draheim, facing a mandatory-minimum 10-year sentence, unsuccessfully argued that she qualified for "safety-valve relief." The court reasoned that she was the leader of her enterprise. Lewis unsuccessfully contended that he should be sentenced based only on his conviction, not other "relevant conduct." The Seventh Circuit affirmed Draheim's sentence but vacated as to Lewis. The fact that the defendant has engaged in other drug transactions is not, alone, sufficient to justify treating those transactions as relevant conduct for sentencing purposes.

Read Opinion Are you a lawyer? **Annotate this case**.

Bakor v. Barr

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-3011
Opinion Date: May 7, 2020
Judge: Steven M. Colloton
Areas of Law: Criminal Law, Immigration Law

The Eighth Circuit denied a petition for review of the BIA's determination that defendant committed two crimes involving moral turpitude. The court held that the BIA did not err in determining that petitioner's conviction for the Minnesota crimes of Criminal Sexual Conduct in the Fifth Degree and knowing failure to comply with Minnesota's sex offender registration statute were crimes involving moral turpitude. The court also held that petitioner failed to exhaust his remaining arguments and therefore declined to consider them.

Read Opinion Are you a lawyer? **Annotate this case**.

Smith v. Titus

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-2915
Opinion Date: May 5, 2020
Judge: Steven M. Colloton
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Eighth Circuit affirmed the district court's denial of habeas relief to petitioner based on his claim that the trial court violated his Sixth Amendment right to a public trial when it briefly closed the courtroom to spectators. The district court denied relief based on the ground that the Minnesota Supreme Court's decision was neither contrary to, nor an unreasonable application of, clearly established federal law. The court agreed and held that it was not objectively unreasonable for the Minnesota Supreme Court to deem it constitutional under the Sixth Amendment for the trial court to explain the parameters of an earlier public order on evidentiary issues in a brief nonpublic proceeding before the jury was sworn.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Becerra

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-2777
Opinion Date: May 7, 2020
Judge: Stras
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's conviction for two counts of being a felon in possession of a firearm and ammunition. The court held that there was more than enough evidence for defendant's probation officer and other officers to believe defendant had a firearm on him. Therefore, the officers had probable cause to arrest him without a warrant. The court also held that defendant was in custody when he made both statements at issue. In this case, the "request for clarification" of defendant's statement that he had "something" in his car did not require Miranda warnings. Furthermore,

because the bulge in defendant's pocket could have been a gun or other weapon that would have posed a danger to the officers and others, they could ask about it without the formality of Miranda warnings. The court joined its sister circuits in declining to recognize the innocent-possessor defense. The court held that the district court did not err in excluding defendant's proposed testimony that he had found the handgun in his car earlier in the day and was about to hand it over to his probation officer. The court reasoned that, even if defendant intended to turn over the gun (or the ammunition) to his probation officer, it is still a crime to knowingly possess it in the first place. Finally, the court held that the district court did not err in denying defendant a sentencing reduction for acceptance of responsibility; the district court considered defendant's mitigation arguments at sentencing; and the district court did not abuse its discretion by imposing a within-Guidelines sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Haynes

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1607
Opinion Date: May 5, 2020
Judge: Raymond W. Gruender
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's conviction and sentence for being a felon in possession of a firearm. The court held that the government did not violate the Speedy Trial Act, and defendant failed to offer any evidence showing that Iowa and federal prosecutors colluded. Furthermore, the district court did not abuse its discretion by failing to hold an evidentiary hearing regarding the existence of collusion. The court also held that the district court did not err in denying the motion to suppress where defendant was not unlawfully seized. In this case, prior to producing the marijuana cigarette, the officer did not ask defendant any questions but merely ordered him off the bus, particularly as the smell of marijuana alerted the officer that evidence of a more serious crime than failure to use a turn signal might be uncovered during the stop. Finally, the court held that defendant was not unlawfully searched when the officer conducted a pat-down search incident to arrest; the evidence was sufficient to support defendant's conviction;

defendant's Rehaif claim failed because there was sufficient evidence that he knew of his prohibited status; and defendant's sentence was not substantively unreasonable nor an abuse of the district court's discretion.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Roberts

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1176
Opinion Date: May 1, 2020
Judge: Steven M. Colloton
Areas of Law: Criminal Law

The Eighth Circuit vacated defendant's sentence imposed after he pleaded guilty to unlawful possession of a firearm as a previously convicted felon. The court held that, although the district court properly applied a four-level increase for possession of a firearm "in connection with another felony offense" under USSG 2K2.1(b)(6)(B), but that a two-level increase for "using a minor to commit a crime" under USSG 3B1.4 should not have applied. In this case, the evidence showed only that defendant engaged in an arm's-length transaction with a minor. The court held that this mere joint participation in an offense as a partner, does not amount to "use" of a minor "to commit the offense" of unlawful possession of a firearm by a felon. Accordingly, the court remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Wright

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1081
Opinion Date: May 5, 2020
Judge: Erickson
Areas of Law: Criminal Law

The Eighth Circuit affirmed the district court's restitution order and certain special conditions of defendant's supervised release imposed after he pleaded guilty to sex trafficking of a child. The court found no error in the district court's restitution amount of $20,000, holding that the evidence

supported the amount in light of the aggregate harm to the victim. The court also held that the special conditions -- including a requirement that defendant participate in sex offender treatment including psychological testing and polygraph examinations, a prohibition against contact with any minors without pre-approval, and a requirement that defendant seek prior approval before using temporary commercial lodging, such as a hotel or motel -- where reasonably related to both the offense of conviction and to defendant's history of sexual contact with minor females.

Read Opinion Are you a lawyer? **Annotate this case**.

Benson v. Chappell

Court: US Court of Appeals for the Ninth Circuit
Docket: 13-99004
Opinion Date: May 1, 2020
Judge: Consuelo Maria Callahan
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Ninth Circuit affirmed the district court's denial of petitioner's habeas corpus petition challenging his California conviction and death sentence for murder and other crimes. Petitioner raised two certified claims and two uncertified claims. The panel held that petitioner failed to show that the California Supreme Court's denials of his claims were unreasonable determinations of the facts or contrary to clearly established federal law. In this case, the California Supreme Court reasonably determined that an officer's misstatement during petitioner's interrogation that there was no death penalty in California did not prompt petitioner's confessions. Furthermore, petitioner failed to show that his statements were not knowing, voluntary, and intelligent. Even if petitioner were able to show that trial counsel was ineffective in not fully investigating his abuse as a child or his alleged organic brain injury, the panel held that the state court could reasonably have determined that any shortcoming in trial counsel's investigation was not prejudicial. Finally, the panel granted a certificate of appealability on petitioner's two uncertified claims and held that the state court reasonably rejected the claims that his trial counsel should have impeached the government's case and the prosecutor withheld material, exculpatory evidence.

Read Opinion Are you a lawyer? **Annotate this case**.

Mero v. Barr

Court: US Court of Appeals for the Ninth Circuit
Docket: 17-70929
Opinion Date: May 1, 2020
Judge: Paul Jeffrey Watford
Areas of Law: Criminal Law, Immigration Law

The Ninth Circuit granted in part a petition for review of the BIA's finding that petitioner was removable based on his conviction for possession of visual presentation depicting sexual conduct of a person under 16 years of age, in violation of Nevada Revised Statutes (N.R.S.) 200.730. Applying the categorical approach, the panel compared the elements of N.R.S. 200.730 with the applicable definition of "sexual abuse of a minor," which requires proof of three elements. The panel held that N.R.S. 200.730 punishes a broader range of conduct because the Nevada statute does not require proof that the offender participated in sexual conduct with a minor. Therefore, petitioner's conviction did not qualify as sexual abuse of a minor. The panel explained that, with a possession-only offense such as N.R.S. 200.730, the minor depicted in the image is not the direct object of the offender's conduct, which is a necessary predicate for the offense to qualify as sexual abuse of a minor.

Read Opinion Are you a lawyer? **Annotate this case**.

Romero-Millan v. Barr

Court: US Court of Appeals for the Ninth Circuit
Dockets: 16-73915, 17-72893, 18-71555
Opinion Date: May 4, 2020
Areas of Law: Criminal Law

The Ninth Circuit certified the following questions of state law to the Arizona Supreme Court: 1. Is Arizona's possession of drug paraphernalia statute, A.R.S. 13-3415, divisible as to drug type? 2. Is Arizona's drug possession statute, A.R.S. 13-3408, divisible as to drug type? 3. Put another way, is jury unanimity (or concurrence) required as to which drug or drugs listed in

A.R.S. 13-3401(6), (19), (20), or (23) was involved in an offense under either statute?

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Yang

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-10341
Opinion Date: May 4, 2020
Judge: Piersol
Areas of Law: Criminal Law

The Ninth Circuit affirmed the district court's denial of defendant's motion to suppress after he pleaded guilty to receipt of stolen mail and being a prohibited person in possession of a firearm. Defendant moved to suppress the evidence seized from his residence and the statements he made to law enforcement on the basis that the search warrant obtained by the Postal Inspection Service relied on evidence that was obtained illegally. The panel declined to address the potential Fourth Amendment privacy interests that may be implicated by the warrantless use of this Automatic License Plate Recognition (ALPR) technology, and held that defendant does not have a reasonable expectation of privacy in the historical location data of the Yukon under the facts of this case. The panel found no evidence in the record that Prestige Motors had a policy or practice of allowing lessees to keep cars beyond the rental period and Prestige had made affirmative attempts to repossess the vehicle by activating the GPS unit to locate and disable the vehicle. Therefore, defendant lacked standing to challenge the warrantless search of the database.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Neugin

Court: US Court of Appeals for the Tenth Circuit
Docket: 19-7043
Opinion Date: May 1, 2020
Judge: Scott Milne Matheson, Jr.
Areas of Law: Constitutional Law, Criminal Law

Jack Neugin pled guilty to being a felon in possession of a firearm and ammunition on the condition that he could appeal the district court's denial of his motion to suppress evidence of the ammunition and firearm police found in the bed of his pickup truck. Officers responded to a reported verbal altercation between Neugin and his girlfriend. One of the officers saw ammunition in the back of the truck after he lifted the truck's camper lit do allow the girlfriend to retrieve her belongings. Neugin argued the officers discovered the evidence during an unconstitutional search; the district court concluded the officer was acting "in a lawful position" as "community caretaker," and found no Fourth Amendment violation. The Tenth Circuit reversed, finding that : (1) the officer conducted the without a warrant or probable cause, (2) the community caretaking exception to the warrant requirement does not apply, and (3) the inevitable discovery exception to the exclusionary rule does not apply. The evidence seized should have been suppressed.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Ramon

Court: US Court of Appeals for the Tenth Circuit
Docket: 19-1221
Opinion Date: May 1, 2020
Judge: Gregory Alan Phillips
Areas of Law: Constitutional Law, Criminal Law

In 2016, after serving a federal prison sentence for having possessed a firearm after a felony conviction, Charles Ramon III began serving a mandatory term of supervised release. Before Ramon completed the term, his probation officer filed a petition, soon followed by two superseding petitions, to revoke Ramon's supervised release. At the revocation hearing, the district court found three violations—two for possessing a controlled substance and one for again illegally possessing a firearm. Of these, the most serious was Ramon's illegal possession of a firearm—a Grade B violation. For this, the court imposed the statutory maximum sentence of twenty-four months in prison. During the revocation hearing, the government mentioned that it might seek to indict Ramon for illegally possessing a firearm (the conduct in part underlying the revocation). Mindful of this, the district court ordered that Ramon's twenty-four-month sentence run

"consecutively to any sentences imposed previously or prospectively in federal or state court." At the hearing, Ramon did not object to the district court's running his sentence consecutively to future federal sentences. On appeal, Ramon argued that the district court exceeded its sentencing authority under 18 U.S.C. 3584(a) by ordering that Ramon's sentence run consecutively to future federal sentences. By the terms of 18 U.S.C. 3584(a), the Tenth Circuit determined the district court did err. But Ramon failed to object to this at trial, and on appeal, failed to show that the error was plain, thus, judgment was affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Richards

Court: US Court of Appeals for the Tenth Circuit
Docket: 19-8044
Opinion Date: May 6, 2020
Judge: Baldock
Areas of Law: Constitutional Law, Criminal Law

In 2018, the Wyoming Division of Criminal Investigation (DCI) obtained a search warrant to review the contents of Defendant–Appellant Joshua Richards' Tumblr account. During the search and subsequent investigation, DCI agents discovered Defendant had re-blogged videos and images of child pornography to his private Tumblr so he could later access and view the materials. Defendant ultimately pleaded guilty to one count of accessing with intent to view child pornography. He was sentenced to twenty-four months' imprisonment followed by five years of supervised release. The district court imposed several special conditions of supervised release, which, as relevant here, related to drugs and alcohol and required Defendant to submit to polygraph testing. On appeal, Defendant argued the district court erred in imposing these special conditions. He also challenged the length of his prison sentence as substantively unreasonable. The Tenth Circuit determined the alcohol and drug conditions did not directly conflict with the relevant policy statement in the sentencing guidelines, so the district court's decision to impose the conditions was not manifestly unreasonable. And given the circumstances of the case, the Court determined the trial court did not abuse its discretion in imposing Defendant's twenty-four month sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

Andrews v. Warden

Court: US Court of Appeals for the Eleventh Circuit
Docket: 19-12443
Opinion Date: May 5, 2020
Judge: William Holcombe Pryor, Jr.
Areas of Law: Criminal Law

The Eleventh Circuit affirmed the district court's denial of habeas relief under 28 U.S.C. 2241. Plaintiff alleged that President Obama commuted his "total sentence" of imprisonment, which included the 37 months of imprisonment that he served as part of his 2003 sentence. Based on the terms of the commutation order, the Constitution, and Supreme Court precedent, the court could not say that the Bureau erred in excluding the 37-month term of imprisonment from its recalculation.

Read Opinion Are you a lawyer? **Annotate this case**.

Hollis v. United States

Court: US Court of Appeals for the Eleventh Circuit
Docket: 19-11323
Opinion Date: May 6, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Eleventh Circuit affirmed the district court's denial of petitioner's motion to vacate his sentence under 28 U.S.C. 2255. The court held that petitioner cannot prove that his counsel rendered ineffective assistance, because petitioner's prior convictions in Alabama categorically qualify as predicate offenses under both the Armed Career Criminal Act and the career-offender provision of the Guidelines, and his prior conviction in Georgia qualifies as a predicate offense under the Act. Therefore, counsel did not perform deficiently by failing to raise a meritless objection.

Read Opinion Are you a lawyer? **Annotate this case**.

Knight v. Florida Department of Corrections

Court: US Court of Appeals for the Eleventh Circuit
Docket: 18-12488
Opinion Date: May 1, 2020
Judge: Newsom
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Eleventh Circuit affirmed the district court's denial of a 28 U.S.C. 2254 petition for habeas relief. Petitioner alleged that his counsel rendered ineffective assistance under Strickland v. Washington, 466 U.S. 668 (1984), by failing to adequately investigate and present mitigating evidence during the sentencing phase of his capital-murder trial. The court held that, even assuming that counsel performed deficiently in failing to investigate and present the mitigation evidence that petitioner now raises—thus satisfying the first prong of the two-part Strickland standard that governs ineffective-assistance claims—petitioner failed to carry his burden of demonstrating resulting prejudice.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Evans

Court: US Court of Appeals for the Eleventh Circuit
Docket: 17-15323
Opinion Date: May 6, 2020
Judge: Grant
Areas of Law: Criminal Law

The Eleventh Circuit affirmed defendant's conviction and sentence for being a felon in possession of a firearm. The court held that, given the totality of the circumstances, it was reasonable for officers, mistaking a dog's whimper for a person in distress, to enter defendant's home without a warrant. Therefore, defendant's challenge to the district court's denial of his motion to suppress evidence failed. The court upheld the district court's imposition of a 22 offense level finding because defendant possessed a semiautomatic firearm capable of accepting a large capacity magazine under USSG 2K2.1(a)(3)(A)(i) (2016). The court also upheld defendant's sentencing enhancement under USSG 2K2.1(b)(4)(B) for possessing a rifle that had an

obliterated serial number.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. McLellan

Court: US Court of Appeals for the Eleventh Circuit
Docket: 18-13289
Opinion Date: May 6, 2020
Judge: Boggs
Areas of Law: Criminal Law

The Eleventh Circuit affirmed defendant's conviction for two counts of being a felon in possession of a firearm. The court held that the district court did not abuse its discretion in permitting one of his arresting officers to offer testimony at trial on the correlation between guns and drug activity and to suggest that defendant was selling drugs; the court declined to evaluate the applicability of the Armed Career Criminal Act (ACCA), because the district court would have imposed the same sentence regardless of whether the mandatory minimum applied; and the court rejected defendant's claim under Rehaif v. United States, 139 S. Ct. 2191 (2019), and held that there was no plain error in the district court's failure to instruct the jury of the knowledge-of-status element and any error from the lack of a knowledge-of-status element in defendant's plea colloquy did not affect his substantial rights. Finally, the court remanded for clarification of the judgment to reflect the sentence the district court said it would have imposed if the Armed Career Criminal Act did not apply.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Russell

Court: US Court of Appeals for the Eleventh Circuit
Docket: 18-11202
Opinion Date: May 4, 2020
Judge: Charles R. Wilson
Areas of Law: Criminal Law

Defendant was convicted of possessing a firearm and ammunition as an immigrant illegally or unlawfully in the United States. After defendant

appealed his conviction and sentence, the Supreme Court issued its decision in Rehaif v. United States, 588 U.S. ___, 139 S. Ct. 2191 (2019), which reversed a decision from this court and held that under 18 U.S.C. 922(g), the government must prove that a defendant knew "his status as a person barred from possessing a firearm" when he knowingly possessed a firearm. The Eleventh Circuit held that defendant established the necessary prejudice under plain error review and vacated defendant's section 922(g) conviction, remanding for further proceedings. In this case, the district court committed an error that was made plain by the Supreme Court in Rehaif. Furthermore, defendant has sufficiently shown a reasonable probability that but for the error, the outcome of his trial would have been different.

Read Opinion Are you a lawyer? **Annotate this case**.

Welch v. United States

Court: US Court of Appeals for the Eleventh Circuit
Docket: 14-15733
Opinion Date: May 6, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Eleventh Circuit affirmed the district court's denial of petitioner's 28 U.S.C. 2255 motion to vacate his sentence. The court held that defendant's prior 1996 Florida convictions for robbery qualified as violent felonies under the Armed Career Criminal Act's (ACCA) elements clause, and rejected his contention that the court's decision in his direct appeal carved out a narrow exception to pre-1997 Florida robbery convictions obtained in Florida's Fourth District Court of Appeal. The court also held that petitioner's prior Florida felony battery conviction was a violent felony under the ACCA in light of the court's holding in United States v. Vail-Bailon, 868 F.3d 1293 (11th Cir. 2017) (en banc), cert. denied, 138 S. Ct. 2620 (2018).

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Trujillo

Court: Arizona Supreme Court
Docket: CR-18-0531-PR

Opinion Date: May 4, 2020
Judge: Gould
Areas of Law: Constitutional Law, Criminal Law

The Supreme Court held that, for purposes of imposing mandatory sex offender registration under Ariz. Rev. Stat. 13-3821(A)(3), a judge has the authority to make the necessary factual finding that the victim is under the age of eighteen and that Arizona's sex offender registration statutes are civil regulatory statutes, not criminal penalties. Defendant was convicted by a jury of one count of sexual abuse. In reaching its verdict the jury determined that the victim was "fifteen or more years of age." At sentencing, the trial court ordered Defendant to register as a sex offender. Defendant objected, arguing that, pursuant to Apprendi v. New Jersey, 530 U.S. 466 (2000), a jury was required to find whether Defendant was under eighteen pursuant to section 13-3821(A)(3). The trial court denied the objection. The court of appeals affirmed. The Supreme Court affirmed, holding (1) Apprendi does not apply to factual findings that are necessary to impose registration because sex offender registration is a civil regulatory requirement, not a criminal penalty; and (2) the trial judge did not violate Apprendi by determining that the victim was under eighteen.

Read Opinion Are you a lawyer? **Annotate this case**.

Barnett v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 181
Opinion Date: May 7, 2020
Judge: Hudson
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's "motion for credit for time spent in custody," holding that the circuit court's findings were not clearly erroneous. In his motion, Appellant alleged that he was entitled to 312 days of jail-time credit and that the circuit court should enter a new sentencing order nunc pro tunc that reflected the correct amount of jail-time credit. The circuit court denied the motion. The Supreme Court affirmed, holding that the circuit court's denial of Appellant's motion was not clearly erroneous because Appellant failed to demonstrate a clerical error subject to correction.

Read Opinion Are you a lawyer? **Annotate this case**.

Mason v. Kelley

Court: Arkansas Supreme Court
Citation: 2020 Ark. 182
Opinion Date: May 7, 2020
Judge: Rhonda K. Wood
Areas of Law: Criminal Law

The Supreme Court affirmed the order of the circuit court dismissing Appellant's pro se petition for writ of habeas corpus, holding that Appellant stated no ground on which the writ could issue. Appellant was convicted of aggravated robbery, theft of property, and second-degree battery and sentenced as a habitual offender to an aggregate term of 660 months' imprisonment. The court of appeals affirmed. Appellant later petitioned for writ of habeas corpus, asserting that the trial court misapplied Arkansas's habitual-offender statutes. The circuit court dismissed the petition. The Supreme Court affirmed, holding that the issues Appellant raised in his petition for the writ should have been raised at trial, on direct appeal, or in a petition for postconviction relief.

Read Opinion Are you a lawyer? **Annotate this case**.

Ray v. Kelley

Court: Arkansas Supreme Court
Citation: 2020 Ark. 184
Opinion Date: May 7, 2020
Judge: Wynne
Areas of Law: Criminal Law

The Supreme Court dismissed Appellant's appeal from an order denying his pro se petition for permission to reinvest jurisdiction in the trial court to consider a petition for writ of error coram nobis, holding that the circuit court had no jurisdiction to consider the petition. Appellant entered negotiated guilty pleas to rape and other offenses. Appellant later filed a petition for writ of error coram nobis in the Chicot County Circuit Court, the court where he

was incarcerated, setting out two grounds for coram nobis relief. The circuit court denied the petition. The Supreme Court dismissed Appellant's appeal, holding that jurisdiction lay in the trial court where Appellant was convicted, which in this case was the Ashley County Circuit Court. Therefore, the Chicot County Circuit Court was without jurisdiction to address Appellant's coram nobis petition.

Read Opinion Are you a lawyer? **Annotate this case**.

Walker v. Kelley

Court: Arkansas Supreme Court
Citation: 2020 Ark. 183
Opinion Date: May 7, 2020
Judge: Rhonda K. Wood
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's pro se petition for declaratory judgment, holding that Appellant could not use a declaratory-judgment action to collaterally attack his criminal conviction. Appellant was convicted of first-degree murder and second-degree unlawful discharge of a firearm from a vehicle. The court of appeals affirmed. Years later, Appellant filed a petition for declaratory judgment alleging that he was denied due process in his criminal trial when the court admitted the prior testimony of an unavailable witness and that this admission violated the Confrontation Clause. The circuit court denied the petition. The Supreme Court affirmed, holding that a declaratory judgment action provided no relief on these grounds.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Flores

Court: Supreme Court of California
Docket: S116307
Opinion Date: May 4, 2020
Judge: Kruger
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction of three counts of first

degree murder and his sentence of death, holding that the three or four minor errors at Defendant's trial were harmless and did not interfere with his due process right to a fair trial. Specifically, the Supreme Court held (1) no error occurred during jury selection; (2) Defendant was not prejudiced by any misstatements by the prosecutor; (3) assuming certain evidence was inadmissible, the court's admonition to the jury and the court's instruction cured the resultant harm; (4) the trial court erred in admitting testimony that the victim was afraid of Defendant, but the error was harmless; and (5) Defendant's remaining allegations of error were without merit.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. Law

Court: California Courts of Appeal
Docket: E072845(Fourth Appellate District)
Opinion Date: May 5, 2020
Judge: Slough
Areas of Law: Constitutional Law, Criminal Law

In 2001, appellant Terrell Law and his codefendant Brett May committed a home invasion robbery, during which one of them shot and killed one of the residents. They were tried jointly in 2006 before two separately empaneled juries who found them both guilty of first degree felony murder with the special circumstance described in Penal Code section 190.2(a)(17(A) and (d). Though Law's jury found he was not the shooter, they nonetheless concluded he was a "major participant" in the underlying robbery and acted "with reckless indifference to human life." In 2018, the Legislature enacted Senate Bill No. 1437 (2017-2018 Reg. Sess.) which, among other things, amended the definition of felony murder in Penal Code section 189. The legislation also added Penal Code section 1170.95, which established a procedure for vacating murder convictions predating the amendment that could not be sustained under the new definition of felony murder. Law challenged the trial court's summary denial of his section 1170.95 petition to vacate his murder conviction, arguing the trial court erred by reviewing his record of conviction and determining the jury's true finding on the special circumstance rendered him ineligible for relief. The Court of Appeal concluded it was proper for a trial court to review the record of conviction when determining whether a section 1170.95 petitioner had stated a prima

facie claim for relief. Additionally, the Court concluded Law "undoubtedly qualifies" as a major participant who acted with reckless indifference to human life, a conclusion that rendered him ineligible for relief under section 1170.95. The Court therefore affirmed the order denying his petition.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. Sanchez

Court: California Courts of Appeal
Docket: E072647(Fourth Appellate District)
Opinion Date: May 7, 2020
Judge: Menetrez
Areas of Law: Constitutional Law, Criminal Law

Victor Sanchez was charged with first degree murder, but pled guilty to voluntary manslaughter. He filed a petition under Penal Code section 1170.95 to vacate that conviction. The trial court denied the petition, concluding that Sanchez was ineligible for relief because he was not convicted of murder. After review, the Court of Appeal joined other courts that held section 1170.95 did not apply to defendants convicted of voluntary manslaughter. The Court also rejected Sanchez's argument that section 1170.95 violated equal protection.

Read Opinion Are you a lawyer? **Annotate this case**.

Galeotti v. International Union of Operating Engineers

Court: California Courts of Appeal
Docket: A157785(First Appellate District)
Opinion Date: May 6, 2020
Judge: Henry E. Needham, Jr.
Areas of Law: Criminal Law, Labor & Employment Law, White Collar Crime

Galeotti, a former Union Local 3 employee, filed a complaint against Local 3 and three of individual union leaders, alleging that the individual defendants required union employees to pay them money to keep their jobs, lied about the reason for collecting the money, and caused Local 3 to terminate Galeotti's employment when he failed to pay the full amount demanded. The trial court dismissed his second amended complaint without leave to amend.

The court of appeal reversed in part, reasoning that a threat to terminate employment can provide a basis for an extortion claim and that the allegations of the second amended complaint stated a cause of action for wrongful termination in violation of the public policy underlying the extortion statutes. The complaint stated a cause of action for violations of the Racketeer Influenced and Corrupt Organizations Act (RICO; 18 U.S.C. 1961), based on the predicate acts of extortion, but did not state a cause of action for interference with prospective economic advantage.

Read Opinion Are you a lawyer? **Annotate this case**.

In re I.A.

Court: California Courts of Appeal
Docket: B296549(Second Appellate District)
Opinion Date: May 4, 2020
Judge: Tangeman
Areas of Law: Criminal Law, Juvenile Law

Where a juvenile court vacates its true finding on a generic murder allegation and redesignates it as a finding on an uncharged target offense, and does so before a minor has had the opportunity to contest the court's findings or orders, the minor may challenge the sufficiency of the evidence of the redesignated offense on appeal. The Court of Appeal held that there was insufficient evidence to support the juvenile court's decision sustaining the allegations that I.A. possessed a concealable firearm and committed vandalism. Therefore, the court reversed the juvenile court's findings, vacating the jurisdiction and disposition order and dismissing the Welfare and Institutions Code section 602 petition.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Edwards

Court: California Courts of Appeal
Docket: A158055(First Appellate District)
Opinion Date: May 1, 2020
Judge: Petrou
Areas of Law: Criminal Law

In 2006, Edwards fired an assault weapon into an apartment, killing the victim. Edwards pled guilty to possession of a firearm as a felon and was convicted of second-degree murder and shooting into an inhabited dwelling. Following the enactment of Senate Bill 1437, Edwards filed a Penal Code 1170.95 resentencing petition, checking form boxes indicating that he was convicted under a theory of felony murder or murder under the natural and probable consequences doctrine and that he could not now be convicted of 1st or 2nd-degree murder because of changes to Penal Code 188 and 189. Edwards submitted the jury instructions and the transcript of the prosecutor's closing remarks that Edwards acted with "both express malice, specific intent to kill, as well as implied malice," described as "an intentional act, the natural consequences of which are dangerous to human life, and at the time that the individual acted, they knew of the danger, and they deliberately acted with conscious disregard." The court denied the petition, finding that Edwards was convicted on a valid theory of murder that survived the statutory changes. The court of appeal affirmed. The superior court did not err in considering the record of conviction. Edwards could not meet the statutory prerequisites for even filing a section 1170.95 petition because he was not charged or convicted of second-degree felony murder or murder under the natural or probable consequences doctrine directed at accomplice liability.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Thomkins

Court: California Courts of Appeal
Docket: A141375(First Appellate District)
Opinion Date: May 1, 2020
Judge: Streeter
Areas of Law: Criminal Law

On Easter night in 2011, gunfire erupted at an Oakland bar-restaurant, leaving two people dead and five wounded. Thompkins and Fox were convicted of two counts of first-degree murder for the benefit of a criminal street gang, with firearm discharge enhancements, a multiple-murder special circumstance, and five counts of attempted murder with great bodily injury findings, gang enhancements, and firearm discharge enhancements.

Thompkins was convicted as the shooter and Fox as an accomplice. Both were sentenced to life in prison without possibility of parole, plus 224 years to life. After Thompkins was sentenced, Fox stated under oath he was the actual shooter and Thompkins knew nothing about Fox's intentions. Thompkins claimed this new testimony, and his attorney's incompetent reaction entitled him to a new trial and submitted a declaration by another gang member who was present that night. The court of appeal concluded that Thompkins's attorney was not ineffective for failing to bring a motion to recall the sentence followed by a new trial motion because Thompkins failed to show prejudice. The attempted murder convictions and related enhancements must be reversed for both defendants based on the flawed kill zone instruction. Introducing evidence that defendants admitted their gang affiliation at jail intake violated the defendants' privilege against self-incrimination but was harmless. There was some evidentiary error that was harmless due to the wealth of admissible evidence establishing the gang enhancements. Arguments based on the statutory amendments to Penal Code 188 and 189 must be raised in the trial court (section 1170.95). The case must be remanded so the judge may exercise his discretion whether to impose or strike the firearm enhancements on under Penal Code 12022.53.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Torres

Court: California Courts of Appeal
Docket: B295043(Second Appellate District)
Opinion Date: May 4, 2020
Judge: Wiley
Areas of Law: Criminal Law

After the trial court admitted a witness's former testimony, the Court of Appeal applied People v. Roldan (2012) 205 Cal.App.4th 969, 975–985, and reversed. Roldan held that, before invoking the former testimony exception, prosecutors should react appropriately to the impending deportation risk by following four steps: alert the defense to the risk; videotape the preliminary hearing testimony; use judicial measures to try to delay deportation; and consider an array of other specific measures. In this case, the prosecution conceded that prosecutors were simply unaware of Roldan and did not comply with it. The court held that Roldan controls the court's analysis

because the facts about prosecutorial diligence are weaker here than they were in Roldan, where the appellate court held for the defense. In this case, the record before deportation is of prosecutorial inaction where the prosecution's brief in this court admits the investigating officer did not do anything to ensure that the witness would not be deported, nor is there other evidence of prosecutorial efforts to delay the witness's departure or to videotape his testimony at the preliminary hearing.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Triplett

Court: California Courts of Appeal
Docket: B298914(Second Appellate District)
Opinion Date: May 1, 2020
Judge: Frances Rothschild
Areas of Law: Criminal Law

Defendant was convicted of assault with a deadly weapon, carjacking, and attempted murder. In the published portion of the opinion, the Court of Appeal held that the trial court erred by denying defense counsel's request to inform the jurors that they could have testimony of certain witnesses read back to them. The court also held that, under the circumstances in this case, the error was harmless.

Read Opinion Are you a lawyer? **Annotate this case**.

Colorado In Interest of G.S.S.

Court: Colorado Supreme Court
Citation: 2020 CO 32
Opinion Date: May 4, 2020
Judge: Brian D. Boatright
Areas of Law: Constitutional Law, Criminal Law, Juvenile Law

After being charged, fourteen-year-old G.S.S. was detained for more than three months without bail, even though he had not entered a plea and had not been tried on the charges against him. At that point, G.S.S.'s counsel filed a motion to dismiss, arguing that G.S.S.'s "right to a speedy trial" had been violated under section 19-2-509(4)(b), C.R.S. (2019). The trial court

agreed and dismissed the case against G.S.S. with prejudice, and the court of appeals affirmed in Colorado in Interest of G.S.S., 2019 COA 4M, __ P.3d __. The Colorado Supreme Court then granted certiorari to determine the proper remedy for a violation of the sixty-day limit in section 19-2-509(4)(b). The Supreme Court determined the remedy for a section 19-2-509(4)(b) violation was for the trial court to immediately hold a bail hearing and order the juvenile's release. Accordingly, the judgment of the court of appeals was reversed.

Read Opinion Are you a lawyer? **Annotate this case**.

Barringer v. Halkitis

Court: Florida Supreme Court
Docket: SC19-1071
Opinion Date: May 7, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court held that Jay Barringer's quo warranto petition filed in this case was a frivolous proceeding brought before the Supreme Court by a state prisoner and sanctioned Barringer by barring him from filing any further pro se requests for relief related to his criminal case. Barringer was convicted of one count of attempted sexual battery of a victim less than twelve years old and sentenced to twenty-five-years' imprisonment. In 2011, Barringer began filing petitions in the Supreme Court. The Court did not grant the relief sought in any of Barringer's filings. In the instant quo warranto petition Barringer challenged his conviction on the ground that the information was defective, a claim Barringer previously raised by way of a habeas petition. The Supreme Court denied the petition and found that Barringer abused the Court's limited judicial resources. The Court sanctioned Barringer by directing the Clerk of Court to reject any future pleadings or other requests for relief submitted by Barringer that are related to his criminal case, unless such filings are signed by a member of The Florida Bar in good standing.

Read Opinion Are you a lawyer? **Annotate this case**.

Franqui v. State

Court: Florida Supreme Court
Docket: SC19-203
Opinion Date: May 7, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the order of the circuit court denying Appellant's claim of intellectual disability, raised in successive motions for postconviction relief under Fla. R. Crim. P. 3.851, holding that the circuit court did not err in denying relief. Appellant was convicted of first-degree murder and sentenced to death in two separate cases. After the United States Supreme Court decided Hall v. Florida, 572 U.S. 701 (2014), Appellant filed successive motions for postconviction relief in both of his capital cases, asserting that the circuit court's denials of his previous claims of intellectual disability were based on the court's improper interpretation of Florida's intellectual disability statute. The circuit court summarily denied the motions. The Supreme Court reversed and remanded for an evidentiary hearing on the issue of intellectual disability. After a hearing, the circuit court denied the claim. The Supreme Court affirmed, holding (1) the circuit court did not err in denying Appellant's intellectual disability claim; and (2) Appellant was not entitled to relief under Hurst v. Florida, 136 S. Ct. 616 (2016), or Hurst v. State, 202 So. 3d 40 (Fla. 2016).

Read Opinion Are you a lawyer? **Annotate this case**.

Hicks v. State

Court: Florida Supreme Court
Docket: SC19-1978
Opinion Date: May 7, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court denied the instant mandamus petition filed by Hicks and sanctioned Hicks by barring him from filing any further pro se requests for relief related to his criminal case. Hicks was convicted of one count of lewd and lascivious conduct by a person over eighteen years of age on a victim under sixteen years of age. Since 2016, Hicks filed thirteen pro se requests for relief in the Supreme Court related to his criminal case. The

Court did not grant the relief sought in any of Hicks' filings. In the instant petition, Hicks sought a writ of mandamus compelling the circuit court to comply with the requirements of Fla. R. Crim. P. 3.850 by filing a copy of an order denying his second postconviction motion with the clerk of court. The Supreme Court dismissed the petition and found that Hicks abused this Court's limited judicial resources. The Court directed the Clerk of Court to reject any future pleadings or other requests for relief submitted by Hicks that are related to his criminal case, unless such filings are signed by a member of The Florida Bar in good standing.

Read Opinion Are you a lawyer? **Annotate this case**.

Burley v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0356
Opinion Date: May 4, 2020
Judge: Boggs
Areas of Law: Constitutional Law, Criminal Law

In 1992, Douglas Burley pled guilty to malice murder. He moved for an out-of-time appeal in 2019, claiming that his right to appeal was frustrated by his plea counsel's erroneous advice that he could not appeal his conviction because it was the product of a guilty plea. The trial court denied Burley's motion. After review, the Georgia Supreme Court vacated the trial court's judgment and remanded the case with direction to hold a hearing to determine whether ineffective assistance of counsel frustrated Burley's right to appeal.

Read Opinion Are you a lawyer? **Annotate this case**.

Carter v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0022
Opinion Date: May 4, 2020
Judge: David E. Nahmias
Areas of Law: Construction Law, Criminal Law

Brandon Carter was convicted by jury of malice murder and two firearm offenses in connection with the shooting death of Terrance Baker. On appeal, Carter contended the trial court erred by admitting certain hearsay statements into evidence and by violating his constitutional right to be present during his trial. Finding no reversible error, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Clarke v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0258
Opinion Date: May 4, 2020
Judge: Ellington
Areas of Law: Constitutional Law, Criminal Law

Rupert Clark was convicted by jury for the malice murder of his wife, Rosemarie Lebert-Clark. He was also convicted of possession of a firearm during the commission of a felony. On appeal, he argued he received ineffective assistance of trial counsel, and that the trial court erred in admitting certain evidence, violated the continuing witness rule by sending out with the deliberating jury printouts of text messages, and by failing to instruct the jury that a defendant's uncorroborated confession was not alone sufficient to warrant a conviction. Finding no reversible error after reviewing the trial court record, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Collins v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0195
Opinion Date: May 4, 2020
Judge: Harold D. Melton
Areas of Law: Constitutional Law, Criminal Law

Renita Collins was tried for murder along with co-defendant Michael Stallworth. Collins appealed her convictions for murder and possession of a firearm while in commission of a felony in connection with the shooting

death of Keith Jacobs. On appeal. Collins contended she was denied a fair trial due to juror misconduct, the trial court abused its discretion by not allowing her to subpoena juror testimony to show that misconduct had occurred, and the trial court abused its discretion when it failed to excuse a prospective juror for cause. Finding no reversible error, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Dawson v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0217
Opinion Date: May 4, 2020
Judge: Warren
Areas of Law: Constitutional Law, Criminal Law

Lavaris Dawson was convicted by jury of felony murder and other crimes in connection with the shooting death of Mamadou Camara. On appeal, Dawson challenged the sufficiency of the evidence supporting his convictions, and argued the trial court erred in admitting Dawson's statements to a detective during an interview because those statements were impermissibly induced by a hope of benefit, and that Dawson was denied his due process right to a timely appeal. After review, the Georgia Supreme Court disagreed and affirmed Dawson's convictions.

Read Opinion Are you a lawyer? **Annotate this case**.

Evans v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0007
Opinion Date: May 4, 2020
Judge: McMillan
Areas of Law: Constitutional Law, Criminal Law

Jimmy Evans was convicted by jury for murder and other crimes relating to the 2006 deaths of Tavoris Calhoun and Dezmon Thomas. On appeal, Evans argued that because he was visibly intoxicated at the time he made statements to law enforcement and consented to a search of his home and

person, the statements and consent were involuntarily given and the trial court should have granted his motion for new trial on this ground. Furthermore, Evans argued that his trial counsel was ineffective for failing to file a motion to suppress at trial on the same basis. Because Evans failed to show error or ineffective assistance of counsel, the Georgia Supreme Court affirmed his conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Hill v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0285
Opinion Date: May 4, 2020
Judge: Harold D. Melton
Areas of Law: Constitutional Law, Criminal Law

Esco Hill was convicted by jury of malice murder and other crimes relating to the stabbing death of Alford Morris in 2014. On appeal, Hill argued the trial court committed reversible error by requiring him to be visibly shackled for the duration of his six-day trial. After review of the trial court record, the Georgia Supreme Court concurred this was reversible error, consequently, reversed judgment of conviction. Because the Court concluded the evidence at trial was sufficient to sustain Hill's conviction, the State could re-try him. The Court did not address Hill's remaining enumerations of error, "as they are not likely to recur in the event of a retrial."

Read Opinion Are you a lawyer? **Annotate this case**.

Oliver v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0489
Opinion Date: May 4, 2020
Judge: McMillan
Areas of Law: Constitutional Law, Criminal Law

Jacquan Oliver entered a negotiated plea of guilty to felony murder in connection with the shooting death of Alexander Mixon. He appealed his

conviction and sentence, arguing that the trial court abused its discretion in finding a factual basis for his plea, and in determining the plea was voluntarily, knowingly and intelligently made. Finding no merit to these contentions, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Rosser v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0103
Opinion Date: May 4, 2020
Judge: Bethel
Areas of Law: Constitutional Law, Criminal Law

Larry Rosser was convicted by jury of malice murder and other crimes in connection with the death of Alexis Vereen. On appeal, Rosser challenged the sufficiency of the evidence presented against him at trial, and argued the trial court erred by not granting his motion for a mistrial, and by allowing the State to introduce a portion of Rosser's custodial statement to law enforcement. In addition, he argued he received constitutionally ineffective assistance of trial counsel. Finding no reversible error after reviewing the trial court record, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Spencer v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0871
Opinion Date: May 4, 2020
Judge: Keith R. Blackwell
Areas of Law: Constitutional Law, Criminal Law

Christopher Spencer was convicted by jury of murder and other crimes in connection with the fatal shootings of Sylvia Watson and Samuel White. Spencer appealed, claiming only that the evidence was insufficient to support his convictions. Finding no reversible error after reviewing the trial court record, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Styles v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0236
Opinion Date: May 4, 2020
Judge: Ellington
Areas of Law: Constitutional Law, Criminal Law

Derrick Styles was convicted by jury of felony murder and other crimes in connection with the shooting death of Alberto Lumens and the armed robbery fo Juan Lumens Garcia. On appeal, Styles contended the trial court erred in admitting into evidence a recording of an inculpatory telephone conversation between himself and a witness. He also argued his trial counsel was ineffective for failing to object to an allegedly improper comment by the prosecutor during closing argument. Finding no merit to these contentions, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Whitehead v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0171
Opinion Date: May 4, 2020
Judge: Ellington
Areas of Law: Constitutional Law, Criminal Law

Javis Whitehead was convicted by jury of murder and other crimes in connection with the shooting death of Dominique Larry. On appeal, Whitehead challenged the sufficiency of the evidence presented to rebut his claim of self-defense and to convict him for murder beyond a reasonable doubt. He also argued the trial court erred in denying his motion to suppress his custodial statement, and in refusing to excuse for cause the District Attorney from the panel of prospective jurors prior to the conclusion of voir dire. Finding no merit to these contentions, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Idaho v. Blythe

Court: Idaho Supreme Court - Criminal
Docket: 46992
Opinion Date: May 4, 2020
Judge: Roger S. Burdick
Areas of Law: Constitutional Law, Criminal Law

Nicholas Blythe appealed after he was convicted of possessing a controlled substance. He conditionally pled guilty, reserving the right to challenge his sentence. On appeal, he argued the district court erred in denying his motion to suppress certain evidence found because the evidence presented at trial was found in violation of Blythe's Fourth Amendment rights. After review, the Idaho Supreme Court determined the search at issue took place before an arrest occurred, and because no rationale justifying a search incident to arrest was sufficiently present here, the search of Blythe's shoes was not a valid search incident to arrest. Therefore, the district court erred in holding that the search was reasonable under the Fourth Amendment. Blythe's conviction was vacated, the district court order denying Blythe's motion to suppress was reversed, and the matter remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

Idaho v. Glodowski

Court: Idaho Supreme Court - Criminal
Docket: 47131
Opinion Date: May 6, 2020
Judge: Roger S. Burdick
Areas of Law: Constitutional Law, Criminal Law

David Glodowski appealed after he was convicted for failing to update his sex-offender registration in violation of Idaho Code section 18-8309. He argued the district court erred by ruling that his prior conviction under a Wisconsin statute was "substantially equivalent" to Idaho statutes that required sex-offender registration in Idaho. After review, the Idaho Supreme Court determined the district court improperly allowed the State to seek a

redetermination of the “substantially equivalent” element given that the Idaho Bureau of Criminal Identification made a final determination on that element. However, because the State put forth sufficient evidence to prove that element, and the district court’s jury instruction accomplished the same purpose, the Supreme Court concluded the error was harmless. Accordingly, the Court found no reversible error in the district court’s decision to grant the State’s motion and provide the jury instruction. Therefore, judgment of conviction was affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Idaho v. Jones

Court: Idaho Supreme Court - Criminal
Docket: 45905
Opinion Date: May 4, 2020
Judge: Roger S. Burdick
Areas of Law: Constitutional Law, Criminal Law

Timothy Jones was convicted by jury of trafficking heroin and possession of drug paraphernalia. On appeal, he argued the trial court erred in admitting certain evidence regarding his probation status, a knife found in the initial police search of his person, and that the trial court abused its discretion in arriving at his sentence. Finding no reversible error, the Idaho Supreme Court affirmed Jones' conviction and sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Gordon

Court: Iowa Supreme Court
Docket: 18-1099
Opinion Date: May 1, 2020
Judge: Brent R. Appel
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction for assault on a peace officer with a dangerous weapon, a felony, and several misdemeanors, holding that Defendant did not receive ineffective assistance of counsel. After Defendant pleaded guilty, he absconded. He was later returned to

custody. On appeal, Defendant argued that he received ineffective assistance of counsel because the plea bargain contained an unlawful term. Specifically, Defendant argued that the plea bargain's provision that he would be released from jail for a forty-eight-hour furlough after pleading guilty was illegal and that his trial counsel committed ineffective assistance in obtaining the illegal benefit for him. The Supreme Court affirmed, holding that where Defendant entered into the plea agreement with the illegally lenient sentence, he could not benefit from that sentence and then attack the plea bargain.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Craig

Court: Kansas Supreme Court
Docket: 119660
Opinion Date: May 1, 2020
Judge: Dan Biles
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's conviction and sentence for first-degree felony murder, holding that there was no error in the proceedings below. A jury found Defendant guilty of both first-degree felony murder and second-degree intentional murder. At sentencing, Defendant moved for a new trial and judgment notwithstanding the verdict, arguing that the jury must have had reasonable doubt on the first-degree felony murder theory because it convicted him of second-degree murder for the same killing. The district court dismissed the second-degree murder conviction and sentenced Defendant for the felony murder over his objection. The Supreme Court affirmed, holding (1) the district court did not err when it sentenced Defendant on felony murder instead of declaring a mistrial because Defendant did not establish that the jury failed to find each element of the felony murder beyond a reasonable doubt or that the jury's first- and second-degree murder verdicts were so irreconcilable as to require a new trial; and (2) the district court did not err in declining to give an instruction on voluntary intoxication.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Lemmie

Court: Kansas Supreme Court
Docket: 119439
Opinion Date: May 1, 2020
Judge: Carol A. Beier
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's convictions of first-degree felony murder, aggravated robbery, conspiracy to commit aggravated robbery, criminal possession of a firearm, fleeing and eluding, and interference with law enforcement, holding that Defendant's arguments on appeal failed. Specifically, the Supreme Court held (1) any possible violation of Defendant's Fifth Amendment right in the admission of a witness's testimony about Defendant giving the witness phone passcodes was undoubtedly harmless; (2) the district court did not err by admitting hearsay statements as statements of a coconspirator and contemporaneous statements; (3) the State introduced sufficient evidence to convict Defendant of first-degree murder; and (4) the district judge did not abuse its discretion by admitting testimony that Defendant was upset over a meth pipe that went missing.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Mullen

Court: Maine Supreme Judicial Court
Citation: 2020 ME 56
Opinion Date: May 5, 2020
Judge: Connors
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed Defendant's conviction for reckless conduct and aggravated criminal mischief, holding that the trial court did not abuse its discretion by offering Defendant a continuance of the trial in lieu of excluding his medical records. On appeal, Defendant argued that the trial court abused its discretion by denying his motion to suppress his personal medical records as a sanction for the State's late seizure of the records. The Supreme Judicial Court agreed that the State's conduct undermined the purpose of Maine Rule of Unified Criminal Procedure 18(b) but that the court's offer of a continuance in lieu of the exclusion of the evidence

constituted an appropriate response to the State's conduct.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. Billingslea

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12715
Opinion Date: April 30, 2020
Judge: Cypher
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Judicial Court affirmed Defendant's convictions and the decision of the Appeals Court denying Defendant's motion to vacate the entry of his appeal from his convictions in that court and to have the case entered directly in the Supreme Judicial Court, holding that a direct appeal from the third conviction of a habitual offender pursuant to Mass. Gen. Laws ch. 279, 25(b) may be entered in the Appeals Court. Defendant was indicted for serious felonies arising from a brutal attack and rape. In addition to charging the specific felony, each indictment also alleged that the sentence for that felony should be enhanced pursuant to the habitual criminal provision Mass. Gen. Laws ch. 279, 25(a) or the habitual offender provision of section 25(b), or both. After he was convicted, Defendant moved to have the case entered directly in the Supreme Judicial Court. The Appeals Court denied the motion. The Supreme Judicial Court affirmed Defendant's convictions, holding (1) this direct appeal was entitled to the unique review prescribed by Mass Gen. Laws ch. 278, 33E, and the Appeals Court may conduct such section 33E review; (2) Defendant was not impermissibly allowed to waive his right to a jury trial on the sentencing enhancement provisions of the indictments; and (3) Defendant was not entitled to reversal of his convictions on any other ground.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. Martin

Court: Massachusetts Supreme Judicial Court
Docket: SJC-08768
Opinion Date: May 5, 2020

Judge: Ralph D. Gants
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Judicial Court affirmed Defendant's conviction of murder in the first degree and the denial of his motion for a new trial and declined to exercise its authority under Mass. Gen. Laws ch. 278E to reduce Defendant's conviction to murder in the second degree, holding that Defendant was not entitled to relief on any of his allegations of error. Defendant was convicted of murder in the first degree on the theory of felony-murder. Defendant filed a motion for a new trial, which was denied. The Supreme Judicial Court affirmed, holding (1) Defendant's motion for a new trial was correctly denied because Defendant was not prejudiced by counsel's ineffective assistance; (2) this Court declines to extend the reach of the Court's holding in Commonwealth v. Brown, 477 Mass. 805 (2017), to Defendant's case; and (3) trial judge erred when he declined Defendant's request that the jury be instructed on the elements of voluntary and involuntary manslaughter, but the error was not prejudicial in the context of the judge's other instructions.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. Tavares

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12631
Opinion Date: May 6, 2020
Judge: Lowy
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed Defendant's conviction of murder in the first degree on theories of deliberate premeditation and extreme atrocity or cruelty and declined to exercise its power pursuant to Mass. Gen. Laws ch. 278, 33E to reduce the conviction to manslaughter, holding that there was no reversible error in the proceedings below. Specifically, the Supreme Judicial Court held (1) the trial judge did not err by denying Defendant's requests for a jury instruction pursuant to Commonwealth v. Croft, 345 Mass. 143 (1962); (2) the trial judge did not err by denying Defendant's motions for a required finding of not guilty under Croft because a rational jury could have found that Defendant was guilty of murder in the first degree

on both the theories of premeditation and extreme atrocity or cruelty; and (3) there was no basis for reducing Defendant's sentence or ordering a new trial.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Branch

Court: Minnesota Supreme Court
Docket: A18-1055
Opinion Date: May 6, 2020
Judge: Lorie Skjerven Gildea
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's sentences for drive-by shooting at an occupied vehicle and second-degree assault, holding that Minn. Stat. 609.035 did not prohibit the sentences for both offenses when the crimes arose from a single behavioral incident. The district court sentenced Defendant to forty-eight months for drive-by shooting at an occupied vehicle and thirty-six months for second-degree assault and imposed the two sentences to run concurrently. The court of appeals affirmed. The Supreme Court affirmed, holding that, under this Court's analysis in State v. Ferguson, 808 N.W.2d 586 (Minn. 2012), the district court properly imposed multiple sentences in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

Galloway v. Mississippi

Court: Supreme Court of Mississippi
Citation: 2018-CA-01427-SCT
Opinion Date: May 7, 2020
Judge: Beam
Areas of Law: Constitutional Law, Criminal Law

Leslie Galloway appealed the denial of his 2015 petition for post-conviction relief (PCR) pertaining to his 2007 guilty plea to carjacking, a conviction that was used as an aggravating circumstance in Galloway's 2010 capital-murder trial at which Galloway received a death sentence. Galloway claimed in the petition that his defense counsel Wendy Martin had an actual

conflict of interest because, before becoming his defense counsel, Martin had served as an assistant district attorney in the same case, unbeknownst to Galloway. The trial court ruled that Galloway's PCR claim was time barred under Mississippi's Uniform Post-Conviction Collateral Relief Act (UPCCRA), having been filed more than seven years after Galloway's conviction for carjacking. The trial court alternatively found no merit to Galloway's PCR claim, time bar notwithstanding. Accordingly, the trial court denied Galloway's PCR petition. The Mississippi Supreme Court agreed with the trial court that Galloway's PCR claim was time barred under the UPCCRA. The Court also agreed there was no merit to Galloway's PCR claim.

Read Opinion Are you a lawyer? **Annotate this case**.

City of Missoula v. Zerbst

Court: Montana Supreme Court
Citation: 2020 MT 108
Opinion Date: May 5, 2020
Judge: Beth Baker
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court reversed Defendant's conviction for sexual assault, holding that the municipal court erred when it instructed the jury on a definition of "consent" from the 2017 sexual assault statute and not the applicable 2015 statute, and the erroneous jury instruction prejudicially affected Defendant's substantial rights. At trial, the court instructed the jury, over Defendant's objection, on the definition of consent contained in recent amendments to the sexual assault statute. On appeal, Defendant argued that the municipal court failed to apply the correct law when instructing the jury on the elements of the claimed offense. The district court denied the appeal. The Supreme Court reversed, holding (1) the instructions, as a whole, did not fully and fairly instruct the jury on the law applicable to the case; and (2) Defendant's substantial due process right was prejudiced by the erroneous jury instruction.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Degarmo

Court: Nebraska Supreme Court
Citation: 305 Neb. 680
Opinion Date: May 1, 2020
Judge: Stacy
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction of driving under the influence, holding that Defendant consented to a chemical test of his urine and, therefore, the results of the urine test were admissible. A law enforcement officer stopped Defendant for an expired registration. Based on his observations, the officer, a certified drug recognition evaluation expert, administered field sobriety tests. The officer concluded that Defendant was under the influence of marijuana arrested Defendant for driving under the influence and then took him to a detoxification center. Thereafter, a chemical test of Defendant's urine confirmed the presence of marijuana. On appeal, Defendant challenged the admission of the results of the urine test. The Supreme Court affirmed, holding that Defendant voluntarily consented to the warrantless search of his urine, and therefore, the search fell within a recognized exception to the warrant requirement.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Holz

Court: New York Court of Appeals
Citation: 2020 NY Slip Op 02682
Opinion Date: May 7, 2020
Judge: Fahey
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Court of Appeals held that N.Y. Crim. Proc. Law (CPL) 710.70(2) grants a defendant the right to review of a suppression decision when the order related exclusively to a count that was satisfied by a guilty plea but was not one to which the defendant pleaded guilty. Defendant was charged with two counts of burglary in the second degree. The first count related to a laptop computer, and the second count related to jewelry. Defendant moved to suppress the jewelry, but Supreme Court denied the motion. Defendant then pleaded guilty to one count of burglary in the second degree as charged in the count pertaining to the theft of the laptop computer, in satisfaction of the

count charging the burglary of jewelry. On appeal, Defendant argued that Supreme Court erred in denying his motion to suppress the jewelry. The Appellate Division affirmed, concluding that it was jurisdictionally precluded from reviewing the suppression order. The Court of Appeals reversed, holding (1) Defendant's right to appellate review of Supreme Court's suppression order was secured by CPL 710.70(2); and (2) because the Appellate Division did not reach the underlying suppression question the case must be remitted to the Appellate Division for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Maffei

Court: New York Court of Appeals
Citation: 2020 NY Slip Op 02680
Opinion Date: May 7, 2020
Judge: DiFiore
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Court of Appeals affirmed the order of the Appellate Division concluding on direct appeal that Defendant was not entitled to relief on his ineffective assistance of counsel claim, holding that Defendant, on this record, did not sustain his burden to establish that counsel was constitutionally ineffective. After a jury trial, Defendant was convicted of second-degree murder. On appeal, Defendant argued that his trial counsel's failure to challenge a prospective juror constituted ineffective assistance of counsel. The Appellate Division affirmed. The Court of Appeals affirmed, holding (1) the record was inadequate to review Defendant's ineffective assistance of counsel claim; and (2) the appropriate procedure for the litigation of Defendant's challenge to his counsel's performance was a N.Y. Crim. Proc. Law 440.10 motion.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Bailey

Court: North Carolina Supreme Court
Docket: 360A19
Opinion Date: May 1, 2020

Judge: Davis
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the decision of the court of appeals affirming the order of the trial court denying Defendant's motion to suppress evidence seized during the execution of a search warrant, holding that the warrant supported by probable cause. Defendant pled guilty to the offense of trafficking in cocaine while preserving his right to appeal the denial of his motion to suppress. On appeal, Defendant argued that the trial court erred in denying his motion to suppress because the facts contained in the affidavit were insufficient to establish probable cause to search his residence. The court of appeals affirmed. The Supreme Court affirmed, holding that the affidavit contained facts that were sufficient to provide a nexus between the residence and suspected criminal activity, and therefore, the warrant was supported by probable cause.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Ellis

Court: North Carolina Supreme Court
Docket: 340A19
Opinion Date: May 1, 2020
Judge: Robin E. Hudson
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court reversed the decision of the Court of Appeals affirming the trial court's denial of Defendant's motion to suppress evidence, holding that there was no reasonable suspicion to justify the law enforcement officer's stop when Defendant signaled with his middle finger from the passenger side window of a moving vehicle. While assisting a stranded motorist, the officer turned his attention to another car traveling on the roadway, a white SUV. Defendant had his arm outside the passenger window and gestured with his middle finger, making an up-and-down motion. Believing that Defendant was committing the crime of disorderly conduct, the officer pursued and then stopped the SUV. At trial, Defendant moved to suppress the officer's testimony, arguing that there was no reasonable suspicion to justify the stop. The trial court denied the motion. Defendant pleaded guilty to resisting, delaying, or obstructing a public

officer. The court of appeals affirmed the trial court's denial of Defendant's motion to suppress. The Supreme Court reversed, holding that the specific, articulable facts did not establish reasonable suspicion of the crime of disorderly conduct.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Hobbs

Court: North Carolina Supreme Court
Docket: 263PA18
Opinion Date: May 1, 2020
Judge: Earls
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court reversed Defendant's conviction, holding that the trial court clearly erred in ruling that Defendant failed to prove purposeful discrimination with respect to the State's use of peremptory challenges to strike three jurors without considering all of the evidence presented by Defendant. Defendant was found guilty of one count of first-degree murder and other crimes. On appeal, Defendant argued that the trial court erred by failing to grant three objections that he made under Batson v. Kentucky, 476 U.S. 79 (1986). The court of appeals affirmed Defendant's convictions. The Supreme Court reversed, holding (1) the court of appeals erred in its analysis of Defendant's Batson claims with respect to the three jurors; and (2) as to all three jurors, remand was required for reconsideration of whether Defendant proved purposeful discrimination in each case.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Mylett

Court: North Carolina Supreme Court
Docket: 6A19
Opinion Date: May 1, 2020
Judge: Earls
Areas of Law: Criminal Law

The Supreme Court reversed the decision of the court of appeals affirming the trial court's judgment convicting Defendant for conspiracy to commit

harassment of a juror, holding that the trial court erred in denying Defendant's motion to dismiss the conspiracy charge for insufficient evidence. Defendant was convicted of conspiracy to commit harassment of a juror because of his actions at a courthouse following his twin brother's conviction for assault on a government official. On appeal, the court of appeals concluded that the trial court did not err in denying Defendant's motion to dismiss the conspiracy charge for insufficient evidence. The Supreme Court reversed, holding that the evidence in Defendant's trial was insufficient to raise anything more than mere conjecture that he had made an agreement with another person to threaten or intimidate a juror.

Read Opinion Are you a lawyer? **Annotate this case**.

Dodge v. North Dakota

Court: North Dakota Supreme Court
Citation: 2020 ND 100
Opinion Date: May 7, 2020
Judge: Gerald W. VandeWalle
Areas of Law: Constitutional Law, Criminal Law

Richard Dodge appealed from a district court order denying his application for post-conviction relief. Dodge was charged with five felonies and a misdemeanor in December 2015. Dodge was appointed counsel. In April 2016, Dodge's counsel moved the court to withdraw because the attorney-client relationship was "irreparably broken and rendered unreasonably difficult." The court granted the motion, and Dodge was appointed substitute counsel in May 2016. In July 2016, Dodge himself filed a "motion to dismiss counsel." The court denied Dodge's motion. Five months after the deadline for motions and plea agreements, Dodge's counsel sought to have Dodge submit to a psychiatric examination. This request was denied, the trial court found no evidence, and the the court itself made no observations, that Dodge was incompetent to stand trial. After this denial, Dodge himself again moved to dismiss his trial counsel, and due to the allegations Dodge made in his motion, counsel moved to withdraw. The trial court denied both motions, and instead, required the attorney to appear as standby counsel and assist Dodge during trial if requested, but relieved him of any further obligations to consult with Dodge. The case proceeded to trial. At the beginning of trial, the court gave Dodge the option of representing himself or

having his attorney represent him. Dodge chose to have his attorney represent him. Because his attorney had not prepared for trial and had no communication with Dodge since he moved to withdraw, Dodge's attorney asked for a brief recess to consult with Dodge. During the recess, a settlement was reached. Dodge agreed to enter Alford pleas on all counts, waived a presentence investigation, and agreed to be sentenced immediately after entering his pleas. Dodge was immediately sentenced following his guilty pleas, and thereafter sought post-conviction relief on grounds he was not competent to enter his pleas, and that he received ineffective assistance of trial counsel. After review, the North Dakota Supreme Court concluded the district court's finding that Dodge was competent when he entered his pleas was not clearly erroneous, and disposed of his claim of ineffective assistance of counsel.

Read Opinion Are you a lawyer? **Annotate this case**.

Hewitt v. NDDOT

Court: North Dakota Supreme Court
Citation: 2020 ND 102
Opinion Date: May 7, 2020
Judge: Lisa K. Fair McEvers
Areas of Law: Criminal Law, Government & Administrative Law

Larry Hewitt appealed a district court judgment affirming the North Dakota Department of Transportation's revocation of his driving privileges. Hewitt claimed the Department's hearing file was improperly admitted at the administrative hearing. After review, the North Dakota Supreme Court affirmed, concluding the hearing file was properly admitted as a self-authenticating copy of an official record.

Read Opinion Are you a lawyer? **Annotate this case**.

Kastet v. NDDOT

Court: North Dakota Supreme Court
Citation: 2020 ND 91
Opinion Date: May 7, 2020
Judge: Daniel J. Crothers

Areas of Law: Criminal Law, Government & Administrative Law

The North Dakota Department of Transportation (Department) appealed the district court's reversing a hearing officer's decision suspending Holden Kastet's driving privileges for 365 days. The Department argued the hearing officer did not abuse his discretion in admitting the chemical breath test, and State Highway Patrol Trooper King scrupulously complied with the approved method for testing Kastet's breath on the Intoxilyzer 8000. After review, the North Dakota Supreme Court concurred with the Department and reversed the district court judgment. The matter was remanded with instructions to reinstate the hearing officer's decision.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Dahl

Court: North Dakota Supreme Court
Citation: 2020 ND 87
Opinion Date: May 7, 2020
Judge: Jerod E. Tufte
Areas of Law: Constitutional Law, Criminal Law

The State of North Dakota appealed a district court order denying its motion to resume prosecution against Matthew Dahl and dismissing the case. In December 2014, the State charged Dahl with two counts of theft. Dahl did not appear on the charges until he was arrested on a bench warrant in February 2017. In mid-April 2017, the State mailed Dahl a pretrial diversion agreement. Dahl signed and returned the notarized agreement dated May 3, 2017. On May 9, 2017, the state's attorney signed and filed the agreement with the district court, and the court approved the agreement the same day. Under the agreement, the State agreed to suspend prosecution for "two years from the date of execution" conditioned on Dahl's timely payment of restitution. Dahl failed to make minimum monthly restitution payments. On June 6, 2019, the State moved to resume prosecution, alleging Dahl violated the pretrial diversion agreement by his non-payment. The district court held a hearing on the State's motion in August 2019. The court concluded the pretrial agreement was executed when Dahl signed it on May 3, 2017. The court then denied the State's motion to resume prosecution as untimely under N.D.R.Crim.P. 32.2(d)(2), and dismissed the complaint

against Dahl. After review, the North Dakota Supreme Court reversed, concluding the district court erred in determining the State's motion was untimely, and remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Foster

Court: North Dakota Supreme Court
Citation: 2020 ND 85
Opinion Date: May 7, 2020
Judge: Jon J. Jensen
Areas of Law: Constitutional Law, Criminal Law

Akeem Foster was convicted by jury of Terrorizing and Carrying a Concealed Weapon. Foster contended on appeal he was denied a fair trial because he was asked during cross-examination if other witnesses were lying and because the prosecutor expressed personal beliefs about the evidence during closing arguments. Foster also argued there was insufficient evidence to convict him of either charge. After review, the North Dakota Supreme Court affirmed Foster's conviction for Carrying a Concealed Weapon, but reversed his conviction for Terrorizing. The Court found Foster was improperly asked to provide an opinion on the veracity and credibility of the State's witnesses. The improper questioning was prejudicial and denied Foster a fair trial on the terrorizing charge.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Kolstad

Court: North Dakota Supreme Court
Citation: 2020 ND 97
Opinion Date: May 7, 2020
Judge: Gerald W. VandeWalle
Areas of Law: Constitutional Law, Criminal Law

In December 2018, Officer Nelson of the University of North Dakota Police Department conducted a traffic stop of Stanley Kolstad for suspicion of driving under the influence. Kolstad performed field sobriety tests and a preliminary breath test (PBT). Prior to performing the PBT, Kolstad informed

Nelson that he had asthma. Nelson testified he was unable to obtain a PBT result because Kolstad was filling his cheeks with air while performing the test. Kolstad was arrested for DUI and refusing to submit to a chemical test. Kolstad was transported to the UND police station to be given an Intoxilyzer breath test. Prior to the Intoxilyzer test, Nelson read Kolstad the implied consent advisory. But, because Nelson was not a certified operator of the Intoxilyzer machine, Officer Waltz conducted the test. Prior to the test, Kolstad informed Waltz he had asthma. The Intoxilyzer test results were deficient. Waltz testified Kolstad was not providing enough air for the test machine to provide a valid result. Kolstad was charged with driving under the influence and refusing to submit to a chemical test. Kolstad's counsel made a discovery request to the State seeking copies of any audio or video recordings taken by police officers. Kolstad's counsel also requested the State inform him whether any sound or video recordings taken of Kolstad were subsequently "altered, edited, destroyed, or discarded." The State provided Kolstad's counsel with dash camera footage from Nelson's police car that had been taken at the scene of the arrest, but the State did not provide any body camera footage from either Nelson or Waltz. Upon learning that Waltz's body camera footage was successfully uploaded to UND servers, Kolstad's counsel moved to dismiss the case because the State did not provide any body camera footage in discovery as requested. The district court ultimately dismissed the refusal to submit to a chemical breath test charge as a sanction for failing to provide the body camera footage. The State appealed, arguing the alleged discovery violation did not rise to a constitutional violation of Kolstad's due process rights, and the district court abused its discretion in dismissing the refusal charge. Kolstad argued the district court's order dismissing the refusal charge was not appealable, and if it was, the court did not abuse its discretion in dismissing the charge. The North Dakota Supreme Court concluded there was nothing in the record to indicate the district court adequately considered an alternative or less severe sanction to dismissal, and by not considering a less severe sanction, the trial court erred. The district court's order dismissing the refusal charge was reversed, and the matter remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Michel

Court: North Dakota Supreme Court
Citation: 2020 ND 101
Opinion Date: May 7, 2020
Judge: Jerod E. Tufte
Areas of Law: Constitutional Law, Criminal Law

Kevin Michel was convicted by jury of knowingly receiving stolen property. Jamestown Police began investigating theft of tires from Northwest Tire in October 2017. About ten months later, Thomas Melland and Andrew Heckelsmiller became suspects in the investigation. Heckelsmiller told police he had sold stolen tires to Michel. In August 2018, Detective LeRoy Gross spoke with Michel about the stolen tires. Michel acknowledged he had bought tires from Heckelsmiller and Melland. Michel also told Detective Gross he stopped buying tires from Heckelsmiller and Melland after seeing a Facebook post from Northwest Tire offering a $500 reward for information regarding stolen tires. Detective Gross told Michel, "There's going to be a lot of restitution these two boys are going to have to come up with unless we can get some tires back." Michel said he had sold several of the tires but still had some of them. Michel turned over seven new tires to Detective Gross. Representatives from Northwest Tire and J&L Service identified the tires as some of those stolen from their shops. During the jury's deliberations, the jury submitted a note with written questions to the court. Michel argued on appeal the district court erred by not specifically answering the jury's questions and instead referring them to the existing jury instructions. After review, the North Dakota Supreme Court affirmed the criminal judgment, except as to the award of restitution. The award was reversed because the district court awarded more than what was required to make the victims whole. The matter was remanded for a redetermination of restitution.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Wayland

Court: North Dakota Supreme Court
Citation: 2020 ND 106
Opinion Date: May 7, 2020
Judge: Jon J. Jensen
Areas of Law: Constitutional Law, Criminal Law

Joey Wayland appealed after he was convicted by jury of Theft of Property and Possession of Drug Paraphernalia. Wayland contended his case should have been dismissed because his right to a speedy trial was violated by a continuance of his trial from March 11, 2019 to April 8, 2019. Wayland also contended the district court violated his right to remain silent by ordering him to submit to a mental health evaluation. Finding no reversible error, the North Dakota Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Schwindt v. Sorel

Court: North Dakota Supreme Court
Citation: 2020 ND 92
Opinion Date: May 7, 2020
Judge: Lisa K. Fair McEvers
Areas of Law: Constitutional Law, Criminal Law, Government & Administrative Law

Gregory Schwindt appealed a district court judgment affirming a Department of Transportation hearing officer's revocation of his driving privileges for 180 days. Schwindt argued North Dakota's implied consent and refusal laws were unconstitutional, the hearing officer erred by considering the results of the horizontal gaze nystagmus (HGN) test, and the hearing officer erred in finding he refused to take a chemical test. After review, the North Dakota Supreme Court concluded the hearing officer's findings of fact were supported by a preponderance of the evidence, the conclusions of law were sustained by the findings of fact, and the decision to revoke Schwindt's driving privileges was in accordance with the law.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. McDougald v. Greene

Court: Supreme Court of Ohio
Citation: 2020-Ohio-2782
Opinion Date: May 6, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court denied a writ of mandamus sought by Relator to

compel Respondent, the public-records custodian at the Southern Ohio Correctional Facility (SOCF), to provide Relator with three public records and to pay Relator statutory damages and court costs associated with this litigation, holding that Relator was not entitled to either a writ of mandamus nor statutory damages. When Relator was an inmate at SOCF he submitted a public-records request to Respondent seeking three documents. Respondent provided one of the three documents. Relator then filed a complaint for a writ of mandamus seeking an order compelling Respondent to provide the two documents and to pay statutory damages and court costs associated with this litigation. The Supreme Court denied the writ of mandamus on the merits, holding that Respondent's response to Relator fully satisfied Respondent's obligations under Ohio Rev. Code 149.43, and therefore, Relator was not entitled a writ of mandamus, and there was no basis to award statutory damages.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Parker Bey v. Byrd

Court: Supreme Court of Ohio
Citation: 2020-Ohio-2766
Opinion Date: May 5, 2020
Judge: Maureen O'Connor
Areas of Law: Criminal Law

The Supreme Court affirmed in part and reversed in part the judgment of the court of appeals denying Appellant's complaint for a writ of mandamus to compel the Cuyahoga County Clerk of Courts to produce various court records and denying the clerk's request that Appellant be declared a vexatious litigator, holding that the court of appeals erred in denying Appellant's complaint on the grounds that he did not invoke the Rules of Superintendence as the basis for his request. Appellant sought copies of journal entries from his criminal case and a copy of the clerk of courts' records-retention schedule. The clerk largely denied the request. Appellant then filed a complaint for a writ of mandamus. The court of appeals denied Appellant's request for mandamus relief, concluding that the clerk had no clear legal duty to provide the requested records. The Supreme Court reversed, holding (1) this action to compel the production of journal entries from a 1995 case was properly brought under the Public Records Act; and

(2) this Court declines to impose sanctions on Appellant or to declare him a vexatious litigator.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Dangler

Court: Supreme Court of Ohio
Citation: 2020-Ohio-2765
Opinion Date: May 5, 2020
Judge: DeWine
Areas of Law: Criminal Law

The Supreme Court reversed the judgment of the court of appeals vacating Defendant's conviction and sentence and reinstated the trial court's acceptance of Defendant's plea of no contest to sexual battery, holding that the trial court did not completely fail to comply with Crim.R.11(C)(2)(a), and there was nothing in the record to support a conclusion that Defendant would not have entered his plea had the trial court been more detailed in its explanation. On appeal, Defendant sought to vacate his plea of no contest, arguing that his plea was invalid because the trial court erred by not explaining more fully the obligations and restrictions that went with his status as a sex offender, in violation of Crim. R. 11(C)(2)(a). The court of appeals vacated the conviction without requiring Defendant to show prejudice, concluding that the trial court had completely failed to comply with Crim. R. 11(C)(2)(a). The Supreme Court reversed, holding (1) the trial court did not completely failed to comply with Crim R. 11(C)(2)(a)'s maximum-penalty-advisement requirement; and (2) because Defendant did not establish prejudice, he was not entitled to have his no-contest plea vacated for a failure to comply with Crim.R. 11(C).

Read Opinion Are you a lawyer? **Annotate this case**.

Oregon v. Haji

Court: Oregon Supreme Court
Docket: S066254
Opinion Date: May 7, 2020
Judge: Nakamoto

Areas of Law: Constitutional Law, Criminal Law

After a grand jury issued an indictment charging defendant Hanad Ali Haji with multiple offenses, the district attorney determined that the indictment could be challenged by demurrer because the basis for joining those offenses was not expressly alleged. Instead of seeking another indictment from the grand jury, the district attorney obtained leave from the trial court to amend the indictment by adding allegations specifying the statutory basis for joinder, without adding factual allegations about the crimes. Defendant was convicted on some of the charges at trial, and the Court of Appeals affirmed. The issue this case presented for the Oregon Supreme Court's review centered on whether the district attorney could add allegations specifying the statutory basis for joinder of multiple offenses to an indictment instead of resubmitting the case to the grand jury. The Supreme Court determined that neither the statute permitting joinder of multiple offenses in a single indictment nor Article VII (Amended), section 5(6), of the Oregon Constitution precluded a district attorney, with approval of the trial court, from amending an indictment to add allegations specifying the statutory basis for joinder of multiple offenses. The Supreme Court affirmed the decision of the Court of Appeals, based in part on different reasoning, and affirmed the judgment of the circuit court.

Read Opinion Are you a lawyer? **Annotate this case**.

South Carolina v. Durant

Court: South Carolina Supreme Court
Docket: 27964
Opinion Date: May 6, 2020
Judge: Kaye Gorenflo Hearn
Areas of Law: Constitutional Law, Criminal Law

Appellant Larry Durant was convicted of second-degree criminal sexual conduct (CSC) for sexually abusing a teenage girl in his church office where he served as the pastor. Durant contended the trial court improperly permitted the State to introduce evidence of prior sexual abuse allegations as evidence of a common scheme or plan under Rule 404(b), SCRE, and that the State committed a "Brady" violation by failing to accurately disclose the criminal history of its witness. After review, the South Carolina Supreme

Court affirmed the admissibility of the girls' testimony. "[W]hile the State failed to disclose the criminal background information of its witness, we find this information was not material." The Court found Durant exercised his position of trust, authority, and spiritual leadership to hold private prayer meetings with teen girls who had grown up in his church. He told them he was praying for their health and good fortune, and represented that part of this process was touching them sexually and having intercourse. Durant then warned the girls of misfortune if they refused or told anyone. Moreover, he used scripture as a means of grooming the children into performing sex acts. "These facts demonstrate the requisite logical connection between the prior acts of sexual abuse and the one forming the basis of the crime charged." The Court therefore affirmed Durant's conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

South Carolina v. Perry

Court: South Carolina Supreme Court
Docket: 27963
Opinion Date: May 6, 2020
Judge: Few
Areas of Law: Constitutional Law, Criminal Law

Petitioner Wallace Perry was convicted on two counts of criminal sexual conduct (CSC) with a minor in the first degree and two counts of CSC with a minor in the second degree for sexually assaulting two of his biological daughters. Prior to Perry's trial, the State made a motion to admit the testimony of Perry's stepdaughter from an earlier marriage that Perry sexually assaulted her twenty-two to twenty-seven years earlier. The State argued the trial court should not exclude the stepdaughter's testimony under Rule 404(b) of the South Carolina Rules of Evidence because it fit the "common scheme or plan" exception. Perry objected to this testimony. The trial court initially reserved ruling on the issue, but later indicated it was inclined to allow the stepdaughter to testify. The jury convicted Perry on all counts, and the trial court sentenced him to thirty years in prison. The court of appeals affirmed. The South Carolina Supreme Court determined it was not enough to meet the "logical connection" standard for admission of other crimes under the common scheme or plan exception to Rule 404(b) that the defendant previously committed the same crime. "When evidence of other

crimes is admitted based solely on the similarity of a previous crime, the evidence serves only the purpose prohibited by Rule 404(b), and allows the jury to convict the defendant on the improper inference of propensity that because he did it before, he must have done it again. ...The common scheme or plan exception demands more." The Supreme Court held State must show a logical connection between the other crime and the crime charged such that the evidence of other crimes "reasonably tends to prove a material fact in issue." The State must also convince the trial court that the probative force of the evidence when used for this legitimate purpose is not substantially outweighed by the danger of unfair prejudice from the inherent tendency of the evidence to show the defendant's propensity to commit similar crimes. In this case, the State did not meet its burden. Conviction was reversed and the matter remanded for a new trial.

Read Opinion Are you a lawyer? **Annotate this case**.

South Carolina v. Quinn

Court: South Carolina Supreme Court
Docket: 27966
Opinion Date: May 6, 2020
Judge: Kaye Gorenflo Hearn
Areas of Law: Constitutional Law, Criminal Law, White Collar Crime

Respondent Rick Quinn, Jr. was a former member of the South Carolina House of Representatives, representing constituents in Richland and Lexington counties from 1989-2004 and 2010-2017 and serving as House Majority Leader from 1999- 2004. He owned and operated a mail business called Mail Marketing Strategies (MMS) in Columbia, while his father owned and operated a political consulting firm, Richard Quinn & Associates (RQ&A). In 2014, Attorney General Alan Wilson designated First Circuit Solicitor David Pascoe as special prosecutor to conduct a State grand jury investigation into alleged public corruption committed by current and former members of the South Carolina General Assembly. This case arose from a prior state grand jury investigation of former House Speaker Bobby Harrell, which resulted in six counts of misusing campaign funds, to which he pleaded guilty. During the course of the investigation into Speaker Harrell, SLED uncovered potentially criminal conduct by Representative Jimmy Merrill and Representative Rick Quinn, and a second grand jury

investigation was initiated to investigate the conduct of these individuals. The investigation focused on Quinn's practice of using his office as House Majority Leader and leader of the House Republican Caucus to direct mailing and political services to his family's businesses. Quinn only admitted to a limited set of facts supporting the indictment. Believing the plea lacked a sufficient basis, the State moved to vacate Quinn's guilty plea, reconsider the sentence, and for the trial court's recusal. The State appealed the order denying its motions. After review, the South Carolina Supreme Court determined that the State could not appeal the guilty plea, the trial court did not abuse its discretion in sentencing, and there was no evidence of judicial bias or prejudice requiring the court to recuse itself. Therefore, the Court dismissed the State's appeal of the guilty plea, and affirmed as to all other issues.

Read Opinion Are you a lawyer? **Annotate this case**.

Texas v. Arellano

Court: Texas Court of Criminal Appeals
Docket: PD-0287-19
Opinion Date: May 6, 2020
Judge: Slaughter
Areas of Law: Constitutional Law, Criminal Law

After Appellee Cesar Ramiro Arellano was arrested for driving while intoxicated, the arresting officer, Phillip Garcia, prepared a probable cause affidavit to support a search warrant for a blood draw. Officer Garcia submitted his sworn affidavit to the on-duty magistrate. Using a cursive signature, the magistrate signed the blank signature line of a form search warrant authorizing the search and seizure of Appellee's blood. Below the signature line appeared the words, "Magistrate, Victoria County, Texas." Aside from the cursive signature, the magistrate's name was not typed or handwritten anywhere on the warrant. Upon execution of the search warrant, Appellee was charged with DWI. In the trial court, Appellee filed a motion to suppress all evidence stemming from the blood draw. At the pretrial suppression hearing, Appellee argued that the search warrant to obtain the blood specimen was facially invalid because the magistrate's signature was illegible in violation of the requirements of Code of Criminal Procedure Article 18.04(5). The trial court agreed, the court of appeals

concurred, and the evidence was suppressed because of the illegible signature. The Texas Court of Criminal Appeals disagreed with both lower courts, finding the court of appeals erred in holding that reliance on the statutory good-faith exception was automatically precluded based on an illegible magistrate's signature in violation of Code of Criminal Procedure Article 18.04(5). Because the remaining issues in the case were not properly addressed by the court of appeals, judgment was vacated and the matter remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

About Justia Opinion Summaries

Justia Weekly Opinion Summaries is a free service, with 63 different newsletters, each covering a different practice area.

Justia also provides 68 daily jurisdictional newsletters, covering every federal appellate court and the highest courts of all US states.

All daily and weekly Justia newsletters are free. Subscribe or modify your newsletter subscription preferences at daily.justia.com.

You may freely redistribute this email in whole.

About Justia

Justia is an online platform that provides the community with open access to the law, legal information, and lawyers.

Contact Us | Privacy Policy

Unsubscribe From This Newsletter
or unsubscribe from all Justia newsletters immediately **here.**

Justia | 1380 Pear Ave #2B, Mountain View, CA 94043

From: Criminal Law - Justia Weekly Opinion Summaries
To: Grassia, Michael (POL)
Subject: Latest 111 Cases This Week: Kelly v. United States (U.S.), Gomes v. Silva (1st Cir.), United States v. Perez-Couvertier (1st Cir.)
Date: Friday, May 8, 2020 9:07:33 AM

If you are unable to see this message, click here to view it in a web browser.

Justia Weekly Opinion Summaries

Criminal Law
May 8, 2020

Table of Contents

Kelly v. United States
Criminal Law, Government & Administrative Law, White Collar Crime
US Supreme Court

Gomes v. Silva
Civil Rights, Constitutional Law, Criminal Law

US Court of Appeals for the First Circuit

United States v. Perez-Couvertier
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the First Circuit

United States v. Haverkamp
Criminal Law
US Court of Appeals for the Second Circuit

United States v. Mladen
Criminal Law, Trusts & Estates
US Court of Appeals for the Second Circuit

United States v. Richardson
Criminal Law
US Court of Appeals for the Second Circuit

United States v. Rosemond
Criminal Law
US Court of Appeals for the Second Circuit

United States v. Lacerda
Criminal Law, White Collar Crime
US Court of Appeals for the Third Circuit

Cucalon v. Barr
Criminal Law, Immigration Law
US Court of Appeals for the Fourth Circuit

United States v. Doctor
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Lewis
Criminal Law
US Court of Appeals for the Fourth Circuit

United States v. Jordan
Criminal Law
US Court of Appeals for the Fifth Circuit

United States v. Longoria
Criminal Law
US Court of Appeals for the Fifth Circuit

United States v. McNabb
Criminal Law
US Court of Appeals for the Fifth Circuit

Andrews v. Wayne County
Civil Rights, Constitutional Law, Criminal Law

US Court of Appeals for the Sixth Circuit

Hicks v. Scott
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Sixth Circuit

Moody v. United States
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Sixth Circuit

United States v. Foreman
Criminal Law
US Court of Appeals for the Sixth Circuit

United States v. Smith
Criminal Law
US Court of Appeals for the Sixth Circuit

Kirkman v. Thompson
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

Tuduj v. Newbold
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

United States v. Gibson
Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

United States v. Howell
Constitutional Law, Criminal Law
US Court of Appeals for the Seventh Circuit

United States v. Lewis
Criminal Law
US Court of Appeals for the Seventh Circuit

Bakor v. Barr
Criminal Law, Immigration Law
US Court of Appeals for the Eighth Circuit

Smith v. Titus
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Becerra
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Haynes
Criminal Law

US Court of Appeals for the Eighth Circuit

United States v. Roberts
Criminal Law
US Court of Appeals for the Eighth Circuit

United States v. Wright
Criminal Law
US Court of Appeals for the Eighth Circuit

Benson v. Chappell
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Ninth Circuit

Mero v. Barr
Criminal Law, Immigration Law
US Court of Appeals for the Ninth Circuit

Romero-Millan v. Barr
Criminal Law
US Court of Appeals for the Ninth Circuit

United States v. Yang
Criminal Law
US Court of Appeals for the Ninth Circuit

United States v. Neugin
Constitutional Law, Criminal Law
US Court of Appeals for the Tenth Circuit

United States v. Ramon
Constitutional Law, Criminal Law
US Court of Appeals for the Tenth Circuit

United States v. Richards
Constitutional Law, Criminal Law
US Court of Appeals for the Tenth Circuit

Andrews v. Warden
Criminal Law
US Court of Appeals for the Eleventh Circuit

Hollis v. United States
Criminal Law
US Court of Appeals for the Eleventh Circuit

Knight v. Florida Department of Corrections
Civil Rights, Constitutional Law, Criminal Law
US Court of Appeals for the Eleventh Circuit

United States v. Evans
Criminal Law

US Court of Appeals for the Eleventh Circuit

United States v. McLellan
Criminal Law
US Court of Appeals for the Eleventh Circuit

United States v. Russell
Criminal Law
US Court of Appeals for the Eleventh Circuit

Welch v. United States
Criminal Law
US Court of Appeals for the Eleventh Circuit

State v. Trujillo
Constitutional Law, Criminal Law
Arizona Supreme Court

Barnett v. State
Criminal Law
Arkansas Supreme Court

Mason v. Kelley
Criminal Law
Arkansas Supreme Court

Ray v. Kelley
Criminal Law
Arkansas Supreme Court

Walker v. Kelley
Criminal Law
Arkansas Supreme Court

People v. Flores
Civil Rights, Constitutional Law, Criminal Law
Supreme Court of California

California v. Law
Constitutional Law, Criminal Law
California Courts of Appeal

California v. Sanchez
Constitutional Law, Criminal Law
California Courts of Appeal

Galeotti v. International Union of Operating Engineers
Criminal Law, Labor & Employment Law, White Collar Crime
California Courts of Appeal

In re I.A.
Criminal Law, Juvenile Law

California Courts of Appeal

People v. Edwards
Criminal Law
California Courts of Appeal

People v. Thomkins
Criminal Law
California Courts of Appeal

People v. Torres
Criminal Law
California Courts of Appeal

People v. Triplett
Criminal Law
California Courts of Appeal

Colorado In Interest of G.S.S.
Constitutional Law, Criminal Law, Juvenile Law
Colorado Supreme Court

Barringer v. Halkitis
Criminal Law
Florida Supreme Court

Franqui v. State
Criminal Law
Florida Supreme Court

Hicks v. State
Criminal Law
Florida Supreme Court

Burley v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Carter v. Georgia
Construction Law, Criminal Law
Supreme Court of Georgia

Clarke v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Collins v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Dawson v. Georgia
Constitutional Law, Criminal Law

Supreme Court of Georgia

Evans v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Hill v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Oliver v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Rosser v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Spencer v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Styles v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Whitehead v. Georgia
Constitutional Law, Criminal Law
Supreme Court of Georgia

Idaho v. Blythe
Constitutional Law, Criminal Law
Idaho Supreme Court - Criminal

Idaho v. Glodowski
Constitutional Law, Criminal Law
Idaho Supreme Court - Criminal

Idaho v. Jones
Constitutional Law, Criminal Law
Idaho Supreme Court - Criminal

State v. Gordon
Civil Rights, Constitutional Law, Criminal Law
Iowa Supreme Court

State v. Craig
Criminal Law
Kansas Supreme Court

State v. Lemmie
Criminal Law

Kansas Supreme Court

State v. Mullen
Criminal Law
Maine Supreme Judicial Court

Commonwealth v. Billingslea
Civil Rights, Constitutional Law, Criminal Law
Massachusetts Supreme Judicial Court

Commonwealth v. Martin
Civil Rights, Constitutional Law, Criminal Law
Massachusetts Supreme Judicial Court

Commonwealth v. Tavares
Criminal Law
Massachusetts Supreme Judicial Court

State v. Branch
Criminal Law
Minnesota Supreme Court

Galloway v. Mississippi
Constitutional Law, Criminal Law
Supreme Court of Mississippi

City of Missoula v. Zerbst
Civil Rights, Constitutional Law, Criminal Law
Montana Supreme Court

State v. Degarmo
Civil Rights, Constitutional Law, Criminal Law
Nebraska Supreme Court

People v. Holz
Civil Rights, Constitutional Law, Criminal Law
New York Court of Appeals

People v. Maffei
Civil Rights, Constitutional Law, Criminal Law
New York Court of Appeals

State v. Bailey
Civil Rights, Constitutional Law, Criminal Law
North Carolina Supreme Court

State v. Ellis
Civil Rights, Constitutional Law, Criminal Law
North Carolina Supreme Court

State v. Hobbs
Civil Rights, Constitutional Law, Criminal Law

North Carolina Supreme Court

State v. Mylett
Criminal Law
North Carolina Supreme Court

Dodge v. North Dakota
Constitutional Law, Criminal Law
North Dakota Supreme Court

Hewitt v. NDDOT
Criminal Law, Government & Administrative Law
North Dakota Supreme Court

Kastet v. NDDOT
Criminal Law, Government & Administrative Law
North Dakota Supreme Court

North Dakota v. Dahl
Constitutional Law, Criminal Law
North Dakota Supreme Court

North Dakota v. Foster
Constitutional Law, Criminal Law
North Dakota Supreme Court

North Dakota v. Kolstad
Constitutional Law, Criminal Law
North Dakota Supreme Court

North Dakota v. Michel
Constitutional Law, Criminal Law
North Dakota Supreme Court

North Dakota v. Wayland
Constitutional Law, Criminal Law
North Dakota Supreme Court

Schwindt v. Sorel
Constitutional Law, Criminal Law, Government & Administrative Law
North Dakota Supreme Court

State ex rel. McDougald v. Greene
Criminal Law
Supreme Court of Ohio

State ex rel. Parker Bey v. Byrd
Criminal Law
Supreme Court of Ohio

State v. Dangler
Criminal Law

Supreme Court of Ohio

Oregon v. Haji
Constitutional Law, Criminal Law
Oregon Supreme Court

South Carolina v. Durant
Constitutional Law, Criminal Law
South Carolina Supreme Court

South Carolina v. Perry
Constitutional Law, Criminal Law
South Carolina Supreme Court

South Carolina v. Quinn
Constitutional Law, Criminal Law, White Collar Crime
South Carolina Supreme Court

Texas v. Arellano
Constitutional Law, Criminal Law
Texas Court of Criminal Appeals

COVID-19 Updates: Law & Legal Resources Related to Coronavirus

Click here to remove Verdict from subsequent Justia newsletter(s).

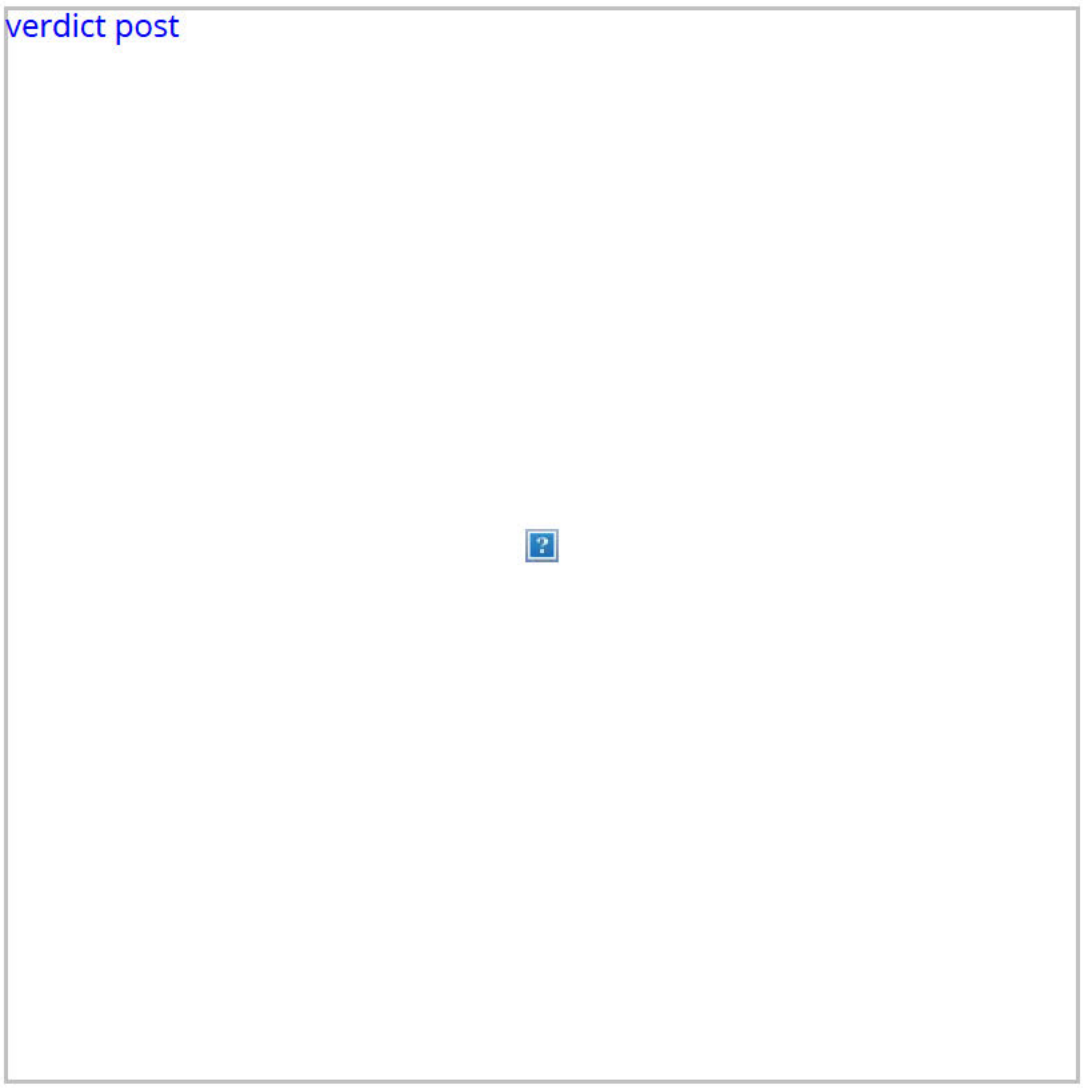
New on Verdict

Legal Analysis and Commentary

Department of Justice Once Again Proves Its Loyalty to the President, Not the Rule of Law

AUSTIN SARAT

verdict post



Austin Sarat—Associate Provost, Associate Dean of the Faculty, and William Nelson Cromwell Professor of Jurisprudence and Political Science at Amherst College—comments on the recent news that the Justice Department will seek dismissal of charges against Michael Flynn. Sarat suggests that because the decision does not seem to advance the fair administration of justice in this case, the court should take the unusual step of refusing to grant the prosecutor's motion to dismiss.

Read More

Criminal Law Opinions

Kelly v. United States

Court: US Supreme Court
Docket: 18-1059
Opinion Date: May 7, 2020
Judge: Elena Kagan
Areas of Law: Criminal Law, Government & Administrative Law, White Collar Crime

During former New Jersey Governor Christie's 2013 reelection campaign, Fort Lee's mayor refused to endorse Christie. Kelly, Christie's Deputy Chief of Staff, Port Authority Deputy Executive Director, Baroni, and another official decided to reduce from three to one the number of lanes reserved at the George Washington Bridge's toll plaza for Fort Lee's commuters. To disguise the political retribution, the lane realignment was said to be for a traffic study. Port Authority traffic engineers were asked to collect some numbers. An extra toll collector was paid overtime. The lane realignment caused four days of gridlock, ending only when the Port Authority's Executive Director learned of the scheme. The Third Circuit affirmed the convictions of Baroni and Kelly for wire fraud, fraud on a federally funded program, and conspiracy to commit those crimes. The Supreme Court reversed. The scheme did not aim to obtain money or property. The wire fraud statute refers to "any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses," 18 U.S.C. 1343. The federal-program fraud statute bars "obtain[ing] by fraud" the "property" (including money) of a federally funded program or entity, section 666(a)(1)(A). The statutes are limited to the protection of property rights and do not authorize federal prosecutors to set standards of good government. The Court rejected arguments that the defendants sought to take control of the Bridge's physical lanes or to deprive the Port Authority of the costs of compensating employees. Their realignment of the access lanes was an exercise of regulatory power; a scheme to alter a regulatory choice is not one to take government property. The time and labor of the employees were an incidental byproduct of that regulatory object. Neither defendant sought to obtain the services that the employees provided.

Read Opinion Are you a lawyer? **Annotate this case**.

Gomes v. Silva

Court: US Court of Appeals for the First Circuit
Docket: 19-1656

Opinion Date: May 1, 2020
Judge: Stahl
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The First Circuit affirmed the judgment of the district court denying Appellant's petition for a writ of habeas corpus, holding that, under the highly deferential standard prescribed by the Antiterrorism and Effective Death Penalty Act for federal habeas review of state criminal convictions, Appellant's claims to habeas relief failed. Appellant was convicted in a Massachusetts superior court of murder in the first degree and related crimes. The Supreme Judicial Court (SJC) affirmed the convictions. Appellant subsequently petitioned the District Court for the District of Massachusetts for a writ of habeas corpus. The district court denied the petition but granted a certificate of appealability. The First Circuit affirmed, holding (1) sufficient evidence supported Appellant's conviction for first-degree murder as a joint venturer, and the SJC's sufficiency determination was not unreasonable; and (2) the SJC reasonably determined that the trial court's admission into evidence of certain items did not constitute error.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Perez-Couvertier

Court: US Court of Appeals for the First Circuit
Docket: 16-2186
Opinion Date: May 7, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The First Circuit affirmed Defendant's conviction of possessing with intent to distribute controlled substances in a protected area and conspiring to distribute controlled substances in a protected area, holding that the district court did not plainly err with respect to any of Defendant's challenges. Specifically, the First Circuit held (1) the district court did not commit plain error in admitting evidence of the conspiracy's activities occurring after he withdrew from the conspiracy or, alternatively, in not instructing the jury to ignore such evidence; (2) the district court did not plainly err in admitting evidence of a drug trafficking organization's violent acts; and (3) the delay between Defendant's indictment and arrest did not violate his Sixth Amendment right to a speedy trial.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Haverkamp

Court: US Court of Appeals for the Second Circuit
Docket: 18-3735
Opinion Date: May 4, 2020
Judge: Barrington D. Parker
Areas of Law: Criminal Law

Defendant pleaded guilty to one count of distribution and receipt of child pornography and one count of possession of child pornography. The district court sentenced him to 121 months of imprisonment, followed by five years of supervised release, and imposed a $200 mandatory special assessment under 18 U.S.C. 3013, as well as a $10,000 assessment under 18 U.S.C. 3014. The Second Circuit held that the district court did not abuse its discretion in sentencing defendant and his sentence was substantively reasonable. The court held that the text of the Justice for Victims of Trafficking Act (JVTA), 18 U.S.C. 3014, taken as a whole and in its context, is straightforwardly meant to be applied on a per-offender, not a per-count, basis. In this case, the district court erroneously applied the special assessment on a per-count, rather than per-offender, basis. Finally, the court held that the computer monitoring condition in question was reasonably related to the nature of defendant's offense. Accordingly, the court affirmed in part, vacated in part, and remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Mladen

Court: US Court of Appeals for the Second Circuit
Docket: 18-0616
Opinion Date: May 6, 2020
Judge: Amalya Lyle Kearse
Areas of Law: Criminal Law, Trusts & Estates

After defendant died while his appeal was pending, counsel moved for

abatement of all incidents of the prosecution, requesting that the appeal be dismissed without a decision on the merits, that defendant's conviction be vacated, and that the matter be remanded to the district court with instructions to dismiss the indictment and order repayment to defendant's estate of the $20,000 fine and $100 special assessment. Because defendant was convicted upon his plea of guilty, and he neither did nor was permitted to challenge on appeal the merits of his conviction, the Second Circuit denied as without merit so much of the motion as seeks (1) vacatur of his conviction, (2) dismissal of the count of the indictment on which he was convicted, and (3) repayment of the mandatory $100 special assessment. The court granted so much of the motion as requests dismissal of this appeal and a remand to the district court for vacatur of the imposed terms of imprisonment and supervised release and for an order requiring that the paid fine of $20,000 be repaid to defendant's estate.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Richardson

Court: US Court of Appeals for the Second Circuit
Docket: 19-412
Opinion Date: May 5, 2020
Judge: Menashi
Areas of Law: Criminal Law

The Second Circuit affirmed defendant's conviction for distribution and possession with intent to distribute a controlled substance. The court held that the district court did not procedurally err by applying the career offender sentencing enhancement pursuant to USSG 4B1.1 because defendant's prior convictions of conspiracy to distribute a controlled substance in violation of 21 U.S.C. 841(a)(1) and 846, and attempted criminal possession of a controlled substance in violation of N.Y. Penal Law 220.16(1), qualify as controlled substance offenses, as defined in USSG 4B1.2(b). The court also held that the district court did not substantively err in sentencing defendant, because it properly considered his criminal history and accounted for his need for mental health and substance abuse treatment.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Rosemond

Court: US Court of Appeals for the Second Circuit
Docket: 18-3561
Opinion Date: May 1, 2020
Judge: Chin
Areas of Law: Criminal Law

The Second Circuit affirmed defendant's conviction for murder-for-hire, conspiracy to commit murder-for-hire, murder through use of a firearm, and possession of a firearm during a murder-for-hire conspiracy. Defendant owned Czar Entertainment, a music management company that represented hip-hop, rap and R&B artists such as Jayceon Taylor, also known as "The Game." Taylor was a member of G-Unit, a rap group run by Curtis Jackson, also known as "50 Cent." Defendant's crimes stemmed from a rivalry with Violator Records, the company that managed G-Unit. The court rejected defendant's contention that his attorney was ineffective because he conceded that defendant paid for the victim to be shot, even though he told counsel not to make this concession. The court held that defendant failed to show that this was objectively unreasonable or that he would have been found not guilty had a different argument been advanced. In this case, there was ample evidence supporting counsel's strategy to concede that defendant ordered a shooting where, among other things, the government's key witness, who participated in the conspiracy and lured the victim to be shot, testified that defendant agreed to pay the shooter. The court also held that the district court did not abuse its broad discretion by admitting prior bad-act evidence under Federal Rule of Evidence 404(b)(1).

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Lacerda

Court: US Court of Appeals for the Third Circuit
Docket: 15-2812
Opinion Date: May 5, 2020
Judge: Porter
Areas of Law: Criminal Law, White Collar Crime

VOG billed itself as an advocacy group helping victims of timeshare fraud get out of their timeshare debts. A jury determined that VOG had actually

defrauded its customers and that three individual defendants (including Lacerda) were each knowing participants in that fraud. Lacerda was sentenced to 324 months' imprisonment for his leading role in the fraudulent enterprise. The Third Circuit affirmed the respective convictions and sentences. The court rejected a claim of impermissible "overview testimony" by an FBI agent; an officer who is familiar with an investigation or was personally involved may tell the story of that investigation—how the investigation began, who was involved, and what techniques were used, and, with a proper foundation, may offer lay opinion testimony and testify about matters within his personal knowledge. The district court did not abuse its discretion when it disqualified defense counsel based on a conflict of interest; when it denied replacement counsel's motion for a continuance; when it excluded from evidence, as hearsay, an email sent by Lacerda to VOG's former CFO; in exercising its sentencing discretion; or by ordering the forfeiture of all VOG's gross proceeds.

Read Opinion Are you a lawyer? **Annotate this case**.

Cucalon v. Barr

Court: US Court of Appeals for the Fourth Circuit
Dockets: 18-1292, 18-2206
Opinion Date: May 7, 2020
Judge: Barbara Milano Keenan
Areas of Law: Criminal Law, Immigration Law

The Fourth Circuit denied petitions for review of the BIA's final order of removal. Applying the modified categorical approach, the court held that defendant's prior conviction for distribution of cocaine under Virginia Code 18.2-248, including distribution of that substance as an accommodation under Virginia Code 18.2-248(D), satisfies the federal definitions of an "aggravated felony" and of a crime "relating to a controlled substance" pursuant to 8 U.S.C. 1227(a)(2)(A)(iii), 1227(a)(2)(B)(i). The court also held that the district court did not abuse its discretion in denying petitioner's motion to reconsider.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Doctor

Court: US Court of Appeals for the Fourth Circuit
Docket: 18-4874
Opinion Date: May 4, 2020
Judge: Roger L. Gregory
Areas of Law: Criminal Law

The Fourth Circuit affirmed the district court's revocation of defendant's supervised release and resulting sentence. The court held that the district court did not clearly err in finding the government proved he committed the assault underlying the supervised release violation; the district court did not commit plain error by adopting the violation report when announcing defendant committed Violation One; and, even if the district court erred in sentencing defendant for a Grade A violation, the error was harmless.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Lewis

Court: US Court of Appeals for the Fourth Circuit
Docket: 19-4028
Opinion Date: May 4, 2020
Judge: Barbara Milano Keenan
Areas of Law: Criminal Law

Defendant was convicted for possessing a firearm as a felon and sentenced to 63 months' imprisonment and a three-year period of supervised release. The district court additionally recommended, without explanation, that defendant receive addiction treatment while incarcerated and ordered, as a special condition of his supervised release, that defendant participate in an addiction treatment program. The Fourth Circuit held that defendant's sentence is procedurally unreasonable because the district court failed to provide an adequate explanation for imposing as a special condition of supervised release the requirement of addiction treatment. The court also held that the district court failed to address defendant's nonfrivolous mitigation arguments. Therefore, the court remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Jordan

Court: US Court of Appeals for the Fifth Circuit
Docket: 19-40499
Opinion Date: May 1, 2020
Judge: Jennifer Walker Elrod
Areas of Law: Criminal Law

The Fifth Circuit affirmed the district court's grant of defendants' motion for a new trial on the basis of prejudicial outside influence on the jury. The court held that the district court did not abuse its broad discretion in granting the motion for a new trial without holding an evidentiary hearing. To the extent there is a bright-line rule applicable to allegations of outside influence on the jury, the court held that it was not applicable to this case. Furthermore, the district court did not abuse its discretion in exercising its prerogative, within broadly defined parameters, to handle the allegation of outside influence in the least disruptive manner possible in this unusual case. Finally, the district court permissibly concluded that the evidence showed a sufficient likelihood of prejudice to shift the burden to the Government, and that the Government did not (and could not) show "no reasonable possibility that the jury's verdict was influenced by" the CSO's comments.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Longoria

Court: US Court of Appeals for the Fifth Circuit
Docket: 19-20201
Opinion Date: May 5, 2020
Judge: Gregg Costa
Areas of Law: Criminal Law

The Fifth Circuit held that the base offense level of 20 was proper for defendant's felon-in-possession crime involving a semiautomatic firearm that is capable of accepting a large capacity magazine. In this case, defendant failed to show that the district court clearly erred in relying on the FBI's agent statement about what was found in the apartment. The court clarified any confusion and held that the 2013 amendment to the commentary on the acceptance-of-responsibility Guideline does not clearly overrule its caselaw allowing the government to withhold the third point for

acceptance of responsibility when it must litigate a suppression motion. The court held that Amendment 775 does not contain the unequivocal override needed to get past the court's precedent. Therefore, the court affirmed defendant's sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. McNabb

Court: US Court of Appeals for the Fifth Circuit
Docket: 19-50265
Opinion Date: May 1, 2020
Judge: Costa
Areas of Law: Criminal Law

The Fifth Circuit affirmed defendant's sentence imposed after he pleaded guilty to possessing a gun after having been convicted of a felony. The court held that defendant is not entitled to relief on his claim that the government breached the plea deal, and thus his appellate waiver remains enforceable. Accordingly, defendant's challenges to his sentence must be dismissed.

Read Opinion Are you a lawyer? **Annotate this case**.

Andrews v. Wayne County

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-1992
Opinion Date: May 4, 2020
Judge: Suhrheinrich
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Canton Police received a 911 call from Andrews, who stated that his fiance, White, had physically attacked him. Officers arrested White. Andrews later took White's medications to the jail; a “KOP” policy allows inmates to keep certain drugs for self-administration. During an intake interview, White admitted to attempting to harm herself or commit suicide in the past but said she was not thinking of harming herself or having suicidal thoughts. An R.N. later evaluated White for nearly two hours, reported White’s chief complaints were “anxiety and depression,” and contacted a pharmacy to verify White’s prescriptions. The R.N. claims White did not exhibit any psychotic behavior,

suicidal ideation, or psychiatric distress but ordered further evaluation. The next day, White was found on the floor with vomit on her face. She stated repeatedly that she took too many pills. The next day, White died in the hospital. The cause of death was Verapamil toxicity. The Sixth Circuit affirmed the rejection of a suit under 42 U.S.C. 1983 on summary judgment. A pretrial detainee does not have an automatic right to a suicide screening. The court rejected an argument that the KOP Policy was deficient because it allows inmates in need of a psychological evaluation to participate before a psychiatrist's assessment of proper housing. The County had no history of suicides relative to the program, so any purported failure to train its employees in suicide risk assessment did not cause White's death.

Read Opinion Are you a lawyer? **Annotate this case**.

Hicks v. Scott

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-3410
Opinion Date: May 1, 2020
Judge: Gibbons
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Cincinnati officers Scott and Moore responded to a reported incident of menacing. Two people alleged that Quandavier had driven by their home that night and threatened to kill them and that Quandavier carried guns. Officer Loreaux identified a vehicle fitting the description. Officers Scott, Moore, Schneider, and Loreaux, standing where the vehicle was parked, heard a voice. Thinking that it was likely Quandavier, they knocked on the exterior door of the residence. It swung open. Three officers entered without a warrant or exigent circumstances. Loreaux remained outside. Neither Scott nor Moore recall announcing their presence or identifying themselves. Inside and upstairs, Scott knocked on a closed door. As it opened, Scott "saw the barrel of a rifle pointed at [her] face." Moore and Schneider also saw Quandavier "nonchalantly" panning the rifle from left to right. Moore reached for its barrel as Scott fired her weapon. Moore did not instruct Quandavier to drop his rifle nor did Scott issue any commands before firing. Quandavier collapsed. The officers immediately radioed for paramedics. Before the officers applied handcuffs or provided first aid, they heard another voice and conducted a sweep. Quandavier died at the scene

without receiving medical attention. In a suit under 42 U.S.C. 1983 for unlawful entry, excessive force, and deliberate indifference to a serious medical need, plus state claims, the district court granted the defendants summary judgment, citing qualified immunity. The Sixth Circuit reversed in part. The district court erred by granting qualified immunity to Scott, Moore, and Schneider on the unlawful entry claim. The court affirmed as to the excessive force, deliberate indifference, and state-law battery claims, and remanded for evaluation of municipal liability and wrongful death claims.

Read Opinion Are you a lawyer? **Annotate this case**.

Moody v. United States

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-5015
Opinion Date: May 6, 2020
Judge: Thapar
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

At Moody's trial, the government produced a video of Moody cooking crack on his stove and waving a handgun while he mused about life in "the game" (drug trafficking). The court ruled that most of the video was admissible. Moody then tried to persuade the jury that the video was filmed more than five years before his indictment, putting it outside the statute of limitations. The jury convicted Moody. Due to prior felony drug convictions, Moody received enhanced, mandatory-minimum life sentences on several counts. He appealed on evidentiary grounds relating to the video. The Sixth Circuit affirmed. Later, Moody raised new claims on collateral review, 28 U.S.C. 2255. The district court found each claim meritless; most were also procedurally defaulted. The court authorized Moody to appeal. The Sixth Circuit dismissed the appeal, stating that none of the claims should have been certified. Reasonable jurists could not doubt that the district court properly denied relief on Moody's claims that he was deprived of his statute-of-limitations defense (violating due process); that the past convictions for his sentencing enhancements were not charged in the indictment or found by the jury; and that his previous lawyers failed to raise the first two claims sooner, violating his right to effective assistance of counsel.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Foreman

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-1827
Opinion Date: May 7, 2020
Judge: Gibbons
Areas of Law: Criminal Law

In 2006, Foreman pled guilty to possession with intent to distribute 50 or more grams of cocaine base, possession with intent to distribute cocaine powder, and possession of a firearm during and in furtherance of a drug trafficking crime. Foreman admitted that he was responsible for approximately 135 grams of crack cocaine and 250 grams of cocaine powder. Foreman had a final Guidelines range of 322-387 months; he was sentenced to 240 months' imprisonment with respect to each drug conviction, to run concurrently, and 60 months' imprisonment for the firearms conviction, to run consecutively. When the First Step Act of 2018 made the Fair Sentencing Act retroactive, Foreman sought relief. The district court held that Foreman was not entitled to a plenary resentencing and declined to revisit his career offender status or hold an in-person hearing, then weighed the new statutory range applicable to Foreman's drug offenses, his recalculated Guidelines range, and the 18 U.S.C. 3553(a) factors, and reduced Foreman's total sentence to 172 months on each drug offense, to run concurrently, plus the mandatory consecutive 60 months on the firearms offense. The Sixth Circuit affirmed. Nothing in the First Step Act entitles a defendant to a plenary resentencing. First Step Act resentencings are not shielded from review for reasonableness; the district court thoroughly explained its rationale, carefully examining Foreman's circumstances, the amended penalty provisions, and the resulting changes to Foreman's Guidelines range.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Smith

Court: US Court of Appeals for the Sixth Circuit
Docket: 19-1724
Opinion Date: May 6, 2020

Judge: Bush
Areas of Law: Criminal Law

In 2006, Smith was convicted of conspiracy to distribute and to possess with intent to distribute 500 grams or more of powder or 50 grams or more of cocaine base (crack cocaine); possession with intent to distribute 50 grams or more of cocaine base (crack cocaine); possession with intent to distribute 500 grams or more of cocaine powder; and being a felon in possession of a firearm. The court imposed a mandatory minimum life sentence. The Fair Sentencing Act subsequently lowered the penalty for cocaine-base offenses, made retroactive through the First Step Act. Smith moved for relief and received a reduced sentence of 360 months, the bottom of the new Guideline range for the counts impacted by the Fair Sentencing Act, to run concurrent to his existing 360-month sentence for his powder cocaine count that was not affected by the Fair Sentencing Act. The Sixth Circuit affirmed, rejecting an argument that the court should have imposed a below-Guideline sentence for all counts. The First Step Act is a limited grant of authority to impose a reduced sentence for certain offenses and does not require a plenary resentencing proceeding. Even assuming the court's obligation to explain its reasons for imposing the modified sentence was akin to that which applies in initial sentencing, the court's use of a modified AO 247 form order to explain its decision was not procedurally unreasonable.

Read Opinion Are you a lawyer? **Annotate this case**.

Kirkman v. Thompson

Court: US Court of Appeals for the Seventh Circuit
Docket: 19-1904
Opinion Date: May 7, 2020
Judge: William Joseph Bauer
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Following a 1992 fight that involved Johnson, Herron, and Walker, two shooters shot the three men. Johnson survived. In the hospital, Johnson described a shooter by the street name "Duke," where Duke lived, and Duke's car. Johnson identified Duke and his accomplice from a photo array. Police pulled over a vehicle matching Johnson's description and arrested

the driver, Kirkman, and the passenger, who matched the general description of the second shooter. Kirkman had a tattoo of Duke on his arm. Police took additional photos and presented a second photo array to Johnson, who identified them as the shooters. At trial, Johnson identified Kirkman and his passenger as the shooters. There was disputed testimony about the cause of the fight. Convicted of murder and aggravated battery with a firearm, Kirkman was sentenced to life in prison. Johnson had a change of heart and submitted an affidavit, identifying Ford and an unknown man as the shooters. At Kirkman's post-conviction hearing, Johnson testified that he and his family had been threatened. Other testimony was inconsistent with Johnson's. Illinois courts denied post-conviction relief, finding that Johnson's recantation lacked credibility. Johnson later pleaded guilty for perjury but failed to specify which statement was false. The Seventh Circuit affirmed the denial of federal habeas relief. Illinois courts found Johnson's recantation lacked credibility. An evidentiary hearing satisfied Kirkman's due process rights. The Illinois trial court's determination defeated Kirkman's innocence and perjured testimony claims.

Read Opinion Are you a lawyer? **Annotate this case**.

Tuduj v. Newbold

Court: US Court of Appeals for the Seventh Circuit
Docket: 19-1699
Opinion Date: May 1, 2020
Judge: Per Curiam
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

Illinois prisoner Tuduj, having received extensive dental treatment, filed a "deliberate indifference" suit under 42 U.S.C. 1983 against his dentists and prison officials. The court recruited counsel to assist Tuduj in filing an amended complaint that complied with the Federal Rules of Civil Procedure. Counsel defended against two summary judgment motions, one arguing that Tuduj had not exhausted his administrative remedies and another on the merits While the motions were pending, Tuduj moved "for leave to represent himself," stating that he was "concerned that his counsel has filed a structurally, technically and legally insufficient response doomed to be denied." He asked to file his own brief, except "in the event this Honorable Court deems counsel's response … legally sufficient and Grants same[,]

Plaintiff would be open to continued effective representation." A magistrate denied Tuduj's motion, stating that Tuduj "varie[d] between saying he would like to" represent himself and "indicating that he is happy with counsel's representation as long as he prevails." The district judge granted the motions for summary judgment, citing professional judgment and finding "no competent evidence" of any policy that unlawfully influenced dental-treatment decisions. The Seventh Circuit rejected Tuduj's argument that the court wrongly denied his "unqualified" right to proceed pro se under 28 U.S.C. 1654, the due process clause, the equal protection clause, and the Seventh Amendment. The district court permissibly denied his equivocal request.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Gibson

Court: US Court of Appeals for the Seventh Circuit
Docket: 19-1402
Opinion Date: May 7, 2020
Judge: William Joseph Bauer
Areas of Law: Constitutional Law, Criminal Law

Officer Garrison encountered Gibson, a suspected drug trafficker, walking with a companion. Although initially a consensual encounter, Garrison questioned Gibson and his companion and briefly detained Gibson. After Gibson and his companion departed, Garrison spotted a methamphetamine pipe under his patrol vehicle. Local law enforcement conducted a traffic stop of Gibson's vehicle in the curtilage of his driveway. A drug detection dog signaled the presence of a controlled substance in the vehicle, though nothing was found. Earlier that day, Gibson's wife had met with DEA agents to tell them about methamphetamine inside the home. Police used information Mrs. Gibson had provided to obtain a search warrant. The search of the home uncovered drugs, drug paraphernalia, currency, and AK-47 rifles, which led to Gibson's arrest. Gibson moved to suppress all evidence seized during the search, alleging he was detained without reasonable suspicion, unlawfully frisked, arrested without probable cause, stopped without probable cause or reasonable suspicion, and the traffic stop exceeded a permissible scope. Upon learning of his wife's cooperation, Gibson also argued her statement was insufficiently attenuated to justify the

search warrant. The Seventh Circuit affirmed the denial of the motion. Mrs. Gibson's voluntary statement with DEA agents was independently sufficient to sustain findings of probable cause and sufficiently attenuated from subsequent events to preclude suppression.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Howell

Court: US Court of Appeals for the Seventh Circuit
Docket: 18-3157
Opinion Date: May 4, 2020
Judge: Scudder
Areas of Law: Constitutional Law, Criminal Law

In December 2012, Chicago Police officers responded to an anonymous call reporting a Hispanic man in a black sweater and black hat, carrying a bag, and climbing under a warehouse fence. They found someone who matched the description. After stopping and frisking him, they determined he was not engaged in any crime. Howell, walking toward the police, was white and wearing a black jacket and dark hat. When an officer approached to speak to him, Howell did not answer, looked panicked, and put his hands in his pockets. The officer patted Howell down and found a gun in his jacket. A federal gun charge followed. Howell unsuccessfully moved to suppress the gun. The Seventh Circuit reversed the denial of his suppression motion and vacated his conviction for possessing that gun. The court noted that the facts in the pretrial record differed significantly from those presented at trial, where the arresting officer testified that he decided to proceed with the pat-down only after Howell ignored a directive to remove his hands from his pockets. Viewing the pretrial record as a whole, the police lacked reasonable suspicion to frisk Howell. The court did not reverse Howell's conviction on a second gun charge that resulted from the execution of a warrant to search Howell's apartment three months after the initial stop and the ensuing discovery of more guns and ammunition.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Lewis

Court: US Court of Appeals for the Seventh Circuit
Dockets: 19-1911, 19-1262
Opinion Date: May 7, 2020
Judge: Joel Martin Flaum
Areas of Law: Criminal Law

In 2016-2018, Draheim managed a conspiracy, responsible for at least 38 packages of methamphetamine sent from California to La Crosse, Wisconsin. Draheim supervised at least 11 associates who accepted shipments on her behalf, sent money transfers to California, distributed the meth, rented storage lockers, and collected money owed to her. Draheim provided vehicles. After agents placed a wiretap on her phone and seized several packages of meth en route to Draheim, her California supplier forced Draheim to find a new source. Draheim contacted Lewis, recently out of jail but still involved in the "meth scene." Lewis agreed to purchase meth from a new supplier. During the planned transaction, agents seized the package, which contained 28.6 grams of nearly pure meth. Police subsequently arrested Draheim after they found her daughter dead at home from an overdose; they took Lewis into custody for violating the terms of his state supervision. Both pleaded guilty to meth distribution offenses, 21 U.S.C. 841, 846. Draheim, facing a mandatory-minimum 10-year sentence, unsuccessfully argued that she qualified for "safety-valve relief." The court reasoned that she was the leader of her enterprise. Lewis unsuccessfully contended that he should be sentenced based only on his conviction, not other "relevant conduct." The Seventh Circuit affirmed Draheim's sentence but vacated as to Lewis. The fact that the defendant has engaged in other drug transactions is not, alone, sufficient to justify treating those transactions as relevant conduct for sentencing purposes.

Read Opinion Are you a lawyer? **Annotate this case**.

Bakor v. Barr

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-3011
Opinion Date: May 7, 2020
Judge: Steven M. Colloton
Areas of Law: Criminal Law, Immigration Law

The Eighth Circuit denied a petition for review of the BIA's determination

that defendant committed two crimes involving moral turpitude. The court held that the BIA did not err in determining that petitioner's conviction for the Minnesota crimes of Criminal Sexual Conduct in the Fifth Degree and knowing failure to comply with Minnesota's sex offender registration statute were crimes involving moral turpitude. The court also held that petitioner failed to exhaust his remaining arguments and therefore declined to consider them.

Read Opinion Are you a lawyer? **Annotate this case**.

Smith v. Titus

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-2915
Opinion Date: May 5, 2020
Judge: Steven M. Colloton
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Eighth Circuit affirmed the district court's denial of habeas relief to petitioner based on his claim that the trial court violated his Sixth Amendment right to a public trial when it briefly closed the courtroom to spectators. The district court denied relief based on the ground that the Minnesota Supreme Court’s decision was neither contrary to, nor an unreasonable application of, clearly established federal law. The court agreed and held that it was not objectively unreasonable for the Minnesota Supreme Court to deem it constitutional under the Sixth Amendment for the trial court to explain the parameters of an earlier public order on evidentiary issues in a brief nonpublic proceeding before the jury was sworn.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Becerra

Court: US Court of Appeals for the Eighth Circuit
Docket: 18-2777
Opinion Date: May 7, 2020
Judge: Stras
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's conviction for two counts of being a

felon in possession of a firearm and ammunition. The court held that there was more than enough evidence for defendant's probation officer and other officers to believe defendant had a firearm on him. Therefore, the officers had probable cause to arrest him without a warrant. The court also held that defendant was in custody when he made both statements at issue. In this case, the "request for clarification" of defendant's statement that he had "something" in his car did not require Miranda warnings. Furthermore, because the bulge in defendant's pocket could have been a gun or other weapon that would have posed a danger to the officers and others, they could ask about it without the formality of Miranda warnings. The court joined its sister circuits in declining to recognize the innocent-possessor defense. The court held that the district court did not err in excluding defendant's proposed testimony that he had found the handgun in his car earlier in the day and was about to hand it over to his probation officer. The court reasoned that, even if defendant intended to turn over the gun (or the ammunition) to his probation officer, it is still a crime to knowingly possess it in the first place. Finally, the court held that the district court did not err in denying defendant a sentencing reduction for acceptance of responsibility; the district court considered defendant's mitigation arguments at sentencing; and the district court did not abuse its discretion by imposing a within-Guidelines sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Haynes

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1607
Opinion Date: May 5, 2020
Judge: Raymond W. Gruender
Areas of Law: Criminal Law

The Eighth Circuit affirmed defendant's conviction and sentence for being a felon in possession of a firearm. The court held that the government did not violate the Speedy Trial Act, and defendant failed to offer any evidence showing that Iowa and federal prosecutors colluded. Furthermore, the district court did not abuse its discretion by failing to hold an evidentiary hearing regarding the existence of collusion. The court also held that the district court did not err in denying the motion to suppress where defendant

was not unlawfully seized. In this case, prior to producing the marijuana cigarette, the officer did not ask defendant any questions but merely ordered him off the bus, particularly as the smell of marijuana alerted the officer that evidence of a more serious crime than failure to use a turn signal might be uncovered during the stop. Finally, the court held that defendant was not unlawfully searched when the officer conducted a pat-down search incident to arrest; the evidence was sufficient to support defendant's conviction; defendant's Rehaif claim failed because there was sufficient evidence that he knew of his prohibited status; and defendant's sentence was not substantively unreasonable nor an abuse of the district court's discretion.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Roberts

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1176
Opinion Date: May 1, 2020
Judge: Steven M. Colloton
Areas of Law: Criminal Law

The Eighth Circuit vacated defendant's sentence imposed after he pleaded guilty to unlawful possession of a firearm as a previously convicted felon. The court held that, although the district court properly applied a four-level increase for possession of a firearm "in connection with another felony offense" under USSG 2K2.1(b)(6)(B), but that a two-level increase for "using a minor to commit a crime" under USSG 3B1.4 should not have applied. In this case, the evidence showed only that defendant engaged in an arm's-length transaction with a minor. The court held that this mere joint participation in an offense as a partner, does not amount to "use" of a minor "to commit the offense" of unlawful possession of a firearm by a felon. Accordingly, the court remanded for resentencing.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Wright

Court: US Court of Appeals for the Eighth Circuit
Docket: 19-1081

Opinion Date: May 5, 2020
Judge: Erickson
Areas of Law: Criminal Law

The Eighth Circuit affirmed the district court's restitution order and certain special conditions of defendant's supervised release imposed after he pleaded guilty to sex trafficking of a child. The court found no error in the district court's restitution amount of $20,000, holding that the evidence supported the amount in light of the aggregate harm to the victim. The court also held that the special conditions -- including a requirement that defendant participate in sex offender treatment including psychological testing and polygraph examinations, a prohibition against contact with any minors without pre-approval, and a requirement that defendant seek prior approval before using temporary commercial lodging, such as a hotel or motel -- where reasonably related to both the offense of conviction and to defendant's history of sexual contact with minor females.

Read Opinion Are you a lawyer? **Annotate this case**.

Benson v. Chappell

Court: US Court of Appeals for the Ninth Circuit
Docket: 13-99004
Opinion Date: May 1, 2020
Judge: Consuelo Maria Callahan
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Ninth Circuit affirmed the district court's denial of petitioner's habeas corpus petition challenging his California conviction and death sentence for murder and other crimes. Petitioner raised two certified claims and two uncertified claims. The panel held that petitioner failed to show that the California Supreme Court's denials of his claims were unreasonable determinations of the facts or contrary to clearly established federal law. In this case, the California Supreme Court reasonably determined that an officer's misstatement during petitioner's interrogation that there was no death penalty in California did not prompt petitioner's confessions. Furthermore, petitioner failed to show that his statements were not knowing, voluntary, and intelligent. Even if petitioner were able to show that trial counsel was ineffective in not fully investigating his abuse as a child or his alleged organic brain injury, the panel held that the state court could

reasonably have determined that any shortcoming in trial counsel's investigation was not prejudicial. Finally, the panel granted a certificate of appealability on petitioner's two uncertified claims and held that the state court reasonably rejected the claims that his trial counsel should have impeached the government's case and the prosecutor withheld material, exculpatory evidence.

Read Opinion Are you a lawyer? **Annotate this case**.

Mero v. Barr

Court: US Court of Appeals for the Ninth Circuit
Docket: 17-70929
Opinion Date: May 1, 2020
Judge: Paul Jeffrey Watford
Areas of Law: Criminal Law, Immigration Law

The Ninth Circuit granted in part a petition for review of the BIA's finding that petitioner was removable based on his conviction for possession of visual presentation depicting sexual conduct of a person under 16 years of age, in violation of Nevada Revised Statutes (N.R.S.) 200.730. Applying the categorical approach, the panel compared the elements of N.R.S. 200.730 with the applicable definition of "sexual abuse of a minor," which requires proof of three elements. The panel held that N.R.S. 200.730 punishes a broader range of conduct because the Nevada statute does not require proof that the offender participated in sexual conduct with a minor. Therefore, petitioner's conviction did not qualify as sexual abuse of a minor. The panel explained that, with a possession-only offense such as N.R.S. 200.730, the minor depicted in the image is not the direct object of the offender's conduct, which is a necessary predicate for the offense to qualify as sexual abuse of a minor.

Read Opinion Are you a lawyer? **Annotate this case**.

Romero-Millan v. Barr

Court: US Court of Appeals for the Ninth Circuit
Dockets: 16-73915, 17-72893, 18-71555
Opinion Date: May 4, 2020

Areas of Law: Criminal Law

The Ninth Circuit certified the following questions of state law to the Arizona Supreme Court: 1. Is Arizona's possession of drug paraphernalia statute, A.R.S. 13-3415, divisible as to drug type? 2. Is Arizona's drug possession statute, A.R.S. 13-3408, divisible as to drug type? 3. Put another way, is jury unanimity (or concurrence) required as to which drug or drugs listed in A.R.S. 13-3401(6), (19), (20), or (23) was involved in an offense under either statute?

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Yang

Court: US Court of Appeals for the Ninth Circuit
Docket: 18-10341
Opinion Date: May 4, 2020
Judge: Piersol
Areas of Law: Criminal Law

The Ninth Circuit affirmed the district court's denial of defendant's motion to suppress after he pleaded guilty to receipt of stolen mail and being a prohibited person in possession of a firearm. Defendant moved to suppress the evidence seized from his residence and the statements he made to law enforcement on the basis that the search warrant obtained by the Postal Inspection Service relied on evidence that was obtained illegally. The panel declined to address the potential Fourth Amendment privacy interests that may be implicated by the warrantless use of this Automatic License Plate Recognition (ALPR) technology, and held that defendant does not have a reasonable expectation of privacy in the historical location data of the Yukon under the facts of this case. The panel found no evidence in the record that Prestige Motors had a policy or practice of allowing lessees to keep cars beyond the rental period and Prestige had made affirmative attempts to repossess the vehicle by activating the GPS unit to locate and disable the vehicle. Therefore, defendant lacked standing to challenge the warrantless search of the database.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Neugin

Court: US Court of Appeals for the Tenth Circuit
Docket: 19-7043
Opinion Date: May 1, 2020
Judge: Scott Milne Matheson, Jr.
Areas of Law: Constitutional Law, Criminal Law

Jack Neugin pled guilty to being a felon in possession of a firearm and ammunition on the condition that he could appeal the district court's denial of his motion to suppress evidence of the ammunition and firearm police found in the bed of his pickup truck. Officers responded to a reported verbal altercation between Neugin and his girlfriend. One of the officers saw ammunition in the back of the truck after he lifted the truck's camper lit do allow the girlfriend to retrieve her belongings. Neugin argued the officers discovered the evidence during an unconstitutional search; the district court concluded the officer was acting "in a lawful position" as "community caretaker," and found no Fourth Amendment violation. The Tenth Circuit reversed, finding that : (1) the officer conducted the without a warrant or probable cause, (2) the community caretaking exception to the warrant requirement does not apply, and (3) the inevitable discovery exception to the exclusionary rule does not apply. The evidence seized should have been suppressed.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Ramon

Court: US Court of Appeals for the Tenth Circuit
Docket: 19-1221
Opinion Date: May 1, 2020
Judge: Gregory Alan Phillips
Areas of Law: Constitutional Law, Criminal Law

In 2016, after serving a federal prison sentence for having possessed a firearm after a felony conviction, Charles Ramon III began serving a mandatory term of supervised release. Before Ramon completed the term, his probation officer filed a petition, soon followed by two superseding petitions, to revoke Ramon’s supervised release. At the revocation hearing, the district court found three violations—two for possessing a controlled

substance and one for again illegally possessing a firearm. Of these, the most serious was Ramon's illegal possession of a firearm—a Grade B violation. For this, the court imposed the statutory maximum sentence of twenty-four months in prison. During the revocation hearing, the government mentioned that it might seek to indict Ramon for illegally possessing a firearm (the conduct in part underlying the revocation). Mindful of this, the district court ordered that Ramon's twenty-four-month sentence run "consecutively to any sentences imposed previously or prospectively in federal or state court." At the hearing, Ramon did not object to the district court's running his sentence consecutively to future federal sentences. On appeal, Ramon argued that the district court exceeded its sentencing authority under 18 U.S.C. 3584(a) by ordering that Ramon's sentence run consecutively to future federal sentences. By the terms of 18 U.S.C. 3584(a), the Tenth Circuit determined the district court did err. But Ramon failed to object to this at trial, and on appeal, failed to show that the error was plain, thus, judgment was affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Richards

Court: US Court of Appeals for the Tenth Circuit
Docket: 19-8044
Opinion Date: May 6, 2020
Judge: Baldock
Areas of Law: Constitutional Law, Criminal Law

In 2018, the Wyoming Division of Criminal Investigation (DCI) obtained a search warrant to review the contents of Defendant–Appellant Joshua Richards' Tumblr account. During the search and subsequent investigation, DCI agents discovered Defendant had re-blogged videos and images of child pornography to his private Tumblr so he could later access and view the materials. Defendant ultimately pleaded guilty to one count of accessing with intent to view child pornography. He was sentenced to twenty-four months' imprisonment followed by five years of supervised release. The district court imposed several special conditions of supervised release, which, as relevant here, related to drugs and alcohol and required Defendant to submit to polygraph testing. On appeal, Defendant argued the district court erred in imposing these special conditions. He also challenged

the length of his prison sentence as substantively unreasonable. The Tenth Circuit determined the alcohol and drug conditions did not directly conflict with the relevant policy statement in the sentencing guidelines, so the district court's decision to impose the conditions was not manifestly unreasonable. And given the circumstances of the case, the Court determined the trial court did not abuse its discretion in imposing Defendant's twenty-four month sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

Andrews v. Warden

Court: US Court of Appeals for the Eleventh Circuit
Docket: 19-12443
Opinion Date: May 5, 2020
Judge: William Holcombe Pryor, Jr.
Areas of Law: Criminal Law

The Eleventh Circuit affirmed the district court's denial of habeas relief under 28 U.S.C. 2241. Plaintiff alleged that President Obama commuted his "total sentence" of imprisonment, which included the 37 months of imprisonment that he served as part of his 2003 sentence. Based on the terms of the commutation order, the Constitution, and Supreme Court precedent, the court could not say that the Bureau erred in excluding the 37-month term of imprisonment from its recalculation.

Read Opinion Are you a lawyer? **Annotate this case**.

Hollis v. United States

Court: US Court of Appeals for the Eleventh Circuit
Docket: 19-11323
Opinion Date: May 6, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Eleventh Circuit affirmed the district court's denial of petitioner's motion to vacate his sentence under 28 U.S.C. 2255. The court held that petitioner cannot prove that his counsel rendered ineffective assistance, because petitioner's prior convictions in Alabama categorically qualify as predicate

offenses under both the Armed Career Criminal Act and the career-offender provision of the Guidelines, and his prior conviction in Georgia qualifies as a predicate offense under the Act. Therefore, counsel did not perform deficiently by failing to raise a meritless objection.

Read Opinion Are you a lawyer? **Annotate this case**.

Knight v. Florida Department of Corrections

Court: US Court of Appeals for the Eleventh Circuit
Docket: 18-12488
Opinion Date: May 1, 2020
Judge: Newsom
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Eleventh Circuit affirmed the district court's denial of a 28 U.S.C. 2254 petition for habeas relief. Petitioner alleged that his counsel rendered ineffective assistance under Strickland v. Washington, 466 U.S. 668 (1984), by failing to adequately investigate and present mitigating evidence during the sentencing phase of his capital-murder trial. The court held that, even assuming that counsel performed deficiently in failing to investigate and present the mitigation evidence that petitioner now raises—thus satisfying the first prong of the two-part Strickland standard that governs ineffective-assistance claims—petitioner failed to carry his burden of demonstrating resulting prejudice.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Evans

Court: US Court of Appeals for the Eleventh Circuit
Docket: 17-15323
Opinion Date: May 6, 2020
Judge: Grant
Areas of Law: Criminal Law

The Eleventh Circuit affirmed defendant's conviction and sentence for being a felon in possession of a firearm. The court held that, given the totality of the circumstances, it was reasonable for officers, mistaking a dog's whimper for a person in distress, to enter defendant's home without a warrant.

Therefore, defendant's challenge to the district court's denial of his motion to suppress evidence failed. The court upheld the district court's imposition of a 22 offense level finding because defendant possessed a semiautomatic firearm capable of accepting a large capacity magazine under USSG 2K2.1(a)(3)(A)(i) (2016). The court also upheld defendant's sentencing enhancement under USSG 2K2.1(b)(4)(B) for possessing a rifle that had an obliterated serial number.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. McLellan

Court: US Court of Appeals for the Eleventh Circuit
Docket: 18-13289
Opinion Date: May 6, 2020
Judge: Boggs
Areas of Law: Criminal Law

The Eleventh Circuit affirmed defendant's conviction for two counts of being a felon in possession of a firearm. The court held that the district court did not abuse its discretion in permitting one of his arresting officers to offer testimony at trial on the correlation between guns and drug activity and to suggest that defendant was selling drugs; the court declined to evaluate the applicability of the Armed Career Criminal Act (ACCA), because the district court would have imposed the same sentence regardless of whether the mandatory minimum applied; and the court rejected defendant's claim under Rehaif v. United States, 139 S. Ct. 2191 (2019), and held that there was no plain error in the district court's failure to instruct the jury of the knowledge-of-status element and any error from the lack of a knowledge-of-status element in defendant's plea colloquy did not affect his substantial rights. Finally, the court remanded for clarification of the judgment to reflect the sentence the district court said it would have imposed if the Armed Career Criminal Act did not apply.

Read Opinion Are you a lawyer? **Annotate this case**.

United States v. Russell

Court: US Court of Appeals for the Eleventh Circuit

Docket: 18-11202
Opinion Date: May 4, 2020
Judge: Charles R. Wilson
Areas of Law: Criminal Law

Defendant was convicted of possessing a firearm and ammunition as an immigrant illegally or unlawfully in the United States. After defendant appealed his conviction and sentence, the Supreme Court issued its decision in Rehaif v. United States, 588 U.S. ___, 139 S. Ct. 2191 (2019), which reversed a decision from this court and held that under 18 U.S.C. 922(g), the government must prove that a defendant knew "his status as a person barred from possessing a firearm" when he knowingly possessed a firearm. The Eleventh Circuit held that defendant established the necessary prejudice under plain error review and vacated defendant's section 922(g) conviction, remanding for further proceedings. In this case, the district court committed an error that was made plain by the Supreme Court in Rehaif. Furthermore, defendant has sufficiently shown a reasonable probability that but for the error, the outcome of his trial would have been different.

Read Opinion Are you a lawyer? **Annotate this case**.

Welch v. United States

Court: US Court of Appeals for the Eleventh Circuit
Docket: 14-15733
Opinion Date: May 6, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Eleventh Circuit affirmed the district court's denial of petitioner's 28 U.S.C. 2255 motion to vacate his sentence. The court held that defendant's prior 1996 Florida convictions for robbery qualified as violent felonies under the Armed Career Criminal Act's (ACCA) elements clause, and rejected his contention that the court's decision in his direct appeal carved out a narrow exception to pre-1997 Florida robbery convictions obtained in Florida's Fourth District Court of Appeal. The court also held that petitioner's prior Florida felony battery conviction was a violent felony under the ACCA in light of the court's holding in United States v. Vail-Bailon, 868 F.3d 1293 (11th Cir. 2017) (en banc), cert. denied, 138 S. Ct. 2620 (2018).

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Trujillo

Court: Arizona Supreme Court
Docket: CR-18-0531-PR
Opinion Date: May 4, 2020
Judge: Gould
Areas of Law: Constitutional Law, Criminal Law

The Supreme Court held that, for purposes of imposing mandatory sex offender registration under Ariz. Rev. Stat. 13-3821(A)(3), a judge has the authority to make the necessary factual finding that the victim is under the age of eighteen and that Arizona's sex offender registration statutes are civil regulatory statutes, not criminal penalties. Defendant was convicted by a jury of one count of sexual abuse. In reaching its verdict the jury determined that the victim was "fifteen or more years of age." At sentencing, the trial court ordered Defendant to register as a sex offender. Defendant objected, arguing that, pursuant to Apprendi v. New Jersey, 530 U.S. 466 (2000), a jury was required to find whether Defendant was under eighteen pursuant to section 13-3821(A)(3). The trial court denied the objection. The court of appeals affirmed. The Supreme Court affirmed, holding (1) Apprendi does not apply to factual findings that are necessary to impose registration because sex offender registration is a civil regulatory requirement, not a criminal penalty; and (2) the trial judge did not violate Apprendi by determining that the victim was under eighteen.

Read Opinion Are you a lawyer? **Annotate this case**.

Barnett v. State

Court: Arkansas Supreme Court
Citation: 2020 Ark. 181
Opinion Date: May 7, 2020
Judge: Hudson
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's "motion for credit for time spent in custody," holding that the

circuit court's findings were not clearly erroneous. In his motion, Appellant alleged that he was entitled to 312 days of jail-time credit and that the circuit court should enter a new sentencing order nunc pro tunc that reflected the correct amount of jail-time credit. The circuit court denied the motion. The Supreme Court affirmed, holding that the circuit court's denial of Appellant's motion was not clearly erroneous because Appellant failed to demonstrate a clerical error subject to correction.

Read Opinion Are you a lawyer? **Annotate this case**.

Mason v. Kelley

Court: Arkansas Supreme Court
Citation: 2020 Ark. 182
Opinion Date: May 7, 2020
Judge: Rhonda K. Wood
Areas of Law: Criminal Law

The Supreme Court affirmed the order of the circuit court dismissing Appellant's pro se petition for writ of habeas corpus, holding that Appellant stated no ground on which the writ could issue. Appellant was convicted of aggravated robbery, theft of property, and second-degree battery and sentenced as a habitual offender to an aggregate term of 660 months' imprisonment. The court of appeals affirmed. Appellant later petitioned for writ of habeas corpus, asserting that the trial court misapplied Arkansas's habitual-offender statutes. The circuit court dismissed the petition. The Supreme Court affirmed, holding that the issues Appellant raised in his petition for the writ should have been raised at trial, on direct appeal, or in a petition for postconviction relief.

Read Opinion Are you a lawyer? **Annotate this case**.

Ray v. Kelley

Court: Arkansas Supreme Court
Citation: 2020 Ark. 184
Opinion Date: May 7, 2020
Judge: Wynne
Areas of Law: Criminal Law

The Supreme Court dismissed Appellant's appeal from an order denying his pro se petition for permission to reinvest jurisdiction in the trial court to consider a petition for writ of error coram nobis, holding that the circuit court had no jurisdiction to consider the petition. Appellant entered negotiated guilty pleas to rape and other offenses. Appellant later filed a petition for writ of error coram nobis in the Chicot County Circuit Court, the court where he was incarcerated, setting out two grounds for coram nobis relief. The circuit court denied the petition. The Supreme Court dismissed Appellant's appeal, holding that jurisdiction lay in the trial court where Appellant was convicted, which in this case was the Ashley County Circuit Court. Therefore, the Chicot County Circuit Court was without jurisdiction to address Appellant's coram nobis petition.

Read Opinion Are you a lawyer? **Annotate this case**.

Walker v. Kelley

Court: Arkansas Supreme Court
Citation: 2020 Ark. 183
Opinion Date: May 7, 2020
Judge: Rhonda K. Wood
Areas of Law: Criminal Law

The Supreme Court affirmed the judgment of the circuit court denying Appellant's pro se petition for declaratory judgment, holding that Appellant could not use a declaratory-judgment action to collaterally attack his criminal conviction. Appellant was convicted of first-degree murder and second-degree unlawful discharge of a firearm from a vehicle. The court of appeals affirmed. Years later, Appellant filed a petition for declaratory judgment alleging that he was denied due process in his criminal trial when the court admitted the prior testimony of an unavailable witness and that this admission violated the Confrontation Clause. The circuit court denied the petition. The Supreme Court affirmed, holding that a declaratory judgment action provided no relief on these grounds.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Flores

Court: Supreme Court of California
Docket: S116307
Opinion Date: May 4, 2020
Judge: Kruger
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction of three counts of first degree murder and his sentence of death, holding that the three or four minor errors at Defendant's trial were harmless and did not interfere with his due process right to a fair trial. Specifically, the Supreme Court held (1) no error occurred during jury selection; (2) Defendant was not prejudiced by any misstatements by the prosecutor; (3) assuming certain evidence was inadmissible, the court's admonition to the jury and the court's instruction cured the resultant harm; (4) the trial court erred in admitting testimony that the victim was afraid of Defendant, but the error was harmless; and (5) Defendant's remaining allegations of error were without merit.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. Law

Court: California Courts of Appeal
Docket: E072845(Fourth Appellate District)
Opinion Date: May 5, 2020
Judge: Slough
Areas of Law: Constitutional Law, Criminal Law

In 2001, appellant Terrell Law and his codefendant Brett May committed a home invasion robbery, during which one of them shot and killed one of the residents. They were tried jointly in 2006 before two separately empaneled juries who found them both guilty of first degree felony murder with the special circumstance described in Penal Code section 190.2(a)(17(A) and (d). Though Law's jury found he was not the shooter, they nonetheless concluded he was a "major participant" in the underlying robbery and acted "with reckless indifference to human life." In 2018, the Legislature enacted Senate Bill No. 1437 (2017-2018 Reg. Sess.) which, among other things, amended the definition of felony murder in Penal Code section 189. The legislation also added Penal Code section 1170.95, which established a procedure for vacating murder convictions predating the amendment that could not be sustained under the new definition of felony murder. Law

challenged the trial court's summary denial of his section 1170.95 petition to vacate his murder conviction, arguing the trial court erred by reviewing his record of conviction and determining the jury's true finding on the special circumstance rendered him ineligible for relief. The Court of Appeal concluded it was proper for a trial court to review the record of conviction when determining whether a section 1170.95 petitioner had stated a prima facie claim for relief. Additionally, the Court concluded Law "undoubtedly qualifies" as a major participant who acted with reckless indifference to human life, a conclusion that rendered him ineligible for relief under section 1170.95. The Court therefore affirmed the order denying his petition.

Read Opinion Are you a lawyer? **Annotate this case**.

California v. Sanchez

Court: California Courts of Appeal
Docket: E072647(Fourth Appellate District)
Opinion Date: May 7, 2020
Judge: Menetrez
Areas of Law: Constitutional Law, Criminal Law

Victor Sanchez was charged with first degree murder, but pled guilty to voluntary manslaughter. He filed a petition under Penal Code section 1170.95 to vacate that conviction. The trial court denied the petition, concluding that Sanchez was ineligible for relief because he was not convicted of murder. After review, the Court of Appeal joined other courts that held section 1170.95 did not apply to defendants convicted of voluntary manslaughter. The Court also rejected Sanchez's argument that section 1170.95 violated equal protection.

Read Opinion Are you a lawyer? **Annotate this case**.

Galeotti v. International Union of Operating Engineers

Court: California Courts of Appeal
Docket: A157785(First Appellate District)
Opinion Date: May 6, 2020
Judge: Henry E. Needham, Jr.
Areas of Law: Criminal Law, Labor & Employment Law, White Collar Crime

Galeotti, a former Union Local 3 employee, filed a complaint against Local 3 and three of individual union leaders, alleging that the individual defendants required union employees to pay them money to keep their jobs, lied about the reason for collecting the money, and caused Local 3 to terminate Galeotti's employment when he failed to pay the full amount demanded. The trial court dismissed his second amended complaint without leave to amend. The court of appeal reversed in part, reasoning that a threat to terminate employment can provide a basis for an extortion claim and that the allegations of the second amended complaint stated a cause of action for wrongful termination in violation of the public policy underlying the extortion statutes. The complaint stated a cause of action for violations of the Racketeer Influenced and Corrupt Organizations Act (RICO; 18 U.S.C. 1961), based on the predicate acts of extortion, but did not state a cause of action for interference with prospective economic advantage.

Read Opinion Are you a lawyer? **Annotate this case**.

In re I.A.

Court: California Courts of Appeal
Docket: B296549(Second Appellate District)
Opinion Date: May 4, 2020
Judge: Tangeman
Areas of Law: Criminal Law, Juvenile Law

Where a juvenile court vacates its true finding on a generic murder allegation and redesignates it as a finding on an uncharged target offense, and does so before a minor has had the opportunity to contest the court's findings or orders, the minor may challenge the sufficiency of the evidence of the redesignated offense on appeal. The Court of Appeal held that there was insufficient evidence to support the juvenile court's decision sustaining the allegations that I.A. possessed a concealable firearm and committed vandalism. Therefore, the court reversed the juvenile court's findings, vacating the jurisdiction and disposition order and dismissing the Welfare and Institutions Code section 602 petition.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Edwards

Court: California Courts of Appeal
Docket: A158055(First Appellate District)
Opinion Date: May 1, 2020
Judge: Petrou
Areas of Law: Criminal Law

In 2006, Edwards fired an assault weapon into an apartment, killing the victim. Edwards pled guilty to possession of a firearm as a felon and was convicted of second-degree murder and shooting into an inhabited dwelling. Following the enactment of Senate Bill 1437, Edwards filed a Penal Code 1170.95 resentencing petition, checking form boxes indicating that he was convicted under a theory of felony murder or murder under the natural and probable consequences doctrine and that he could not now be convicted of 1st or 2nd-degree murder because of changes to Penal Code 188 and 189. Edwards submitted the jury instructions and the transcript of the prosecutor's closing remarks that Edwards acted with "both express malice, specific intent to kill, as well as implied malice," described as "an intentional act, the natural consequences of which are dangerous to human life, and at the time that the individual acted, they knew of the danger, and they deliberately acted with conscious disregard." The court denied the petition, finding that Edwards was convicted on a valid theory of murder that survived the statutory changes. The court of appeal affirmed. The superior court did not err in considering the record of conviction. Edwards could not meet the statutory prerequisites for even filing a section 1170.95 petition because he was not charged or convicted of second-degree felony murder or murder under the natural or probable consequences doctrine directed at accomplice liability.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Thomkins

Court: California Courts of Appeal
Docket: A141375(First Appellate District)
Opinion Date: May 1, 2020
Judge: Streeter
Areas of Law: Criminal Law

On Easter night in 2011, gunfire erupted at an Oakland bar-restaurant, leaving two people dead and five wounded. Thompkins and Fox were convicted of two counts of first-degree murder for the benefit of a criminal street gang, with firearm discharge enhancements, a multiple-murder special circumstance, and five counts of attempted murder with great bodily injury findings, gang enhancements, and firearm discharge enhancements. Thompkins was convicted as the shooter and Fox as an accomplice. Both were sentenced to life in prison without possibility of parole, plus 224 years to life. After Thompkins was sentenced, Fox stated under oath he was the actual shooter and Thompkins knew nothing about Fox's intentions. Thompkins claimed this new testimony, and his attorney's incompetent reaction entitled him to a new trial and submitted a declaration by another gang member who was present that night. The court of appeal concluded that Thompkins's attorney was not ineffective for failing to bring a motion to recall the sentence followed by a new trial motion because Thompkins failed to show prejudice. The attempted murder convictions and related enhancements must be reversed for both defendants based on the flawed kill zone instruction. Introducing evidence that defendants admitted their gang affiliation at jail intake violated the defendants' privilege against self-incrimination but was harmless. There was some evidentiary error that was harmless due to the wealth of admissible evidence establishing the gang enhancements. Arguments based on the statutory amendments to Penal Code 188 and 189 must be raised in the trial court (section 1170.95). The case must be remanded so the judge may exercise his discretion whether to impose or strike the firearm enhancements on under Penal Code 12022.53.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Torres

Court: California Courts of Appeal
Docket: B295043(Second Appellate District)
Opinion Date: May 4, 2020
Judge: Wiley
Areas of Law: Criminal Law

After the trial court admitted a witness's former testimony, the Court of Appeal applied People v. Roldan (2012) 205 Cal.App.4th 969, 975–985, and reversed. Roldan held that, before invoking the former testimony exception,

prosecutors should react appropriately to the impending deportation risk by following four steps: alert the defense to the risk; videotape the preliminary hearing testimony; use judicial measures to try to delay deportation; and consider an array of other specific measures. In this case, the prosecution conceded that prosecutors were simply unaware of Roldan and did not comply with it. The court held that Roldan controls the court's analysis because the facts about prosecutorial diligence are weaker here than they were in Roldan, where the appellate court held for the defense. In this case, the record before deportation is of prosecutorial inaction where the prosecution's brief in this court admits the investigating officer did not do anything to ensure that the witness would not be deported, nor is there other evidence of prosecutorial efforts to delay the witness's departure or to videotape his testimony at the preliminary hearing.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Triplett

Court: California Courts of Appeal
Docket: B298914(Second Appellate District)
Opinion Date: May 1, 2020
Judge: Frances Rothschild
Areas of Law: Criminal Law

Defendant was convicted of assault with a deadly weapon, carjacking, and attempted murder. In the published portion of the opinion, the Court of Appeal held that the trial court erred by denying defense counsel's request to inform the jurors that they could have testimony of certain witnesses read back to them. The court also held that, under the circumstances in this case, the error was harmless.

Read Opinion Are you a lawyer? **Annotate this case**.

Colorado In Interest of G.S.S.

Court: Colorado Supreme Court
Citation: 2020 CO 32
Opinion Date: May 4, 2020
Judge: Brian D. Boatright

Areas of Law: Constitutional Law, Criminal Law, Juvenile Law

After being charged, fourteen-year-old G.S.S. was detained for more than three months without bail, even though he had not entered a plea and had not been tried on the charges against him. At that point, G.S.S.'s counsel filed a motion to dismiss, arguing that G.S.S.'s "right to a speedy trial" had been violated under section 19-2-509(4)(b), C.R.S. (2019). The trial court agreed and dismissed the case against G.S.S. with prejudice, and the court of appeals affirmed in Colorado in Interest of G.S.S., 2019 COA 4M, __ P.3d __. The Colorado Supreme Court then granted certiorari to determine the proper remedy for a violation of the sixty-day limit in section 19-2-509(4)(b). The Supreme Court determined the remedy for a section 19-2-509(4)(b) violation was for the trial court to immediately hold a bail hearing and order the juvenile's release. Accordingly, the judgment of the court of appeals was reversed.

Read Opinion Are you a lawyer? **Annotate this case**.

Barringer v. Halkitis

Court: Florida Supreme Court
Docket: SC19-1071
Opinion Date: May 7, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court held that Jay Barringer's quo warranto petition filed in this case was a frivolous proceeding brought before the Supreme Court by a state prisoner and sanctioned Barringer by barring him from filing any further pro se requests for relief related to his criminal case. Barringer was convicted of one count of attempted sexual battery of a victim less than twelve years old and sentenced to twenty-five-years' imprisonment. In 2011, Barringer began filing petitions in the Supreme Court. The Court did not grant the relief sought in any of Barringer's filings. In the instant quo warranto petition Barringer challenged his conviction on the ground that the information was defective, a claim Barringer previously raised by way of a habeas petition. The Supreme Court denied the petition and found that Barringer abused the Court's limited judicial resources. The Court sanctioned Barringer by directing the Clerk of Court to reject any future

pleadings or other requests for relief submitted by Barringer that are related to his criminal case, unless such filings are signed by a member of The Florida Bar in good standing.

Read Opinion Are you a lawyer? **Annotate this case**.

Franqui v. State

Court: Florida Supreme Court
Docket: SC19-203
Opinion Date: May 7, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court affirmed the order of the circuit court denying Appellant's claim of intellectual disability, raised in successive motions for postconviction relief under Fla. R. Crim. P. 3.851, holding that the circuit court did not err in denying relief. Appellant was convicted of first-degree murder and sentenced to death in two separate cases. After the United States Supreme Court decided Hall v. Florida, 572 U.S. 701 (2014), Appellant filed successive motions for postconviction relief in both of his capital cases, asserting that the circuit court's denials of his previous claims of intellectual disability were based on the court's improper interpretation of Florida's intellectual disability statute. The circuit court summarily denied the motions. The Supreme Court reversed and remanded for an evidentiary hearing on the issue of intellectual disability. After a hearing, the circuit court denied the claim. The Supreme Court affirmed, holding (1) the circuit court did not err in denying Appellant's intellectual disability claim; and (2) Appellant was not entitled to relief under Hurst v. Florida, 136 S. Ct. 616 (2016), or Hurst v. State, 202 So. 3d 40 (Fla. 2016).

Read Opinion Are you a lawyer? **Annotate this case**.

Hicks v. State

Court: Florida Supreme Court
Docket: SC19-1978
Opinion Date: May 7, 2020
Judge: Per Curiam

Areas of Law: Criminal Law

The Supreme Court denied the instant mandamus petition filed by Hicks and sanctioned Hicks by barring him from filing any further pro se requests for relief related to his criminal case. Hicks was convicted of one count of lewd and lascivious conduct by a person over eighteen years of age on a victim under sixteen years of age. Since 2016, Hicks filed thirteen pro se requests for relief in the Supreme Court related to his criminal case. The Court did not grant the relief sought in any of Hicks' filings. In the instant petition, Hicks sought a writ of mandamus compelling the circuit court to comply with the requirements of Fla. R. Crim. P. 3.850 by filing a copy of an order denying his second postconviction motion with the clerk of court. The Supreme Court dismissed the petition and found that Hicks abused this Court's limited judicial resources. The Court directed the Clerk of Court to reject any future pleadings or other requests for relief submitted by Hicks that are related to his criminal case, unless such filings are signed by a member of The Florida Bar in good standing.

Read Opinion Are you a lawyer? **Annotate this case**.

Burley v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0356
Opinion Date: May 4, 2020
Judge: Boggs
Areas of Law: Constitutional Law, Criminal Law

In 1992, Douglas Burley pled guilty to malice murder. He moved for an out-of-time appeal in 2019, claiming that his right to appeal was frustrated by his plea counsel's erroneous advice that he could not appeal his conviction because it was the product of a guilty plea. The trial court denied Burley's motion. After review, the Georgia Supreme Court vacated the trial court's judgment and remanded the case with direction to hold a hearing to determine whether ineffective assistance of counsel frustrated Burley's right to appeal.

Read Opinion Are you a lawyer? **Annotate this case**.

Carter v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0022
Opinion Date: May 4, 2020
Judge: David E. Nahmias
Areas of Law: Construction Law, Criminal Law

Brandon Carter was convicted by jury of malice murder and two firearm offenses in connection with the shooting death of Terrance Baker. On appeal, Carter contended the trial court erred by admitting certain hearsay statements into evidence and by violating his constitutional right to be present during his trial. Finding no reversible error, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Clarke v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0258
Opinion Date: May 4, 2020
Judge: Ellington
Areas of Law: Constitutional Law, Criminal Law

Rupert Clark was convicted by jury for the malice murder of his wife, Rosemarie Lebert-Clark. He was also convicted of possession of a firearm during the commission of a felony. On appeal, he argued he received ineffective assistance of trial counsel, and that the trial court erred in admitting certain evidence, violated the continuing witness rule by sending out with the deliberating jury printouts of text messages, and by failing to instruct the jury that a defendant's uncorroborated confession was not alone sufficient to warrant a conviction. Finding no reversible error after reviewing the trial court record, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Collins v. Georgia

Court: Supreme Court of Georgia

Docket: S20A0195
Opinion Date: May 4, 2020
Judge: Harold D. Melton
Areas of Law: Constitutional Law, Criminal Law

Renita Collins was tried for murder along with co-defendant Michael Stallworth. Collins appealed her convictions for murder and possession of a firearm while in commission of a felony in connection with the shooting death of Keith Jacobs. On appeal. Collins contended she was denied a fair trial due to juror misconduct, the trial court abused its discretion by not allowing her to subpoena juror testimony to show that misconduct had occurred, and the trial court abused its discretion when it failed to excuse a prospective juror for cause. Finding no reversible error, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Dawson v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0217
Opinion Date: May 4, 2020
Judge: Warren
Areas of Law: Constitutional Law, Criminal Law

Lavaris Dawson was convicted by jury of felony murder and other crimes in connection with the shooting death of Mamadou Camara. On appeal, Dawson challenged the sufficiency of the evidence supporting his convictions, and argued the trial court erred in admitting Dawson's statements to a detective during an interview because those statements were impermissibly induced by a hope of benefit, and that Dawson was denied his due process right to a timely appeal. After review, the Georgia Supreme Court disagreed and affirmed Dawson's convictions.

Read Opinion Are you a lawyer? **Annotate this case**.

Evans v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0007

Opinion Date: May 4, 2020
Judge: McMillan
Areas of Law: Constitutional Law, Criminal Law

Jimmy Evans was convicted by jury for murder and other crimes relating to the 2006 deaths of Tavoris Calhoun and Dezmon Thomas. On appeal, Evans argued that because he was visibly intoxicated at the time he made statements to law enforcement and consented to a search of his home and person, the statements and consent were involuntarily given and the trial court should have granted his motion for new trial on this ground. Furthermore, Evans argued that his trial counsel was ineffective for failing to file a motion to suppress at trial on the same basis. Because Evans failed to show error or ineffective assistance of counsel, the Georgia Supreme Court affirmed his conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Hill v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0285
Opinion Date: May 4, 2020
Judge: Harold D. Melton
Areas of Law: Constitutional Law, Criminal Law

Esco Hill was convicted by jury of malice murder and other crimes relating to the stabbing death of Alford Morris in 2014. On appeal, Hill argued the trial court committed reversible error by requiring him to be visibly shackled for the duration of his six-day trial. After review of the trial court record, the Georgia Supreme Court concurred this was reversible error, consequently, reversed judgment of conviction. Because the Court concluded the evidence at trial was sufficient to sustain Hill's conviction, the State could re-try him. The Court did not address Hill's remaining enumerations of error, "as they are not likely to recur in the event of a retrial."

Read Opinion Are you a lawyer? **Annotate this case**.

Oliver v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0489
Opinion Date: May 4, 2020
Judge: McMillan
Areas of Law: Constitutional Law, Criminal Law

Jacquan Oliver entered a negotiated plea of guilty to felony murder in connection with the shooting death of Alexander Mixon. He appealed his conviction and sentence, arguing that the trial court abused its discretion in finding a factual basis for his plea, and in determining the plea was voluntarily, knowingly and intelligently made. Finding no merit to these contentions, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Rosser v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0103
Opinion Date: May 4, 2020
Judge: Bethel
Areas of Law: Constitutional Law, Criminal Law

Larry Rosser was convicted by jury of malice murder and other crimes in connection with the death of Alexis Vereen. On appeal, Rosser challenged the sufficiency of the evidence presented against him at trial, and argued the trial court erred by not granting his motion for a mistrial, and by allowing the State to introduce a portion of Rosser's custodial statement to law enforcement. In addition, he argued he received constitutionally ineffective assistance of trial counsel. Finding no reversible error after reviewing the trial court record, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Spencer v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0871
Opinion Date: May 4, 2020
Judge: Keith R. Blackwell

Areas of Law: Constitutional Law, Criminal Law

Christopher Spencer was convicted by jury of murder and other crimes in connection with the fatal shootings of Sylvia Watson and Samuel White. Spencer appealed, claiming only that the evidence was insufficient to support his convictions. Finding no reversible error after reviewing the trial court record, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Styles v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0236
Opinion Date: May 4, 2020
Judge: Ellington
Areas of Law: Constitutional Law, Criminal Law

Derrick Styles was convicted by jury of felony murder and other crimes in connection with the shooting death of Alberto Lumens and the armed robbery fo Juan Lumens Garcia. On appeal, Styles contended the trial court erred in admitting into evidence a recording of an inculpatory telephone conversation between himself and a witness. He also argued his trial counsel was ineffective for failing to object to an allegedly improper comment by the prosecutor during closing argument. Finding no merit to these contentions, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Whitehead v. Georgia

Court: Supreme Court of Georgia
Docket: S20A0171
Opinion Date: May 4, 2020
Judge: Ellington
Areas of Law: Constitutional Law, Criminal Law

Javis Whitehead was convicted by jury of murder and other crimes in connection with the shooting death of Dominique Larry. On appeal, Whitehead challenged the sufficiency of the evidence presented to rebut his

claim of self-defense and to convict him for murder beyond a reasonable doubt. He also argued the trial court erred in denying his motion to suppress his custodial statement, and in refusing to excuse for cause the District Attorney from the panel of prospective jurors prior to the conclusion of voir dire. Finding no merit to these contentions, the Georgia Supreme Court affirmed conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

Idaho v. Blythe

Court: Idaho Supreme Court - Criminal
Docket: 46992
Opinion Date: May 4, 2020
Judge: Roger S. Burdick
Areas of Law: Constitutional Law, Criminal Law

Nicholas Blythe appealed after he was convicted of possessing a controlled substance. He conditionally pled guilty, reserving the right to challenge his sentence. On appeal, he argued the district court erred in denying his motion to suppress certain evidence found because the evidence presented at trial was found in violation of Blythe's Fourth Amendment rights. After review, the Idaho Supreme Court determined the search at issue took place before an arrest occurred, and because no rationale justifying a search incident to arrest was sufficiently present here, the search of Blythe's shoes was not a valid search incident to arrest. Therefore, the district court erred in holding that the search was reasonable under the Fourth Amendment. Blythe's conviction was vacated, the district court order denying Blythe's motion to suppress was reversed, and the matter remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

Idaho v. Glodowski

Court: Idaho Supreme Court - Criminal
Docket: 47131
Opinion Date: May 6, 2020
Judge: Roger S. Burdick

Areas of Law: Constitutional Law, Criminal Law

David Glodowski appealed after he was convicted for failing to update his sex-offender registration in violation of Idaho Code section 18-8309. He argued the district court erred by ruling that his prior conviction under a Wisconsin statute was "substantially equivalent" to Idaho statutes that required sex-offender registration in Idaho. After review, the Idaho Supreme Court determined the district court improperly allowed the State to seek a redetermination of the "substantially equivalent" element given that the Idaho Bureau of Criminal Identification made a final determination on that element. However, because the State put forth sufficient evidence to prove that element, and the district court's jury instruction accomplished the same purpose, the Supreme Court concluded the error was harmless. Accordingly, the Court found no reversible error in the district court's decision to grant the State's motion and provide the jury instruction. Therefore, judgment of conviction was affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Idaho v. Jones

Court: Idaho Supreme Court - Criminal
Docket: 45905
Opinion Date: May 4, 2020
Judge: Roger S. Burdick
Areas of Law: Constitutional Law, Criminal Law

Timothy Jones was convicted by jury of trafficking heroin and possession of drug paraphernalia. On appeal, he argued the trial court erred in admitting certain evidence regarding his probation status, a knife found in the initial police search of his person, and that the trial court abused its discretion in arriving at his sentence. Finding no reversible error, the Idaho Supreme Court affirmed Jones' conviction and sentence.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Gordon

Court: Iowa Supreme Court

Docket: 18-1099
Opinion Date: May 1, 2020
Judge: Brent R. Appel
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction for assault on a peace officer with a dangerous weapon, a felony, and several misdemeanors, holding that Defendant did not receive ineffective assistance of counsel. After Defendant pleaded guilty, he absconded. He was later returned to custody. On appeal, Defendant argued that he received ineffective assistance of counsel because the plea bargain contained an unlawful term. Specifically, Defendant argued that the plea bargain's provision that he would be released from jail for a forty-eight-hour furlough after pleading guilty was illegal and that his trial counsel committed ineffective assistance in obtaining the illegal benefit for him. The Supreme Court affirmed, holding that where Defendant entered into the plea agreement with the illegally lenient sentence, he could not benefit from that sentence and then attack the plea bargain.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Craig

Court: Kansas Supreme Court
Docket: 119660
Opinion Date: May 1, 2020
Judge: Dan Biles
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's conviction and sentence for first-degree felony murder, holding that there was no error in the proceedings below. A jury found Defendant guilty of both first-degree felony murder and second-degree intentional murder. At sentencing, Defendant moved for a new trial and judgment notwithstanding the verdict, arguing that the jury must have had reasonable doubt on the first-degree felony murder theory because it convicted him of second-degree murder for the same killing. The district court dismissed the second-degree murder conviction and sentenced Defendant for the felony murder over his objection. The Supreme Court affirmed, holding (1) the district court did not err when it sentenced Defendant on felony murder instead of declaring a mistrial because

Defendant did not establish that the jury failed to find each element of the felony murder beyond a reasonable doubt or that the jury's first- and second-degree murder verdicts were so irreconcilable as to require a new trial; and (2) the district court did not err in declining to give an instruction on voluntary intoxication.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Lemmie

Court: Kansas Supreme Court
Docket: 119439
Opinion Date: May 1, 2020
Judge: Carol A. Beier
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's convictions of first-degree felony murder, aggravated robbery, conspiracy to commit aggravated robbery, criminal possession of a firearm, fleeing and eluding, and interference with law enforcement, holding that Defendant's arguments on appeal failed. Specifically, the Supreme Court held (1) any possible violation of Defendant's Fifth Amendment right in the admission of a witness's testimony about Defendant giving the witness phone passcodes was undoubtedly harmless; (2) the district court did not err by admitting hearsay statements as statements of a coconspirator and contemporaneous statements; (3) the State introduced sufficient evidence to convict Defendant of first-degree murder; and (4) the district judge did not abuse its discretion by admitting testimony that Defendant was upset over a meth pipe that went missing.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Mullen

Court: Maine Supreme Judicial Court
Citation: 2020 ME 56
Opinion Date: May 5, 2020
Judge: Connors
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed Defendant's conviction for reckless

conduct and aggravated criminal mischief, holding that the trial court did not abuse its discretion by offering Defendant a continuance of the trial in lieu of excluding his medical records. On appeal, Defendant argued that the trial court abused its discretion by denying his motion to suppress his personal medical records as a sanction for the State's late seizure of the records. The Supreme Judicial Court agreed that the State's conduct undermined the purpose of Maine Rule of Unified Criminal Procedure 18(b) but that the court's offer of a continuance in lieu of the exclusion of the evidence constituted an appropriate response to the State's conduct.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. Billingslea

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12715
Opinion Date: April 30, 2020
Judge: Cypher
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Judicial Court affirmed Defendant's convictions and the decision of the Appeals Court denying Defendant's motion to vacate the entry of his appeal from his convictions in that court and to have the case entered directly in the Supreme Judicial Court, holding that a direct appeal from the third conviction of a habitual offender pursuant to Mass. Gen. Laws ch. 279, 25(b) may be entered in the Appeals Court. Defendant was indicted for serious felonies arising from a brutal attack and rape. In addition to charging the specific felony, each indictment also alleged that the sentence for that felony should be enhanced pursuant to the habitual criminal provision Mass. Gen. Laws ch. 279, 25(a) or the habitual offender provision of section 25(b), or both. After he was convicted, Defendant moved to have the case entered directly in the Supreme Judicial Court. The Appeals Court denied the motion. The Supreme Judicial Court affirmed Defendant's convictions, holding (1) this direct appeal was entitled to the unique review prescribed by Mass Gen. Laws ch. 278, 33E, and the Appeals Court may conduct such section 33E review; (2) Defendant was not impermissibly allowed to waive his right to a jury trial on the sentencing enhancement provisions of the indictments; and (3) Defendant was not entitled to reversal of his convictions on any other ground.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. Martin

Court: Massachusetts Supreme Judicial Court
Docket: SJC-08768
Opinion Date: May 5, 2020
Judge: Ralph D. Gants
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Judicial Court affirmed Defendant's conviction of murder in the first degree and the denial of his motion for a new trial and declined to exercise its authority under Mass. Gen. Laws ch. 278E to reduce Defendant's conviction to murder in the second degree, holding that Defendant was not entitled to relief on any of his allegations of error. Defendant was convicted of murder in the first degree on the theory of felony-murder. Defendant filed a motion for a new trial, which was denied. The Supreme Judicial Court affirmed, holding (1) Defendant's motion for a new trial was correctly denied because Defendant was not prejudiced by counsel's ineffective assistance; (2) this Court declines to extend the reach of the Court's holding in Commonwealth v. Brown, 477 Mass. 805 (2017), to Defendant's case; and (3) trial judge erred when he declined Defendant's request that the jury be instructed on the elements of voluntary and involuntary manslaughter, but the error was not prejudicial in the context of the judge's other instructions.

Read Opinion Are you a lawyer? **Annotate this case**.

Commonwealth v. Tavares

Court: Massachusetts Supreme Judicial Court
Docket: SJC-12631
Opinion Date: May 6, 2020
Judge: Lowy
Areas of Law: Criminal Law

The Supreme Judicial Court affirmed Defendant's conviction of murder in the first degree on theories of deliberate premeditation and extreme atrocity

or cruelty and declined to exercise its power pursuant to Mass. Gen. Laws ch. 278, 33E to reduce the conviction to manslaughter, holding that there was no reversible error in the proceedings below. Specifically, the Supreme Judicial Court held (1) the trial judge did not err by denying Defendant's requests for a jury instruction pursuant to Commonwealth v. Croft, 345 Mass. 143 (1962); (2) the trial judge did not err by denying Defendant's motions for a required finding of not guilty under Croft because a rational jury could have found that Defendant was guilty of murder in the first degree on both the theories of premeditation and extreme atrocity or cruelty; and (3) there was no basis for reducing Defendant's sentence or ordering a new trial.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Branch

Court: Minnesota Supreme Court
Docket: A18-1055
Opinion Date: May 6, 2020
Judge: Lorie Skjerven Gildea
Areas of Law: Criminal Law

The Supreme Court affirmed Defendant's sentences for drive-by shooting at an occupied vehicle and second-degree assault, holding that Minn. Stat. 609.035 did not prohibit the sentences for both offenses when the crimes arose from a single behavioral incident. The district court sentenced Defendant to forty-eight months for drive-by shooting at an occupied vehicle and thirty-six months for second-degree assault and imposed the two sentences to run concurrently. The court of appeals affirmed. The Supreme Court affirmed, holding that, under this Court's analysis in State v. Ferguson, 808 N.W.2d 586 (Minn. 2012), the district court properly imposed multiple sentences in this case.

Read Opinion Are you a lawyer? **Annotate this case**.

Galloway v. Mississippi

Court: Supreme Court of Mississippi
Citation: 2018-CA-01427-SCT

Opinion Date: May 7, 2020
Judge: Beam
Areas of Law: Constitutional Law, Criminal Law

Leslie Galloway appealed the denial of his 2015 petition for post-conviction relief (PCR) pertaining to his 2007 guilty plea to carjacking, a conviction that was used as an aggravating circumstance in Galloway's 2010 capital-murder trial at which Galloway received a death sentence. Galloway claimed in the petition that his defense counsel Wendy Martin had an actual conflict of interest because, before becoming his defense counsel, Martin had served as an assistant district attorney in the same case, unbeknownst to Galloway. The trial court ruled that Galloway's PCR claim was time barred under Mississippi's Uniform Post-Conviction Collateral Relief Act (UPCCRA), having been filed more than seven years after Galloway's conviction for carjacking. The trial court alternatively found no merit to Galloway's PCR claim, time bar notwithstanding. Accordingly, the trial court denied Galloway's PCR petition. The Mississippi Supreme Court agreed with the trial court that Galloway's PCR claim was time barred under the UPCCRA. The Court also agreed there was no merit to Galloway's PCR claim.

Read Opinion Are you a lawyer? **Annotate this case**.

City of Missoula v. Zerbst

Court: Montana Supreme Court
Citation: 2020 MT 108
Opinion Date: May 5, 2020
Judge: Beth Baker
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court reversed Defendant's conviction for sexual assault, holding that the municipal court erred when it instructed the jury on a definition of "consent" from the 2017 sexual assault statute and not the applicable 2015 statute, and the erroneous jury instruction prejudicially affected Defendant's substantial rights. At trial, the court instructed the jury, over Defendant's objection, on the definition of consent contained in recent amendments to the sexual assault statute. On appeal, Defendant argued that the municipal court failed to apply the correct law when instructing the jury on the elements of the claimed offense. The district court denied the

appeal. The Supreme Court reversed, holding (1) the instructions, as a whole, did not fully and fairly instruct the jury on the law applicable to the case; and (2) Defendant's substantial due process right was prejudiced by the erroneous jury instruction.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Degarmo

Court: Nebraska Supreme Court
Citation: 305 Neb. 680
Opinion Date: May 1, 2020
Judge: Stacy
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed Defendant's conviction of driving under the influence, holding that Defendant consented to a chemical test of his urine and, therefore, the results of the urine test were admissible. A law enforcement officer stopped Defendant for an expired registration. Based on his observations, the officer, a certified drug recognition evaluation expert, administered field sobriety tests. The officer concluded that Defendant was under the influence of marijuana arrested Defendant for driving under the influence and then took him to a detoxification center. Thereafter, a chemical test of Defendant's urine confirmed the presence of marijuana. On appeal, Defendant challenged the admission of the results of the urine test. The Supreme Court affirmed, holding that Defendant voluntarily consented to the warrantless search of his urine, and therefore, the search fell within a recognized exception to the warrant requirement.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Holz

Court: New York Court of Appeals
Citation: 2020 NY Slip Op 02682
Opinion Date: May 7, 2020
Judge: Fahey
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Court of Appeals held that N.Y. Crim. Proc. Law (CPL) 710.70(2) grants a defendant the right to review of a suppression decision when the order related exclusively to a count that was satisfied by a guilty plea but was not one to which the defendant pleaded guilty. Defendant was charged with two counts of burglary in the second degree. The first count related to a laptop computer, and the second count related to jewelry. Defendant moved to suppress the jewelry, but Supreme Court denied the motion. Defendant then pleaded guilty to one count of burglary in the second degree as charged in the count pertaining to the theft of the laptop computer, in satisfaction of the count charging the burglary of jewelry. On appeal, Defendant argued that Supreme Court erred in denying his motion to suppress the jewelry. The Appellate Division affirmed, concluding that it was jurisdictionally precluded from reviewing the suppression order. The Court of Appeals reversed, holding (1) Defendant's right to appellate review of Supreme Court's suppression order was secured by CPL 710.70(2); and (2) because the Appellate Division did not reach the underlying suppression question the case must be remitted to the Appellate Division for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

People v. Maffei

Court: New York Court of Appeals
Citation: 2020 NY Slip Op 02680
Opinion Date: May 7, 2020
Judge: DiFiore
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Court of Appeals affirmed the order of the Appellate Division concluding on direct appeal that Defendant was not entitled to relief on his ineffective assistance of counsel claim, holding that Defendant, on this record, did not sustain his burden to establish that counsel was constitutionally ineffective. After a jury trial, Defendant was convicted of second-degree murder. On appeal, Defendant argued that his trial counsel's failure to challenge a prospective juror constituted ineffective assistance of counsel. The Appellate Division affirmed. The Court of Appeals affirmed, holding (1) the record was inadequate to review Defendant's ineffective assistance of counsel claim; and (2) the appropriate procedure for the litigation of Defendant's challenge to his counsel's performance was a N.Y. Crim. Proc.

Law 440.10 motion.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Bailey

Court: North Carolina Supreme Court
Docket: 360A19
Opinion Date: May 1, 2020
Judge: Davis
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court affirmed the decision of the court of appeals affirming the order of the trial court denying Defendant's motion to suppress evidence seized during the execution of a search warrant, holding that the warrant supported by probable cause. Defendant pled guilty to the offense of trafficking in cocaine while preserving his right to appeal the denial of his motion to suppress. On appeal, Defendant argued that the trial court erred in denying his motion to suppress because the facts contained in the affidavit were insufficient to establish probable cause to search his residence. The court of appeals affirmed. The Supreme Court affirmed, holding that the affidavit contained facts that were sufficient to provide a nexus between the residence and suspected criminal activity, and therefore, the warrant was supported by probable cause.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Ellis

Court: North Carolina Supreme Court
Docket: 340A19
Opinion Date: May 1, 2020
Judge: Robin E. Hudson
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court reversed the decision of the Court of Appeals affirming the trial court's denial of Defendant's motion to suppress evidence, holding that there was no reasonable suspicion to justify the law enforcement officer's stop when Defendant signaled with his middle finger from the passenger side window of a moving vehicle. While assisting a stranded

motorist, the officer turned his attention to another car traveling on the roadway, a white SUV. Defendant had his arm outside the passenger window and gestured with his middle finger, making an up-and-down motion. Believing that Defendant was committing the crime of disorderly conduct, the officer pursued and then stopped the SUV. At trial, Defendant moved to suppress the officer's testimony, arguing that there was no reasonable suspicion to justify the stop. The trial court denied the motion. Defendant pleaded guilty to resisting, delaying, or obstructing a public officer. The court of appeals affirmed the trial court's denial of Defendant's motion to suppress. The Supreme Court reversed, holding that the specific, articulable facts did not establish reasonable suspicion of the crime of disorderly conduct.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Hobbs
Court: North Carolina Supreme Court
Docket: 263PA18
Opinion Date: May 1, 2020
Judge: Earls
Areas of Law: Civil Rights, Constitutional Law, Criminal Law

The Supreme Court reversed Defendant's conviction, holding that the trial court clearly erred in ruling that Defendant failed to prove purposeful discrimination with respect to the State's use of peremptory challenges to strike three jurors without considering all of the evidence presented by Defendant. Defendant was found guilty of one count of first-degree murder and other crimes. On appeal, Defendant argued that the trial court erred by failing to grant three objections that he made under Batson v. Kentucky, 476 U.S. 79 (1986). The court of appeals affirmed Defendant's convictions. The Supreme Court reversed, holding (1) the court of appeals erred in its analysis of Defendant's Batson claims with respect to the three jurors; and (2) as to all three jurors, remand was required for reconsideration of whether Defendant proved purposeful discrimination in each case.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Mylett

Court: North Carolina Supreme Court
Docket: 6A19
Opinion Date: May 1, 2020
Judge: Earls
Areas of Law: Criminal Law

The Supreme Court reversed the decision of the court of appeals affirming the trial court's judgment convicting Defendant for conspiracy to commit harassment of a juror, holding that the trial court erred in denying Defendant's motion to dismiss the conspiracy charge for insufficient evidence. Defendant was convicted of conspiracy to commit harassment of a juror because of his actions at a courthouse following his twin brother's conviction for assault on a government official. On appeal, the court of appeals concluded that the trial court did not err in denying Defendant's motion to dismiss the conspiracy charge for insufficient evidence. The Supreme Court reversed, holding that the evidence in Defendant's trial was insufficient to raise anything more than mere conjecture that he had made an agreement with another person to threaten or intimidate a juror.

Read Opinion Are you a lawyer? **Annotate this case**.

Dodge v. North Dakota

Court: North Dakota Supreme Court
Citation: 2020 ND 100
Opinion Date: May 7, 2020
Judge: Gerald W. VandeWalle
Areas of Law: Constitutional Law, Criminal Law

Richard Dodge appealed from a district court order denying his application for post-conviction relief. Dodge was charged with five felonies and a misdemeanor in December 2015. Dodge was appointed counsel. In April 2016, Dodge’s counsel moved the court to withdraw because the attorney-client relationship was “irreparably broken and rendered unreasonably difficult.” The court granted the motion, and Dodge was appointed substitute counsel in May 2016. In July 2016, Dodge himself filed a “motion to dismiss counsel.” The court denied Dodge’s motion. Five months after the deadline for motions and plea agreements, Dodge's counsel sought to have Dodge submit to a psychiatric examination. This request was denied, the trial court

found no evidence, and the the court itself made no observations, that Dodge was incompetent to stand trial. After this denial, Dodge himself again moved to dismiss his trial counsel, and due to the allegations Dodge made in his motion, counsel moved to withdraw. The trial court denied both motions, and instead, required the attorney to appear as standby counsel and assist Dodge during trial if requested, but relieved him of any further obligations to consult with Dodge. The case proceeded to trial. At the beginning of trial, the court gave Dodge the option of representing himself or having his attorney represent him. Dodge chose to have his attorney represent him. Because his attorney had not prepared for trial and had no communication with Dodge since he moved to withdraw, Dodge's attorney asked for a brief recess to consult with Dodge. During the recess, a settlement was reached. Dodge agreed to enter Alford pleas on all counts, waived a presentence investigation, and agreed to be sentenced immediately after entering his pleas. Dodge was immediately sentenced following his guilty pleas, and thereafter sought post-conviction relief on grounds he was not competent to enter his pleas, and that he received ineffective assistance of trial counsel. After review, the North Dakota Supreme Court concluded the district court's finding that Dodge was competent when he entered his pleas was not clearly erroneous, and disposed of his claim of ineffective assistance of counsel.

Read Opinion Are you a lawyer? **Annotate this case**.

Hewitt v. NDDOT

Court: North Dakota Supreme Court
Citation: 2020 ND 102
Opinion Date: May 7, 2020
Judge: Lisa K. Fair McEvers
Areas of Law: Criminal Law, Government & Administrative Law

Larry Hewitt appealed a district court judgment affirming the North Dakota Department of Transportation's revocation of his driving privileges. Hewitt claimed the Department's hearing file was improperly admitted at the administrative hearing. After review, the North Dakota Supreme Court affirmed, concluding the hearing file was properly admitted as a self-authenticating copy of an official record.

Read Opinion Are you a lawyer? **Annotate this case**.

Kastet v. NDDOT

Court: North Dakota Supreme Court
Citation: 2020 ND 91
Opinion Date: May 7, 2020
Judge: Daniel J. Crothers
Areas of Law: Criminal Law, Government & Administrative Law

The North Dakota Department of Transportation (Department) appealed the district court's reversing a hearing officer's decision suspending Holden Kastet's driving privileges for 365 days. The Department argued the hearing officer did not abuse his discretion in admitting the chemical breath test, and State Highway Patrol Trooper King scrupulously complied with the approved method for testing Kastet's breath on the Intoxilyzer 8000. After review, the North Dakota Supreme Court concurred with the Department and reversed the district court judgment. The matter was remanded with instructions to reinstate the hearing officer's decision.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Dahl

Court: North Dakota Supreme Court
Citation: 2020 ND 87
Opinion Date: May 7, 2020
Judge: Jerod E. Tufte
Areas of Law: Constitutional Law, Criminal Law

The State of North Dakota appealed a district court order denying its motion to resume prosecution against Matthew Dahl and dismissing the case. In December 2014, the State charged Dahl with two counts of theft. Dahl did not appear on the charges until he was arrested on a bench warrant in February 2017. In mid-April 2017, the State mailed Dahl a pretrial diversion agreement. Dahl signed and returned the notarized agreement dated May 3, 2017. On May 9, 2017, the state's attorney signed and filed the agreement with the district court, and the court approved the agreement the same day. Under the agreement, the State agreed to suspend prosecution for "two

years from the date of execution" conditioned on Dahl's timely payment of restitution. Dahl failed to make minimum monthly restitution payments. On June 6, 2019, the State moved to resume prosecution, alleging Dahl violated the pretrial diversion agreement by his non-payment. The district court held a hearing on the State's motion in August 2019. The court concluded the pretrial agreement was executed when Dahl signed it on May 3, 2017. The court then denied the State's motion to resume prosecution as untimely under N.D.R.Crim.P. 32.2(d)(2), and dismissed the complaint against Dahl. After review, the North Dakota Supreme Court reversed, concluding the district court erred in determining the State's motion was untimely, and remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Foster

Court: North Dakota Supreme Court
Citation: 2020 ND 85
Opinion Date: May 7, 2020
Judge: Jon J. Jensen
Areas of Law: Constitutional Law, Criminal Law

Akeem Foster was convicted by jury of Terrorizing and Carrying a Concealed Weapon. Foster contended on appeal he was denied a fair trial because he was asked during cross-examination if other witnesses were lying and because the prosecutor expressed personal beliefs about the evidence during closing arguments. Foster also argued there was insufficient evidence to convict him of either charge. After review, the North Dakota Supreme Court affirmed Foster's conviction for Carrying a Concealed Weapon, but reversed his conviction for Terrorizing. The Court found Foster was improperly asked to provide an opinion on the veracity and credibility of the State's witnesses. The improper questioning was prejudicial and denied Foster a fair trial on the terrorizing charge.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Kolstad

Court: North Dakota Supreme Court

Citation: 2020 ND 97
Opinion Date: May 7, 2020
Judge: Gerald W. VandeWalle
Areas of Law: Constitutional Law, Criminal Law

In December 2018, Officer Nelson of the University of North Dakota Police Department conducted a traffic stop of Stanley Kolstad for suspicion of driving under the influence. Kolstad performed field sobriety tests and a preliminary breath test (PBT). Prior to performing the PBT, Kolstad informed Nelson that he had asthma. Nelson testified he was unable to obtain a PBT result because Kolstad was filling his cheeks with air while performing the test. Kolstad was arrested for DUI and refusing to submit to a chemical test. Kolstad was transported to the UND police station to be given an Intoxilyzer breath test. Prior to the Intoxilyzer test, Nelson read Kolstad the implied consent advisory. But, because Nelson was not a certified operator of the Intoxilyzer machine, Officer Waltz conducted the test. Prior to the test, Kolstad informed Waltz he had asthma. The Intoxilyzer test results were deficient. Waltz testified Kolstad was not providing enough air for the test machine to provide a valid result. Kolstad was charged with driving under the influence and refusing to submit to a chemical test. Kolstad's counsel made a discovery request to the State seeking copies of any audio or video recordings taken by police officers. Kolstad's counsel also requested the State inform him whether any sound or video recordings taken of Kolstad were subsequently "altered, edited, destroyed, or discarded." The State provided Kolstad's counsel with dash camera footage from Nelson's police car that had been taken at the scene of the arrest, but the State did not provide any body camera footage from either Nelson or Waltz. Upon learning that Waltz's body camera footage was successfully uploaded to UND servers, Kolstad's counsel moved to dismiss the case because the State did not provide any body camera footage in discovery as requested. The district court ultimately dismissed the refusal to submit to a chemical breath test charge as a sanction for failing to provide the body camera footage. The State appealed, arguing the alleged discovery violation did not rise to a constitutional violation of Kolstad's due process rights, and the district court abused its discretion in dismissing the refusal charge. Kolstad argued the district court's order dismissing the refusal charge was not appealable, and if it was, the court did not abuse its discretion in dismissing the charge. The North Dakota Supreme Court concluded there was nothing in the record to indicate the district court adequately considered an

alternative or less severe sanction to dismissal, and by not considering a less severe sanction, the trial court erred. The district court's order dismissing the refusal charge was reversed, and the matter remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Michel

Court: North Dakota Supreme Court
Citation: 2020 ND 101
Opinion Date: May 7, 2020
Judge: Jerod E. Tufte
Areas of Law: Constitutional Law, Criminal Law

Kevin Michel was convicted by jury of knowingly receiving stolen property. Jamestown Police began investigating theft of tires from Northwest Tire in October 2017. About ten months later, Thomas Melland and Andrew Heckelsmiller became suspects in the investigation. Heckelsmiller told police he had sold stolen tires to Michel. In August 2018, Detective LeRoy Gross spoke with Michel about the stolen tires. Michel acknowledged he had bought tires from Heckelsmiller and Melland. Michel also told Detective Gross he stopped buying tires from Heckelsmiller and Melland after seeing a Facebook post from Northwest Tire offering a $500 reward for information regarding stolen tires. Detective Gross told Michel, "There's going to be a lot of restitution these two boys are going to have to come up with unless we can get some tires back." Michel said he had sold several of the tires but still had some of them. Michel turned over seven new tires to Detective Gross. Representatives from Northwest Tire and J&L Service identified the tires as some of those stolen from their shops. During the jury's deliberations, the jury submitted a note with written questions to the court. Michel argued on appeal the district court erred by not specifically answering the jury's questions and instead referring them to the existing jury instructions. After review, the North Dakota Supreme Court affirmed the criminal judgment, except as to the award of restitution. The award was reversed because the district court awarded more than what was required to make the victims whole. The matter was remanded for a redetermination of restitution.

Read Opinion Are you a lawyer? **Annotate this case**.

North Dakota v. Wayland

Court: North Dakota Supreme Court
Citation: 2020 ND 106
Opinion Date: May 7, 2020
Judge: Jon J. Jensen
Areas of Law: Constitutional Law, Criminal Law

Joey Wayland appealed after he was convicted by jury of Theft of Property and Possession of Drug Paraphernalia. Wayland contended his case should have been dismissed because his right to a speedy trial was violated by a continuance of his trial from March 11, 2019 to April 8, 2019. Wayland also contended the district court violated his right to remain silent by ordering him to submit to a mental health evaluation. Finding no reversible error, the North Dakota Supreme Court affirmed.

Read Opinion Are you a lawyer? **Annotate this case**.

Schwindt v. Sorel

Court: North Dakota Supreme Court
Citation: 2020 ND 92
Opinion Date: May 7, 2020
Judge: Lisa K. Fair McEvers
Areas of Law: Constitutional Law, Criminal Law, Government & Administrative Law

Gregory Schwindt appealed a district court judgment affirming a Department of Transportation hearing officer's revocation of his driving privileges for 180 days. Schwindt argued North Dakota's implied consent and refusal laws were unconstitutional, the hearing officer erred by considering the results of the horizontal gaze nystagmus (HGN) test, and the hearing officer erred in finding he refused to take a chemical test. After review, the North Dakota Supreme Court concluded the hearing officer's findings of fact were supported by a preponderance of the evidence, the conclusions of law were sustained by the findings of fact, and the decision to revoke Schwindt's driving privileges was in accordance with the law.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. McDougald v. Greene

Court: Supreme Court of Ohio
Citation: 2020-Ohio-2782
Opinion Date: May 6, 2020
Judge: Per Curiam
Areas of Law: Criminal Law

The Supreme Court denied a writ of mandamus sought by Relator to compel Respondent, the public-records custodian at the Southern Ohio Correctional Facility (SOCF), to provide Relator with three public records and to pay Relator statutory damages and court costs associated with this litigation, holding that Relator was not entitled to either a writ of mandamus nor statutory damages. When Relator was an inmate at SOCF he submitted a public-records request to Respondent seeking three documents. Respondent provided one of the three documents. Relator then filed a complaint for a writ of mandamus seeking an order compelling Respondent to provide the two documents and to pay statutory damages and court costs associated with this litigation. The Supreme Court denied the writ of mandamus on the merits, holding that Respondent's response to Relator fully satisfied Respondent's obligations under Ohio Rev. Code 149.43, and therefore, Relator was not entitled a writ of mandamus, and there was no basis to award statutory damages.

Read Opinion Are you a lawyer? **Annotate this case**.

State ex rel. Parker Bey v. Byrd

Court: Supreme Court of Ohio
Citation: 2020-Ohio-2766
Opinion Date: May 5, 2020
Judge: Maureen O'Connor
Areas of Law: Criminal Law

The Supreme Court affirmed in part and reversed in part the judgment of the court of appeals denying Appellant's complaint for a writ of mandamus to compel the Cuyahoga County Clerk of Courts to produce various court records and denying the clerk's request that Appellant be declared a vexatious litigator, holding that the court of appeals erred in denying Appellant's complaint on the grounds that he did not invoke the Rules of

Superintendence as the basis for his request. Appellant sought copies of journal entries from his criminal case and a copy of the clerk of courts' records-retention schedule. The clerk largely denied the request. Appellant then filed a complaint for a writ of mandamus. The court of appeals denied Appellant's request for mandamus relief, concluding that the clerk had no clear legal duty to provide the requested records. The Supreme Court reversed, holding (1) this action to compel the production of journal entries from a 1995 case was properly brought under the Public Records Act; and (2) this Court declines to impose sanctions on Appellant or to declare him a vexatious litigator.

Read Opinion Are you a lawyer? **Annotate this case**.

State v. Dangler

Court: Supreme Court of Ohio
Citation: 2020-Ohio-2765
Opinion Date: May 5, 2020
Judge: DeWine
Areas of Law: Criminal Law

The Supreme Court reversed the judgment of the court of appeals vacating Defendant's conviction and sentence and reinstated the trial court's acceptance of Defendant's plea of no contest to sexual battery, holding that the trial court did not completely fail to comply with Crim.R.11(C)(2)(a), and there was nothing in the record to support a conclusion that Defendant would not have entered his plea had the trial court been more detailed in its explanation. On appeal, Defendant sought to vacate his plea of no contest, arguing that his plea was invalid because the trial court erred by not explaining more fully the obligations and restrictions that went with his status as a sex offender, in violation of Crim. R. 11(C)(2)(a). The court of appeals vacated the conviction without requiring Defendant to show prejudice, concluding that the trial court had completely failed to comply with Crim. R. 11(C)(2)(a). The Supreme Court reversed, holding (1) the trial court did not completely failed to comply with Crim R. 11(C)(2)(a)'s maximum-penalty-advisement requirement; and (2) because Defendant did not establish prejudice, he was not entitled to have his no-contest plea vacated for a failure to comply with Crim.R. 11(C).

Read Opinion Are you a lawyer? **Annotate this case**.

Oregon v. Haji

Court: Oregon Supreme Court
Docket: S066254
Opinion Date: May 7, 2020
Judge: Nakamoto
Areas of Law: Constitutional Law, Criminal Law

After a grand jury issued an indictment charging defendant Hanad Ali Haji with multiple offenses, the district attorney determined that the indictment could be challenged by demurrer because the basis for joining those offenses was not expressly alleged. Instead of seeking another indictment from the grand jury, the district attorney obtained leave from the trial court to amend the indictment by adding allegations specifying the statutory basis for joinder, without adding factual allegations about the crimes. Defendant was convicted on some of the charges at trial, and the Court of Appeals affirmed. The issue this case presented for the Oregon Supreme Court's review centered on whether the district attorney could add allegations specifying the statutory basis for joinder of multiple offenses to an indictment instead of resubmitting the case to the grand jury. The Supreme Court determined that neither the statute permitting joinder of multiple offenses in a single indictment nor Article VII (Amended), section 5(6), of the Oregon Constitution precluded a district attorney, with approval of the trial court, from amending an indictment to add allegations specifying the statutory basis for joinder of multiple offenses. The Supreme Court affirmed the decision of the Court of Appeals, based in part on different reasoning, and affirmed the judgment of the circuit court.

Read Opinion Are you a lawyer? **Annotate this case**.

South Carolina v. Durant

Court: South Carolina Supreme Court
Docket: 27964
Opinion Date: May 6, 2020
Judge: Kaye Gorenflo Hearn
Areas of Law: Constitutional Law, Criminal Law

Appellant Larry Durant was convicted of second-degree criminal sexual conduct (CSC) for sexually abusing a teenage girl in his church office where he served as the pastor. Durant contended the trial court improperly permitted the State to introduce evidence of prior sexual abuse allegations as evidence of a common scheme or plan under Rule 404(b), SCRE, and that the State committed a "Brady" violation by failing to accurately disclose the criminal history of its witness. After review, the South Carolina Supreme Court affirmed the admissibility of the girls' testimony. "[W]hile the State failed to disclose the criminal background information of its witness, we find this information was not material." The Court found Durant exercised his position of trust, authority, and spiritual leadership to hold private prayer meetings with teen girls who had grown up in his church. He told them he was praying for their health and good fortune, and represented that part of this process was touching them sexually and having intercourse. Durant then warned the girls of misfortune if they refused or told anyone. Moreover, he used scripture as a means of grooming the children into performing sex acts. "These facts demonstrate the requisite logical connection between the prior acts of sexual abuse and the one forming the basis of the crime charged." The Court therefore affirmed Durant's conviction.

Read Opinion Are you a lawyer? **Annotate this case**.

South Carolina v. Perry

Court: South Carolina Supreme Court
Docket: 27963
Opinion Date: May 6, 2020
Judge: Few
Areas of Law: Constitutional Law, Criminal Law

Petitioner Wallace Perry was convicted on two counts of criminal sexual conduct (CSC) with a minor in the first degree and two counts of CSC with a minor in the second degree for sexually assaulting two of his biological daughters. Prior to Perry's trial, the State made a motion to admit the testimony of Perry's stepdaughter from an earlier marriage that Perry sexually assaulted her twenty-two to twenty-seven years earlier. The State argued the trial court should not exclude the stepdaughter's testimony under Rule 404(b) of the South Carolina Rules of Evidence because it fit the

"common scheme or plan" exception. Perry objected to this testimony. The trial court initially reserved ruling on the issue, but later indicated it was inclined to allow the stepdaughter to testify. The jury convicted Perry on all counts, and the trial court sentenced him to thirty years in prison. The court of appeals affirmed. The South Carolina Supreme Court determined it was not enough to meet the "logical connection" standard for admission of other crimes under the common scheme or plan exception to Rule 404(b) that the defendant previously committed the same crime. "When evidence of other crimes is admitted based solely on the similarity of a previous crime, the evidence serves only the purpose prohibited by Rule 404(b), and allows the jury to convict the defendant on the improper inference of propensity that because he did it before, he must have done it again. ...The common scheme or plan exception demands more." The Supreme Court held State must show a logical connection between the other crime and the crime charged such that the evidence of other crimes "reasonably tends to prove a material fact in issue." The State must also convince the trial court that the probative force of the evidence when used for this legitimate purpose is not substantially outweighed by the danger of unfair prejudice from the inherent tendency of the evidence to show the defendant's propensity to commit similar crimes. In this case, the State did not meet its burden. Conviction was reversed and the matter remanded for a new trial.

Read Opinion Are you a lawyer? **Annotate this case**.

South Carolina v. Quinn

Court: South Carolina Supreme Court
Docket: 27966
Opinion Date: May 6, 2020
Judge: Kaye Gorenflo Hearn
Areas of Law: Constitutional Law, Criminal Law, White Collar Crime

Respondent Rick Quinn, Jr. was a former member of the South Carolina House of Representatives, representing constituents in Richland and Lexington counties from 1989-2004 and 2010-2017 and serving as House Majority Leader from 1999- 2004. He owned and operated a mail business called Mail Marketing Strategies (MMS) in Columbia, while his father owned and operated a political consulting firm, Richard Quinn & Associates (RQ&A). In 2014, Attorney General Alan Wilson designated First Circuit

Solicitor David Pascoe as special prosecutor to conduct a State grand jury investigation into alleged public corruption committed by current and former members of the South Carolina General Assembly. This case arose from a prior state grand jury investigation of former House Speaker Bobby Harrell, which resulted in six counts of misusing campaign funds, to which he pleaded guilty. During the course of the investigation into Speaker Harrell, SLED uncovered potentially criminal conduct by Representative Jimmy Merrill and Representative Rick Quinn, and a second grand jury investigation was initiated to investigate the conduct of these individuals. The investigation focused on Quinn's practice of using his office as House Majority Leader and leader of the House Republican Caucus to direct mailing and political services to his family's businesses. Quinn only admitted to a limited set of facts supporting the indictment. Believing the plea lacked a sufficient basis, the State moved to vacate Quinn's guilty plea, reconsider the sentence, and for the trial court's recusal. The State appealed the order denying its motions. After review, the South Carolina Supreme Court determined that the State could not appeal the guilty plea, the trial court did not abuse its discretion in sentencing, and there was no evidence of judicial bias or prejudice requiring the court to recuse itself. Therefore, the Court dismissed the State's appeal of the guilty plea, and affirmed as to all other issues.

Read Opinion Are you a lawyer? **Annotate this case**.

Texas v. Arellano

Court: Texas Court of Criminal Appeals
Docket: PD-0287-19
Opinion Date: May 6, 2020
Judge: Slaughter
Areas of Law: Constitutional Law, Criminal Law

After Appellee Cesar Ramiro Arellano was arrested for driving while intoxicated, the arresting officer, Phillip Garcia, prepared a probable cause affidavit to support a search warrant for a blood draw. Officer Garcia submitted his sworn affidavit to the on-duty magistrate. Using a cursive signature, the magistrate signed the blank signature line of a form search warrant authorizing the search and seizure of Appellee's blood. Below the signature line appeared the words, "Magistrate, Victoria County, Texas."

Aside from the cursive signature, the magistrate's name was not typed or handwritten anywhere on the warrant. Upon execution of the search warrant, Appellee was charged with DWI. In the trial court, Appellee filed a motion to suppress all evidence stemming from the blood draw. At the pretrial suppression hearing, Appellee argued that the search warrant to obtain the blood specimen was facially invalid because the magistrate's signature was illegible in violation of the requirements of Code of Criminal Procedure Article 18.04(5). The trial court agreed, the court of appeals concurred, and the evidence was suppressed because of the illegible signature. The Texas Court of Criminal Appeals disagreed with both lower courts, finding the court of appeals erred in holding that reliance on the statutory good-faith exception was automatically precluded based on an illegible magistrate's signature in violation of Code of Criminal Procedure Article 18.04(5). Because the remaining issues in the case were not properly addressed by the court of appeals, judgment was vacated and the matter remanded for further proceedings.

Read Opinion Are you a lawyer? **Annotate this case**.

About Justia Opinion Summaries

Justia Weekly Opinion Summaries is a free service, with 63 different newsletters, each covering a different practice area.

Justia also provides 68 daily jurisdictional newsletters, covering every federal appellate court and the highest courts of all US states.

All daily and weekly Justia newsletters are free. Subscribe or modify your newsletter subscription preferences at daily.justia.com.

You may freely redistribute this email in whole.

About Justia

Justia is an online platform that provides the community with open access to the law, legal information, and lawyers.



Unsubscribe From This Newsletter

or unsubscribe from all Justia newsletters immediately **here.**



Justia | 1380 Pear Ave #2B, Mountain View, CA 94043

From: Sony Electronics, Professional
To: Wilcox, Christopher (POL)
Subject: License Plate Recognition with a Twist of A.I. Intelligent LPR as a Force Multiplier for Law Enforcement Confirmation
Date: Tuesday, July 28, 2020 9:10:04 AM

Thank you for registering for "License Plate Recognition with a Twist of A.I. Intelligent LPR as a Force Multiplier for Law Enforcement".

Utility, Inc. in collaboration with Sony Imaging Products & Solutions, Inc. has developed a Smart Automated License Plate Recognition system (Smart ALPR). Unlike any other ALPR system, this one is powered by an A.I. Engine. With the use of the RocketIoT communications system, the Smart ALPR system can gather real-time information at the edge to enhance alerting capabilities.

Key Points attendees will learn:

· Smart ALPR - What it is & How it is different

· Real-Time Triple Alerting Capabilities

· Benefits of Injecting Local Plate Data

· Historical Data Features for Investigative Purposes

· Added Advantages that ALPR brings to the Agency

· Importance of Sony and Utility's Strategic Partnership

Please send your questions, comments and feedback to: pro.info@sony.com

How To Join The Webinar

Thu, Jul 30, 2020 2:30 PM - 3:30 PM EDT

Add to Calendar: Outlook® Calendar | Google Calendar™ | iCal®

1. Click the link to join the webinar at the specified time and date:

Join Webinar

Note: This link should not be shared with others; it is unique to you.

Before joining, be sure to check system requirements to avoid any connection issues.

2. Choose one of the following audio options:

TO USE YOUR COMPUTER'S AUDIO:
When the webinar begins, you will be connected to audio using your computer's microphone and speakers (VoIP). A headset is recommended.

--OR--

TO USE YOUR TELEPHONE:
If you prefer to use your phone, you must select "Use Telephone" after joining the webinar and call in using the numbers below.
United States: +1 (631) 992-3221
Access Code: 254-026-953
Audio PIN: Shown after joining the webinar

Webinar ID: 730-928-571

To Cancel this Registration

If you can't attend this webinar, you may cancel your registration at any time.



You are receiving this email because you registered for this webinar. Your email address and personal information will be used by the Webinar organizer to communicate with you about this event and their other services. To review the organizer's privacy policy or stop receiving their communications, please contact the organizer directly.

Cancel registration | Stop GoToWebinar emails | Report spam

This email is sent on behalf of the organizer by GoToWebinar.
7414 Hollister Avenue | Goleta, CA 93117 Privacy Policy | Anti-spam Policy | www.gotowebinar.com ©2020 LogMeIn, Inc.

From: WatchGuard
To: McCarthy, Steven (POL)
Subject: License Plate Recognition with WatchGuard In-Car System
Date: Thursday, October 1, 2020 10:18:40 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Small on Grey.jpg

ALPR-in-car-1with WG Logos-blur-email-600

License Plate Recognition with WatchGuard 4RE In-Car Video System

The WatchGuard 4RE Mobile ALPR Solution harnesses the power of the industry-leading WatchGuard 4RE in-car video system and high-definition cameras to detect and match vehicle license plates of interest stored in a database of over 20 billion detections.

Increase Officer Safety - Help distinguish between a routine traffic infraction stop and something potentially more serious.

Proactively Interrupt Crimes - Alert officers to vehicles of interest in real-time, potentially interrupting a string of crime.

Deliver Leads to Solve More Cases - Use historical data to determine a vehicle's proximity to crime scenes, providing leads crucial to an investigation.

Discover the WatchGuard 4RE Mobile ALPR Solution

WatchGuard Video
415 E Exchange Parkway
Allen, TX 75002
USA

You received this email because you are subscribed to Products from WatchGuard Video.

Update your email preferences to choose the types of emails you receive.

Unsubscribe from all future emails

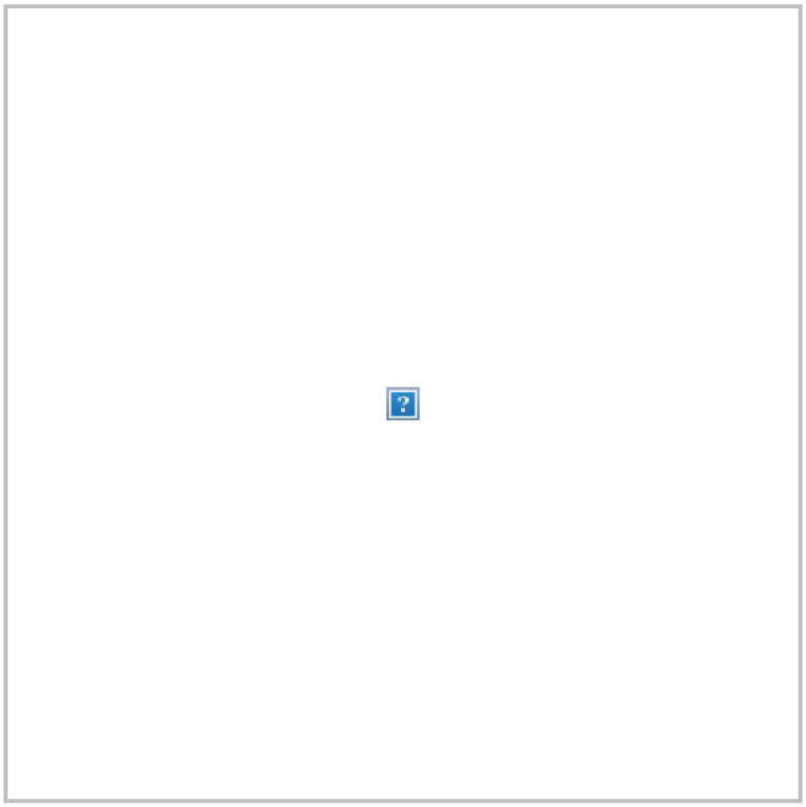
From: Evidence Technology Magazine
To: Elian, Albert (POL)
Subject: Marijuana Analysis in a New Frontier, and More
Date: Tuesday, February 18, 2020 6:34:34 PM

Here's your February issue of ETM's Laboratory News

View this email in your browser



Evidence Technology Magazine • Laboratory News • February 2020



Advertisement

Education & Training

Webinar: Marijuana Analysis in a New Frontier

February 18, 2020 — As part of the continuing ASCLD Train the Director Series, presented by the NIJ's Forensic Technology Center of Excellence, a webinar on March 5 will examine the legal landscape of marijuana and hemp in two specific jurisdictions: one with legalized marijuana and one without. The analytical schemes used in both laboratories will be presented.

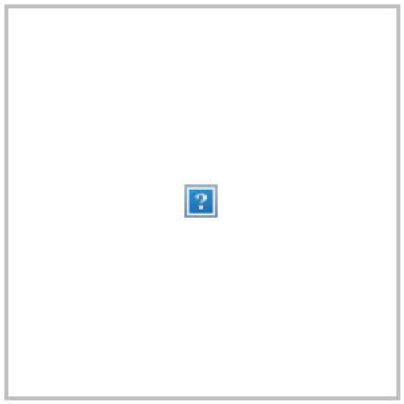
>Read More

DNA Analysis

NY District Court Denies Motion to Preclude DNA Software Analysis

February 6, 2020 — A U.S. District Court for the Eastern District of New York has denied a defendant's motion to preclude expert testimony regarding the results of a DNA analysis produced by using STRmix – forensic software used to resolve mixed DNA profiles.

>Read More



NEW ISSUE! Read the January-February Issue of ETM

Funding Opportunities

Anti-Heroin Task Force Program

February 4, 2020 — The COPS Office Anti-Heroin Task Force (AHTF) Program is a competitive grant solicitation, open to state law enforcement agencies with multijurisdictional reach and interdisciplinary team (e.g. task force) structures, in states with high per capita rates of primary treatment admissions.

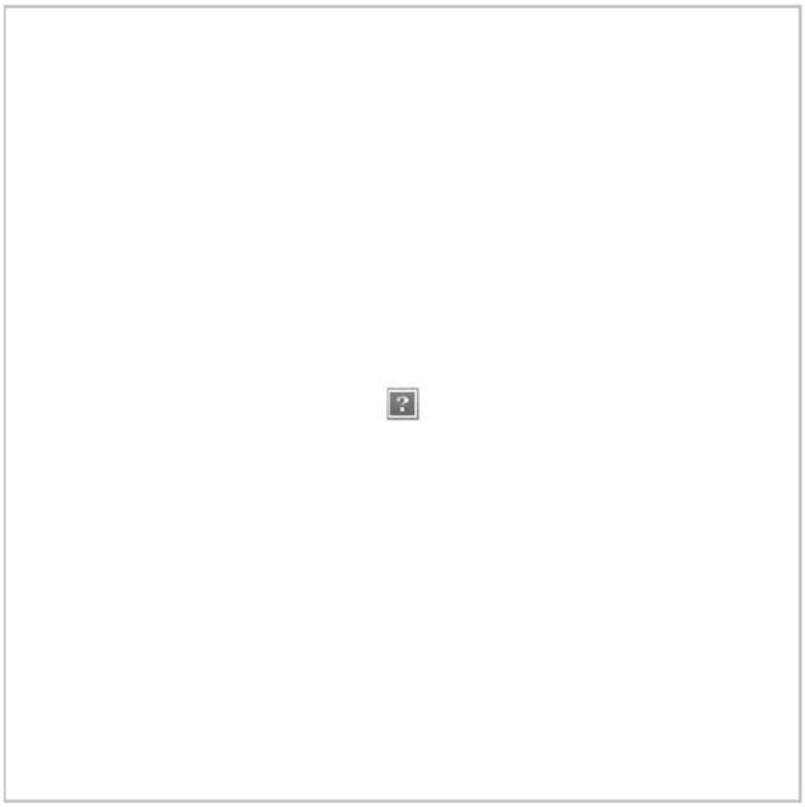
>Read More

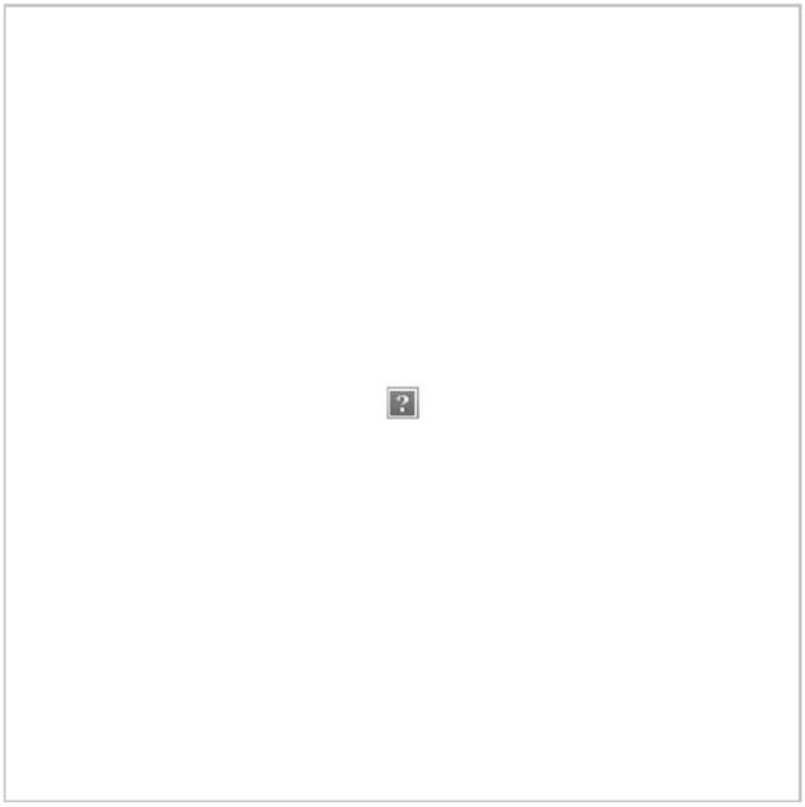
Anti-Methamphetamine Program

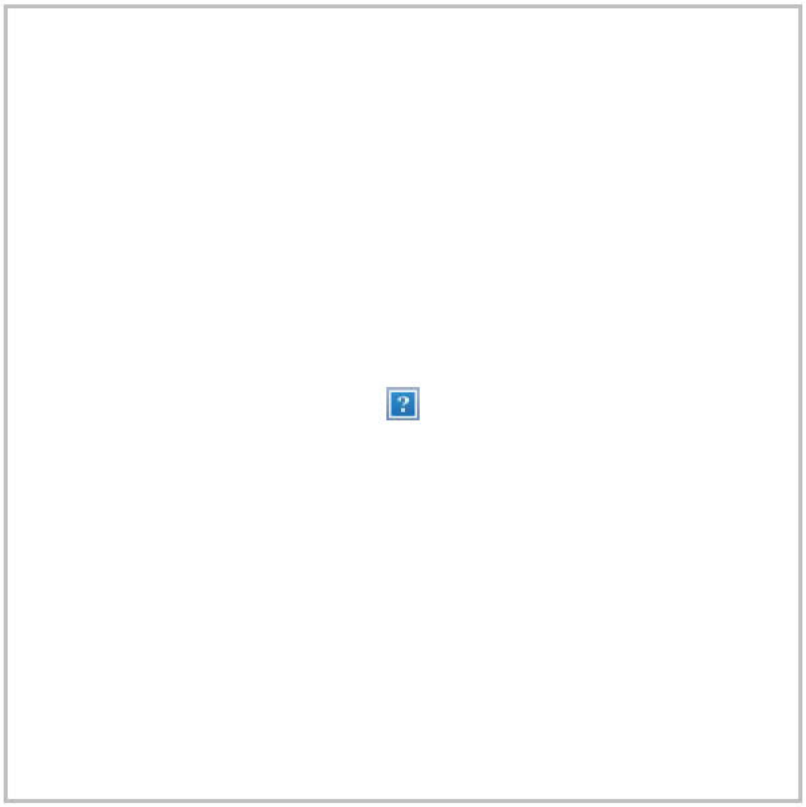
February 18, 2020 — The COPS Anti-Methamphetamine Program (CAMP) is a competitive grant solicitation, open to state law enforcement agencies with multijurisdictional reach and interdisciplinary team (e.g. task force) structures, in states with high seizures of precursor chemicals, finished methamphetamine, laboratories, and laboratory dump seizures.

>Read More

Upcoming Conferences







Vendor News

Cloud Explorer Extracts Google Fit Data

February 18, 2020 — ElcomSoft Co. Ltd. recently announced Elcomsoft Cloud Explorer 2.30, which adds support for health and activity information collected by the Android Google Fit app and synchronized to the user's Google Account. >Read More

Motorola Solutions Adds New Analytics to In-Car Video System

February 13, 2020 — Motorola Solutions recently announced the availability of new video security and analytics capabilities for law enforcement. Automated license plate recognition (ALPR) is now part of the WatchGuard 4RE® in-car video system. >Read More

New Touch Screen Repeating Pipette with Advanced Features

February 13, 2020 — The BRAND® HandyStep® touch S repeating pipette has advanced pipetting features for versatility. In addition to standard pipetting, dispensing, auto dispensing and a proprietary "learn" function, advanced modes include sequential dispensing of different volumes, multi-aspiration of different volumes and a titration mode. >Read More

Companies Partner to Deliver Hybrid Video Management Solution

February 11, 2020 — Arcules, a company focusing on integrated video and access control cloud services, recently announced the commercial availability of the Arcules-XProtect

Hybrid™ VMS Solution in North America and Europe. >Read More

New Desktop 3D Scanner for Tiny Objects

February 11, 2020 — Exact Metrology recently announced the availability of the new Artec Micro 3D scanner. The Artec Micro, an automated, metrology-grade desktop 3D scanner is Artec 3D's most accurate 3D scanner to date, and is used for scanning tiny mechanical parts, such as engine valves or connectors, for inspection and reverse engineering, as well as other small objects for industries such as heritage preservation, dentistry, and medical. >Read More

Subscribe to Evidence Technology Magazine

Open Source Web Intelligence Company Opens Office in U.S.

January 22, 2020 — Cobwebs Technologies — the specialized open-source web intelligence company that supports national security agencies, law enforcement agencies, and corporate security departments in rapidly identifying and locating malicious threat actors on the open, deep, and dark webs — is entering the American market with an office in New York City. With little more than a click, Cobwebs makes it highly difficult for terrorists, active shooters, hackers, and other criminal entities to hide, plan, communicate, or ply their nefarious trade in any part of the online world. >Read More

Nearly Half of First Responders Under-Equipped to Handle Extended Power Outage, Report Finds

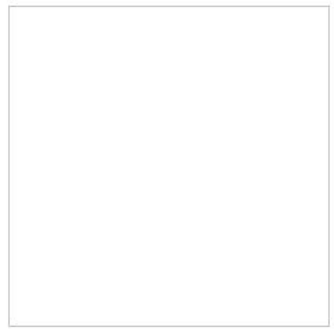
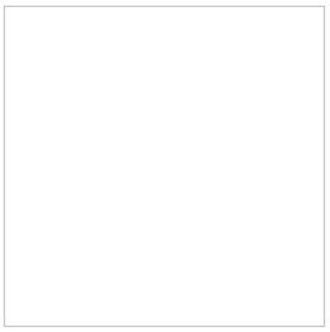
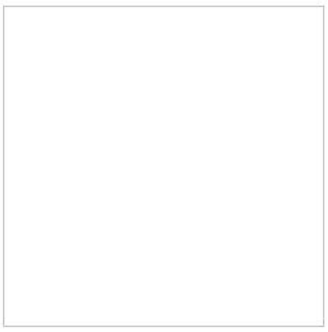
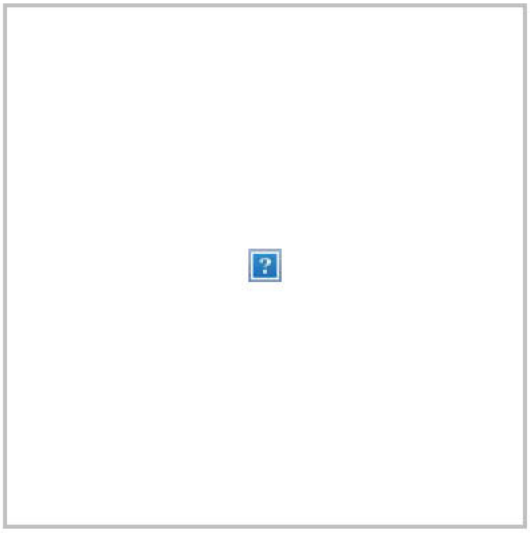
January 23, 2020 — IWCE, an event for the critical communications industry, surveyed more than 597 first responders and public safety professionals to benchmark the current technologies they are using and to understand current technological challenges within the industry. >Read More

Environmentally Friendly Alternative to Canned Air

January 21, 2020 — Canless Air System is a highly effective and environmentally friendly alternative to traditional canned air cleaning products. The line of Hurricane dusters is nontoxic, rechargeable, and provides more power than any canned air competitor. >Read More

---

There's more in the ETM Digital Edition:


Website LinkedIn Twitter Facebook Subscribe

Copyright © 2020 Wordsmith Publishing, All rights reserved.
You are receiving this eNewsletter because you subscribed to Evidence Technology Magazine. You can change your communication preferences at any time by following the links below. Thank you for your readership!

Our mailing address is:
Wordsmith Publishing
PO Box 555
Kearney, MO 64060

Add us to your address book

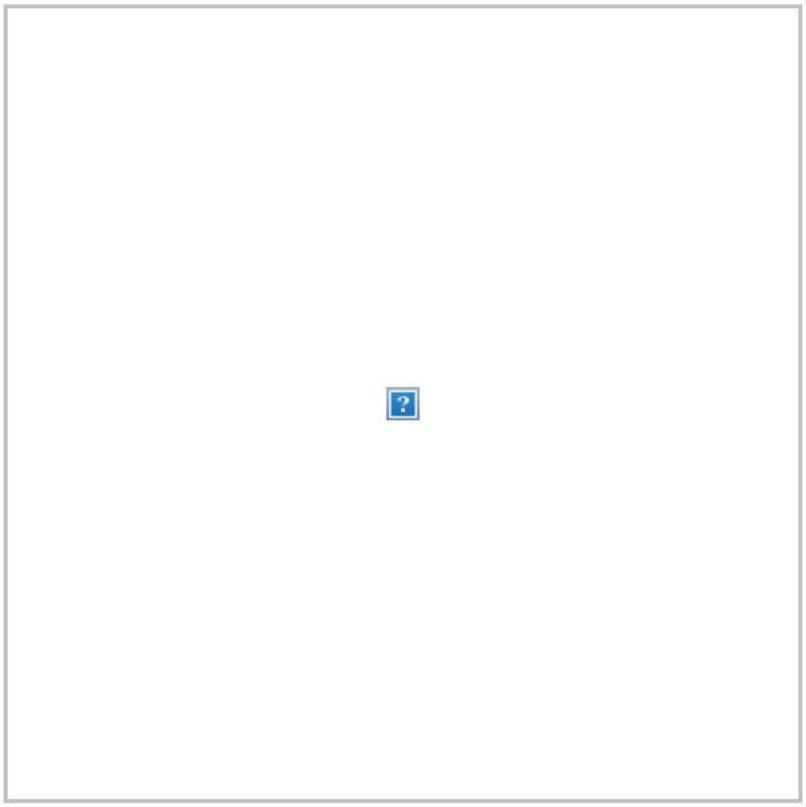
unsubscribe from this list update subscription preferences

From: Evidence Technology Magazine
To: Menendez, Sherri (POL)
Subject: Marijuana Analysis in a New Frontier, and More
Date: Tuesday, February 18, 2020 6:34:29 PM

Here's your February issue of ETM's Laboratory News

View this email in your browser





Advertisement

Education & Training

Webinar: Marijuana Analysis in a New Frontier

February 18, 2020 — As part of the continuing ASCLD Train the Director Series, presented by the NIJ's Forensic Technology Center of Excellence, a webinar on March 5 will examine the legal landscape of marijuana and hemp in two specific jurisdictions: one with legalized marijuana and one without. The analytical schemes used in both laboratories will be presented.

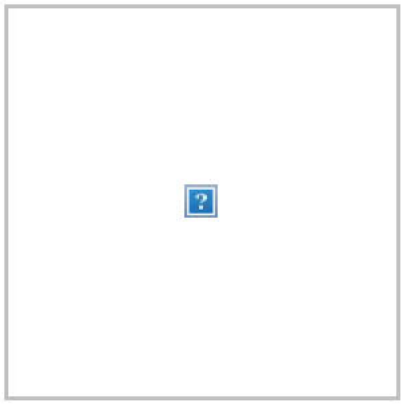
>Read More

DNA Analysis

NY District Court Denies Motion to Preclude DNA Software Analysis

February 6, 2020 — A U.S. District Court for the Eastern District of New York has denied a defendant's motion to preclude expert testimony regarding the results of a DNA analysis produced by using STRmix – forensic software used to resolve mixed DNA profiles.

>Read More



NEW ISSUE! Read the January-February Issue of ETM

Funding Opportunities

Anti-Heroin Task Force Program

February 4, 2020 — The COPS Office Anti-Heroin Task Force (AHTF) Program is a competitive grant solicitation, open to state law enforcement agencies with multijurisdictional reach and interdisciplinary team (e.g. task force) structures, in states with high per capita rates of primary treatment admissions.

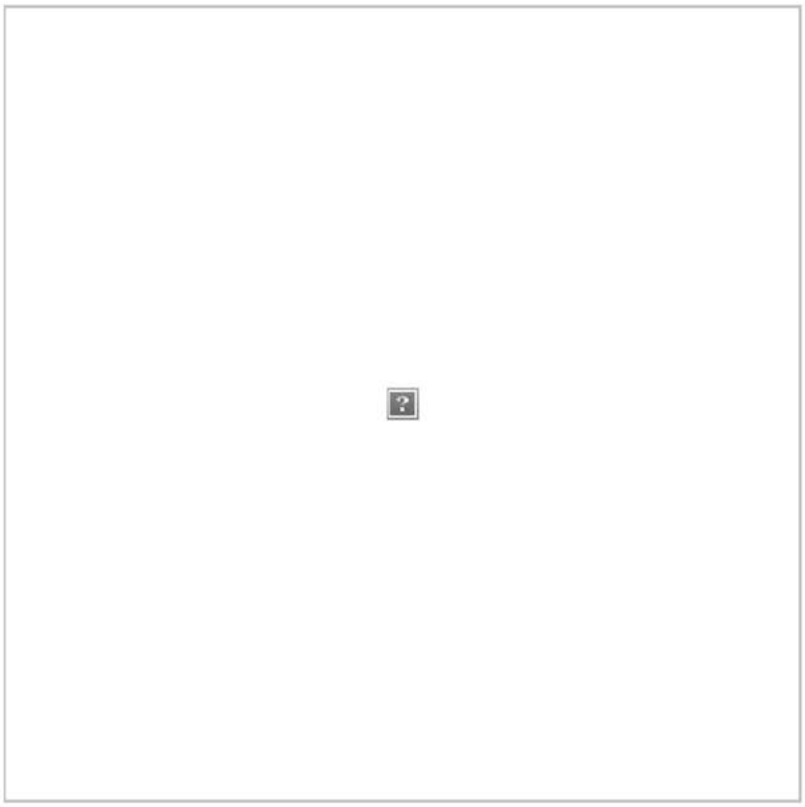
>Read More

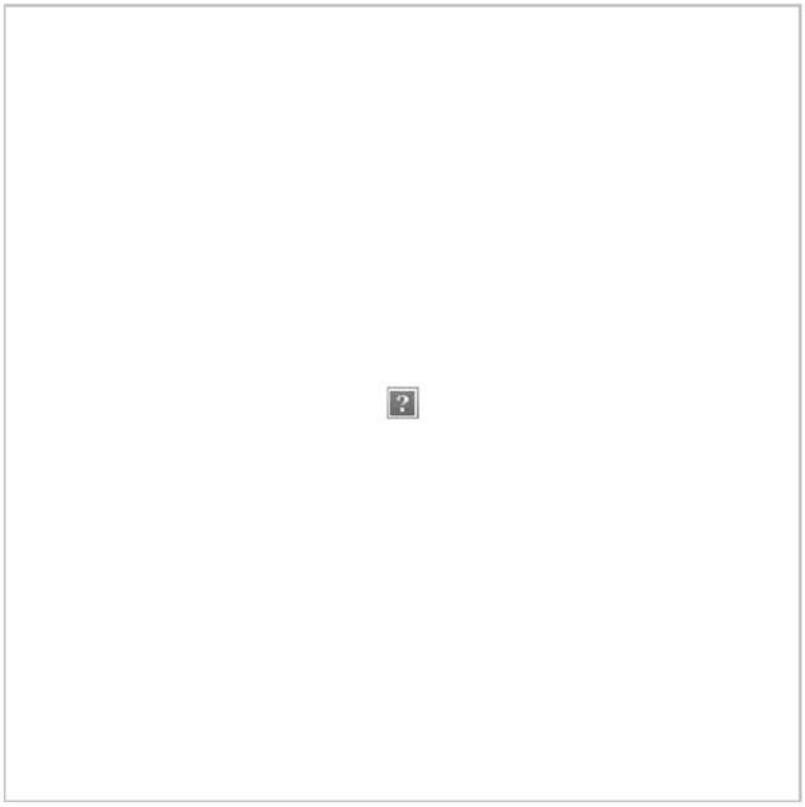
Anti-Methamphetamine Program

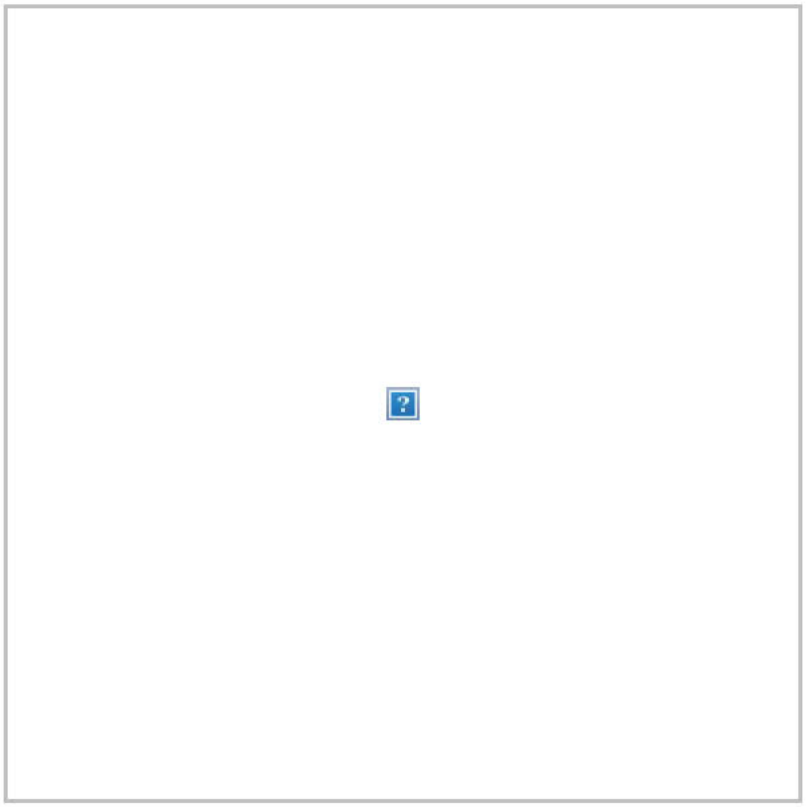
February 18, 2020 — The COPS Anti-Methamphetamine Program (CAMP) is a competitive grant solicitation, open to state law enforcement agencies with multijurisdictional reach and interdisciplinary team (e.g. task force) structures, in states with high seizures of precursor chemicals, finished methamphetamine, laboratories, and laboratory dump seizures.

>Read More

Upcoming Conferences







Vendor News

Cloud Explorer Extracts Google Fit Data

February 18, 2020 — ElcomSoft Co. Ltd. recently announced Elcomsoft Cloud Explorer 2.30, which adds support for health and activity information collected by the Android Google Fit app and synchronized to the user's Google Account. >Read More

Motorola Solutions Adds New Analytics to In-Car Video System

February 13, 2020 — Motorola Solutions recently announced the availability of new video security and analytics capabilities for law enforcement. Automated license plate recognition (ALPR) is now part of the WatchGuard 4RE® in-car video system. >Read More

New Touch Screen Repeating Pipette with Advanced Features

February 13, 2020 — The BRAND® HandyStep® touch S repeating pipette has advanced pipetting features for versatility. In addition to standard pipetting, dispensing, auto dispensing and a proprietary "learn" function, advanced modes include sequential dispensing of different volumes, multi-aspiration of different volumes and a titration mode. >Read More

Companies Partner to Deliver Hybrid Video Management Solution

February 11, 2020 — Arcules, a company focusing on integrated video and access control cloud services, recently announced the commercial availability of the Arcules-XProtect

Hybrid™ VMS Solution in North America and Europe. >Read More

New Desktop 3D Scanner for Tiny Objects

February 11, 2020 — Exact Metrology recently announced the availability of the new Artec Micro 3D scanner. The Artec Micro, an automated, metrology-grade desktop 3D scanner is Artec 3D's most accurate 3D scanner to date, and is used for scanning tiny mechanical parts, such as engine valves or connectors, for inspection and reverse engineering, as well as other small objects for industries such as heritage preservation, dentistry, and medical. >Read More

Subscribe to Evidence Technology Magazine

Open Source Web Intelligence Company Opens Office in U.S.

January 22, 2020 — Cobwebs Technologies — the specialized open-source web intelligence company that supports national security agencies, law enforcement agencies, and corporate security departments in rapidly identifying and locating malicious threat actors on the open, deep, and dark webs — is entering the American market with an office in New York City. With little more than a click, Cobwebs makes it highly difficult for terrorists, active shooters, hackers, and other criminal entities to hide, plan, communicate, or ply their nefarious trade in any part of the online world. >Read More

Nearly Half of First Responders Under-Equipped to Handle Extended Power Outage, Report Finds

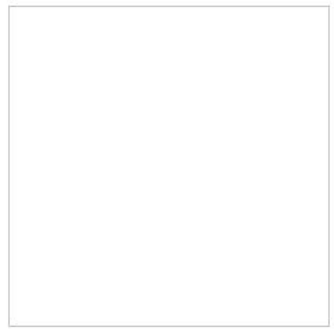
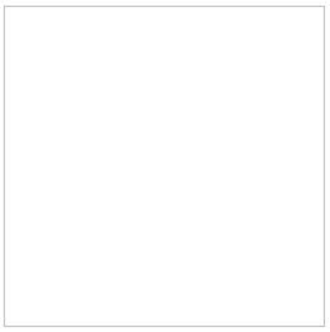
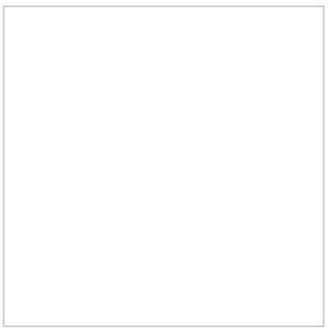
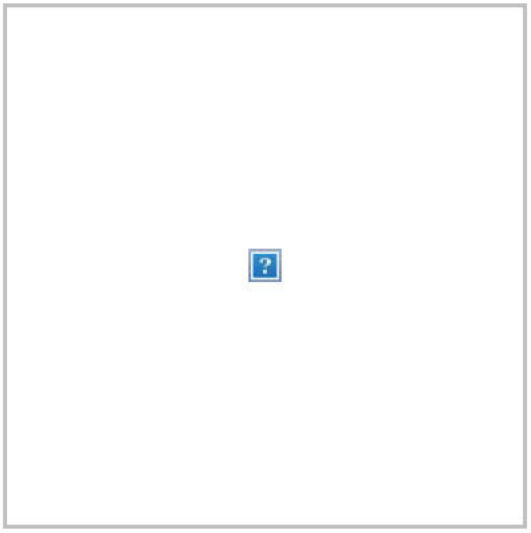
January 23, 2020 — IWCE, an event for the critical communications industry, surveyed more than 597 first responders and public safety professionals to benchmark the current technologies they are using and to understand current technological challenges within the industry. >Read More

Environmentally Friendly Alternative to Canned Air

January 21, 2020 — Canless Air System is a highly effective and environmentally friendly alternative to traditional canned air cleaning products. The line of Hurricane dusters is nontoxic, rechargeable, and provides more power than any canned air competitor. >Read More

---

There's more in the ETM Digital Edition:


Website LinkedIn Twitter Facebook Subscribe

Copyright © 2020 Wordsmith Publishing, All rights reserved.
You are receiving this eNewsletter because you subscribed to Evidence Technology Magazine. You can change your communication preferences at any time by following the links below. Thank you for your readership!

Our mailing address is:
Wordsmith Publishing
PO Box 555
Kearney, MO 64060

Add us to your address book

unsubscribe from this list update subscription preferences

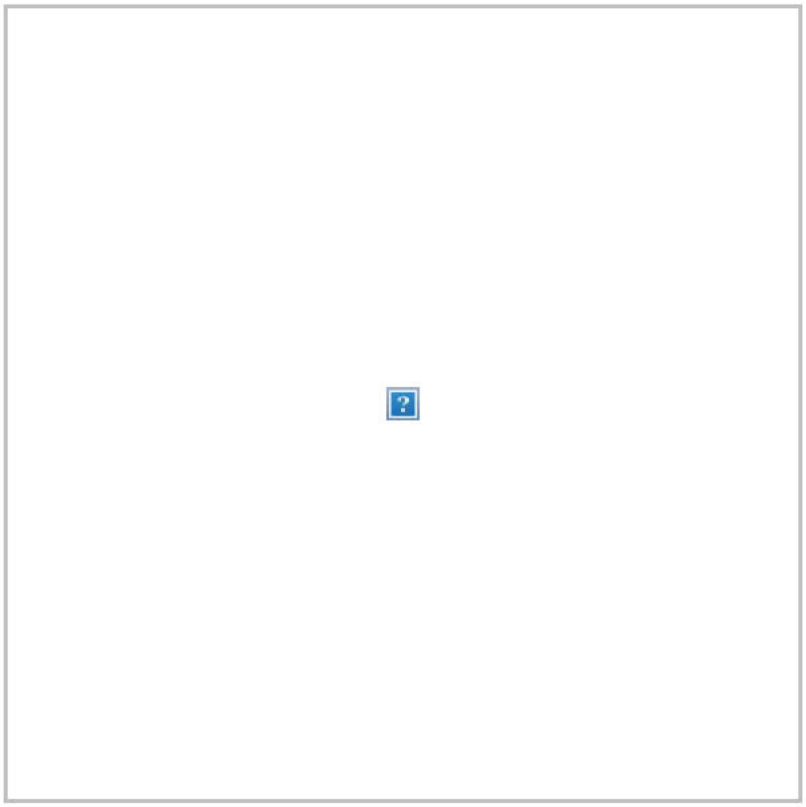
From: Evidence Technology Magazine
To: Girouard, Todd (POL)
Subject: Marijuana Analysis in a New Frontier, and More
Date: Tuesday, February 18, 2020 6:34:20 PM

Here's your February issue of ETM's Laboratory News

View this email in your browser



Evidence Technology Magazine • Laboratory News • February 2020



Advertisement

Education & Training

Webinar: Marijuana Analysis in a New Frontier

February 18, 2020 — As part of the continuing ASCLD Train the Director Series, presented by the NIJ's Forensic Technology Center of Excellence, a webinar on March 5 will examine the legal landscape of marijuana and hemp in two specific jurisdictions: one with legalized marijuana and one without. The analytical schemes used in both laboratories will be presented.

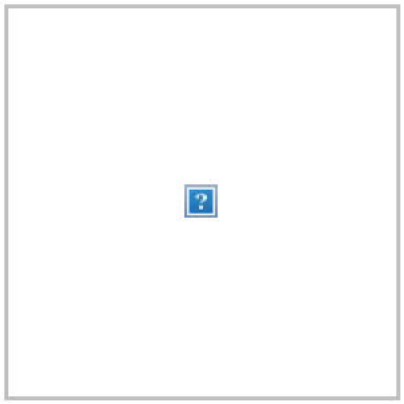
>Read More

DNA Analysis

NY District Court Denies Motion to Preclude DNA Software Analysis

February 6, 2020 — A U.S. District Court for the Eastern District of New York has denied a defendant's motion to preclude expert testimony regarding the results of a DNA analysis produced by using STRmix – forensic software used to resolve mixed DNA profiles.

>Read More



NEW ISSUE! Read the January-February Issue of ETM

Funding Opportunities

Anti-Heroin Task Force Program

February 4, 2020 — The COPS Office Anti-Heroin Task Force (AHTF) Program is a competitive grant solicitation, open to state law enforcement agencies with multijurisdictional reach and interdisciplinary team (e.g. task force) structures, in states with high per capita rates of primary treatment admissions.

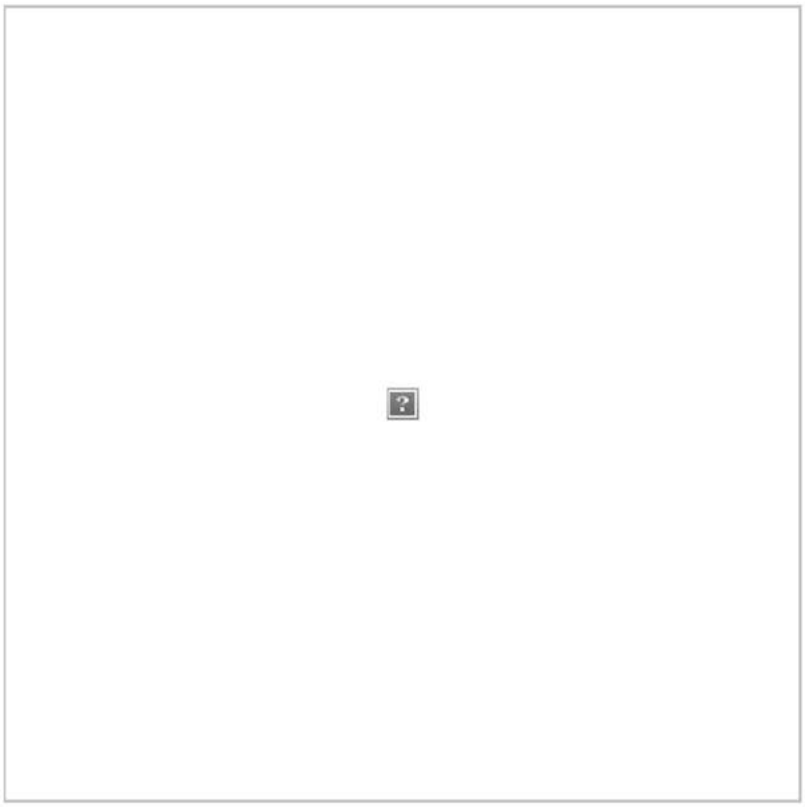
>Read More

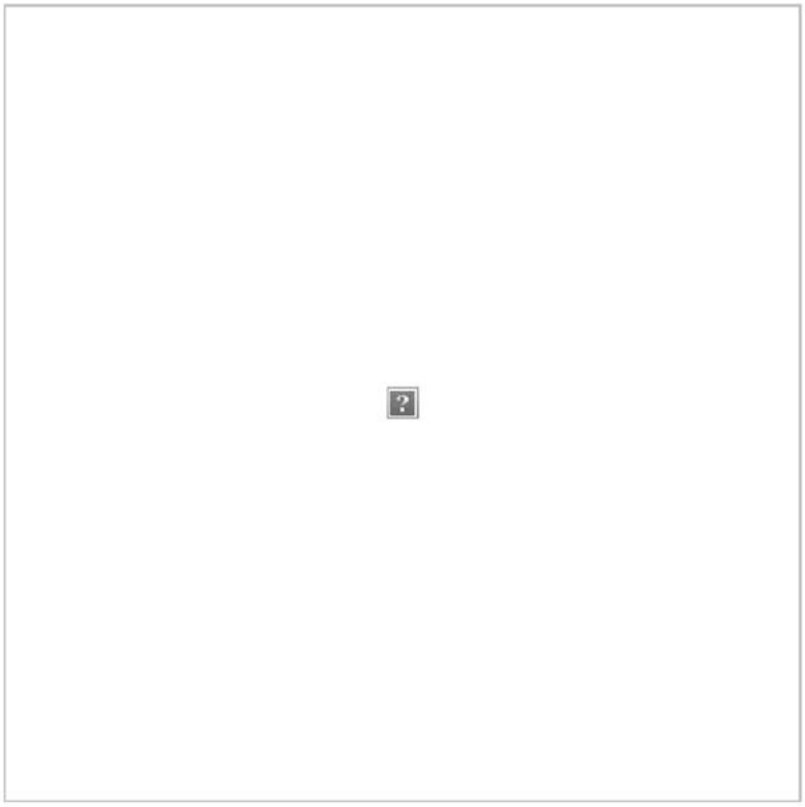
Anti-Methamphetamine Program

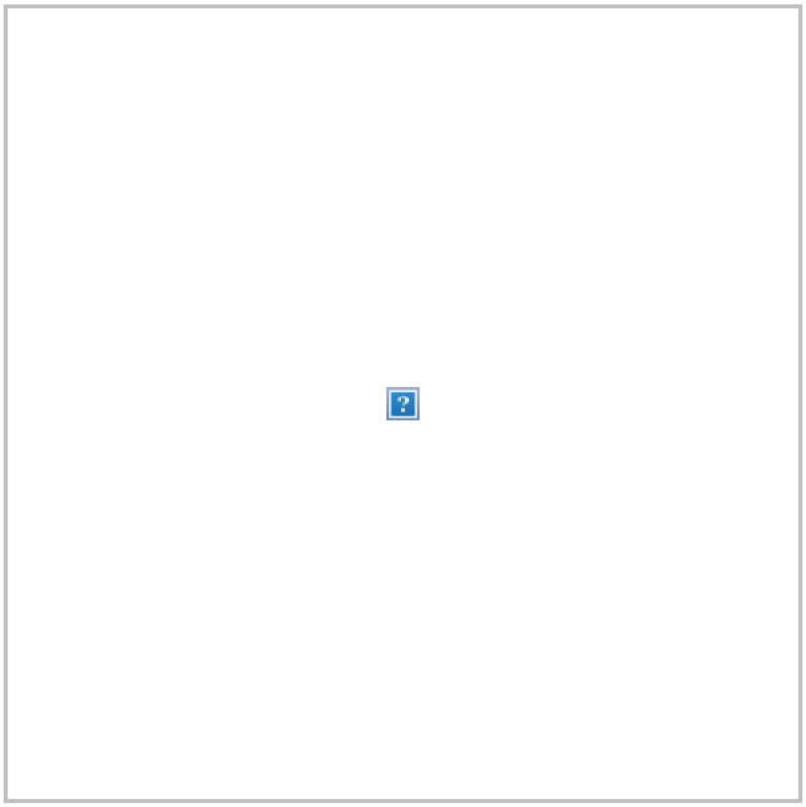
February 18, 2020 — The COPS Anti-Methamphetamine Program (CAMP) is a competitive grant solicitation, open to state law enforcement agencies with multijurisdictional reach and interdisciplinary team (e.g. task force) structures, in states with high seizures of precursor chemicals, finished methamphetamine, laboratories, and laboratory dump seizures.

>Read More

Upcoming Conferences







Vendor News

Cloud Explorer Extracts Google Fit Data

February 18, 2020 — ElcomSoft Co. Ltd. recently announced Elcomsoft Cloud Explorer 2.30, which adds support for health and activity information collected by the Android Google Fit app and synchronized to the user's Google Account. >Read More

Motorola Solutions Adds New Analytics to In-Car Video System

February 13, 2020 — Motorola Solutions recently announced the availability of new video security and analytics capabilities for law enforcement. Automated license plate recognition (ALPR) is now part of the WatchGuard 4RE® in-car video system. >Read More

New Touch Screen Repeating Pipette with Advanced Features

February 13, 2020 — The BRAND® HandyStep® touch S repeating pipette has advanced pipetting features for versatility. In addition to standard pipetting, dispensing, auto dispensing and a proprietary "learn" function, advanced modes include sequential dispensing of different volumes, multi-aspiration of different volumes and a titration mode. >Read More

Companies Partner to Deliver Hybrid Video Management Solution

February 11, 2020 — Arcules, a company focusing on integrated video and access control cloud services, recently announced the commercial availability of the Arcules-XProtect

Hybrid™ VMS Solution in North America and Europe. >Read More

New Desktop 3D Scanner for Tiny Objects

February 11, 2020 — Exact Metrology recently announced the availability of the new Artec Micro 3D scanner. The Artec Micro, an automated, metrology-grade desktop 3D scanner is Artec 3D's most accurate 3D scanner to date, and is used for scanning tiny mechanical parts, such as engine valves or connectors, for inspection and reverse engineering, as well as other small objects for industries such as heritage preservation, dentistry, and medical. >Read More

Subscribe to Evidence Technology Magazine

Open Source Web Intelligence Company Opens Office in U.S.

January 22, 2020 — Cobwebs Technologies — the specialized open-source web intelligence company that supports national security agencies, law enforcement agencies, and corporate security departments in rapidly identifying and locating malicious threat actors on the open, deep, and dark webs — is entering the American market with an office in New York City. With little more than a click, Cobwebs makes it highly difficult for terrorists, active shooters, hackers, and other criminal entities to hide, plan, communicate, or ply their nefarious trade in any part of the online world. >Read More

Nearly Half of First Responders Under-Equipped to Handle Extended Power Outage, Report Finds

January 23, 2020 — IWCE, an event for the critical communications industry, surveyed more than 597 first responders and public safety professionals to benchmark the current technologies they are using and to understand current technological challenges within the industry. >Read More

Environmentally Friendly Alternative to Canned Air

January 21, 2020 — Canless Air System is a highly effective and environmentally friendly alternative to traditional canned air cleaning products. The line of Hurricane dusters is nontoxic, rechargeable, and provides more power than any canned air competitor. >Read More

---

There's more in the ETM Digital Edition:



Website LinkedIn Twitter Facebook Subscribe

Copyright © 2020 Wordsmith Publishing, All rights reserved.
You are receiving this eNewsletter because you subscribed to Evidence Technology Magazine. You can change your communication preferences at any time by following the links below. Thank you for your readership!

Our mailing address is:
Wordsmith Publishing
PO Box 555
Kearney, MO 64060

Add us to your address book

unsubscribe from this list update subscription preferences

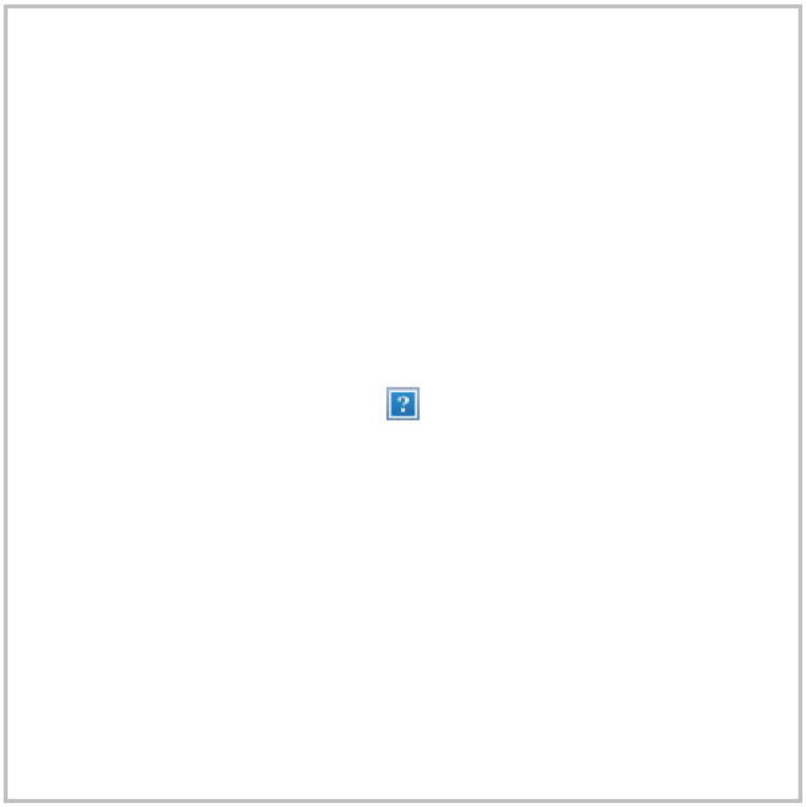
From: Evidence Technology Magazine
To: Hughes, David (POL)
Subject: Marijuana Analysis in a New Frontier, and More
Date: Tuesday, February 18, 2020 6:33:57 PM

Here's your February issue of ETM's Laboratory News

View this email in your browser



Evidence Technology Magazine • Laboratory News • February 2020



Advertisement

Education & Training

Webinar: Marijuana Analysis in a New Frontier

February 18, 2020 — As part of the continuing ASCLD Train the Director Series, presented by the NIJ's Forensic Technology Center of Excellence, a webinar on March 5 will examine the legal landscape of marijuana and hemp in two specific jurisdictions: one with legalized marijuana and one without. The analytical schemes used in both laboratories will be presented.

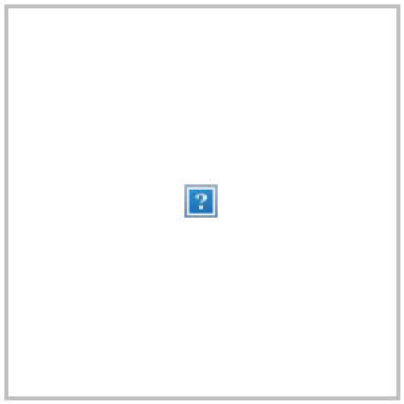
>Read More

DNA Analysis

NY District Court Denies Motion to Preclude DNA Software Analysis

February 6, 2020 — A U.S. District Court for the Eastern District of New York has denied a defendant's motion to preclude expert testimony regarding the results of a DNA analysis produced by using STRmix – forensic software used to resolve mixed DNA profiles.

>Read More



NEW ISSUE! Read the January-February Issue of ETM

Funding Opportunities

Anti-Heroin Task Force Program

February 4, 2020 — The COPS Office Anti-Heroin Task Force (AHTF) Program is a competitive grant solicitation, open to state law enforcement agencies with multijurisdictional reach and interdisciplinary team (e.g. task force) structures, in states with high per capita rates of primary treatment admissions.

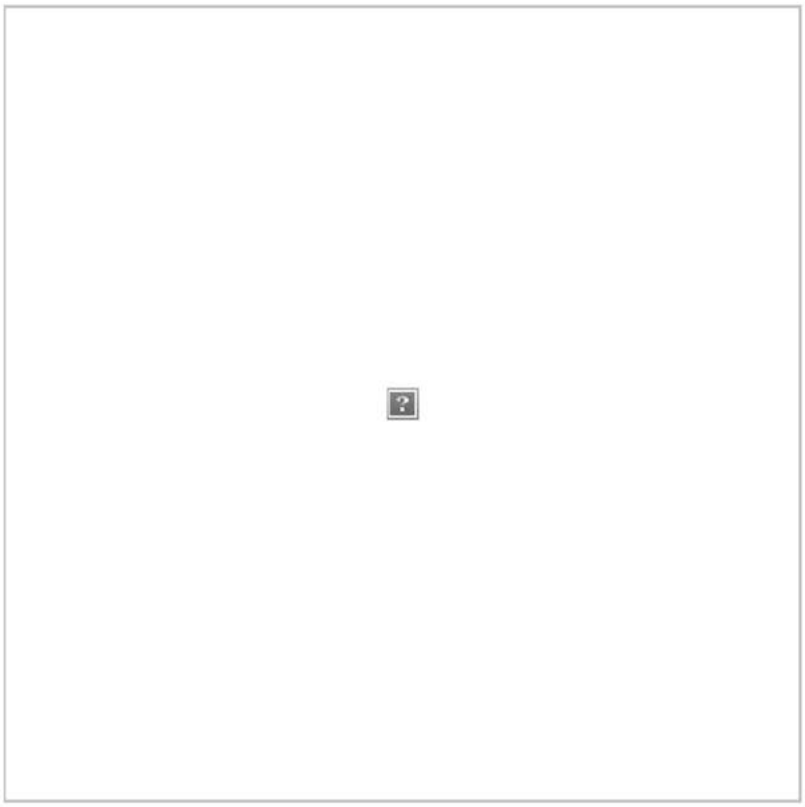
>Read More

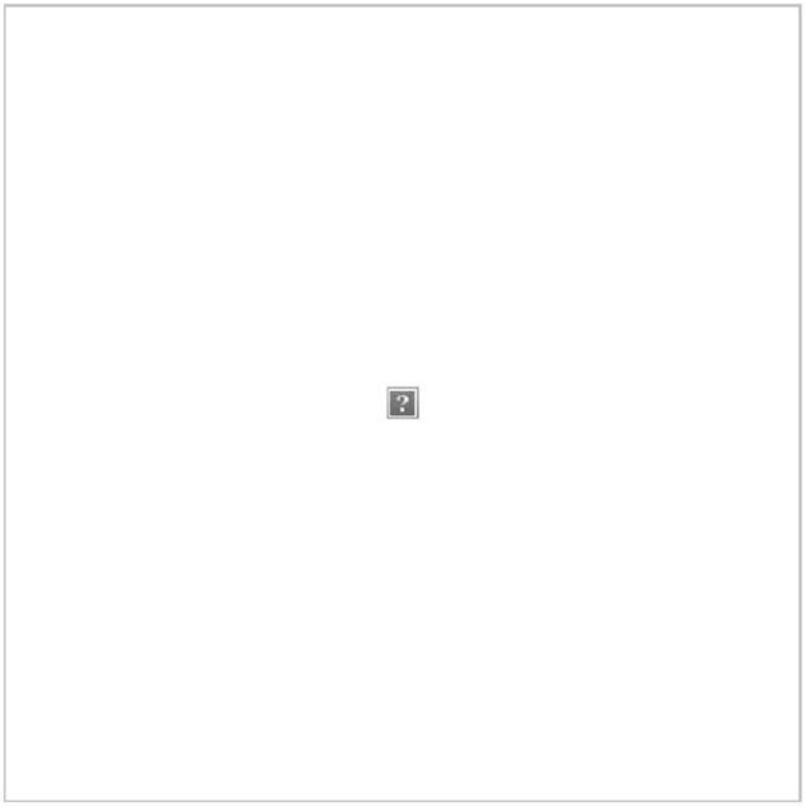
Anti-Methamphetamine Program

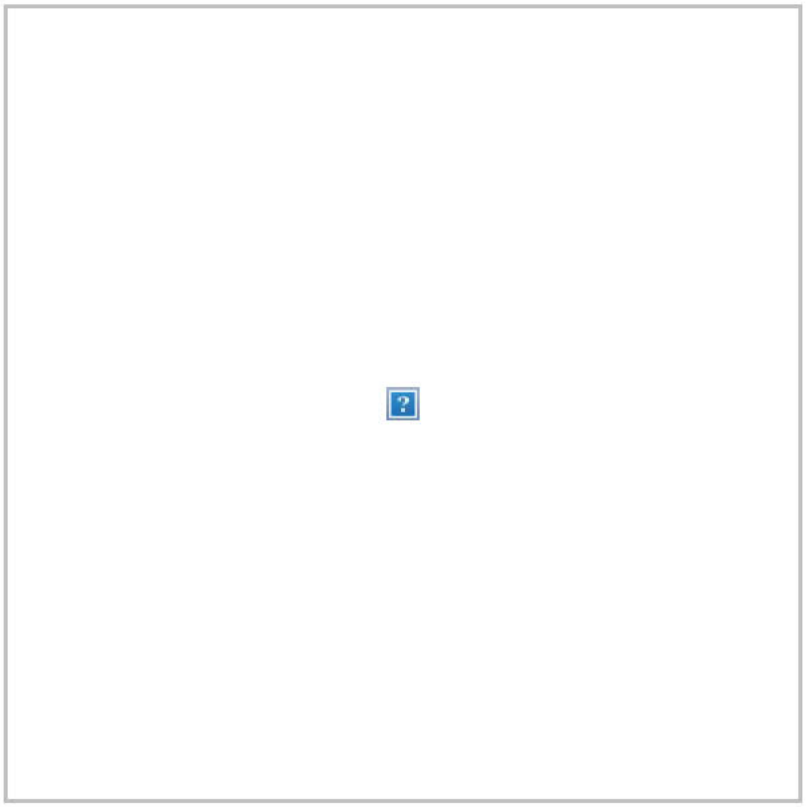
February 18, 2020 — The COPS Anti-Methamphetamine Program (CAMP) is a competitive grant solicitation, open to state law enforcement agencies with multijurisdictional reach and interdisciplinary team (e.g. task force) structures, in states with high seizures of precursor chemicals, finished methamphetamine, laboratories, and laboratory dump seizures.

>Read More

Upcoming Conferences







Vendor News

Cloud Explorer Extracts Google Fit Data

February 18, 2020 — ElcomSoft Co. Ltd. recently announced Elcomsoft Cloud Explorer 2.30, which adds support for health and activity information collected by the Android Google Fit app and synchronized to the user's Google Account. >Read More

Motorola Solutions Adds New Analytics to In-Car Video System

February 13, 2020 — Motorola Solutions recently announced the availability of new video security and analytics capabilities for law enforcement. Automated license plate recognition (ALPR) is now part of the WatchGuard 4RE® in-car video system. >Read More

New Touch Screen Repeating Pipette with Advanced Features

February 13, 2020 — The BRAND® HandyStep® touch S repeating pipette has advanced pipetting features for versatility. In addition to standard pipetting, dispensing, auto dispensing and a proprietary "learn" function, advanced modes include sequential dispensing of different volumes, multi-aspiration of different volumes and a titration mode. >Read More

Companies Partner to Deliver Hybrid Video Management Solution

February 11, 2020 — Arcules, a company focusing on integrated video and access control cloud services, recently announced the commercial availability of the Arcules-XProtect

Hybrid™ VMS Solution in North America and Europe. >Read More

New Desktop 3D Scanner for Tiny Objects

February 11, 2020 — Exact Metrology recently announced the availability of the new Artec Micro 3D scanner. The Artec Micro, an automated, metrology-grade desktop 3D scanner is Artec 3D's most accurate 3D scanner to date, and is used for scanning tiny mechanical parts, such as engine valves or connectors, for inspection and reverse engineering, as well as other small objects for industries such as heritage preservation, dentistry, and medical. >Read More

Subscribe to Evidence Technology Magazine

Open Source Web Intelligence Company Opens Office in U.S.

January 22, 2020 — Cobwebs Technologies — the specialized open-source web intelligence company that supports national security agencies, law enforcement agencies, and corporate security departments in rapidly identifying and locating malicious threat actors on the open, deep, and dark webs — is entering the American market with an office in New York City. With little more than a click, Cobwebs makes it highly difficult for terrorists, active shooters, hackers, and other criminal entities to hide, plan, communicate, or ply their nefarious trade in any part of the online world. >Read More

Nearly Half of First Responders Under-Equipped to Handle Extended Power Outage, Report Finds

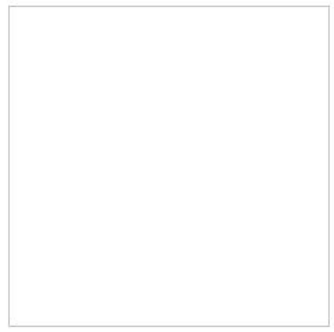
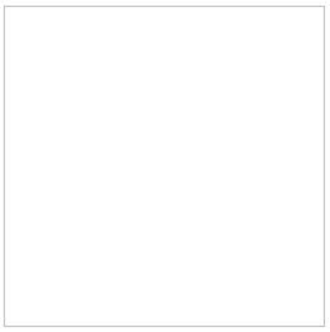
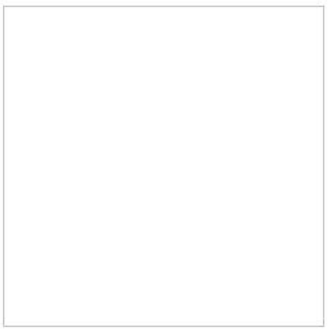
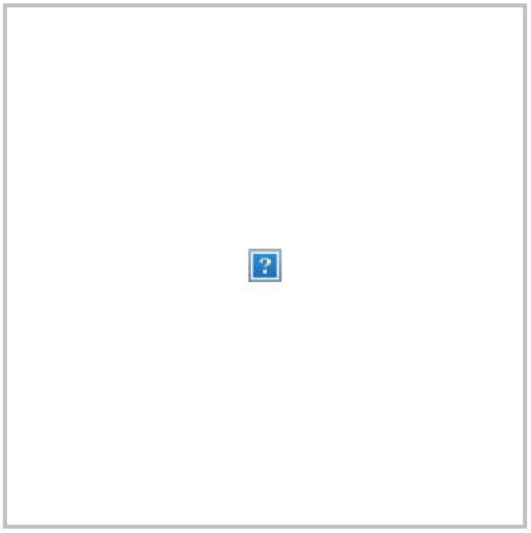
January 23, 2020 — IWCE, an event for the critical communications industry, surveyed more than 597 first responders and public safety professionals to benchmark the current technologies they are using and to understand current technological challenges within the industry. >Read More

Environmentally Friendly Alternative to Canned Air

January 21, 2020 — Canless Air System is a highly effective and environmentally friendly alternative to traditional canned air cleaning products. The line of Hurricane dusters is nontoxic, rechargeable, and provides more power than any canned air competitor. >Read More

---

There's more in the ETM Digital Edition:


Website LinkedIn Twitter Facebook Subscribe

Copyright © 2020 Wordsmith Publishing, All rights reserved.
You are receiving this eNewsletter because you subscribed to Evidence Technology Magazine. You can change your communication preferences at any time by following the links below. Thank you for your readership!

Our mailing address is:
Wordsmith Publishing
PO Box 555
Kearney, MO 64060

Add us to your address book

unsubscribe from this list update subscription preferences

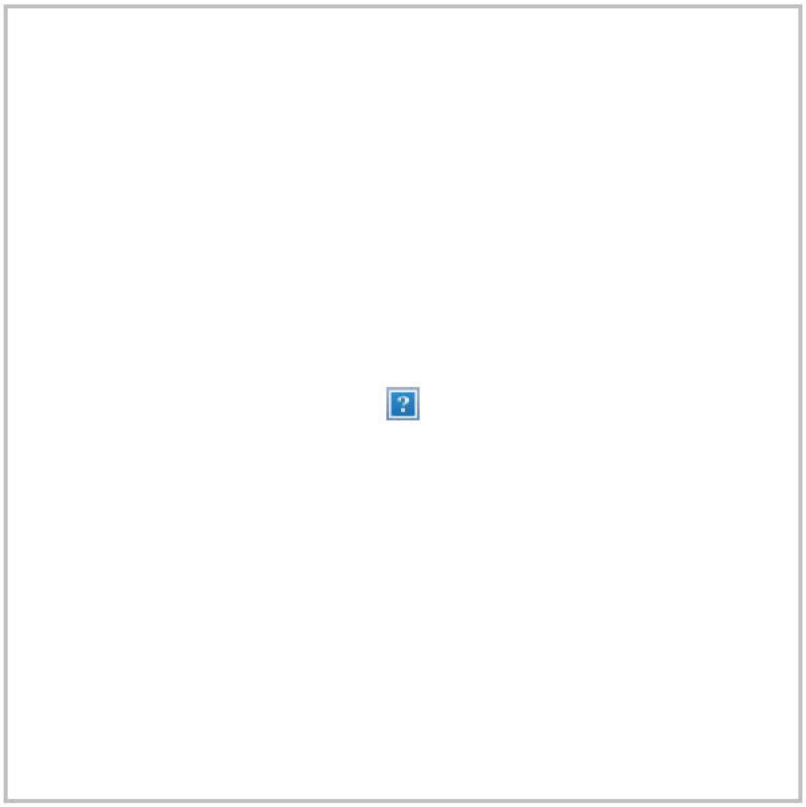
From: Evidence Technology Magazine
To: Saucier, Beth (POL)
Subject: Marijuana Analysis in a New Frontier, and More
Date: Tuesday, February 18, 2020 6:34:40 PM

Here's your February issue of ETM's Laboratory News

View this email in your browser



Evidence Technology Magazine • Laboratory News • February 2020



Advertisement

Education & Training

Webinar: Marijuana Analysis in a New Frontier

February 18, 2020 — As part of the continuing ASCLD Train the Director Series, presented by the NIJ's Forensic Technology Center of Excellence, a webinar on March 5 will examine the legal landscape of marijuana and hemp in two specific jurisdictions: one with legalized marijuana and one without. The analytical schemes used in both laboratories will be presented.

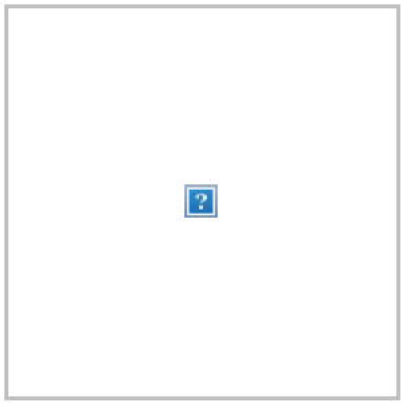
>Read More

DNA Analysis

NY District Court Denies Motion to Preclude DNA Software Analysis

February 6, 2020 — A U.S. District Court for the Eastern District of New York has denied a defendant's motion to preclude expert testimony regarding the results of a DNA analysis produced by using STRmix – forensic software used to resolve mixed DNA profiles.

>Read More



NEW ISSUE! Read the January-February Issue of ETM

Funding Opportunities

Anti-Heroin Task Force Program

February 4, 2020 — The COPS Office Anti-Heroin Task Force (AHTF) Program is a competitive grant solicitation, open to state law enforcement agencies with multijurisdictional reach and interdisciplinary team (e.g. task force) structures, in states with high per capita rates of primary treatment admissions.

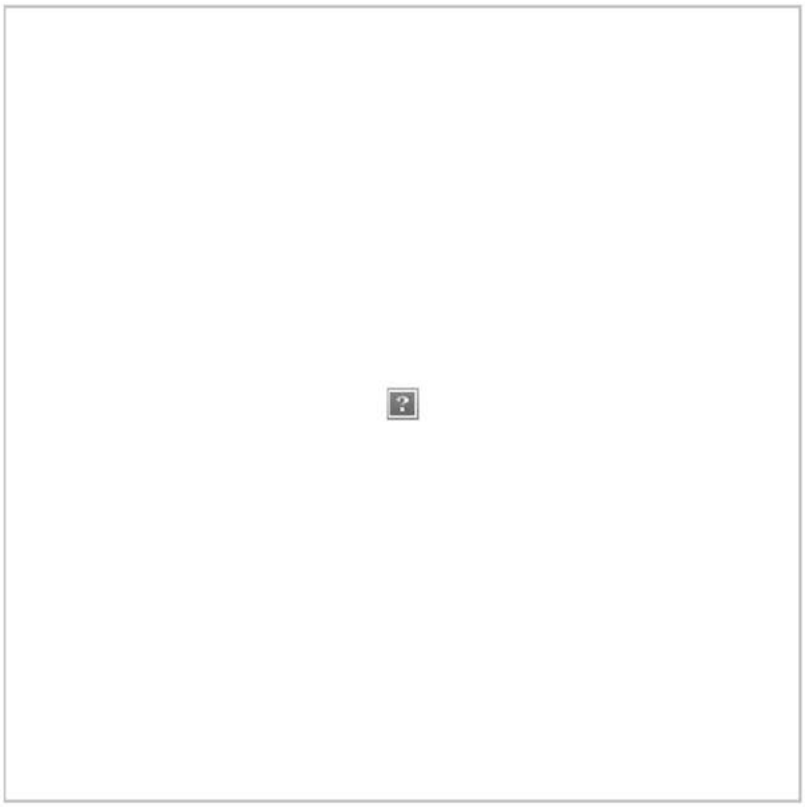
>Read More

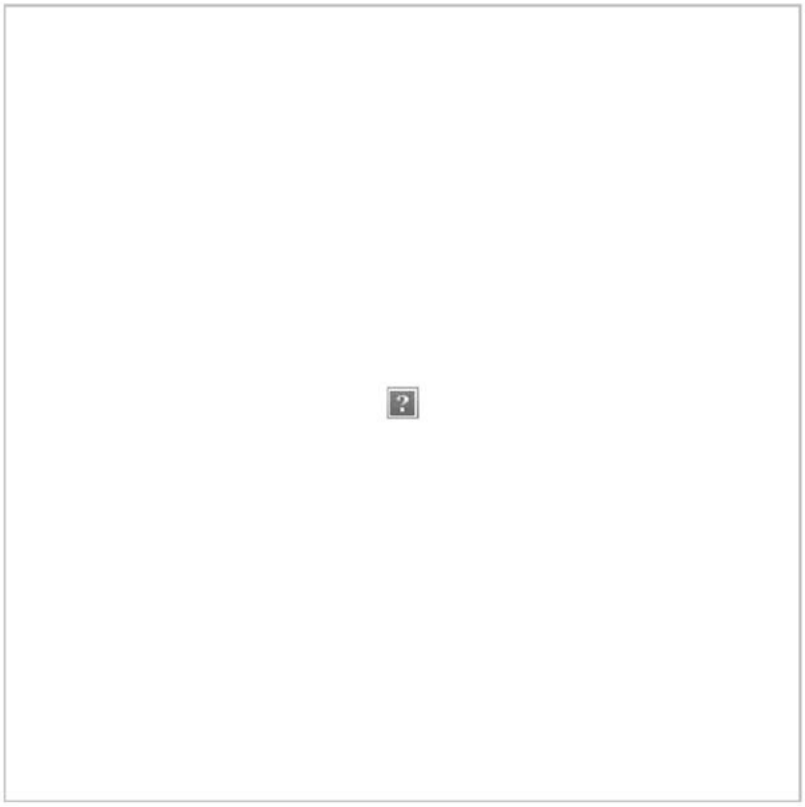
Anti-Methamphetamine Program

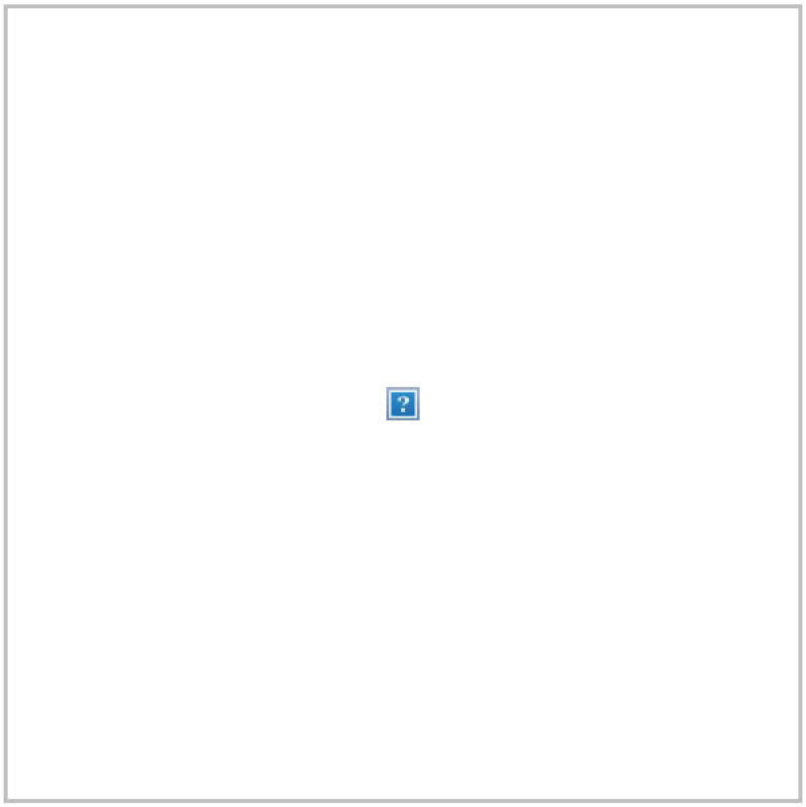
February 18, 2020 — The COPS Anti-Methamphetamine Program (CAMP) is a competitive grant solicitation, open to state law enforcement agencies with multijurisdictional reach and interdisciplinary team (e.g. task force) structures, in states with high seizures of precursor chemicals, finished methamphetamine, laboratories, and laboratory dump seizures.

>Read More

Upcoming Conferences







Vendor News

Cloud Explorer Extracts Google Fit Data

February 18, 2020 — ElcomSoft Co. Ltd. recently announced Elcomsoft Cloud Explorer 2.30, which adds support for health and activity information collected by the Android Google Fit app and synchronized to the user's Google Account. >Read More

Motorola Solutions Adds New Analytics to In-Car Video System

February 13, 2020 — Motorola Solutions recently announced the availability of new video security and analytics capabilities for law enforcement. Automated license plate recognition (ALPR) is now part of the WatchGuard 4RE® in-car video system. >Read More

New Touch Screen Repeating Pipette with Advanced Features

February 13, 2020 — The BRAND® HandyStep® touch S repeating pipette has advanced pipetting features for versatility. In addition to standard pipetting, dispensing, auto dispensing and a proprietary "learn" function, advanced modes include sequential dispensing of different volumes, multi-aspiration of different volumes and a titration mode. >Read More

Companies Partner to Deliver Hybrid Video Management Solution

February 11, 2020 — Arcules, a company focusing on integrated video and access control cloud services, recently announced the commercial availability of the Arcules-XProtect

Hybrid™ VMS Solution in North America and Europe. >Read More

New Desktop 3D Scanner for Tiny Objects

February 11, 2020 — Exact Metrology recently announced the availability of the new Artec Micro 3D scanner. The Artec Micro, an automated, metrology-grade desktop 3D scanner is Artec 3D's most accurate 3D scanner to date, and is used for scanning tiny mechanical parts, such as engine valves or connectors, for inspection and reverse engineering, as well as other small objects for industries such as heritage preservation, dentistry, and medical. >Read More

Subscribe to Evidence Technology Magazine

Open Source Web Intelligence Company Opens Office in U.S.

January 22, 2020 — Cobwebs Technologies — the specialized open-source web intelligence company that supports national security agencies, law enforcement agencies, and corporate security departments in rapidly identifying and locating malicious threat actors on the open, deep, and dark webs — is entering the American market with an office in New York City. With little more than a click, Cobwebs makes it highly difficult for terrorists, active shooters, hackers, and other criminal entities to hide, plan, communicate, or ply their nefarious trade in any part of the online world. >Read More

Nearly Half of First Responders Under-Equipped to Handle Extended Power Outage, Report Finds

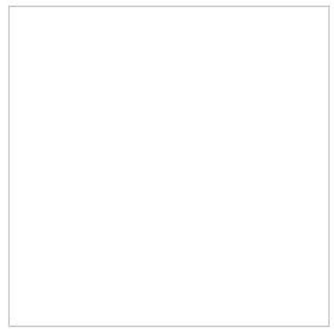
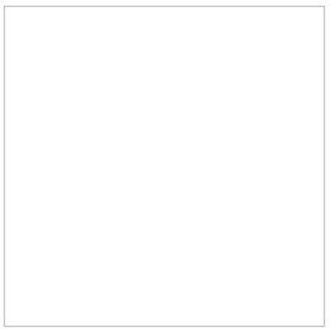
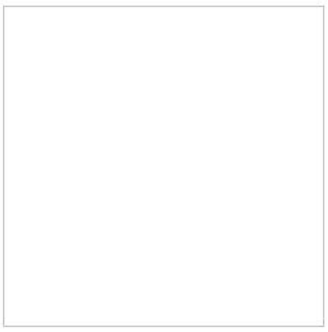
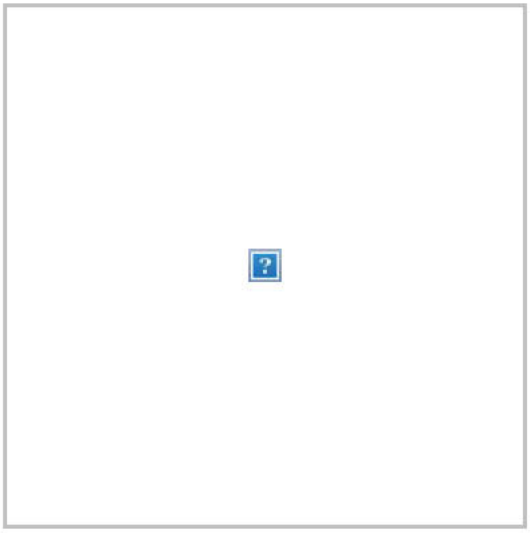
January 23, 2020 — IWCE, an event for the critical communications industry, surveyed more than 597 first responders and public safety professionals to benchmark the current technologies they are using and to understand current technological challenges within the industry. >Read More

Environmentally Friendly Alternative to Canned Air

January 21, 2020 — Canless Air System is a highly effective and environmentally friendly alternative to traditional canned air cleaning products. The line of Hurricane dusters is nontoxic, rechargeable, and provides more power than any canned air competitor. >Read More

---

There's more in the ETM Digital Edition:


Website LinkedIn Twitter Facebook Subscribe

Copyright © 2020 Wordsmith Publishing, All rights reserved.
You are receiving this eNewsletter because you subscribed to Evidence Technology Magazine. You can change your communication preferences at any time by following the links below. Thank you for your readership!

Our mailing address is:
Wordsmith Publishing
PO Box 555
Kearney, MO 64060

Add us to your address book

unsubscribe from this list update subscription preferences

From: 91111-33928506@requests.muckrock.com
To: MSP RAO (POL)
Cc: MSP Legal Section (POL)
Subject: Massachusetts Public Records Law Request: ALPR/Force used by Massachusetts State Police (Massachusetts State Police)
Date: Monday, April 6, 2020 12:38:30 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Massachusetts State Police
PRL Office
470 Worcester Road
Framingham, MA 01702

April 6, 2020

To Whom It May Concern:

Pursuant to the Massachusetts Public Records Law, I hereby request the following records:

1. All use of force reports from Troop E and A at Westfield Massachusetts state police barracks, from January 1, 2017 until the date that this request is processed. (Submitted March 28th 2020)
2. The names of agencies and organizations with which the Agency shares ALPR data;
3. The names of agencies and organizations from which the Agency receives ALPR data;
4. The names of agencies and organizations with which the Agency shares "hot list" information;
5. What is "hot list" information and I would like my personal record of what shows up when my license plate is scanned- License Plate 289ve4, by MSP;**

This information is easily available within the Agency's LEARN system. The simplest way to extract this data is to generate an "Agency Data Sharing Report" PDF file from within LEARN. To do this, a user may simply go to the "Sharing" section of LEARN and select "Output Report." A CSV/XLS file containing these records would also satisfy this request.
The instructions for extracting this data is described on pages 62-63 of the LEARN Agency Manager Guide, which may be found at this link:
https://www.documentcloud.org/documents/3860685-LEARN-5-1-Agency-Manager-Guide html
An example of this record may be found at this link:
https://www.documentcloud.org/documents/3936113-Palos-Verdes-Estates-Police-Department-Data html
A number of other agencies have regularly determined the above information constitutes a public record and have provided an "Agency Data Sharing Report." These agencies include:
Anaheim Police Department, Antioch Police Department, Bakersfield Police Department Chino Police Department, Clovis Police Department, Elk Grove Police Department, Fontana Police Department, Fountain Valley Police Department, Glendora Police Department, Hawthorne Police Department, Irvine Police Department, Livermore Police Department, Lodi Police Department, Long Beach Police Department, Montebello Police Department, Orange Police Department, Palos Verdes Estates Police Department, Red Bluff Police Department ,Sacramento Police Department, San Bernardino Police Department, San Diego Police Department, San Rafael Police Department, San Ramon Police Department, Simi Valley Police Department, and the Tulare Police Department.

I also request that, if appropriate, fees be waived as we believe this request is in the public interest, as suggested but not stipulated by the recommendations of the Massachusetts Supervisor of Public Records. The requested documents will be made available to the general public free of charge as part of the public information service at MuckRock.com, processed by a representative of the news media/press and is made in the process of news gathering and not for commercial usage.

I expect the request to be filled in an accessible format, including for screen readers, which provide text-to-speech for persons unable to read print. Files that are not accessible to screen readers include, for example, .pdf image files as well as physical documents.

In the event that there are fees, I would be grateful if you would inform me of the total charges in advance of fulfilling my request. I would prefer the request filled electronically, by e-mail attachment if available or CD-ROM if not.

Thank you in advance for your anticipated cooperation in this matter. I look forward to receiving your response to this request within 10 business days, as the statute requires.

Sincerely,

mikayla mucha

Filed via MuckRock.com
E-mail (Preferred): 91111-33928506@requests muckrock.com
Upload documents directly: https://accounts muckrock.com/accounts/login/?
url_auth_token=AAATf2QmlOufExPigod_03qbsAc%3A1jLUkz%3AF_Z1qnoQWruMa2ijenkFJ8t362Y&next=https%3A%2F%2Fwww muckrock.com%2Faccounts%2Flogin%2F%3Fnext%3D%252Faccounts%252Fagency_login%252Fmassachusetts-state-police-274%252Falprforce-used-by-massachusetts-state-police-massachusetts-state-police-91111%252F%253Femail%253Dmsp rao%252540state ma.us
Is this email coming to the wrong contact? Something else wrong? Use the above link to let us know.

For mailed responses, please address (see note):
MuckRock News
DEPT MR 91111
411A Highland Ave
Somerville, MA 02144-2516

PLEASE NOTE: This request is not filed by a MuckRock staff member, but is being sent through MuckRock by the above in order to better track, share, and manage public records requests. Also note that improperly addressed (i.e., with the requester's name rather than "MuckRock News" and the department number) requests might be returned as undeliverable.

From: PoliceOne Roll Call
To: McCarthy, Steven (POL)
Subject: Murder charge for Minn. cop; Constable mistakenly killed by deputy
Date: Friday, May 29, 2020 5:10:16 PM

May 29, 2020 | View as webpage

Dear PoliceOne Member,

This morning, Hennepin County Attorney Mike Freeman announced that former Minneapolis police officer Derek Chauvin has been charged with third-degree murder and manslaughter in the death of George Floyd. The charge comes after the city was paralyzed by a third night of rioting and violence, during which protestors set fire to a police precinct. PoliceOne will continue to bring you the latest developments, as well as expert analysis on evolving events. Click here for our complete coverage.

— *The PoliceOne Team*

TOP STORIES

Minneapolis cop who knelt on handcuffed man charged

Derek Chauvin has been charged with third-degree murder and manslaughter

Sheriff: Texas constable mistakenly killed by deputy

Protests over Minn. in-custody death spread across the nation

Utah officer killed in shooting

'Do not do this': Kansas City PD official says police will be shown Minneapolis arrest video

Video: Minneapolis protesters set fire to police precinct

Personal Protective Face Shield From UTM



Ultimate Training Munitions' full front face shield offers secondary protection in conjunction with existing PPE. This shield offers splash protection, blocks airborne debris and is a physical barrier to hands-to-face contact. Take advantage of this invaluable tool.

Available now

World Class Performance Has Arrived!



Freeways, city streets, college campuses, parks, country roads. When duty calls, BMW leads!

Learn more

FEATURED CONTENT



10 crowd control myths

By Lt. Dan Marcou

Both the public and cops have many misconceptions about police crowd control



What does George Floyd's death tell law enforcement?

By Jim Glennon

There are systemic problems in policing that we fail to address at our peril



Opinion: Why use-of-force training is failing

police officers

By Deputy Chief (ret.) Mitch Cunningham

We cannot allow officers to use outdated, ineffective and dangerous techniques

OTHER HIGHLIGHTS



Crowd control, riot response resources for police

By Greg Friese, Editorial Director

As George Floyd protests spread across the U.S., use these PoliceOne articles, resources and expert analysis to prepare officers to respond to civil unrest



Policing Matters Podcast: How

cops can prepare for riots

By Policing Matters Podcast

Doug and Jim discuss how police leaders can prepare for the worst, which could be just one controversial incident away



Photo of the Week: Wildfire patrol

By PoliceOne Members

Utah Bureau of Land Management troopers are patrolling areas at a high risk for wildfires. The goal is to prevent wildfires before they start

FEATURED DEAL



Olight Has the World's First Compact Rechargeable Light With an Adjustable Rail

Get 40% off today!

FEATURED EDUCATION



Earn a $2,500 Scholarship

Develop key leadership skills with this top-ranked online master's degree.

FEATURED COMPANY NEWS

[Free guide] Making the case for ALPR at small to midsize agencies



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: MissionCritical Communications
To: McCarthy, Steven (POL)
Subject: NEWS - P25 CAP for ISSI/CSSI | NPSTC Against FirstNet Interop | 6 GHz Rules
Date: Wednesday, April 8, 2020 12:23:34 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

If you have trouble reading this, go to the online version.
DO NOT REPLY TO THIS EMAIL — Use the link at the bottom of this email to manage preferences or unsubscribe.

April 8, 2020

P25

First P25 CAP ISSI/CSSI Testing Lab Accredited

The P25 CAP plans for ISSI and CSSI testing continue to move forward with the first accredited laboratory, according to DHS S&T officials, who oversee the program ... **READ MORE**

MCPTT

TECHNOLOGY

- **Viewpoint: Is Direct Mode the Holy Grail of Critical Broadband Communications?**
- **Samsung Demos Mission-Critical Video Call on Amazon Cloud Platform**
- **New Initiative to Accelerate Mission-Critical Broadband Testing**
- **DHS Assesses Drones for Public Safety Over 4-Day Project**
- **Illinois Court's Coronavirus Order Does Not Affect Motorola-Hytera Deadlines**

Thank You Responders

REGULATORY

- **NPSTC Files Against FirstNet Interoperability, T-Mobile Files in Favor**
- **FCC Chairman Moves Forward on Rules to Allow Wi-Fi at 6 GHz**
- **8 Senators Urge Senate to Include T-Band in Upcoming Coronavirus Legislation**
- **T-Mobile US Completes Merger with Sprint**
- **Committee to Assist FCC in Reviewing Foreign Participation Licenses**
- **FCC Proposes $20K Fine Against NYC Station for EAS Tone Broadcast**
- **FCC Reminds State and Local Governments on WEA for COVID-19 Alerts**

SUBSCRIBE

WEBINARS ON DEMAND

Topic: Protecting Critical Communication Systems from Interference
Cost: FREE
Sponsored by: Anritsu
WATCH ON DEMAND

Topic: Enforcing First Responder In-Building Radio Coverage
Cost: FREE
Sponsored by: Freedom, an Astronics company
WATCH ON DEMAND

eLearning

MOST READ STORIES

FirstNet MCPTT
AT&T announced a "controlled introduction" of MCPTT.

COVID-19 Pandemic
Fire officials offered advice for fighting the pandemic.

EVENTS

• EWA Asks FCC for Wireless System Buildout Extensions

E-Books

BUSINESS

• AT&T Offers Financial Update
• Discount Two-Way Radio Repairs Radios for Johns Hopkins During Pandemic
• AT&T, Verizon Support Navy Ships During COVID-19 Pandemic
• Verizon Provides Enhanced Compensation for Mission-Critical Employees
• Hytera America Donates DMR Radios to N.Y. EMS Organization
• Sonim Deploys XP8 Devices to Public Safety for COVID-19 Response
• L3Harris Wins $23M Space Contract
• General Devices Offers Direct-to-Patient Telehealth App in NYC
• California Authority Selects Federal Engineering for Fire, EMS Study
• AT&T Announces $200 FirstNet Activation Credit
• Axon Partners with ALPR Provider Flock Safety
• PCTEL Terminates Share Repurchase Program

PEOPLE

• Aviat Promotes Chang, Eliminates COO Position
• V-COMM Promotes Day to Engineering Manager

FOR MORE NEWS, CLICK HERE...

SUBMIT NEWS HERE

Advertise

June 13 – 18: NENA Conference and Expo, Long Beach, California. National Emergency Number Association (NENA): https://nena.org/nena2020

RESOURCE CENTER

Find white papers, e-books and webinars in the Resource Center.
Visit the Resource Center

SUPERGUIDE

SuperGUIDE will help you source nearly 800 wireless equipment and service suppliers by category and type.
Link to SuperGUIDE

CONTACT US

You are receiving this email because you subscribed to MissionCritical Communications.

By requesting a subscription and filling out the subscription form you agreed to be contacted via email, postal mail or other methods, regarding your magazine subscription or related editorial content and industry news. We will never share your information without your explicit permission, you can cancel your subscription and update your preferences at any time, and we will honor your wishes to remove your data from our systems.

Click here to manage your email preferences.

Click here to unsubscribe from MissionCritical Communications magazine.

This email was sent by Pandata Corp., 7108 S. Alton Way, Building H, Centennial, CO, 80112, USA, +1-303-792-2390

Pandata Corp. publishes MissionCritical Communications, RadioResource International and RRMediaGroup.com

Copyright 2020, Pandata Corp. All rights reserved.

From: Dwork, Marcela (NOR)
Subject: News Clips April 17, 2020
Date: Friday, April 17, 2020 10:36:34 AM

Boston Globe

With 30 residents dead, Belmont Manor emerges as another symbol of misery in coronavirus pandemic
By Laura Crimaldi and John R. Ellement Globe Staff, Updated April 16, 2020, 11:52 a.m.

- For more than 50 years, Belmont Manor Nursing and Rehabilitation Center has been the sole option for skilled nursing care in Belmont and the life's work of two generations of the Karger family, which opened the facility in 1967.

- On Thursday, the family-owned nursing home near the open fields and woodlands of the Beaver Brook Reservation emerged as another symbol of misery in the COVID-19 pandemic, after the facility announced the virus had killed 30 patients, accounting for all but one death in Belmont apparently connected to the illness.

- The development came as the state announced 2,263 new infections and 137 new deaths attributed to the coronavirus. The virus has claimed the lives of 1,245 people in Massachusetts, 49 percent of whom lived in long-term care facilities.

- During his daily briefing on Thursday, Governor Charlie Baker urged residents to cooperate with a growing team of "contact tracers" mapping the spread of COVID-19. The project, launched with Boston-based nonprofit Partners in Health, has hired 176 people, and many more will be coming online in the coming weeks. The program, Baker said, will help officials craft strategies to stem the spread of the virus.

- They are interviewing patients about whom they had had close contact with. "We urge residents to take this call and provide the relevant information" if reached by the contact tracers, Baker said. He called the initiative "key to helping the state build a strategy for how we can get back to something like a new normal."

- Baker also provided an update Thursday on the state's supply of personal protective equipment and hospital bed capacity. He said the state has distributed more than 3.8 million pieces of gear, including masks, gloves, and gowns, to hospitals, nursing homes, community health centers, and public safety personnel.

- In the state's hospitals, Baker said, roughly half of the 17,800 beds are in use, with temporary hospitals in Boston and Worcester, as well as temporary

facilities opening soon in Bourne, Lowell, and Dartmouth, available to address any potential overflow as coronavirus cases surge.

- “We do want to be able to rely on those beds if we need them,” Baker said.

- In Belmont, the death toll at Belmont Manor is among the highest publicly disclosed in the state among elder-care facilities.

- “It’s horrible," said Town Administrator Patrice Garvin. "There are just no words to describe it.”

- The state-run Soldiers’ Home in Holyoke had seen 52 deaths as of Thursday, including 44 linked to COVID-19. With a total of 222 positive cases, 81 staffers and 141 residents, the outbreak there is outpacing the toll at a nursing home in Kirkland, Wash., which marked the onset of the US crisis and has been linked to 37 deaths.

- There are 232 long-term care facilities in Massachusetts that have reported at least one case of COVID-19, the state said, and so far 4,798 residents and workers have been infected. State officials said this week that about half of the people who have died of the virus in Massachusetts lived in long-term-care facilities.

- “One thing we know about nursing homes is that it can spread very quickly,” state Secretary of Health and Human Services Marylou Sudders said at a State House news conference.

- The state had assigned a rapid-response clinical team to work with Belmont Manor, she said.

- “Every member of the Belmont Manor team is heartbroken by the losses of beloved members of our community. From the beginning of this pandemic, we have taken every possible step to address this fast-moving situation," said a statement from administrator Stewart Karger, who began working at the facility under his father in 1979.

- The death of a patient on April 1 was the first linked to COVID-19 at Belmont Manor. On Saturday, the town said 13 patients there had died from the virus.

- Then in a letter to families dated Wednesday, Belmont Manor announced that a total of 30 patients had died, including four who had been hospitalized.

- “Every death represents an enormous amount of loss to the families of these individuals,” Karger wrote. “And because many of these residents have been with us for a longer period of time, this feeling of loss is something that we at Belmont Manor share.”

- The letter said 116 residents have tested positive with two test results outstanding. Among employees, 59 have tested positive out of 94 who have been tested. The company said it employs around 190 people.

- Belmont Manor Nursing Home Inc. has a five-star rating from Medicare, which bases its ratings on health inspections, staffing, and quality measures. Belmont Manor's rating is "much above average," according to Medicare. The facility has 135 certified beds.

- Cynthia Lee Segal, 72, died at Belmont Manor on April 9 after becoming infected, her sister said.

- Linda Fritz said Segal developed a fever in late March and later tested positive for COVID-19.

- A nurse facilitated two FaceTime calls for the sisters before Segal died, Fritz said.

- "They were very kind, and I think they are stunned by this happening, too," said Fritz, who lives in Newton.

- Still, Fritz said, the Centers for Disease Control and Prevention made it too difficult to get testing in nursing homes, and plans by the state and Belmont Manor to address the outbreak have proven inadequate.

- "I would like to think that Belmont Manor and the large number of deaths resulting at the nursing home should give nursing homes, the state, and maybe the country many lessons learned for the next wave of the pandemic," she said.

- Garvin said town officials began communicating with Belmont Manor about COVID-19 on March 5 and delivered 900 masks to the facility. On Thursday, she said the town planned to deliver 150 gowns to the nursing home.

- The state said it has been in touch with the facility by phone for two weeks and planned to help the facility with staffing.

- The National Guard has performed 43 tests onsite, and another 190 self-test kits have been delivered to Belmont Manor, the state said.

- Sudders on Thursday said Massachusetts is one of two states offering mobile testing to nursing homes, rest homes, assisted-living facilities, and other state-run care centers.

- As of Thursday, the state had administered 5,883 tests at 279 elder-care

facilities and 10,995 self-test kits had been sent to 103 facilities, Sudders said. The National Guard also planned to visit 11 sites Thursday and administer about 1,300 tests, she said.

WBUR

30 Deaths, Another 86 Positive Tests: Nearly All Belmont Manor Nursing Home Residents Have The Coronavirus
April 16, 2020
Miriam Wasser

- It began with a fever and a dry cough on March 28. The following day, the elderly man was transferred from the Belmont Manor nursing home to the hospital, where he was tested for the coronavirus.

- The results came back positive on March 30, nursing home administrator Stewart Karger told Wicked Local; Belmont Manor, a 135-bed family-owned and operated nursing home, had its first coronavirus case.

- As of April 15, 30 residents have died from COVID-19 -- four of whom had been transferred to the hospital. Another 86 residents have tested positive for the virus, and two others await test results, Belmont Manor spokeswoman Diana Pisciotta said.

- In an email dated April 11, Karger reported that 14 residents had died, meaning that fatalities at the nursing home more than doubled in five days.

- "Every member of the Belmont Manor team is heartbroken by the losses of beloved members of our community," he said in a statement. "From the beginning of this pandemic, we have taken every possible step to address this fast moving situation."

- Meanwhile, 59 of the nursing home's 190 employees have tested positive. Belmont Manor is hoping to get all employees tested soon, Pisciotta said.

- Older adults have been particularly hard hit by the coronavirus because they often have other underlying health issues. In Massachusetts, 37% of people testing positive for the virus are 60 or older, and according to state data, the vast majority of recent fatalities have been people in their 70s and older.

- The state has also reported that as of Wednesday afternoon, 530 people have died from COVID-19 at long-term care facilities in Massachusetts, and another 4,163 residents and employees have tested positive for the virus. To date, 222 long-term care facilities in the state have at least one positive case.

- "This is an incredibly infectious and unpredictable virus that is lethal to the

elderly and those with multiple medical conditions, which is exactly our nursing home resident population," Tara Gregorio, of the Massachusetts Senior Care Association, told WBUR in an email.

- Leaders at Belmont Manor declined interview requests, but noted in a statement that staff are using "aggressive infection control methods" and "carefully monitoring all residents" for signs of the virus.

- Complicating matters at Belmont Manor — and other long-term care facilities — is the fact that some residents who have the virus are asymptomatic. Though the National Guard is testing people at nursing homes around the state, demand still exceeds supply. Earlier this week, Gov. Charlie Baker said that 4,500 seniors at 264 long-term care facilities had been tested, but that another 77 facilities had requested at least 8,600 more tests.

- "Testing is crucial for a number of reasons, but most of all, it gives us the opportunity to identify and then isolate people who have tested positive and to make sure they get treatment," Baker said. "It helps us understand where the outbreaks are and to keep people informed with respect to infection, even if they don't have symptoms, to slow the spread."

- But not everyone at Belmont Manor could get a test easily. An email from Karger dated April 11 said that only symptomatic residents were being tested.

- "We've had the same experience as other long-term care facilities in that at the outset, because of limitations on testing and testing supplies, we were only able to test symptomatic residents," Pisciotta said. She added that the National Guard has come back at least twice, and that as of now, all residents have been tested.

- Lisa Kimball's 96-year-old mother, Sandy Kimball, is one of the people who got tested when the National Guard came back. Kimball said she learned Wednesday that her mother has the virus — despite showing no symptoms.

- The diagnosis, though disheartening, wasn't particularly surprising. Kimball's mother requires assistance for most daily tasks, meaning aides are constantly in contact with her.

- "It's like a petri dish in there," Kimball said. "How can anyone get away from it?"

Boston Globe

Racist 'Zoom-bombing' invades Chinese class at Newton South High
By Matt Berg Globe Correspondent, Updated April 16, 2020, 2:04 p.m.

- On Wednesday morning, a Newton South High School advanced placement

Chinese class was underway on Zoom when hackers infiltrated the group, posting “vile, hate-filled images and speech” directed at the students, officials said.

- The incident, which lasted about three minutes, was part of a phenomenon known as “Zoom-bombing,” when a Zoom call is hacked into by individuals who disrupt a meeting. It was also an example, school officials said, of coronavirus-related racism that has run rampant since the beginning of the pandemic, often directed at the Asian community.

- Joel Stembridge, Newton South’s principal, wrote to the school community Thursday morning, calling the episode “clearly racist, hateful, and horrible.”

- “This was a traumatic experience for our teacher and students, and we will continue to offer support to everyone involved,” Stembridge said via e-mail. “To be clear, an attack on members of our NSHS Asian-American community is an attack on all of us. We will be working on a plan for responding — I will share more about this soon.”

- All Zoom meetings scheduled for Thursday were canceled, allowing the IT department and staff to check security protocols. Classes were to resume Friday, said Julie McDonough, a school spokeswoman.

- “Our counseling staff is reaching out to every student today," McDonough said. “We are scheduling a meeting with student leaders and teachers to plan a response. Hate speech and racism have no place at South and won’t be tolerated.”

- School officials notified students’ families and local police, who were investigating. Teachers and students were working with officials to gather information about the intruders, who did not appear to be associated with the high school, according to Stembridge’s e-mail.

- The intruders may have accessed the meeting through a link to the call that was created before security updates were made in recent weeks, Stembridge said. Hundreds of calls had been successful prior to the incident, he added.

- The intrusion comes as millions of people adopt the online platform for work or education. Since the pandemic started, Zoom has struggled to keep up with security features to prevent such incidents.

- After two Massachusetts schools reported “Zoom-bombing" in March, FBI officials in Boston urged users to take security precautions, such as sending links to participants directly instead of posting links in publicly available areas and making sure users have the most current version of Zoom’s teleconferencing software.

- “This is a trying time for all of us, and events such as these underscore the fragility of this new environment in which we are working,” Stembridge wrote. “We’ll have more work to do to ensure that we can continue to support students and build a safe, connected online community.”

SJC OK’s limited use of license plate readers to secretly collect current location and data of drivers
By John R. Ellement Globe Staff, Updated April 16, 2020, 3:26 p.m.

- In a ruling that hearkened back to British soldiers searching homes with “general warrants” in colonial Massachusetts, the state’s high court ruled Thursday that automatic license plate readers used by the State Police do not violate 21st-century privacy protections — under limited circumstances.

- In its unanimous ruling, the Supreme Judicial Court cautioned that it might elevate privacy issues in future cases if State Police and other law enforcement agencies start tapping information in the secretive data base, known by the acronym of ALPR, without proper justification.

- The court noted that both the federal and state constitutions have strong protections against unlawful search and seizures by law enforcement built into them by founders who had personal experience with the “abuses of arbitrary power under British rule." At that time, soldiers used “general warrants” to rummage through Colonial homes, the court noted

- "The framers had first-hand experience with abuses of arbitrary power under British rule...The surveillance implications of new technologies must be scrutinized carefully, lest scientific advances give police surveillance powers akin to these general warrants," Justice Frank M. Gaziano wrote.

- "Just as police are not permitted to rummage unrestrained through one’s home, so too constitutional safeguards prevent warrantless rummaging through the complex digital trails and location records created merely by participating in modern society," he added.

- But in the case that landed the issue before the SJC — police were alerted any time an alleged drug dealer drove over the Bourne or Sagamore bridges — the court said law enforcement properly used limited data from four cameras installed on the Cape Cod bridges, highly public location that people freely choose to travel on.

- As such, Cape and Islands District Attorney Michael O’Keefe, State and Barnstable police did not violate the constitutional rights of Jason McCarthy when they used the ALPR system to learn when and how often he drove over the bridges during one 74-day period in 2016 and 2017. Nor were his rights violated when real-time alerts allowed police to track McCarthy as he allegedly

twice engaged in alleged drug sales in Barnstable that led to his indictment.

- "While we cannot say precisely how detailed a picture of the defendant's movements must be revealed to invoke constitutional protections, it is not that produced by four cameras at fixed locations on the ends of two bridges," Gaziano wrote.

- McCarthy has pleaded not guilty to all charges.

- O'Keefe applauded the SJC's conclusion while noting that he is among those who do not want to see government have so many surveillance cameras installed that they can track a person from the moment they leave home until the moment they return.

- "When you have cameras everywhere that have the ability to track you, I don't think we want to have that in American society," O'Keefe said. "But we are not there yet. And certainly this case is not an example of that kind of broad overreach…This is a very limited use of cameras [installed] at a fixed point."

- The court acknowledged that the way it resolved the legal questions raised by McCarthy and his defense attorney, Paul Bogosian, creates more legal questions than answers. The American Civil LIberties Union and the Electronic Freedom Foundation had urged the SJC to mandate that police obtain search warrants before accessing ALPRs data or setting up an alert.

- Kade Crockford, director of the Technology for Liberty program at the ACLU of Massachusetts said the SJC has now set the stage for the Legislature to step in and provide more privacy protections for Massachusetts residents.

- "Now that the state's highest court has held that once it crosses a certain threshold, persistent, dragnet surveillance of motorists' movements would violate the Constitution, the ball is now in the legislature's proverbial court to fill in the details," Crockford said in a statement.

- In a footnote, Gaziano wrote that the SJC expects to provide answers to those questions in future cases.

- "In declining to establish a bright-line rule for when the use of ALPRs constitutes a search, we recognize this may bring some interim confusion," Gaziano wrote. "We trust, however, that as our cases develop, this constitutional line gradually and appropriately will come into focus."

- The total number of State Police-installed license plate reading cameras, and where they are, is not publicly known. State Police refused to provide the information to the Globe and it is not part of the evidence in the McCarthy case reviewed by the SJC.

- Data collected from the cameras is maintained in a database for one year under rules issued by the Executive Office of Public Safety and Security.

Coronavirus spreads to 3 state-run facilities for those with mental illness, developmental disabilities
By Matt Rocheleau Globe Staff, Updated April 16, 2020, 10:02 a.m.

- Three state-run medical centers that serve people with chronic conditions, mental illness, and intellectual disabilities are reporting widespread COVID-19 outbreaks among their live-in patients and staff.

- In recent days, teams from either the National Guard or a local ambulance company were brought in to each facility to conduct testing, according to state officials. The spread of the virus presents a particular challenge for these facilities, which are trying to quell the disease while serving a vulnerable group with complex mental and medical conditions.

- State officials said that, as of Tuesday, 67 patients and 46 staff had tested positive at the 394-bed Tewksbury Hospital. At the 255-bed Lemuel Shattuck Hospital in Jamaica Plain, 37 patients and 23 staff had tested positive. Both facilities specialize in providing long-term treatment for adults.

- Officials also identified at least 44 positive cases among residents and 55 staff at the Hogan Regional Center in Danvers, according to the Massachusetts Nurses Association, a union that represents health care workers at each site. The facility houses and provides long-term care for about 120 people with intellectual and development disabilities.

- None of the facilities have seen the same deadly consequences as nursing homes, which serve populations in the age range considered most at risk for complications from coronavirus. Nearly half of the state's deaths have been attributed to those types of long-term care facilities. Still, many of the obstacles that nursing homes face also are prevalent at these chronic care facilities, and officials are preparing for the worst.

- "It is a terribly challenging time, but people have come together and we have leadership [at the facilities] that is determined to get the resources these centers need," said Danna Mauch, president and CEO of the Massachusetts Association for Mental Health, an advocacy group.

- State officials said the facilities have been following federal and state guidelines to protect patients and staff.

- "We are and will continue to do everything in our power to ensure an aggressive and rapid response to COVID-19 confirmed cases at facilities operated and overseen by the Commonwealth," said a statement from the

state’s Executive Office of Health and Human Services.

- Officials said they have implemented measures such as isolating infected patients, restricting visitors, and taking employees’ temperatures and screening for symptoms before they enter buildings. Patients now eat meals in their rooms instead of in common areas.

- However, cutting off access to loved ones and disrupting routines can be particularly hard for people living in such facilities, potentially leading to confusion, anxiety, and depression, advocates said.

- Kathy Marith said her brother Dan, 63, a resident at the Hogan center, recently tested positive for COVID-19. So far, he’s been symptom-free, she said.

- She worries not only for him, but for the facility’s many other residents, especially elderly and frail patients.

- “I’m nervous for all of them,” said Marith, who has been in close contact with the staff, whom she credited with being proactive in trying to prevent the virus’s spread.

- Chronic care facilities have long struggled to maintain adequate staffing, a problem driven by low compensation, according to Mauch, of the mental health advocacy association. That issue has been exacerbated, she said, by the ongoing crisis because workers have had to miss work because they’re sick themselves or caring for loved ones.

- The nurses association, as well as officials at the Service Employees International Union Local 509, said they have urged state officials to provide on-site testing for workers at each facility. So far, widespread testing has been offered only for patients, union officials said. Workers are being tested only if symptomatic, and dozens have tested positive, they said.

- “The only people going in and out of the facilities are the staff,” said nurses association spokesman David Schildmeier. “So it makes no sense to not be testing staff.”

- Union officials said workers have also reported concerns in at least some facilities about the limited availability of personal protective equipment, with some staff rationing supplies such as masks. Peter MacKinnon, president of SEIU Local 509, said some social workers have told the union that because of staffing shortages they’re now being asked to take on front-line duties but without proper training.

- State officials acknowledged staff are being asked to conserve protective gear, but insisted the equipment is available and the state is continuing to try to procure more supplies.

- The state operates a handful of other hospitals and centers across Massachusetts that provide long-term specialty care. Altogether, those facilities have reported just one patient and seven staff members who have tested positive, state officials said, though they declined to provide figures for one facility, the Wrentham Developmental Center.

- The state Department of Developmental Services, which runs the Hogan and Wrentham sites and operates or funds thousands of group homes statewide, said that, across its network, nine residents had died and 276 residents and 321 staff had tested positive for coronavirus, as of Tuesday. Testing is ongoing.

- Tom Frain, whose brother lives in a group home, said while state officials have moved to test nursing home residents across the state, testing for people with developmental disabilities has been done too slowly. “People like my brother — they get nothing.”

- “They’ve been functionally abandoned by the administration,” said Frain, president of COFAR, a local advocacy group for people with intellectual and developmental disabilities. “We’re now in a solid six weeks of this and they did their first testing on Easter Sunday.”

- “What are they waiting for?” he added. “Why is my brother so far at the end of the line?”

Boston Herald

Coronavirus isolation raises concerns among Massachusetts advocates of domestic violence, assault victims
By ERIN TIERNAN | etiernan@bostonherald.com | Boston Herald
PUBLISHED: April 16, 2020 at 8:43 p.m. | UPDATED: April 16, 2020 at 8:43 p.m.

- Stay-at-home advisories are causing concern among advocates who are sounding the alarm for victims of domestic violence and sexual assault who may be trapped inside with their abusers.

- “The isolation that occurs behind the walls of a house fosters sexual abuse, domestic violence, impacts children … it’s happening in our neighborhoods. It happened before this and it’s still happening now,” said Debra Robbin, executive director of Jane Doe Inc., a victims’ advocacy organization.

- Robbin said it’s difficult to gauge just how severe the impact of quarantining and isolation are on survivors, but said it’s important people know there are still resources available. Nonprofits are still operating hotlines and she said support groups and prevention resources have rapidly moved online.

- Arrests for violent crimes often associated with domestic violence, like aggravated and simple assaults, were up by 19% and almost 50% respectively in the months leading up the coronavirus pandemic, according to Boston Police data.

- Last week, the state expanded services accessed through its confidential domestic violence hotline, called SafeLink, to also include resources and support for survivors of sexual assault, Lt. Gov. Karyn Polito announced during the press conference.

- Polito indicated domestic violence and sexual assault reporting is “way down” and the hotline, which is accessible through the state’s 211 system will now directly connect callers to rape crisis centers and domestic violence programs that can provide services.

- “In this time of physical distancing it is critical that we maintain social connection, especially for those who are experiencing domestic violence,” Polito said

- In March, simple assaults were still up 22% even as Gov. Charlie Baker enacted a stay-at-home advisory on March 24 and Boston Mayor Martin Walsh announced arrests were down 21% overall that month.

- “This isolation can mean danger for some members of our City. Make no mistake, you are not alone and no one deserves to be abused. To those in need of help, there are resources available to you. Please reach out if you, or someone you know, is in need of help or safety planning,” Sgt. John Boyle said in a statement.

- It’s difficult to track statistics on actual rates of domestic violence and sexual abuse because of a widespread lack of reporting, Robbin said.

- The coronavirus was cited as a factor in abuse in more than 3,000 calls to the National Domestic Violence Hotline in a three-week span, indicating the pandemic is having an effect.

Law.com

Ahead of the Supreme Court’s First Telephonic Arguments, Some Tips From the Trenches
Morrison & Foerster’s Joseph Palmore recently argued his first telephonic oral argument before the highest court in Massachusetts. He shares his thoughts on what makes a successful session.
By Joseph Palmore | April 16, 2020 at 11:29 AM

- The U.S. Supreme Court announced this week that it will hold oral arguments in May by teleconference and that “[d]etails will be shared as they become available.” Those details matter—they’ll help determine whether the Court’s pandemic-forced innovation will succeed.

- I argued an appeal by phone last week. That gives me exactly one more such argument than many appellate lawyers—who, like me until very recently, have done zero. That doesn’t make me an expert, but my experience has led to thoughts on how the Supreme Court can make the best of this format.

- First a bit of background. I argued before the Massachusetts Supreme Judicial Court, the commonwealth’s highest court. Like the U.S. Supreme Court, it’s hearing arguments by phone. And the Massachusetts court has seven justices, which makes it similar in size to the U.S. Supreme Court. All of this means the Supreme Judicial Court is something of a test case for the justices and court officers now planning the Supreme Court’s phone arguments.

- The Supreme Judicial Court follows this standard format for its phone arguments:

- First, each advocate gets three minutes at the start of their time to speak without interruption.

- Second, justices are recognized in descending order of seniority by the chief justice to ask their questions. The chief justice goes last. After one full round, the chief asks the justices if they have any additional questions.

- Third, while each side still has a formal time limit of 15 minutes, no buzzer or chime marks it. Allowing each justice to ask questions in turn (with a second round when necessary) means that many of the arguments have gone over time.
- Fourth, the argument audio is live-streamed to the general public.

- The Clerk for the Commonwealth Fran Kenneally and his excellent team clearly communicated this format to advocates in advance. The chief justice then reiterated it at the start of each argument.

- The U.S. Supreme Court’s prior practices and already-announced plans mirror some of this. The Supreme Court recently began allowing advocates two minutes of uninterrupted time to open their arguments. And the high court has already announced it will livestream the audio of its telephone arguments. A first for the court, livestreaming is a welcome move in favor of public access to its work.

- The main challenge of telephone arguments at the Supreme Court will be justices’ questioning. A typical Supreme Court argument can be like an 8-on-1

game of ping-pong, in which advocates answer questions in rapid succession from different, often-interrupting Justices. (It's 8-on-1 instead of 9-on-1 because Justice Clarence Thomas is famously silent during oral argument.)

- That free-for-all, rapid-fire mode of argument may be ill-suited to a teleconference. Some federal courts of appeals, like the Federal Circuit, have allowed judges to ask questions in the ordinary, unstructured way during phone arguments without much problem. But what works for a three-judge panel may be unwieldy for a nine-Justice Supreme Court.

- Anyone who has participated in a large conference call knows how common it is for people to talk over each other, awkwardly pause and then do it again. The slight time lag on the phone and the inability to see visual cues that someone is about to speak can make for a frustrating conversation. Those difficulties are compounded when multiple people are eagerly trying to interject or disagree—people like the justices at a typical argument.

- Another problem with attempting the court's traditional, freewheeling approach on the phone would be identifying which Justice is speaking. Veteran court observers may be able to guess a questioning Justice by voice, but first-time advocates and members of the public may not.

- One solution would be to follow the Supreme Judicial Court's approach of having justices ask questions in seniority order. That would avoid cross-talk and limit interruptions. It would also allow participants and listeners to identify a justice who speaks because the chief justice would have called on them. But that format would not allow Justices to easily follow up on other Justices' questions, as often happens in live arguments.

- If the court prefers a less-rigid approach, it could use a hybrid system. Justices could notify the chief justice by email that they have a question, allowing him to call on each in turn. The chief could use this air traffic-control power to spread questions equitably, identify each speaking justice by name and keep the arguments roughly within their assigned time limits.

- On the other side of the equation are the advocates who will argue by phone in May. From the attorney's perspective, what is different about presenting argument by phone? Not much actually. Whether in person, over the phone or on video, the oral advocate's goals are the same: Make the important affirmative points, directly answer questions and know the record and relevant law cold.

- To prepare for my phone argument, I had the same kind of moot courts as always. I did the "in-role" portion telephonically to simulate the coming argument, followed by a debrief session on video. I also made the same kind of argument outline I always do. But, just as I never look at an outline during an in-person argument, I did not do so during the phone argument, preferring

natural conversation to reading.

- A final word on technology and the need for testing. During my argument, audible static could be heard on my line when I spoke, likely due to storms moving through Washington, D.C., at the time. The high court should consider a pre-argument audio check, in which advocates and justices can call in, test sound quality and ensure a good connection.

- I commend the court for proceeding with oral arguments. With careful planning and communication, its telephone sessions will be successful. And they will provide the public valuable access to a part of their government that has shown admirable flexibility in proceeding with its business in these difficult times.

From: PoliceOne Roll Call
To: McCarthy, Steven (POL)
Subject: NJ cops can commandeer medical supplies; Reactivating retirees
Date: Friday, April 3, 2020 4:38:52 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

April 3, 2020 | View as webpage

Dear PoliceOne Member,

What caused you stress two months ago is vastly different from what is causing stress today as the entire world battles COVID-19. As a first responder, you are on the front lines of this fight, which not only causes you concern for your physical safety, but also how you could compromise the safety of your family.

Staying mentally healthy is key to survival. In a recent Lexipol webinar, law enforcement trainer, resilience expert and former paramedic Mike Taigman provided strategies to lower your stress and build resilience during the coronavirus crisis.

"Mike Taigman explained the neuroscience for the increased stress many of us are experiencing and gave immediate, easy-to-use techniques to alleviate some of that stress," said Lexipol Editorial Director Greg Friese. "Many of Mike's suggestions can be put to use as you prepare to go on duty, in the spare minutes between calls for service or on the drive home from another unbelievable shift."

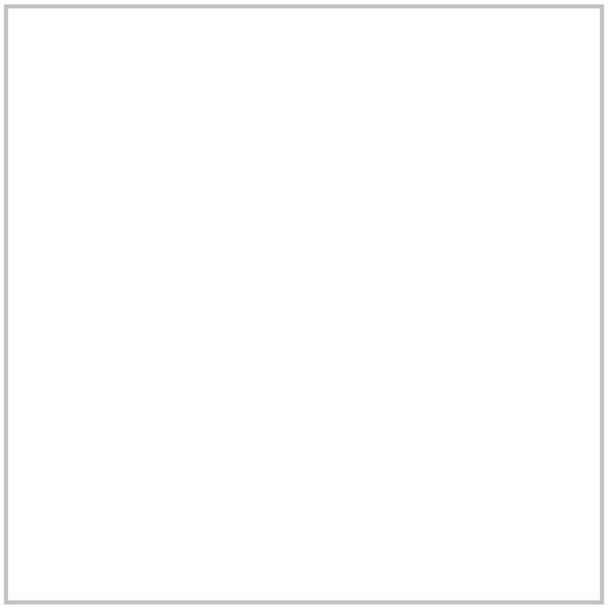
Watch this free on-demand webinar here.

— Nancy Perry
Editor-in-Chief, PoliceOne.com

TOP STORIES

Colo. deputy dies from COVID-19

Deputy Jeff Hopkins, a 19-year veteran of the department, died one day after testing positive for the coronavirus



Calif. deputy dies from COVID-19 complications

NJ state police given power to commandeer medical equipment, supplies for COVID-19 fight

Ill. chiefs ask governor for confirmed COVID-19 patient addresses to boost responder safety

Calif. deputies shop for elderly man who didn't want to leave his home due to COVID-19

Utah officer pays bill after someone 'prank calls' large order at restaurant

ELSAG® ECSS ALPR Data Storage Solution



Leonardo's ELSAG Cloud Storage Solution lets you keep ownership of your ALPR data while giving away the responsibilities of managing a server. Save time and money with ELSAG CSS.

Get the details

LPR Adds Actionable Intelligence to In-Car Video



Your first responders do more — why shouldn't your technology? By joining the power of license plate recognition to a WatchGuard 4RE In-Car system, your team can turn static data into actionable intelligence.

Add LPR today

COVID-19 SPECIAL COVERAGE



Reactivating retirees for police service in times of crisis

By Bob Harrison

Law enforcement leaders should consider ways to clear a path to bring retirees back to work to support public safety



Quick Take: How police leaders can improve officer safety during the COVID-19 crisis

By Sarah Calams

Seattle Police Chief Carmen Best identifies how departments can keep an open line of communication with officers as they respond to the pandemic



Reader poll: 92% say LEOs should get hazard pay during the COVID-19 crisis

By Cole Zercoe

As COVID-19 strengthens its grip on the United States, there's been increasing talk among lawmakers, unions and officers of boosting compensation for LEOs

OTHER HIGHLIGHTS



The hazards of bail reform

By Policing Matters Podcast

Advocates of accused offenders have called for "cash bail" to be ended, citing economic inequities



Photo of the Week: Post-training pose

By PoliceOne Members

After completing building clearance training last month, officers wanted to take a picture...while taking social distancing precautions, of course.

FEATURED JOB



Lateral Police Officer - $10,000 Lateral Signing Bonus, Plus Other Incentives!

Apply now!

FEATURED JOB



Lateral Police Officer - $10,000 Lateral Hiring Incentive

$5882-$7507* monthly - Vancouver, Washington.



PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: WatchGuard
To: McCarthy, Steven (POL)
Subject: Now Available! License Plate Recognition with WatchGuard In-Car System
Date: Tuesday, January 21, 2020 5:40:04 PM

Not rendering correctly? View this email as a web page here.

Small on Grey.jpg

ALPR-in-car-1with WG Logos-blur-email-600

Now Available! License Plate Recognition with WatchGuard 4RE In-Car Video System

The WatchGuard 4RE Mobile ALPR Solution harnesses the power of the industry-leading WatchGuard 4RE in-car video system and high-definition cameras to detect and match vehicle license plates of interest stored in a database of over 20 billion detections.

Increase Officer Safety - Help distinguish between a routine traffic infraction stop and something potentially more serious.

Proactively Interrupt Crimes - Alert officers to vehicles of interest in real-time, potentially interrupting a string of crime.

Deliver Leads to Solve More Cases - Use historical data to determine a vehicle's proximity to crime scenes, providing leads crucial to an investigation.

Discover the WatchGuard 4RE Mobile ALPR Solution

WatchGuard Video
415 E Exchange Parkway
Allen, TX 75002
USA

You received this email because you are subscribed to Products from WatchGuard Video.

Update your email preferences to choose the types of emails you receive.

Unsubscribe from all future emails

2187

From: PoliceGrantsHelp Alert
To: Tapis, Stephen C (POL)
Subject: Pay for ELSAG® License Plate Readers with grant money
Date: Wednesday, September 16, 2020 9:31:18 AM

Having trouble viewing this email? View it in your browser.

Find Grant Money to Pay for ELSAG® Automatic License Plate Reader Technology

We have partnered with PoliceGrantsHelp.com to help you access government grant dollars.

ELSAG Plate Hunter ALPR systems bring incredible efficiencies to real-time policing, security and investigations. Proven force multipliers, our solutions include fixed, mobile and covert plate readers, and our newly released ELSAG Video Plate Hunter 900 – a

low-cost option for tight budgets. All systems assist law enforcement with vehicle-related missions including:

- Recovering stolen vehicles and license plates
- Removing unregistered vehicles and unlicensed drivers from roads
- Finding missing persons
- Finding vehicles suspected of involvement in unlawful activity
- Parking management and enforcement
- Collecting criminal intelligence
- Permit validation and tolling
- Collection of traffic data



There's no better time than now to deploy ELSAG automatic license plate readers.

Get FREE ALPR Grant Help

For information about ELSAG Plate Hunter® ALPR systems, visit **leonardocompany-us.com.**

Selex ES Inc., a Leonardo Company. 4221 Tudor Lane Greensboro NC USA 27410-8105

If you do not wish to receive future Police1 Product Alerts, please unsubscribe.
To change your email address, update your profile. © 2020: Police1.com. All Rights Reserved.
2611 Internet Blvd., Ste. 100, Frisco, TX 75034

2189

From: PoliceGrantsHelp Alert
To: Ramsland, Erik (POL)
Subject: Pay for ELSAG® License Plate Readers with grant money
Date: Wednesday, September 16, 2020 9:30:31 AM

Having trouble viewing this email? View it in your browser.

Find Grant Money to Pay for ELSAG® Automatic License Plate Reader Technology

We have partnered with PoliceGrantsHelp.com to help you access government grant dollars.

ELSAG Plate Hunter ALPR systems bring incredible efficiencies to real-time policing, security and investigations. Proven force multipliers, our solutions include fixed, mobile and covert plate readers, and our newly released ELSAG Video Plate Hunter 900 – a

low-cost option for tight budgets. All systems assist law enforcement with vehicle-related missions including:

- Recovering stolen vehicles and license plates
- Removing unregistered vehicles and unlicensed drivers from roads
- Finding missing persons
- Finding vehicles suspected of involvement in unlawful activity
- Parking management and enforcement
- Collecting criminal intelligence
- Permit validation and tolling
- Collection of traffic data



There's no better time than now to deploy ELSAG automatic license plate readers.

Get FREE ALPR Grant Help

For information about ELSAG Plate Hunter® ALPR systems, visit **leonardocompany-us.com.**

Selex ES Inc., a Leonardo Company. 4221 Tudor Lane Greensboro NC USA 27410-8105

If you do not wish to receive future Police1 Product Alerts, please unsubscribe.
To change your email address, update your profile. © 2020: Police1.com. All Rights Reserved.
2611 Internet Blvd., Ste. 100, Frisco, TX 75034

2191

From: PoliceGrantsHelp Alert
To: Cronin, John E (POL)
Subject: Pay for ELSAG® License Plate Readers with grant money
Date: Wednesday, September 16, 2020 9:04:45 AM

Having trouble viewing this email? View it in your browser.

Find Grant Money to Pay for ELSAG® Automatic License Plate Reader Technology

We have partnered with PoliceGrantsHelp.com to help you access government grant dollars.

ELSAG Plate Hunter ALPR systems bring incredible efficiencies to real-time policing, security and investigations. Proven force multipliers, our solutions include fixed, mobile and covert plate readers, and our newly released ELSAG Video Plate Hunter 900 – a

low-cost option for tight budgets. All systems assist law enforcement with vehicle-related missions including:

- Recovering stolen vehicles and license plates
- Removing unregistered vehicles and unlicensed drivers from roads
- Finding missing persons
- Finding vehicles suspected of involvement in unlawful activity
- Parking management and enforcement
- Collecting criminal intelligence
- Permit validation and tolling
- Collection of traffic data



There's no better time than now to deploy ELSAG automatic license plate readers.

Get FREE ALPR Grant Help

For information about ELSAG Plate Hunter® ALPR systems, visit **leonardocompany-us.com.**

Selex ES Inc., a Leonardo Company. 4221 Tudor Lane Greensboro NC USA 27410-8105

If you do not wish to receive future Police1 Product Alerts, please unsubscribe.
To change your email address, update your profile. © 2020: Police1.com. All Rights Reserved.
2611 Internet Blvd., Ste. 100, Frisco, TX 75034

2193

From: PoliceGrantsHelp Alert
To: Irwin, Patrick (POL)
Subject: Pay for ELSAG® License Plate Readers with grant money
Date: Wednesday, September 16, 2020 9:03:10 AM

Having trouble viewing this email? View it in your browser.

Find Grant Money to Pay for ELSAG® Automatic License Plate Reader Technology

We have partnered with PoliceGrantsHelp.com to help you access government grant dollars.

ELSAG Plate Hunter ALPR systems bring incredible efficiencies to real-time policing, security and investigations. Proven force multipliers, our solutions include fixed, mobile and covert plate readers, and our newly released ELSAG Video Plate Hunter 900 – a

low-cost option for tight budgets. All systems assist law enforcement with vehicle-related missions including:

- Recovering stolen vehicles and license plates
- Removing unregistered vehicles and unlicensed drivers from roads
- Finding missing persons
- Finding vehicles suspected of involvement in unlawful activity
- Parking management and enforcement
- Collecting criminal intelligence
- Permit validation and tolling
- Collection of traffic data



There's no better time than now to deploy ELSAG automatic license plate readers.

Get FREE ALPR Grant Help

For information about ELSAG Plate Hunter® ALPR systems, visit **leonardocompany-us.com.**

Selex ES Inc., a Leonardo Company. 4221 Tudor Lane Greensboro NC USA 27410-8105

If you do not wish to receive future Police1 Product Alerts, please unsubscribe.
To change your email address, update your profile. © 2020: Police1.com. All Rights Reserved.
2611 Internet Blvd., Ste. 100, Frisco, TX 75034

2195

From: PoliceGrantsHelp Alert
To: Conneely, Paul (POL)
Subject: Pay for ELSAG® License Plate Readers with grant money
Date: Wednesday, September 16, 2020 9:02:46 AM

Having trouble viewing this email? View it in your browser.

Find Grant Money to Pay for ELSAG® Automatic License Plate Reader Technology

We have partnered with PoliceGrantsHelp.com to help you access government grant dollars.

ELSAG Plate Hunter ALPR systems bring incredible efficiencies to real-time policing, security and investigations. Proven force multipliers, our solutions include fixed, mobile and covert plate readers, and our newly released ELSAG Video Plate Hunter 900 – a

low-cost option for tight budgets. All systems assist law enforcement with vehicle-related missions including:

- Recovering stolen vehicles and license plates
- Removing unregistered vehicles and unlicensed drivers from roads
- Finding missing persons
- Finding vehicles suspected of involvement in unlawful activity
- Parking management and enforcement
- Collecting criminal intelligence
- Permit validation and tolling
- Collection of traffic data



There's no better time than now to deploy ELSAG automatic license plate readers.

Get FREE ALPR Grant Help

For information about ELSAG Plate Hunter® ALPR systems, visit **leonardocompany-us.com.**

Selex ES Inc., a Leonardo Company. 4221 Tudor Lane Greensboro NC USA 27410-8105

If you do not wish to receive future Police1 Product Alerts, please unsubscribe.
To change your email address, update your profile. © 2020: Police1.com. All Rights Reserved.
2611 Internet Blvd., Ste. 100, Frisco, TX 75034

2197

From: PoliceGrantsHelp Alert
To: Silva, Patrick (POL)
Subject: Pay for ELSAG® License Plate Readers with grant money
Date: Wednesday, September 16, 2020 9:01:38 AM

Having trouble viewing this email? View it in your browser.

Find Grant Money to Pay for ELSAG® Automatic License Plate Reader Technology

We have partnered with PoliceGrantsHelp.com to help you access government grant dollars.

ELSAG Plate Hunter ALPR systems bring incredible efficiencies to real-time policing, security and investigations. Proven force multipliers, our solutions include fixed, mobile and covert plate readers, and our newly released ELSAG Video Plate Hunter 900 – a

low-cost option for tight budgets. All systems assist law enforcement with vehicle-related missions including:

- Recovering stolen vehicles and license plates
- Removing unregistered vehicles and unlicensed drivers from roads
- Finding missing persons
- Finding vehicles suspected of involvement in unlawful activity
- Parking management and enforcement
- Collecting criminal intelligence
- Permit validation and tolling
- Collection of traffic data



There's no better time than now to deploy ELSAG automatic license plate readers.

Get FREE ALPR Grant Help

For information about ELSAG Plate Hunter® ALPR systems, visit **leonardocompany-us.com.**

Selex ES Inc., a Leonardo Company. 4221 Tudor Lane Greensboro NC USA 27410-8105

If you do not wish to receive future Police1 Product Alerts, please unsubscribe.
To change your email address, update your profile. © 2020: Police1.com. All Rights Reserved.
2611 Internet Blvd., Ste. 100, Frisco, TX 75034

2199

From: PoliceGrantsHelp Alert
To: Bernstein, Eric (POL)
Subject: Pay for ELSAG® License Plate Readers with grant money
Date: Wednesday, September 16, 2020 9:31:35 AM

Having trouble viewing this email? View it in your browser.

Find Grant Money to Pay for ELSAG® Automatic License Plate Reader Technology

We have partnered with PoliceGrantsHelp.com to help you access government grant dollars.

ELSAG Plate Hunter ALPR systems bring incredible efficiencies to real-time policing, security and investigations. Proven force multipliers, our solutions include fixed, mobile and covert plate readers, and our newly released ELSAG Video Plate Hunter 900 – a

low-cost option for tight budgets. All systems assist law enforcement with vehicle-related missions including:

- Recovering stolen vehicles and license plates
- Removing unregistered vehicles and unlicensed drivers from roads
- Finding missing persons
- Finding vehicles suspected of involvement in unlawful activity
- Parking management and enforcement
- Collecting criminal intelligence
- Permit validation and tolling
- Collection of traffic data



There's no better time than now to deploy ELSAG automatic license plate readers.

Get FREE ALPR Grant Help

For information about ELSAG Plate Hunter® ALPR systems, visit **leonardocompany-us.com.**

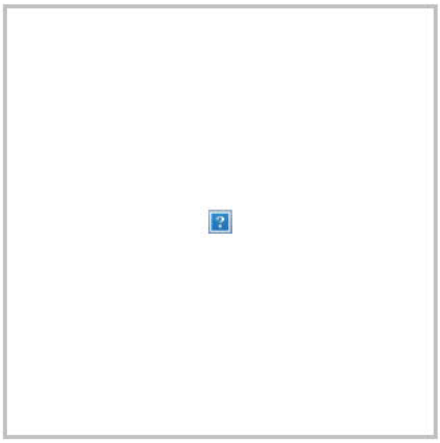
Selex ES Inc., a Leonardo Company. 4221 Tudor Lane Greensboro NC USA 27410-8105

If you do not wish to receive future Police1 Product Alerts, please unsubscribe.
To change your email address, update your profile. © 2020: Police1.com. All Rights Reserved.
2611 Internet Blvd., Ste. 100, Frisco, TX 75034

From: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: Philly OIS unrest continues; LAPD to begin aerial recording of protests
Date: Wednesday, October 28, 2020 5:05:13 PM

October 28, 2020 | View as webpage

TOP STORIES



Philadelphia protests continue; father of man shot by police condemns looting

Violence continued Tuesday over the fatal police shooting of Walter Wallace Jr., who was seen holding a knife



LAPD gets approval to record, save aerial footage of protests

Man's gory Halloween display prompts multiple police calls

Axon releases new features to improve police performance, transparency

Brooklyn businesses, cop cars vandalized; fires set over Philly OIS

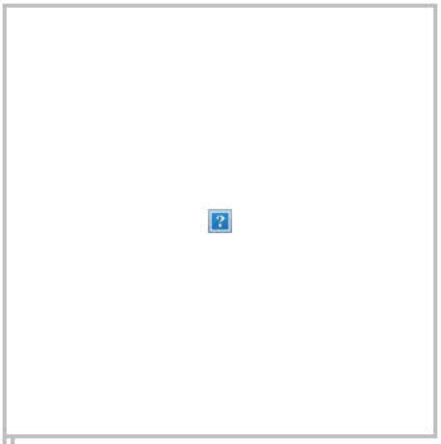
Ga. PD to use drones for some 911 calls

Spotlight: One Company's Dedication to Making Communities Safer With Civil Security Solutions



JENOPTIK which first equipped police vehicles with cameras as far back as 1955, was the first to develop and market ALPR technology in 1979.

Read more



FEATURED CONTENT



Persons in mental health crisis: A primer for police response

By Robert Tornabene

Communities nationwide are changing their response to individuals experiencing a mental health crisis — here's what law enforcement needs to know



Why we are

warriors, guardians and ambassadors

By Gerald Modory

The ambassador philosophy gives credence to the work we have already been doing and should rightfully take credit for

FATIGUE MANAGEMENT



Cops need to engage in tactical napping

By Rob Lawrence

What public safety can learn from the Army's doctrine on readiness



Dead tired: Fighting fatal fatigue in law enforcement

By Policing Matters Podcast

What the research shows about how sleep loss impacts police performance and officer safety



SPONSORED CONTENT



Render laser beams harmless with a simple face shield accessory

Protect officers from harmful laser exposure so they can keep their eyes open to maintain situational awareness.

FEATURED JOB



Lateral and Entry-Level Police Officer
Yakima, Washington

Lateral starting at: $76,548 annual + incentives.
Top Step Officer starting at: $90,900 annual + incentives.

FEATURED JOB



Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

2204

From: PoliceGrantsHelp eNews
To: Cronin, John E (POL)
Subject: Police reform impact on grants; State COVID-19 funding
Date: Tuesday, August 18, 2020 6:29:42 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

August 18, 2020 | View as webpage

Dear PoliceGrantsHelp Member,

In this month's eNews, we look at the impact of police reform on law enforcement grants and how to go beyond federal assistance to get other available funding for COVID-19 response.

Prepare now for 2021 grant applications! New grants can help to enhance capabilities and resources without straining community coffers. Contact PoliceGrantsHelp and use promo code 2021 for 50% off grant writing services. Get a quote today!

— *The PoliceGrantsHelp Team*

FEATURED CONTENT

The impact of police reform on law enforcement grants

By Samantha Dorm

What "reform" will look like in the coming months is unknown, but funding will be needed to address recommendations

GET GRANT ASSISTANCE

PoliceGrantsHelp offers customized grant assistance in several categories. Click on the links below to access free grant services including: research, consulting and application assistance.

- AEDs
- All Terrain Vehicles
- Armored Vehicles
- Boats
- Mobile Command Centers
- NG911
- Narcotics Identification
- Network Solutions

- Body Cameras
- CAD
- Citation Management
- Crime Analysis and Investigation Software
- Drones
- Drug and Alcohol Testing
- Explosives Detection
- Firearms Training
- Forensic 3D Laser Scanners
- In Car Video
- Less Lethal
- License Plate Readers
- Officer Wellness
- Online Training
- Personal Protective Equipment - PPE
- RMS
- Radiation Detection
- Radio Systems
- Radios
- Rapid DNA Analysis
- Risk Management
- Specialty Vehicles
- Training Simulation
- Video Surveillance

ALL GRANTS HELP

Find Grants to Fund Your ELSAG ALPR Systems

Let Leonardo help you find grants to fund ELSAG automatic license plate readers, which effectively aid agency missions and investigations.

Request grant help

Prepare Now for 2021 Grant Projects and Applications

New grants can help enhance capabilities and resources without straining community coffers. Contact PoliceGrantsHelp for assistance preparing your application. Use promo code 2021 for 50% off!

Get a quote today

OTHER HIGHLIGHTS

Beyond federal assistance: State COVID-19 response grants

By PoliceGrantsHelp Staff

Begin collecting data now to qualify for federal pass-through funding, community foundation and

corporate foundation grants for COVID-19-related response

Get Help With Grant Funding for The Genesis Group



The Genesis Group has joined PoliceGrantsHelp to offer your department free grant assistance for radios.

Get started

Need Grant Assistance for Narcotics Identification Products?



908 Devices has partnered with the PoliceGrantsHelp grant experts to offer your department free grant assistance for narcotics identification products.

Get free grant help

UPCOMING GRANTS

Grant	Grant Deadline
Edward Byrne Memorial Justice Assistance Grant (JAG) Program - Local Solicitation	08/19/2020
Firehouse Subs Public Safety Foundation Grants	08/19/2020
Nationwide Foundation Fund	09/01/2020
Siletz Tribal Charitable Contribution Fund	09/01/2020
Alliant Energy Hometown Safety Grant	09/01/2020
New Hampshire Humanities Major Grants	09/15/2020
Local Law Enforcement Block Grant (LLEBG Missouri)	09/25/2020

Interested in finding more grant opportunities?

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

2207

From: PoliceGrantsHelp eNews
To: Conneely, Paul (POL)
Subject: Police reform impact on grants; State COVID-19 funding
Date: Tuesday, August 18, 2020 6:29:37 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

August 18, 2020 | View as webpage

Dear PoliceGrantsHelp Member,

In this month's eNews, we look at the impact of police reform on law enforcement grants and how to go beyond federal assistance to get other available funding for COVID-19 response.

Prepare now for 2021 grant applications! New grants can help to enhance capabilities and resources without straining community coffers. Contact PoliceGrantsHelp and use promo code 2021 for 50% off grant writing services. Get a quote today!

— *The PoliceGrantsHelp Team*

FEATURED CONTENT

The impact of police reform on law enforcement grants

By Samantha Dorm

What "reform" will look like in the coming months is unknown, but funding will be needed to address recommendations

GET GRANT ASSISTANCE

PoliceGrantsHelp offers customized grant assistance in several categories. Click on the links below to access free grant services including: research, consulting and application assistance.

- AEDs
- All Terrain Vehicles
- Armored Vehicles
- Boats
- Mobile Command Centers
- NG911
- Narcotics Identification
- Network Solutions

- Body Cameras
- CAD
- Citation Management
- Crime Analysis and Investigation Software
- Drones
- Drug and Alcohol Testing
- Explosives Detection
- Firearms Training
- Forensic 3D Laser Scanners
- In Car Video
- Less Lethal
- License Plate Readers
- Officer Wellness
- Online Training
- Personal Protective Equipment - PPE
- RMS
- Radiation Detection
- Radio Systems
- Radios
- Rapid DNA Analysis
- Risk Management
- Specialty Vehicles
- Training Simulation
- Video Surveillance

ALL GRANTS HELP

Find Grants to Fund Your ELSAG ALPR Systems

Let Leonardo help you find grants to fund ELSAG automatic license plate readers, which effectively aid agency missions and investigations.

Request grant help

Prepare Now for 2021 Grant Projects and Applications

New grants can help enhance capabilities and resources without straining community coffers. Contact PoliceGrantsHelp for assistance preparing your application. Use promo code 2021 for 50% off!

Get a quote today

OTHER HIGHLIGHTS

Beyond federal assistance: State COVID-19 response grants

By PoliceGrantsHelp Staff

Begin collecting data now to qualify for federal pass-through funding, community foundation and

corporate foundation grants for COVID-19-related response

Get Help With Grant Funding for The Genesis Group

The Genesis Group has joined PoliceGrantsHelp to offer your department free grant assistance for radios.

Get started

Need Grant Assistance for Narcotics Identification Products?

908 Devices has partnered with the PoliceGrantsHelp grant experts to offer your department free grant assistance for narcotics identification products.

Get free grant help

UPCOMING GRANTS

Grant	Grant Deadline
Edward Byrne Memorial Justice Assistance Grant (JAG) Program - Local Solicitation	08/19/2020
Firehouse Subs Public Safety Foundation Grants	08/19/2020
Nationwide Foundation Fund	09/01/2020
Siletz Tribal Charitable Contribution Fund	09/01/2020
Alliant Energy Hometown Safety Grant	09/01/2020
New Hampshire Humanities Major Grants	09/15/2020
Local Law Enforcement Block Grant (LLEBG Missouri)	09/25/2020

Interested in finding more grant opportunities?

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

2210

From: PoliceGrantsHelp eNews
To: Silva, Patrick (POL)
Subject: Police reform impact on grants; State COVID-19 funding
Date: Tuesday, August 18, 2020 6:14:44 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

August 18, 2020 | View as webpage

Dear PoliceGrantsHelp Member,

In this month's eNews, we look at the impact of police reform on law enforcement grants and how to go beyond federal assistance to get other available funding for COVID-19 response.

Prepare now for 2021 grant applications! New grants can help to enhance capabilities and resources without straining community coffers. Contact PoliceGrantsHelp and use promo code 2021 for 50% off grant writing services. Get a quote today!

— *The PoliceGrantsHelp Team*

FEATURED CONTENT

The impact of police reform on law enforcement grants

By Samantha Dorm

What "reform" will look like in the coming months is unknown, but funding will be needed to address recommendations

GET GRANT ASSISTANCE

PoliceGrantsHelp offers customized grant assistance in several categories. Click on the links below to access free grant services including: research, consulting and application assistance.

- AEDs
- All Terrain Vehicles
- Armored Vehicles
- Boats
- Mobile Command Centers
- NG911
- Narcotics Identification
- Network Solutions

- Body Cameras
- CAD
- Citation Management
- Crime Analysis and Investigation Software
- Drones
- Drug and Alcohol Testing
- Explosives Detection
- Firearms Training
- Forensic 3D Laser Scanners
- In Car Video
- Less Lethal
- License Plate Readers
- Officer Wellness
- Online Training
- Personal Protective Equipment - PPE
- RMS
- Radiation Detection
- Radio Systems
- Radios
- Rapid DNA Analysis
- Risk Management
- Specialty Vehicles
- Training Simulation
- Video Surveillance

ALL GRANTS HELP

Find Grants to Fund Your ELSAG ALPR Systems

Let Leonardo help you find grants to fund ELSAG automatic license plate readers, which effectively aid agency missions and investigations.

Request grant help

Prepare Now for 2021 Grant Projects and Applications

New grants can help enhance capabilities and resources without straining community coffers. Contact PoliceGrantsHelp for assistance preparing your application. Use promo code 2021 for 50% off!

Get a quote today

OTHER HIGHLIGHTS

Beyond federal assistance: State COVID-19 response grants

By PoliceGrantsHelp Staff

Begin collecting data now to qualify for federal pass-through funding, community foundation and

corporate foundation grants for COVID-19-related response

Get Help With Grant Funding for The Genesis Group



The Genesis Group has joined PoliceGrantsHelp to offer your department free grant assistance for radios.

Get started

Need Grant Assistance for Narcotics Identification Products?



908 Devices has partnered with the PoliceGrantsHelp grant experts to offer your department free grant assistance for narcotics identification products.

Get free grant help

UPCOMING GRANTS

Grant	Grant Deadline
Edward Byrne Memorial Justice Assistance Grant (JAG) Program - Local Solicitation	08/19/2020
Firehouse Subs Public Safety Foundation Grants	08/19/2020
Nationwide Foundation Fund	09/01/2020
Siletz Tribal Charitable Contribution Fund	09/01/2020
Alliant Energy Hometown Safety Grant	09/01/2020
New Hampshire Humanities Major Grants	09/15/2020
Local Law Enforcement Block Grant (LLEBG Missouri)	09/25/2020

Interested in finding more grant opportunities?

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: PoliceGrantsHelp eNews
To: Ramsland, Erik (POL)
Subject: Police reform impact on grants; State COVID-19 funding
Date: Tuesday, August 18, 2020 5:44:49 PM

August 18, 2020 | View as webpage

Dear PoliceGrantsHelp Member,

In this month's eNews, we look at the impact of police reform on law enforcement grants and how to go beyond federal assistance to get other available funding for COVID-19 response.

Prepare now for 2021 grant applications! New grants can help to enhance capabilities and resources without straining community coffers. Contact PoliceGrantsHelp and use promo code 2021 for 50% off grant writing services. Get a quote today!

— *The PoliceGrantsHelp Team*

FEATURED CONTENT

The impact of police reform on law enforcement grants

By Samantha Dorm

What "reform" will look like in the coming months is unknown, but funding will be needed to address recommendations

GET GRANT ASSISTANCE

PoliceGrantsHelp offers customized grant assistance in several categories. Click on the links below to access free grant services including: research, consulting and application assistance.

- AEDs
- All Terrain Vehicles
- Armored Vehicles
- Boats
- Body Cameras
- CAD
- Citation Management
- Mobile Command Centers
- NG911
- Narcotics Identification
- Network Solutions
- Officer Wellness
- Online Training
- Personal Protective Equipment - PPE

- Crime Analysis and Investigation Software
- Drones
- Drug and Alcohol Testing
- Explosives Detection
- Firearms Training
- Forensic 3D Laser Scanners
- In Car Video
- Less Lethal
- License Plate Readers
- RMS
- Radiation Detection
- Radio Systems
- Radios
- Rapid DNA Analysis
- Risk Management
- Specialty Vehicles
- Training Simulation
- Video Surveillance

ALL GRANTS HELP

Find Grants to Fund Your ELSAG ALPR Systems

Let Leonardo help you find grants to fund ELSAG automatic license plate readers, which effectively aid agency missions and investigations.

Request grant help

Prepare Now for 2021 Grant Projects and Applications

New grants can help enhance capabilities and resources without straining community coffers. Contact PoliceGrantsHelp for assistance preparing your application. Use promo code 2021 for 50% off!

Get a quote today

OTHER HIGHLIGHTS

Beyond federal assistance: State COVID-19 response grants

By PoliceGrantsHelp Staff

Begin collecting data now to qualify for federal pass-through funding, community foundation and corporate foundation grants for COVID-19-

related response

Get Help With Grant Funding for The Genesis Group

The Genesis Group has joined PoliceGrantsHelp to offer your department free grant assistance for radios.

Get started

Need Grant Assistance for Narcotics Identification Products?

908 Devices has partnered with the PoliceGrantsHelp grant experts to offer your department free grant assistance for narcotics identification products.

Get free grant help

UPCOMING GRANTS

Grant	Grant Deadline
Edward Byrne Memorial Justice Assistance Grant (JAG) Program - Local Solicitation	08/19/2020
Firehouse Subs Public Safety Foundation Grants	08/19/2020
Nationwide Foundation Fund	09/01/2020
Siletz Tribal Charitable Contribution Fund	09/01/2020
Alliant Energy Hometown Safety Grant	09/01/2020
New Hampshire Humanities Major Grants	09/15/2020
Local Law Enforcement Block Grant (LLEBG Missouri)	09/25/2020

Interested in finding more grant opportunities?

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: PoliceGrantsHelp eNews
To: Irwin, Patrick (POL)
Subject: Police reform impact on grants; State COVID-19 funding
Date: Tuesday, August 18, 2020 6:59:55 PM

August 18, 2020 | View as webpage

Dear PoliceGrantsHelp Member,

In this month's eNews, we look at the impact of police reform on law enforcement grants and how to go beyond federal assistance to get other available funding for COVID-19 response.

Prepare now for 2021 grant applications! New grants can help to enhance capabilities and resources without straining community coffers. Contact PoliceGrantsHelp and use promo code 2021 for 50% off grant writing services. Get a quote today!

— *The PoliceGrantsHelp Team*

FEATURED CONTENT



The impact of police reform on law enforcement grants

By Samantha Dorm

What "reform" will look like in the coming months is unknown, but funding will be needed to address recommendations

GET GRANT ASSISTANCE

PoliceGrantsHelp offers customized grant assistance in several categories. Click on the links below to access free grant services including: research, consulting and application assistance.

- AEDs
- All Terrain Vehicles
- Armored Vehicles
- Boats
- Body Cameras
- CAD
- Citation Management
- Mobile Command Centers
- NG911
- Narcotics Identification
- Network Solutions
- Officer Wellness
- Online Training
- Personal Protective Equipment - PPE

- Crime Analysis and Investigation Software
- Drones
- Drug and Alcohol Testing
- Explosives Detection
- Firearms Training
- Forensic 3D Laser Scanners
- In Car Video
- Less Lethal
- License Plate Readers
- RMS
- Radiation Detection
- Radio Systems
- Radios
- Rapid DNA Analysis
- Risk Management
- Specialty Vehicles
- Training Simulation
- Video Surveillance

ALL GRANTS HELP

Find Grants to Fund Your ELSAG ALPR Systems

Let Leonardo help you find grants to fund ELSAG automatic license plate readers, which effectively aid agency missions and investigations.

Request grant help

Prepare Now for 2021 Grant Projects and Applications

New grants can help enhance capabilities and resources without straining community coffers. Contact PoliceGrantsHelp for assistance preparing your application. Use promo code 2021 for 50% off!

Get a quote today

OTHER HIGHLIGHTS

Beyond federal assistance: State COVID-19 response grants

By PoliceGrantsHelp Staff

Begin collecting data now to qualify for federal pass-through funding, community foundation and corporate foundation grants for COVID-19-

related response

Get Help With Grant Funding for The Genesis Group

The Genesis Group has joined PoliceGrantsHelp to offer your department free grant assistance for radios.

Get started

Need Grant Assistance for Narcotics Identification Products?

908 Devices has partnered with the PoliceGrantsHelp grant experts to offer your department free grant assistance for narcotics identification products.

Get free grant help

UPCOMING GRANTS

Grant	Grant Deadline
Edward Byrne Memorial Justice Assistance Grant (JAG) Program - Local Solicitation	08/19/2020
Firehouse Subs Public Safety Foundation Grants	08/19/2020
Nationwide Foundation Fund	09/01/2020
Siletz Tribal Charitable Contribution Fund	09/01/2020
Alliant Energy Hometown Safety Grant	09/01/2020
New Hampshire Humanities Major Grants	09/15/2020
Local Law Enforcement Block Grant (LLEBG Missouri)	09/25/2020

Interested in finding more grant opportunities?

PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Weekend Roll Call
To: McCarthy, Steven (POL)
Subject: Police-free stops, "Empire" actor standoff & other top stories
Date: Sunday, July 19, 2020 8:18:05 AM

July 19, 2020 | View as webpage

FEATURED CONTENT



Video: Mich. deputy shoots man wanted for stabbing in face mask dispute

The deputy quickly clears a gun malfunction and fires several rounds at the knife-wielding suspect when he fails to comply



Berkeley moves forward with police-free traffic stops

The city will now work towards forming a separate traffic department that will use unarmed city workers

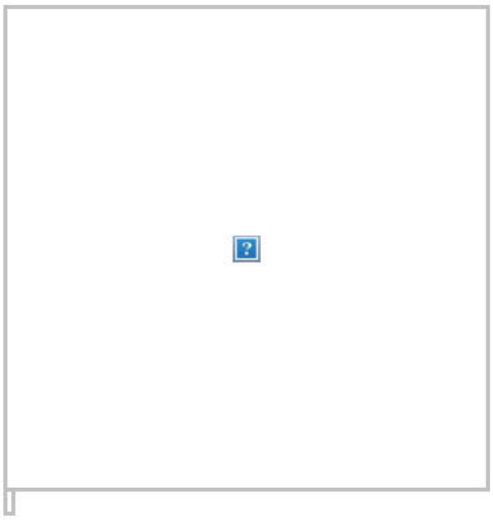


SWAT team arrests 'Empire' actor after 9-hour standoff

The 911 call alleged a woman was assaulted by her husband, an actor on FOX's musical drama series 'Empire'

Webinar: Eliminating Data Silos in Your Evidence Management System

Join the free webinar





on 8/4 at 2 p.m. CT to learn success strategies for managing your digital evidence.

Register now



Video: Suspect puts NYPD cop in headlock during attempted arrest

Two officers were trying to arrest a suspect in a Bronx neighborhood amid a growing crowd



Seattle police: Proposed budget cuts would affect more than half of non-white officers

“Cuts this deep mean we would lose more than 50% of our (black, indigenous, people of color) officers,” the department said



State your case: Should there be residency requirements for sworn personnel?

By Jim Dudley

and Chief Joel Shults Ed.D.
An activist's call for cops to live within the communities they police has received millions of views online

6 Challenges, 6 Tech Solutions to Help LE Agencies During the Pandemic and Beyond



Greater situational awareness, officer safety, better communications and faster response times were already on the wish list – the crisis added new urgency.

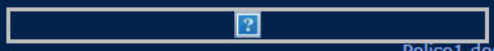
Learn more

Webinar: License Plate Recognition With a Twist of A.I.



Join us for a live webinar with Sony, Utility, and Noblesville Police Department. Unlike any other ALPR system, this one is powered by an A.I. Engine. The Smart ALPR system can gather real-time information at the edge to enhance alerting capabilities.

Register for the webinar



Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Silva, Patrick (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 7:35:47 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

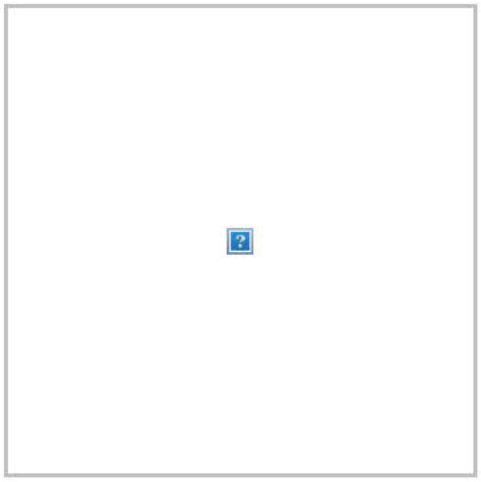
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: zzMullaney, Stephen (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 7:35:31 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

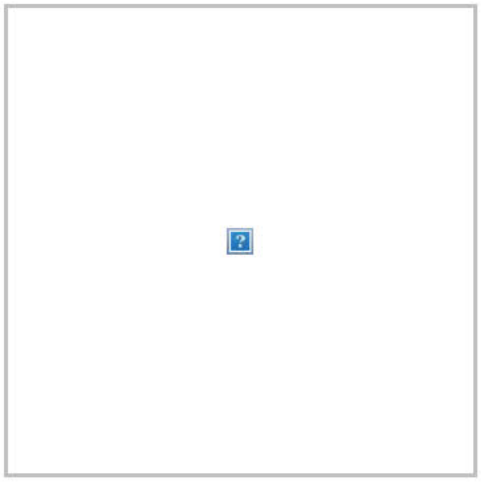
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT

Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey

P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled

5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Paquette, Brian (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 7:35:31 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

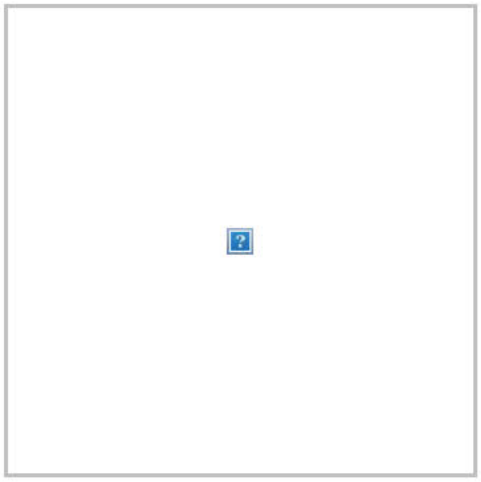
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Seymour, Alexander P (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 7:35:29 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

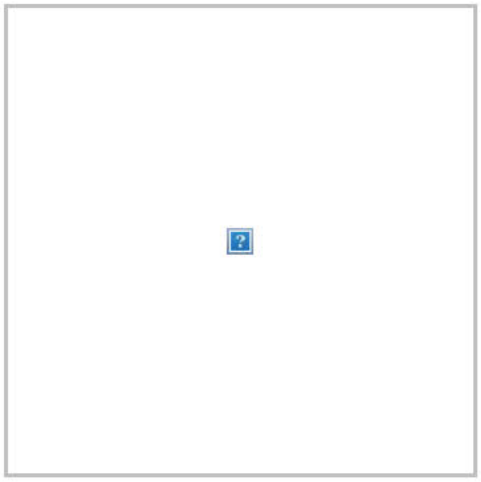
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Joyce, Gina (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 7:35:23 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

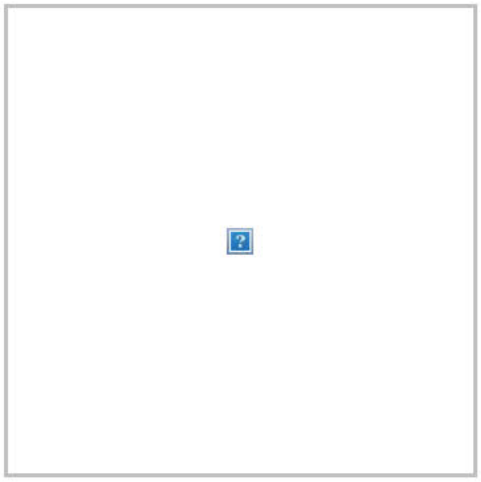
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT

Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey

P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled

5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Joyce, Gina (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 7:35:23 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

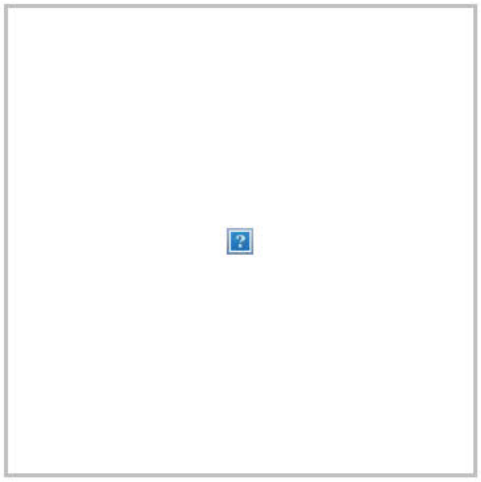
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Spencer, Jonathan (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 7:35:19 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

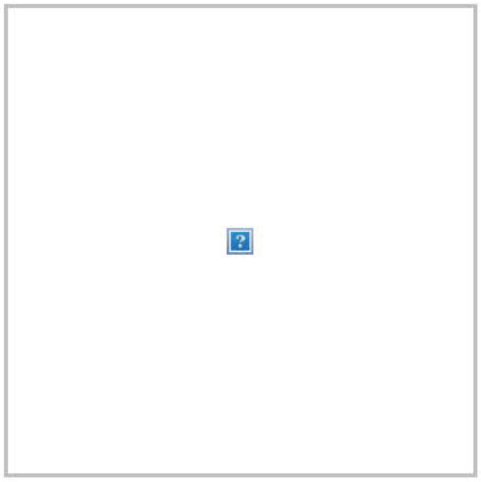
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT

Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey

P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled

5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: zzLyver, Michael (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 7:15:31 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

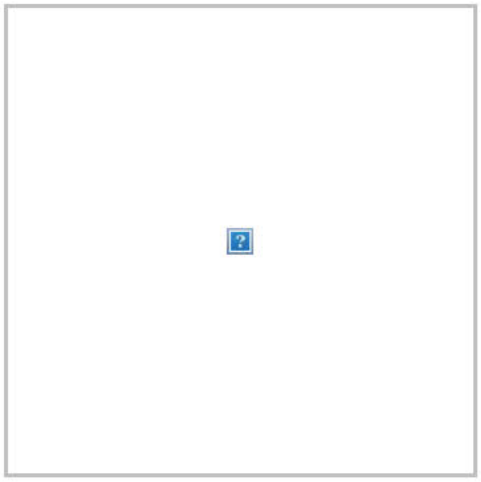
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Cooper, Brian (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 7:15:29 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

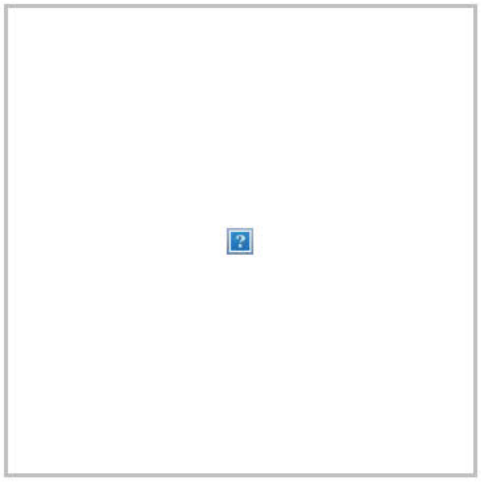
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again

A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations

Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS

Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error

5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing

SPONSORED CONTENT

Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Irwin, Patrick (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 7:15:22 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

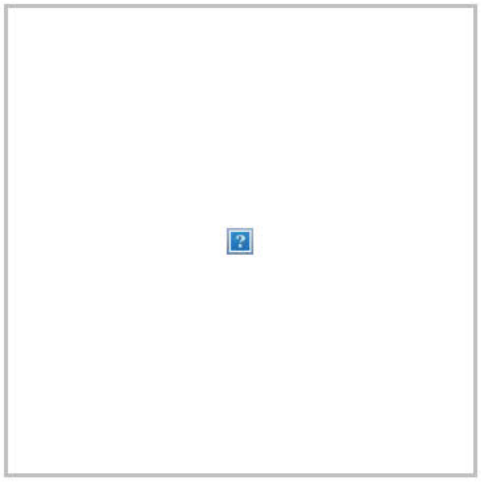
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Goonan, Michael D (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 7:15:17 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

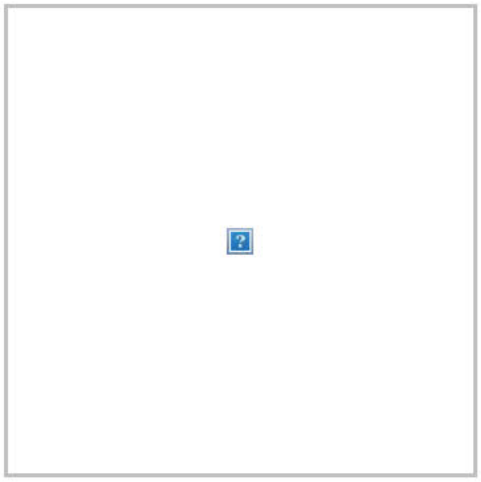
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Breton, Benjamin (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 7:15:11 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

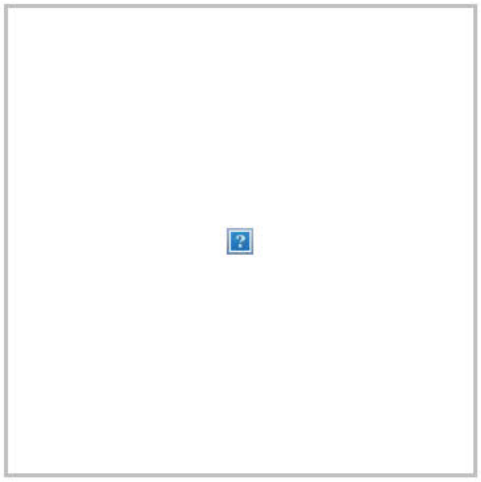
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399

5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive

$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Rizos, Byron (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 6:55:42 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

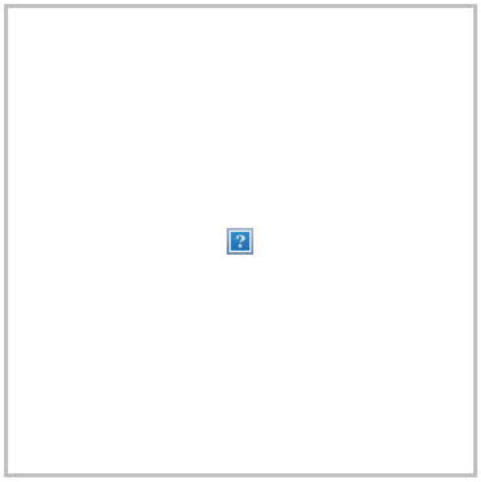
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Lenti, Jeffrey (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 6:55:27 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

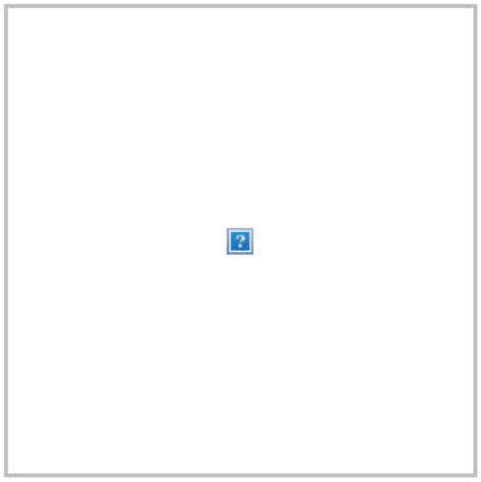
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Barry, Sean (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 6:55:12 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

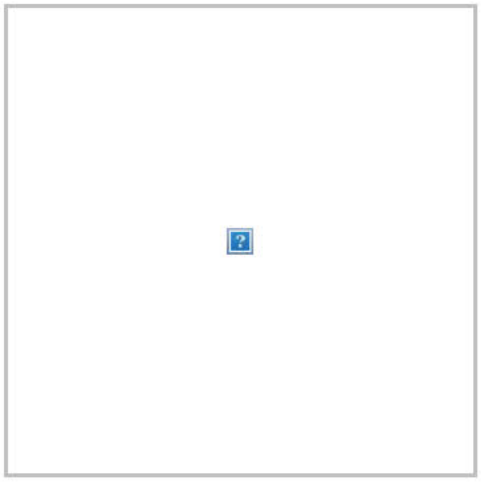
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 6:55:05 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

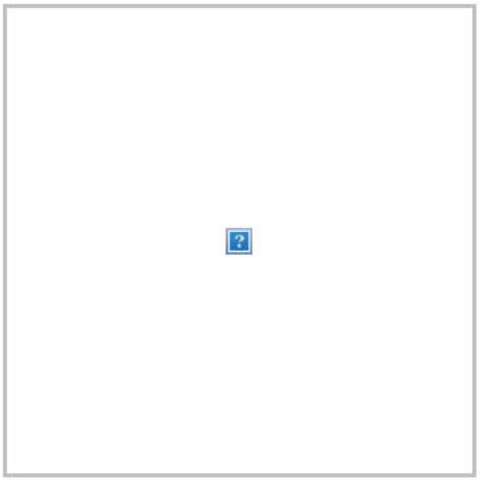
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Cronin, John E (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 6:36:21 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

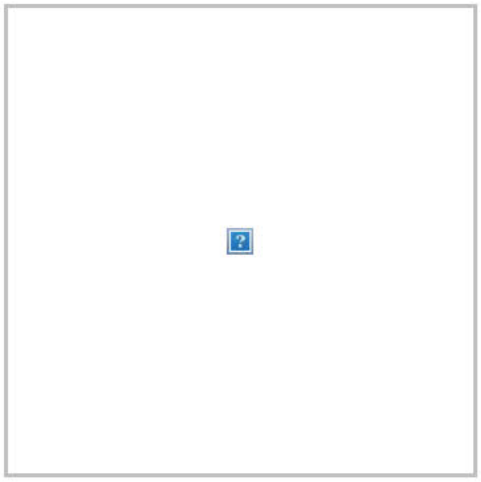
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again

A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations

Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS

Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error

5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing

SPONSORED CONTENT

Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Cannon, Brian (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 6:36:00 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

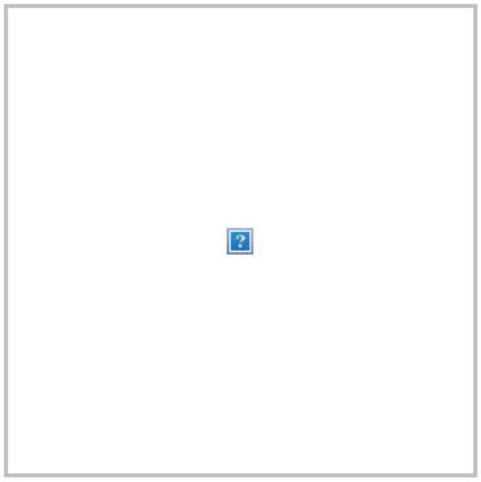
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Cronin, John E (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 6:35:40 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

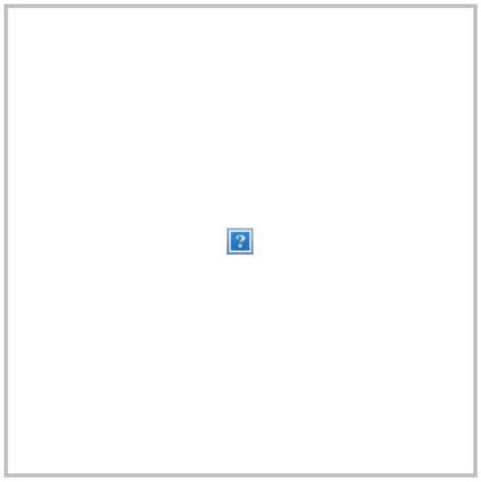
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Willhite, Michael (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 6:34:55 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

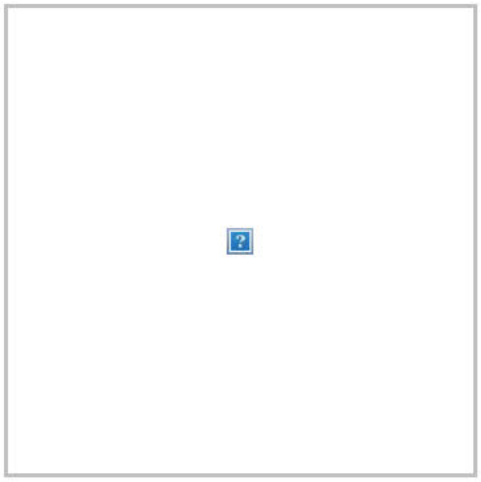
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Davis, Matthew (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 6:15:48 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

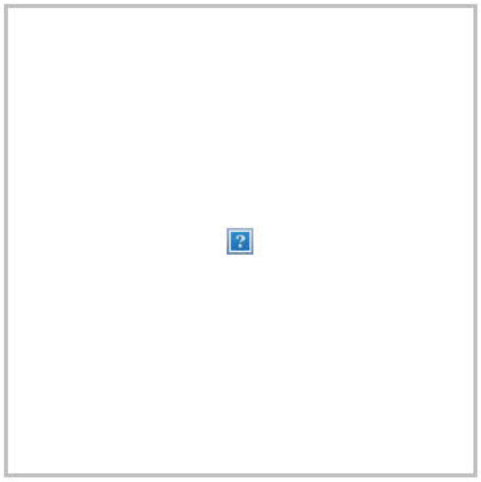
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Keville, Robert (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 6:15:41 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

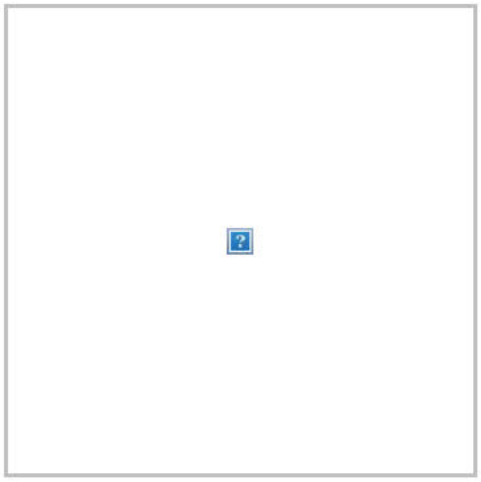
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: benesh, meghann E (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 6:15:40 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

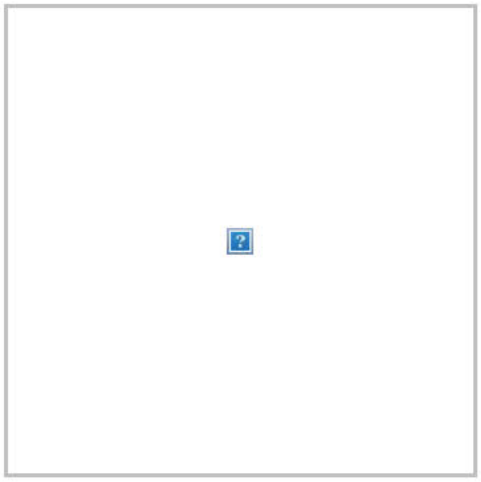
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again

A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations

Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS

Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error

5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing

SPONSORED CONTENT

Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Murgo, Christopher (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 6:15:26 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

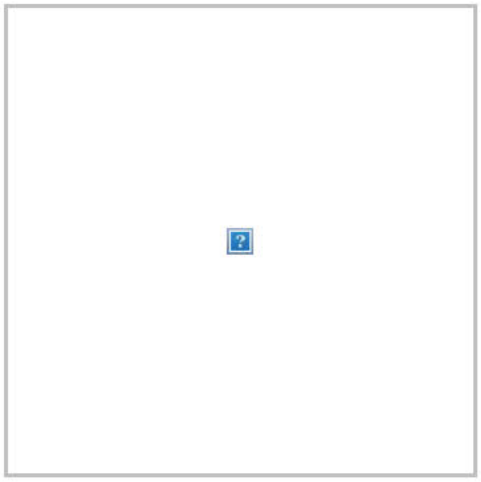
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again

A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations

Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS

Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error

5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing

SPONSORED CONTENT

Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Nee, William (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 6:15:13 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

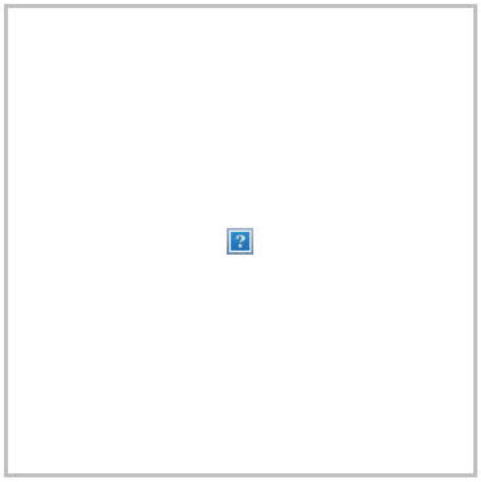
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Clement, Michael (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 6:15:13 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

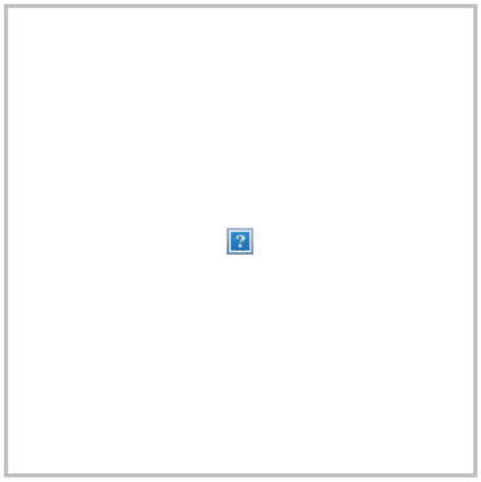
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Seymour, Alexander P (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 5:56:13 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

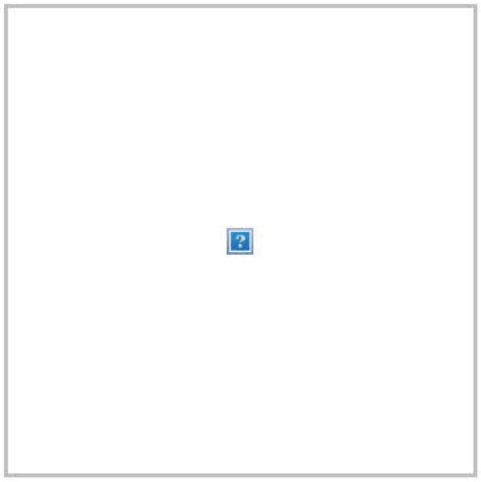
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399

5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive

$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: wanagel@bu.edu
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 5:55:32 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

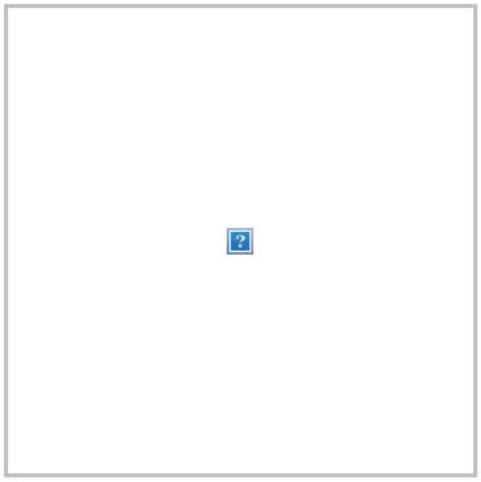
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Mcdonald, Scott (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 5:55:27 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

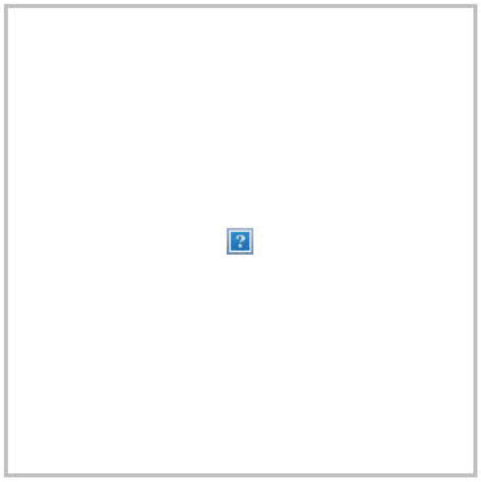
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT

Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey

P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled

5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Johnson, Robert - Captain (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 5:55:25 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

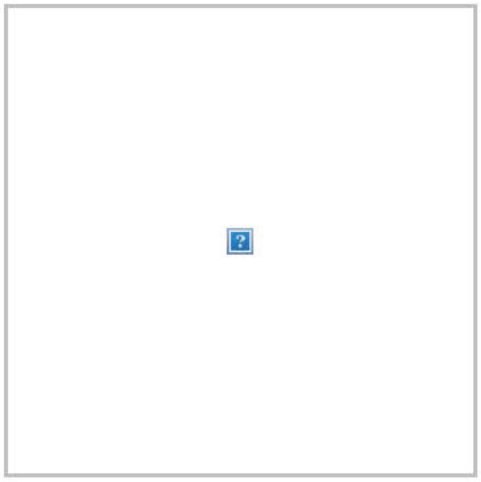
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again

A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations

Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS

Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error

5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing

SPONSORED CONTENT

Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Loiselle, Rachel (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 5:55:23 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

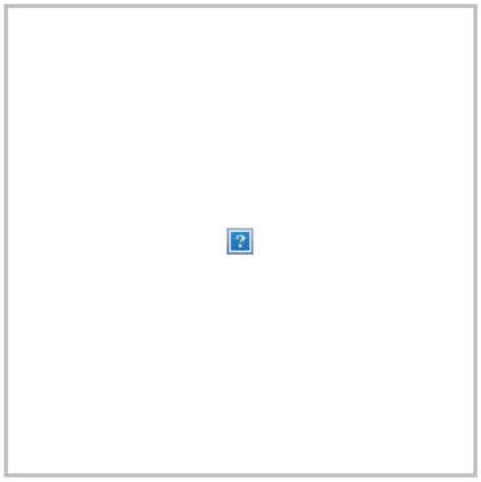
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Tapis, Stephen C (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 5:55:18 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

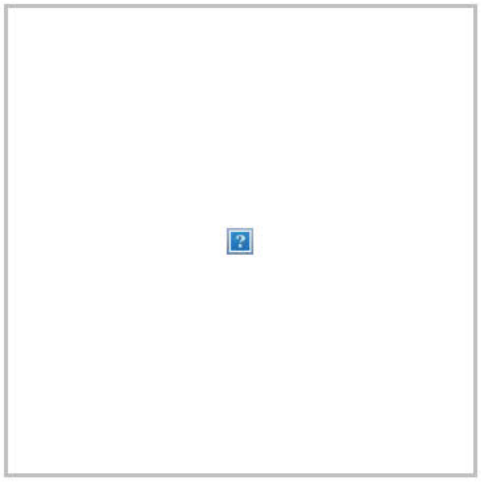
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Grassia, Michael (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 5:55:08 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

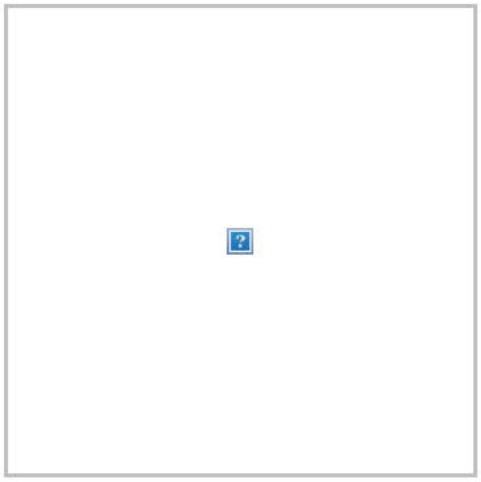
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Lee, Brian (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 5:40:47 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

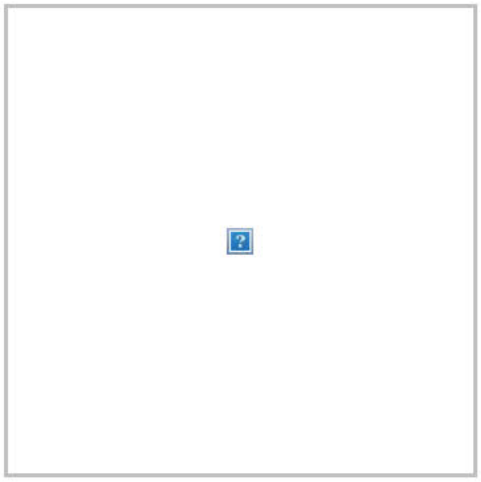
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399

5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive

$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: zzGriffin, Daniel (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 5:37:37 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

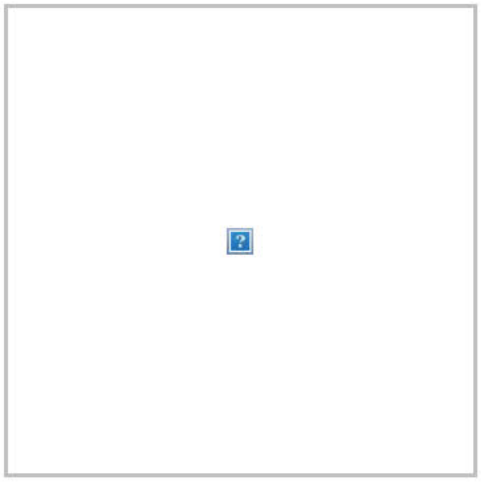
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: zzLeVangie, Dean (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 5:36:13 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

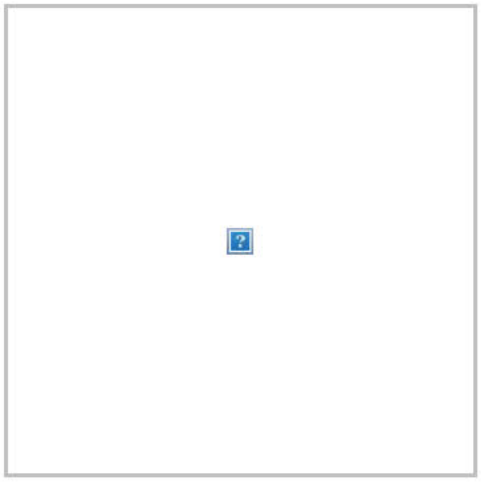
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Williams, Keller (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 5:35:51 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

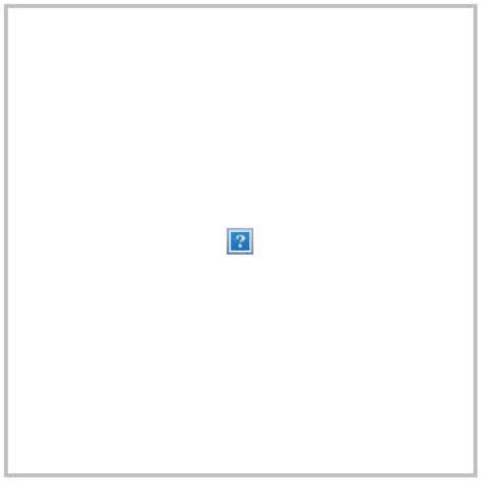
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Conneely, Paul (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 5:16:16 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

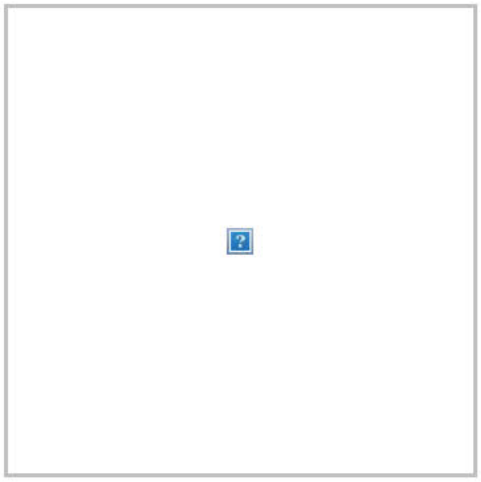
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Upton, Paul (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 5:15:52 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

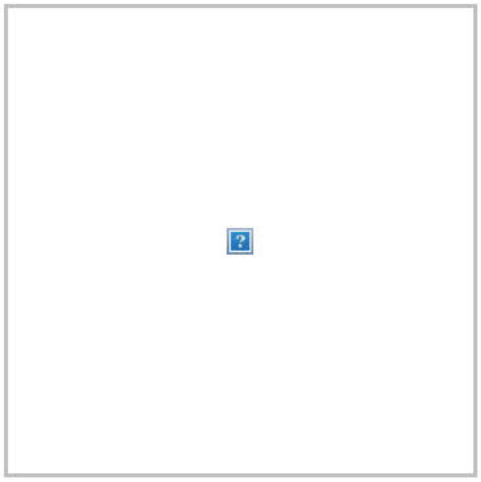
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Roll Call
To: Doyle, Paul (POL)
Subject: Portland LEO attacked in patrol car; Cop gifts car to needy family
Date: Tuesday, October 6, 2020 7:36:18 PM

October 6, 2020 | View as webpage

Dear Police1 Member,

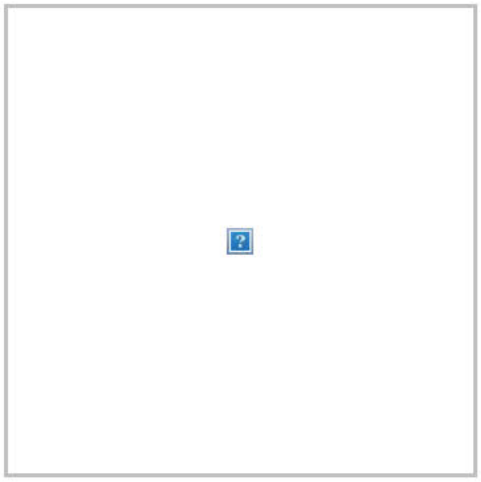
Marijuana is on the ballot again in 2020, with Politico reporting that 1 in 3 Americans could have access to legal recreational pot depending on the results. As the number of states with some form of legal weed increases, the potential impact on law enforcement issues ranging from drug-impaired driving to officer hiring and recruitment is immense.

Police1 and Louisiana State University recently conducted an expansive survey to capture law enforcement attitudes toward marijuana use and enforcement. A total of 3,615 sworn LEOs weighed in on a range of topics, from the use of medicinal marijuana off duty to decriminalization.

Today's newsletter features some highlights from our special report. You can find the full coverage and analysis here.

— *The Police1 Team*

TOP STORIES



Video: Highway patrol helicopter rescues firefighters from Calif. wildfire

Four National Guardsmen found themselves trapped after battling the Bear Fire, officials said

Man smashes patrol car window, pepper-sprays Portland cop, police say

Texas officer charged with murder in fatal store shooting

Conn. police chief, city official plead guilty in hiring scam

Atlanta cop gifts own car to mother of 5

Pursuit lasting about 100 miles ends in fatal police shootout

Eliminate Contraband From Inmate Mail by 100%

TextBehind CAMMP empowers correctional officers with total control on inmate mail

review and approval process on a daily basis with efficiency.

Learn more today

FEATURED CONTENT



Policing in an Era of Legal Marijuana: Cops' opinions on decriminalization, incarceration & more

By Cole Zercoe

A collection of highlights from Police1 and LSU's expansive survey



P1 Research: The marijuana conundrum in law enforcement

By James Dudley

The promise of less crime and calls for service that would accompany legalization of marijuana remains unfulfilled



5 tips for safe, legal and effective drug interdiction

By Lexipol Team

As with all high-risk law enforcement activities, training and preparation is essential

Think Sweat and Stink Are Inevitable Under Your Ballistic Vest? Think Again



A new cooling fabric developed by a cop for cops is designed to keep odor and overheating at bay all day – and longer.

Find out how

Webinar: Pre-employment Background Investigations



Join our free webinar on Tuesday, October 20 at 1 p.m. EST/ 12 p.m. CST / 10 a.m. PST with AWS and Guardian Alliance Technologies to discuss technologies for vetting law enforcement officers before hiring.

Learn more and register

OTHER HIGHLIGHTS



Study: Muzzle position can have major impact on shooting decisions

By Charles Remsberg

New research finds a significant relationship between muzzle position and the likelihood of making a shooting-decision error



5 lessons from a hardware store

By Christopher Littrell

Wisdom applicable to LEOs' life and policing pops up even while vacationing



SPONSORED CONTENT



Webinar: Be ready to take FirstNet into the field

First responders must stay

connected to critical communications in even the harshest conditions. Find out how to take FirstNet capabilities from the vehicle to the data center. Register now.

FEATURED DEAL

Panasonic Toughbook $399
5% discount for Police1 readers

FEATURED JOB

Lateral Police Officer - $10,000 Lateral Hiring Incentive
$5882-$7507* monthly - Vancouver, Washington

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: scott.range@pol.state.ma.us
To: Gavioli, Brian (POL)
Subject: Re: (U-FOUO) Updates re: BlueLeaks Data Breach including the new document: Achieving and Maintaining Best-Practices for Cybersecurity with Third- Party Vendors and Partners
Date: Monday, June 29, 2020 9:39:59 PM

No problem. Tomorrow is good

Sent from my iPhone

> On Jun 29, 2020, at 9:27 PM, Gavioli, Brian (POL) <brian.gavioli@pol.state.ma.us> wrote:
>
> Sorry just saw this ok to call in am?
>
> Sergeant Brian Gavioli
> Massachusetts State Police
> Commonwealth Fusion Center | Massachusetts Cybersecurity Program
> 124 Acton Street
> Maynard, MA 01754
> 978-451-3557 (desk)
> [redacted] (cell)
> 978-451-3700 (24/7)
>
> The preceding email message (including any attachments) contains information that may be confidential, may be protected by the attorney-client or other applicable privileges, or may constitute non-public information. It is intended to be conveyed only to the designated recipient(s) named above. If you are not an intended recipient of this message, please notify the sender by replying to this message and then delete all copies of it from your computer system. Any use, dissemination, distribution, or reproduction of this message by unintended recipients is not authorized and may be unlawful.
>
> ---
>
> **From:** Range, Scott (POL) <scott.range@pol.state.ma.us>
> **Sent:** Monday, June 29, 2020 11:19 AM
> **To:** Gavioli, Brian (POL) <brian.gavioli@pol.state.ma.us>
> **Subject:** FW: (U-FOUO) Updates re: BlueLeaks Data Breach including the new document: Achieving and Maintaining Best-Practices for Cybersecurity with Third- Party Vendors and Partners
>
> Please call me when convenient, Thanks
>
> ---
>
> **From:** Mike Sena [mailto:msena@ncric.ca.gov]
> **Sent:** Saturday, June 27, 2020 4:28 PM
> **To:** Mike Sena
> **Cc:** ciosubcommittee@nfcausa.org
> **Subject:** (U-FOUO) Updates re: BlueLeaks Data Breach including the new document:

Achieving and Maintaining Best-Practices for Cybersecurity with Third- Party Vendors and Partners

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Dear partner,

Please see the attached documents produced by the National Fusion Center Association's Cyber Intelligence Network (CIN) on the BlueLeaks Data Breach over the past seven days. The document titled ***"Achieving and Maintaining Best-Practices for Cybersecurity with Third- Party Vendors and Partners"***, is the most recent document produced and may be distributed to all of your organization's members and partners.

Please see the notes below my signature block for further important updates and e-mail ciosubcommittee@nfcausa.org for any cyber mitigation coordination requests.

Thank you.

Mike

Mike Sena
Chair – Criminal Intelligence Coordinating Council
President – National Fusion Center Association
Chair – HIDTA Intelligence Committee
Executive Director
Northern California High Intensity Drug Trafficking Area
Northern California Regional Intelligence Center
P.O. Box 36102 | San Francisco | CA | 94102
415.725.1000
(24 Hr.) 866.367.8847
msena@ncric.ca.gov
REPORT URGENT THREAT INFORMATION TO THE FBI-JTTF (415) 553-7400
REPORT SUSPICIOUS ACTIVITY TO THE NCRIC https://ncric.ca.gov (866) 367-8847
<image001.png>
<image003.png>

Incident Synopsis:

On Friday, June 19, the group "Distributed Denial of Secrets" (@DDoSecrets) posted a link on Twitter to law enforcement sensitive data that was exfiltrated from a compromised web site services company that hosts numerous law enforcement organizations' websites across the nation. The Houston FBI Office is the lead criminal investigative agency for the data breach. Distributed Denial of Secrets (@DDoSecrets) Twitter account has been suspended and the links to the site containing the stolen data are being blocked by Twitter.

The mitigation response for the breach is being coordinated through partners that represent the cybersecurity resources across the FBI, the National Network of Fusion Centers, HIDTAs, DHS CISA, MS-ISAC's CIS, Los Angeles Sheriff's Department (LASD) and other partners.

It is believed at this time that measures have been taken to reduce further compromise of the web service provider's systems. There is reporting that there may be additional unpublished data that will be posted to the dark web site in the future.

Potential data exposed includes:

- Membership information, and event or training registrations, including officer names, agency/employer, email, and phone numbers
- Past email distributions sent out through the system's e-mail builder, suspicious activity reports (SAR), requests for investigative case support, bulletins, threat assessments, and narcotics seizure data.

Data systems that were **not** directly exposed:

- Deconfliction systems.
- Intelligence management systems.
- Records management data sharing systems.
- ALPR systems.

The FBI is completing the scan of the systems of the web services provider and DHS CISA and the MS-ISAC's Center for Internet Security are standing by to provide support and additional scans of the web service provider's systems.

The service provider has activated two-factor authentication for all users that did not already have the feature activated.

Key Updates:

- **A notification will go out Monday for a call with all HIDTA directors, a separate call for all Fusion Center directors, and a joint call with all FBI Field Offices' Cyber ASACs/SSAs, Fusion Centers, HIDTAs, FBI OPE, DHS I&A, DHS CISA, MS ISAC-CIS, the National White Collar Crime Center, and other partners regarding data breach notification prioritization, coordination and deconfliction.**

The Los Angeles Sheriff's Department (LASD) and LA FBI are in the process of copying the fully downloaded, scanned, and indexed files from the dark web and they will be available next week. Due to the size of the files we are continuing to develop the best data sharing mechanism. Designated data breach points of contact should add their information to the Data Breach POC List. POC List access requests should be sent to ciosubcommittee@nfcausa.org.

- Legal and privacy experts will be developing recommendations for handling the FBI investigative case data as there may be privacy protection and public records act implications for those that download any files from the data breach.

- **As the dark web site contains potential malware, no one should attempt to download material without the proper cyber resources.**

- The Criminal Intelligence Coordinating Council's (CICC) Criminal Intelligence/Information Technology (CI/IT) **Crossroads Committee** will be working with federal partners and all of the major law enforcement associations in America to develop recommendations to enhance and promote nationwide best practices in the field of data breach mitigation and response strategy development. The recommendations will be provided through the CICC to the Global Justice Information Sharing Initiative (Global) for the consideration of and approval of the US Attorney General and other federal executives, including the leadership of DHS, FBI, ONDCP, and the ODNI. If your agency would like to know more about or participate in the Crossroads Committee, please send an email to Tim Best at TBest@iir.com.

For cyber mitigation coordination requests related to this breach please e-mail ciosubcommittee@nfcausa.org.

From: Coliflores, Joseph (WES)
To: Pack, Noah (POL)
Subject: RE:
Date: Tuesday, May 5, 2020 11:28:11 AM

Hi Noah,

I just reread McCarthy (ALPR case) to see what the SJC might say/think.

Are you referring to a pen register? PRTT?

My cell phone is (G.L. c. 4.sec. 7.cl.26 (n)(security) Shoot me a text before calling, but I think I have you in my contacts already.

Joseph G. A. Coliflores
Assistant District Attorney, Appeals Unit
Hampden District Attorney's Office

From: Pack, Noah (POL)
Sent: Tuesday, May 5, 2020 10:25 AM
To: Coliflores, Joseph (WES)
Subject:

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

Can we discuss, when you are available?

Noah

Trooper Noah H. Pack
Massachusetts State Police Detective Unit
Office of the Hampden District Attorney
1500 Main Street, 18th Floor
Springfield, MA 01115-5327
Office (413) 505-5936

This e-mail message is generated from the Office of the Hampden District Attorney and contains information that is confidential and may be privileged as an attorney/client communication or as attorney work product. The information is intended to be disclosed solely to the addressee(s). If you are not the intended recipient, be aware that any disclosure, copying, distribution or use of the contents of this email information is prohibited. If you have received this email in error, please notify the sender by return email and delete it from your computer system.

This e-mail message is generated from the Office of the Hampden District Attorney and contains information that is confidential and may be privileged as an attorney/client communication or as attorney work product. The information is intended to be disclosed solely to the addressee(s). If you are not the intended recipient, be aware that any disclosure, copying, distribution or use of the contents of this email information is prohibited. If you have received this email in error, please notify the sender by return email and delete it from your computer system.

From: Griffin, Robert
To: Egnitz, Brian (POL)
Subject: Re: [EXTERNAL] Re: Flock LPRs to State DB
Date: Tuesday, October 27, 2020 11:46:14 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

I'll check. I've never heard of Rokor.

On Tue, Oct 20, 2020, 9:17 AM Egnitz, Brian (POL) <brian.egnitz@state.ma.us> wrote:

> Hi Ron,
>
> Can you check to see if your vendor has an adapter to Rekor's open ALPR?
>
> Tks, Brian
>
> > On Jul 7, 2020, at 5:19 PM, Griffin, Robert <rgriffin@chelseama.gov> wrote:
> >
> > CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
> >
> > Brian,
> >
> > Last time we spoke, I know you were involved with the LPRs. We just went live [redacted] G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative) At a minimum, I'd like to give you access. But I would also like to work with the state police and see if we can use Flock's API somehow to transfer the data to the State's LPR database. I believe you guys are still using PIPS?
> >
> > Rob
> > 617-438-7331

From: Commonwealth Fusion Center (POL)
To: Lunger, Jennifer A
Subject: Re: [External] RFI - LPR - Case #: 2019-102-217 - Narcotics
Date: Tuesday, July 7, 2020 1:39:47 PM

Received. Thank you for the quick response!

Respectfully,

Sean Bender
Intelligence Analyst
Massachusetts State Police | Commonwealth Fusion Center
470 Worcester Road | Framingham, MA 01702
Phone: (508) 820-2233

CONFIDENTIALITY NOTICE: The information contained in this email and any attachment is privileged and confidential law enforcement information. If you are not the intended recipient, you are hereby notified that any disclosure, dissemination, or copying of this communication is strictly prohibited. If you have received this email in error, please call (978) 451-3700 immediately.

From: Lunger, Jennifer A <jlunger@pa.gov>
Sent: Tuesday, July 7, 2020 1:31 PM
To: Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>
Subject: RE: [External] RFI - [redacted]

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

[redacted]

Respectfully,

Jennifer Lunger | Intelligence Analyst
Western Pennsylvania All Hazards Fusion Center
Pennsylvania State Police | Bureau of Criminal Investigation
150 Hookstown Grade Road | Moon, PA 15108
Phone: 412.423.9245 | Fusion Center E-mail: wpahfc@pa.gov
www.psp.pa.gov

PRIVILEGED AND CONFIDENTIAL COMMUNICATION

Recipients should attempt to update and verify any information contained within this transmission before taking any enforcement action. *The information transmitted is intended only for the person or entity to whom it is addressed and may contain confidential and/or privileged material. Any use of this information other than by the intended recipient is prohibited. If you receive this message in error, please send a reply e-mail to the sender and delete the material from all computers and/or devices. Unintended transmissions shall not constitute waiver of the attorney-*

client or any other privilege.

From: Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>
Sent: Tuesday, July 7, 2020 1:17 PM
Cc: McCabe, Scott (CPI) <scott.mccabe@state.ma.us>
Subject: [External] RFI - [redacted]

ATTENTION: *This email message is from an external sender. Do not open links or attachments from unknown sources. To report suspicious email, forward the message as an attachment to CWOPA_SPAM@pa.gov.*
Good Afternoon, All -

The Commonwealth Fusion Center (MA) is respectfully requesting on behalf of the Massachusetts State Police Cape & Islands Detective Unit, that the below listed vehicle be run through any available Automated License Plate Recognition (ALPR/LPR) system pursuant to an active/ongoing narcotics investigation. Information received by investigators indicates that the suspect vehicle may have traveled from Cape Cod, Massachusetts to Philadelphia, Pennsylvania between 16 June 2020 - 30 June 2020. Investigators are hoping to corroborate this information via LPR data on the vehicle.

[redacted]

Case Information:

[redacted]

Respectfully,

Sean Bender
Intelligence Analyst
Massachusetts State Police | Commonwealth Fusion Center
470 Worcester Road | Framingham, MA 01702
Phone: (508) 820-2233

CONFIDENTIALITY NOTICE: The information contained in this email and any attachment is privileged and confidential law enforcement information. If you are not the intended recipient, you are hereby notified that any disclosure, dissemination, or copying of this communication is strictly prohibited. If you have received this email in error, please call (978) 451-3700 immediately.

From: McCabe, Scott (CPI) <Scott.McCabe@MassMail.State.MA.US>
Sent: Tuesday, July 7, 2020 12:39 PM
To: Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>
Cc: McCabe, Scott (CPI) <Scott.McCabe@MassMail.State.MA.US>
Subject: LPR data for MA [redacted]

[redacted]

Any Questions or if more information is needed, please email or cal [redacted]

Thanks
Sgt Scott McCabe
Cape Cod Task Force
Cape and Islands Detective Unit
Massachusetts State Police

From: Egnitz, Brian (POL)
To: Schwarz, William J
Cc: Jim Charron; Tiffany Tran; Mitchell, Timothy P. (EOTSS)
Subject: Re: [EXTERNAL]RE: Plate reader access
Date: Friday, October 23, 2020 10:41:32 AM

No problem, I'm fairly open next week if you want to do a conference call. BTW, JimSlatter retired, I'm Not sure who is the current EOPSS SCIO.

On Oct 23, 2020, at 9:35 AM, Schwarz, William J <WSchwarz@springfieldpolice.net> wrote:

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

I would just like you to have a quick conversation with our vendors to clarify the process if you can.

Bill

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Friday, October 23, 2020 9:18 AM
To: Schwarz, William J <WSchwarz@springfieldpolice.net>; Jim Charron <jim.charron@motorolasolutions.com>; Tiffany Tran <tiffanytran@motorolasolutions.com>
Cc: Mitchell, Timothy P (MASSIT) <timothy.p.mitchell@state.ma.us>
Subject: [EXTERNAL]RE: Plate reader access

Did EOTSS give you access to the DB? Neology does not support direct access to the SQL nor do I recommend it, it could have unintended consequences to the systems ability to keep up with reads and alerts. The current supported method for sharing BOSS data is via a PIPS plugin. I am currently working with a cloud vendor and the plug in. If the cloud vendor I'm working with pans out we would have an API for you to use. I'll know more in a few weeks, please hold off if possible.

-Brian

From: Schwarz, William J <WSchwarz@springfieldpolice.net>
Sent: Thursday, October 22, 2020 2:38 PM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Jim Charron <jim.charron@motorolasolutions.com>; Tiffany Tran <tiffanytran@motorolasolutions.com>
Subject: Plate reader access

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Brian:

Can we please chat on a conference call about the access credentials and connections to the alpr system? Jim will send out a link if you have a date and time that your available.

Bill

William Schwarz
Director of Crime Analysis / Real Time Analysis Center
130 Pearl St.
Springfield, MA 01105
413-886-5282

From: brian.egnitz@pol.state.ma.us
To: Schwarz, William J
Cc: Jim Charron; Tiffany Tran; Mitchell, Timothy P. (EOTSS)
Subject: Re: [EXTERNAL]RE: Plate reader access
Date: Friday, October 23, 2020 10:41:31 AM

No problem, I'm fairly open next week if you want to do a conference call. BTW, JimSlatter retired, I'm Not sure who is the current EOPSS SCIO.

On Oct 23, 2020, at 9:35 AM, Schwarz, William J <WSchwarz@springfieldpolice.net> wrote:

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

I would just like you to have a quick conversation with our vendors to clarify the process if you can.

Bill

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Friday, October 23, 2020 9:18 AM
To: Schwarz, William J <WSchwarz@springfieldpolice.net>; Jim Charron <jim.charron@motorolasolutions.com>; Tiffany Tran <tiffanytran@motorolasolutions.com>
Cc: Mitchell, Timothy P (MASSIT) <timothy.p.mitchell@state.ma.us>
Subject: [EXTERNAL]RE: Plate reader access

Did EOTSS give you access to the DB? Neology does not support direct access to the SQL nor do I recommend it, it could have unintended consequences to the systems ability to keep up with reads and alerts. The current supported method for sharing BOSS data is via a PIPS plugin. I am currently working with a cloud vendor and the plug in. If the cloud vendor I'm working with pans out we would have an API for you to use. I'll know more in a few weeks, please hold off if possible.

-Brian

From: Schwarz, William J <WSchwarz@springfieldpolice.net>
Sent: Thursday, October 22, 2020 2:38 PM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Jim Charron <jim.charron@motorolasolutions.com>; Tiffany Tran <tiffanytran@motorolasolutions.com>
Subject: Plate reader access

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Brian:

Can we please chat on a conference call about the access credentials and connections to the alpr system? Jim will send out a link if you have a date and time that your available.

Bill

William Schwarz
Director of Crime Analysis / Real Time Analysis Center
130 Pearl St.
Springfield, MA 01105
413-886-5282

From: Schwarz, William J
To: Egnitz, Brian (POL); Jim Charron; Tiffany Tran
Cc: Mitchell, Timothy P. (EOTSS)
Subject: RE: [EXTERNAL]RE: Plate reader access
Date: Friday, October 23, 2020 9:35:16 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

I would just like you to have a quick conversation with our vendors to clarify the process if you can.

Bill

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Friday, October 23, 2020 9:18 AM
To: Schwarz, William J <WSchwarz@springfieldpolice.net>; Jim Charron <jim.charron@motorolasolutions.com>; Tiffany Tran <tiffanytran@motorolasolutions.com>
Cc: Mitchell, Timothy P (MASSIT) <timothy.p.mitchell@state.ma.us>
Subject: [EXTERNAL]RE: Plate reader access

Did EOTSS give you access to the DB? Neology does not support direct access to the SQL nor do I recommend it, it could have unintended consequences to the systems ability to keep up with reads and alerts. The current supported method for sharing BOSS data is via a PIPS plugin. I am currently working with a cloud vendor and the plug in. If the cloud vendor I'm working with pans out we would have an API for you to use. I'll know more in a few weeks, please hold off if possible.

-Brian

From: Schwarz, William J <WSchwarz@springfieldpolice.net>
Sent: Thursday, October 22, 2020 2:38 PM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Jim Charron <jim.charron@motorolasolutions.com>; Tiffany Tran <tiffanytran@motorolasolutions.com>
Subject: Plate reader access

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Brian:

Can we please chat on a conference call about the access credentials and connections to the alpr system? Jim will send out a link if you have a date and time that your available.

Bill

William Schwarz
Director of Crime Analysis / Real Time Analysis Center
130 Pearl St.
Springfield, MA 01105
413-886-5282

From: kloving@groups.io on behalf of Klingenberg, Brianne via groups.io
To: kloving@groups.io
Subject: Re: [kloving] ALPR
Date: Wednesday, December 9, 2020 12:12:23 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Thanks Thane…. Sounds like I won't have much luck for 2007, but I appreciate the info!!

Detective Brianne Klingenberg #2226
Santa Clara County Sheriff's Office – Investigations Division
Missing Persons, Juvenile Crimes, Child Abuse (E/B)
55 West Younger Avenue; San Jose, CA 95110
408-808-4500 / 408-808-4545 Fax

From: kloving@groups.io <kloving@groups.io> **On Behalf Of** Gallagher, Thane
Sent: Wednesday, December 9, 2020 8:45 AM
To: kloving@groups.io
Subject: [EXTERNAL] Re: [kloving] ALPR

Industry standard tends to follow a two-year retention period for most systems, like Vigilant for example. Vigilant adheres to the retention policies of each respective client agency, who pays for their services.

In the federal government, the period is often shorter. For example, the LPRs employed at Ports of Entry by CBP's Office of Field Operations along the southwest and northern border as well as interior Checkpoints operated by the U.S. Border Patrol are on the same network and they only retain 18 months of data.

If you narrow it down to a state, the following link lists most state's laws/retention policies with respect to ALPR data and operation:

https://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plate-readers-alpr-or-alpr-data.aspx

Thane Gallagher
Investigative Technician II

Riverside County District Attorney's Office
Bureau of Investigations/Mid-County Region
MPU
135 North Alessandro
Banning, CA 92220
(951) 922-7194

From: kloving@groups.io <kloving@groups.io> **On Behalf Of** Klingenberg, Brianne via groups.io
Sent: Wednesday, December 9, 2020 8:15 AM
To: kloving@groups.io
Subject: [kloving] ALPR

Good Morning All!

Is anyone aware of an ALPR (License plate reader) system that would date back pretty far? I have a missing person MIA since 2007 and an associated vehicle without any hits on an NCIC Offline search.

Thanks!

Detective Brianne Klingenberg #2226
Santa Clara County Sheriff's Office – Investigations Division
Missing Persons, Juvenile Crimes, Child Abuse (E/B)
55 West Younger Avenue; San Jose, CA 95110
408-808-4539 / 408-808-4545 Fax

Groups.io Links:

You receive all messages sent to this group.

View/Reply Online (#16763) | Reply To Group | Reply To Sender | Mute This Topic | New Topic
Your Subscription | Contact Group Owner | Unsubscribe [john.conron@state.ma.us]

From: kloving@groups.io on behalf of Klingenberg, Brianne
To: kloving@groups.io
Subject: Re: [kloving] ALPR
Date: Wednesday, December 9, 2020 12:12:22 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Thanks Thane…. Sounds like I won't have much luck for 2007, but I appreciate the info!!

Detective Brianne Klingenberg #2226
Santa Clara County Sheriff's Office – Investigations Division
Missing Persons, Juvenile Crimes, Child Abuse (E/B)
55 West Younger Avenue; San Jose, CA 95110
408-808-4500 / 408-808-4545 Fax

From: kloving@groups.io <kloving@groups.io> **On Behalf Of** Gallagher, Thane
Sent: Wednesday, December 9, 2020 8:45 AM
To: kloving@groups.io
Subject: [EXTERNAL] Re: [kloving] ALPR

Industry standard tends to follow a two-year retention period for most systems, like Vigilant for example. Vigilant adheres to the retention policies of each respective client agency, who pays for their services.

In the federal government, the period is often shorter. For example, the LPRs employed at Ports of Entry by CBP's Office of Field Operations along the southwest and northern border as well as interior Checkpoints operated by the U.S. Border Patrol are on the same network and they only retain 18 months of data.

If you narrow it down to a state, the following link lists most state's laws/retention policies with respect to ALPR data and operation:

https://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plate-readers-alpr-or-alpr-data.aspx

Thane Gallagher
Investigative Technician II

Riverside County District Attorney's Office
Bureau of Investigations/Mid-County Region
MPU
135 North Alessandro
Banning, CA 92220
(951) 922-7194

From: kloving@groups.io <kloving@groups.io> **On Behalf Of** Klingenberg, Brianne via groups.io
Sent: Wednesday, December 9, 2020 8:15 AM
To: kloving@groups.io
Subject: [kloving] ALPR

Good Morning All!

Is anyone aware of an ALPR (License plate reader) system that would date back pretty far? I have a missing person MIA since 2007 and an associated vehicle without any hits on an NCIC Offline search.

Thanks!

Detective Brianne Klingenberg #2226
Santa Clara County Sheriff's Office – Investigations Division
Missing Persons, Juvenile Crimes, Child Abuse (E/B)
55 West Younger Avenue; San Jose, CA 95110
408-808-4539 / 408-808-4545 Fax

Groups.io Links:

You receive all messages sent to this group.

View/Reply Online (#16763) | Reply To Group | Reply To Sender | Mute This Topic | New Topic
Your Subscription | Contact Group Owner | Unsubscribe [edward.keefe@pol.state.ma.us]

From: kloving@groups.io on behalf of Klingenberg, Brianne
To: kloving@groups.io
Subject: Re: [kloving] ALPR
Date: Wednesday, December 9, 2020 12:12:03 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Thanks Thane…. Sounds like I won't have much luck for 2007, but I appreciate the info!!

Detective Brianne Klingenberg #2226
Santa Clara County Sheriff's Office – Investigations Division
Missing Persons, Juvenile Crimes, Child Abuse (E/B)
55 West Younger Avenue; San Jose, CA 95110
408-808-4500 / 408-808-4545 Fax

From: kloving@groups.io <kloving@groups.io> **On Behalf Of** Gallagher, Thane
Sent: Wednesday, December 9, 2020 8:45 AM
To: kloving@groups.io
Subject: [EXTERNAL] Re: [kloving] ALPR

Industry standard tends to follow a two-year retention period for most systems, like Vigilant for example. Vigilant adheres to the retention policies of each respective client agency, who pays for their services.

In the federal government, the period is often shorter. For example, the LPRs employed at Ports of Entry by CBP's Office of Field Operations along the southwest and northern border as well as interior Checkpoints operated by the U.S. Border Patrol are on the same network and they only retain 18 months of data.

If you narrow it down to a state, the following link lists most state's laws/retention policies with respect to ALPR data and operation:

https://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plate-readers-alpr-or-alpr-data.aspx

Thane Gallagher
Investigative Technician II

Riverside County District Attorney's Office
Bureau of Investigations/Mid-County Region
MPU
135 North Alessandro
Banning, CA 92220
(951) 922-7194

From: kloving@groups.io <kloving@groups.io> **On Behalf Of** Klingenberg, Brianne via groups.io
Sent: Wednesday, December 9, 2020 8:15 AM
To: kloving@groups.io
Subject: [kloving] ALPR

Good Morning All!

Is anyone aware of an ALPR (License plate reader) system that would date back pretty far? I have a missing person MIA since 2007 and an associated vehicle without any hits on an NCIC Offline search.

Thanks!

Detective Brianne Klingenberg #2226
Santa Clara County Sheriff's Office – Investigations Division
Missing Persons, Juvenile Crimes, Child Abuse (E/B)
55 West Younger Avenue; San Jose, CA 95110
408-808-4539 / 408-808-4545 Fax

Groups.io Links:

You receive all messages sent to this group.

View/Reply Online (#16763) | Reply To Group | Reply To Sender | Mute This Topic | New Topic
Your Subscription | Contact Group Owner | Unsubscribe
[christopher.macdonald@pol.state.ma.us]

From: kloving@groups.io on behalf of Klingenberg, Brianne via groups.io
To: kloving@groups.io
Subject: Re: [kloving] ALPR
Date: Wednesday, December 9, 2020 12:11:46 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Thanks Thane…. Sounds like I won't have much luck for 2007, but I appreciate the info!!

Detective Brianne Klingenberg #2226
Santa Clara County Sheriff's Office – Investigations Division
Missing Persons, Juvenile Crimes, Child Abuse (E/B)
55 West Younger Avenue; San Jose, CA 95110
408-808-4500 / 408-808-4545 Fax

From: kloving@groups.io <kloving@groups.io> **On Behalf Of** Gallagher, Thane
Sent: Wednesday, December 9, 2020 8:45 AM
To: kloving@groups.io
Subject: [EXTERNAL] Re: [kloving] ALPR

Industry standard tends to follow a two-year retention period for most systems, like Vigilant for example. Vigilant adheres to the retention policies of each respective client agency, who pays for their services.

In the federal government, the period is often shorter. For example, the LPRs employed at Ports of Entry by CBP's Office of Field Operations along the southwest and northern border as well as interior Checkpoints operated by the U.S. Border Patrol are on the same network and they only retain 18 months of data.

If you narrow it down to a state, the following link lists most state's laws/retention policies with respect to ALPR data and operation:

https://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plate-readers-alpr-or-alpr-data.aspx

Thane Gallagher
Investigative Technician II

Riverside County District Attorney's Office
Bureau of Investigations/Mid-County Region
MPU
135 North Alessandro
Banning, CA 92220
(951) 922-7194

From: kloving@groups.io <kloving@groups.io> **On Behalf Of** Klingenberg, Brianne via groups.io
Sent: Wednesday, December 9, 2020 8:15 AM
To: kloving@groups.io
Subject: [kloving] ALPR

Good Morning All!

Is anyone aware of an ALPR (License plate reader) system that would date back pretty far? I have a missing person MIA since 2007 and an associated vehicle without any hits on an NCIC Offline search.

Thanks!

Detective Brianne Klingenberg #2226
Santa Clara County Sheriff's Office – Investigations Division
Missing Persons, Juvenile Crimes, Child Abuse (E/B)
55 West Younger Avenue; San Jose, CA 95110
408-808-4539 / 408-808-4545 Fax

Groups.io Links:

You receive all messages sent to this group.

View/Reply Online (#16763) | Reply To Group | Reply To Sender | Mute This Topic | New Topic
Your Subscription | Contact Group Owner | Unsubscribe [thomas.forest@state.ma.us]

From: kloving@groups.io on behalf of Gallagher, Thane via groups.io
To: kloving@groups.io
Subject: Re: [kloving] ALPR
Date: Wednesday, December 9, 2020 11:47:54 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Industry standard tends to follow a two-year retention period for most systems, like Vigilant for example. Vigilant adheres to the retention policies of each respective client agency, who pays for their services.

In the federal government, the period is often shorter. For example, the LPRs employed at Ports of Entry by CBP's Office of Field Operations along the southwest and northern border as well as interior Checkpoints operated by the U.S. Border Patrol are on the same network and they only retain 18 months of data.

If you narrow it down to a state, the following link lists most state's laws/retention policies with respect to ALPR data and operation:

https://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plate-readers-alpr-or-alpr-data.aspx

Thane Gallagher
Investigative Technician II

Riverside County District Attorney's Office
Bureau of Investigations/Mid-County Region
MPU
135 North Alessandro
Banning, CA 92220
(951) 922-7194

From: kloving@groups.io <kloving@groups.io> **On Behalf Of** Klingenberg, Brianne via groups.io

Sent: Wednesday, December 9, 2020 8:15 AM
To: kloving@groups.io
Subject: [kloving] ALPR

Good Morning All!

Is anyone aware of an ALPR (License plate reader) system that would date back pretty far? I have a missing person MIA since 2007 and an associated vehicle without any hits on an NCIC Offline search.

Thanks!

Detective Brianne Klingenberg #2226
Santa Clara County Sheriff's Office – Investigations Division
Missing Persons, Juvenile Crimes, Child Abuse (E/B)
55 West Younger Avenue; San Jose, CA 95110
408-808-4539 / 408-808-4545 Fax

Groups.io Links:

You receive all messages sent to this group.

View/Reply Online (#16761) | Reply To Group | Reply To Sender | Mute This Topic | New Topic
Your Subscription | Contact Group Owner | Unsubscribe [john.conron@state.ma.us]

From: kloving@groups.io on behalf of Gallagher, Thane via groups.io
To: kloving@groups.io
Subject: Re: [kloving] ALPR
Date: Wednesday, December 9, 2020 11:47:39 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Industry standard tends to follow a two-year retention period for most systems, like Vigilant for example. Vigilant adheres to the retention policies of each respective client agency, who pays for their services.

In the federal government, the period is often shorter. For example, the LPRs employed at Ports of Entry by CBP's Office of Field Operations along the southwest and northern border as well as interior Checkpoints operated by the U.S. Border Patrol are on the same network and they only retain 18 months of data.

If you narrow it down to a state, the following link lists most state's laws/retention policies with respect to ALPR data and operation:

https://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plate-readers-alpr-or-alpr-data.aspx

Thane Gallagher
Investigative Technician II

Riverside County District Attorney's Office
Bureau of Investigations/Mid-County Region
MPU
135 North Alessandro
Banning, CA 92220
(951) 922-7194

From: kloving@groups.io <kloving@groups.io> **On Behalf Of** Klingenberg, Brianne via groups.io

Sent: Wednesday, December 9, 2020 8:15 AM
To: kloving@groups.io
Subject: [kloving] ALPR

Good Morning All!

Is anyone aware of an ALPR (License plate reader) system that would date back pretty far? I have a missing person MIA since 2007 and an associated vehicle without any hits on an NCIC Offline search.

Thanks!

Detective Brianne Klingenberg #2226
Santa Clara County Sheriff's Office – Investigations Division
Missing Persons, Juvenile Crimes, Child Abuse (E/B)
55 West Younger Avenue; San Jose, CA 95110
408-808-4539 / 408-808-4545 Fax

Groups.io Links:

You receive all messages sent to this group.

View/Reply Online (#16761) | Reply To Group | Reply To Sender | Mute This Topic | New Topic
Your Subscription | Contact Group Owner | Unsubscribe [william.j.desantis@state.ma.us]

From: kloving@groups.io on behalf of Gallagher, Thane
To: kloving@groups.io
Subject: Re: [kloving] ALPR
Date: Wednesday, December 9, 2020 11:47:39 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Industry standard tends to follow a two-year retention period for most systems, like Vigilant for example. Vigilant adheres to the retention policies of each respective client agency, who pays for their services.

In the federal government, the period is often shorter. For example, the LPRs employed at Ports of Entry by CBP's Office of Field Operations along the southwest and northern border as well as interior Checkpoints operated by the U.S. Border Patrol are on the same network and they only retain 18 months of data.

If you narrow it down to a state, the following link lists most state's laws/retention policies with respect to ALPR data and operation:

https://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plate-readers-alpr-or-alpr-data.aspx

Thane Gallagher
Investigative Technician II

Riverside County District Attorney's Office
Bureau of Investigations/Mid-County Region
MPU
135 North Alessandro
Banning, CA 92220
(951) 922-7194

From: kloving@groups.io <kloving@groups.io> **On Behalf Of** Klingenberg, Brianne via groups.io

Sent: Wednesday, December 9, 2020 8:15 AM
To: kloving@groups.io
Subject: [kloving] ALPR

Good Morning All!

Is anyone aware of an ALPR (License plate reader) system that would date back pretty far? I have a missing person MIA since 2007 and an associated vehicle without any hits on an NCIC Offline search.

Thanks!

Detective Brianne Klingenberg #2226
Santa Clara County Sheriff's Office – Investigations Division
Missing Persons, Juvenile Crimes, Child Abuse (E/B)
55 West Younger Avenue; San Jose, CA 95110
408-808-4539 / 408-808-4545 Fax

Groups.io Links:

You receive all messages sent to this group.

View/Reply Online (#16761) | Reply To Group | Reply To Sender | Mute This Topic | New Topic
Your Subscription | Contact Group Owner | Unsubscribe
[christopher.macdonald@pol.state.ma.us]

From: kloving@groups.io on behalf of Gallagher, Thane
To: kloving@groups.io
Subject: Re: [kloving] ALPR
Date: Wednesday, December 9, 2020 11:47:28 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Industry standard tends to follow a two-year retention period for most systems, like Vigilant for example. Vigilant adheres to the retention policies of each respective client agency, who pays for their services.

In the federal government, the period is often shorter. For example, the LPRs employed at Ports of Entry by CBP's Office of Field Operations along the southwest and northern border as well as interior Checkpoints operated by the U.S. Border Patrol are on the same network and they only retain 18 months of data.

If you narrow it down to a state, the following link lists most state's laws/retention policies with respect to ALPR data and operation:

https://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plate-readers-alpr-or-alpr-data.aspx

Thane Gallagher
Investigative Technician II

Riverside County District Attorney's Office
Bureau of Investigations/Mid-County Region
MPU
135 North Alessandro
Banning, CA 92220
(951) 922-7194

From: kloving@groups.io <kloving@groups.io> **On Behalf Of** Klingenberg, Brianne via groups.io

Sent: Wednesday, December 9, 2020 8:15 AM
To: kloving@groups.io
Subject: [kloving] ALPR

Good Morning All!

Is anyone aware of an ALPR (License plate reader) system that would date back pretty far? I have a missing person MIA since 2007 and an associated vehicle without any hits on an NCIC Offline search.

Thanks!

Detective Brianne Klingenberg #2226
Santa Clara County Sheriff's Office – Investigations Division
Missing Persons, Juvenile Crimes, Child Abuse (E/B)
55 West Younger Avenue; San Jose, CA 95110
408-808-4539 / 408-808-4545 Fax

Groups.io Links:

You receive all messages sent to this group.

View/Reply Online (#16761) | Reply To Group | Reply To Sender | Mute This Topic | New Topic
Your Subscription | Contact Group Owner | Unsubscribe [edward.keefe@pol.state.ma.us]

From: kloving@groups.io on behalf of Gallagher, Thane via groups.io
To: kloving@groups.io
Subject: Re: [kloving] ALPR
Date: Wednesday, December 9, 2020 11:47:26 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Industry standard tends to follow a two-year retention period for most systems, like Vigilant for example. Vigilant adheres to the retention policies of each respective client agency, who pays for their services.

In the federal government, the period is often shorter. For example, the LPRs employed at Ports of Entry by CBP's Office of Field Operations along the southwest and northern border as well as interior Checkpoints operated by the U.S. Border Patrol are on the same network and they only retain 18 months of data.

If you narrow it down to a state, the following link lists most state's laws/retention policies with respect to ALPR data and operation:

https://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plate-readers-alpr-or-alpr-data.aspx

Thane Gallagher
Investigative Technician II

Riverside County District Attorney's Office
Bureau of Investigations/Mid-County Region
MPU
135 North Alessandro
Banning, CA 92220
(951) 922-7194

From: kloving@groups.io <kloving@groups.io> **On Behalf Of** Klingenberg, Brianne via groups.io

Sent: Wednesday, December 9, 2020 8:15 AM
To: kloving@groups.io
Subject: [kloving] ALPR

Good Morning All!

Is anyone aware of an ALPR (License plate reader) system that would date back pretty far? I have a missing person MIA since 2007 and an associated vehicle without any hits on an NCIC Offline search.

Thanks!

Detective Brianne Klingenberg #2226
Santa Clara County Sheriff's Office – Investigations Division
Missing Persons, Juvenile Crimes, Child Abuse (E/B)
55 West Younger Avenue; San Jose, CA 95110
408-808-4539 / 408-808-4545 Fax

Groups.io Links:

You receive all messages sent to this group.

View/Reply Online (#16761) | Reply To Group | Reply To Sender | Mute This Topic | New Topic
Your Subscription | Contact Group Owner | Unsubscribe [thomas.forest@state.ma.us]

From: kloving@groups.io on behalf of Klingenberg, Brianne via groups.io
To: kloving@groups.io
Subject: Re: [kloving] ALPR
Date: Wednesday, December 9, 2020 12:12:52 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Thanks Thane…. Sounds like I won't have much luck for 2007, but I appreciate the info!!

Detective Brianne Klingenberg #2226
Santa Clara County Sheriff's Office – Investigations Division
Missing Persons, Juvenile Crimes, Child Abuse (E/B)
55 West Younger Avenue; San Jose, CA 95110
408-808-4500 / 408-808-4545 Fax

From: kloving@groups.io <kloving@groups.io> **On Behalf Of** Gallagher, Thane
Sent: Wednesday, December 9, 2020 8:45 AM
To: kloving@groups.io
Subject: [EXTERNAL] Re: [kloving] ALPR

Industry standard tends to follow a two-year retention period for most systems, like Vigilant for example. Vigilant adheres to the retention policies of each respective client agency, who pays for their services.

In the federal government, the period is often shorter. For example, the LPRs employed at Ports of Entry by CBP's Office of Field Operations along the southwest and northern border as well as interior Checkpoints operated by the U.S. Border Patrol are on the same network and they only retain 18 months of data.

If you narrow it down to a state, the following link lists most state's laws/retention policies with respect to ALPR data and operation:

https://www.ncsl.org/research/telecommunications-and-information-technology/state-statutes-regulating-the-use-of-automated-license-plate-readers-alpr-or-alpr-data.aspx

Thane Gallagher
Investigative Technician II

Riverside County District Attorney's Office
Bureau of Investigations/Mid-County Region
MPU
135 North Alessandro
Banning, CA 92220
(951) 922-7194

From: kloving@groups.io <kloving@groups.io> **On Behalf Of** Klingenberg, Brianne via groups.io
Sent: Wednesday, December 9, 2020 8:15 AM
To: kloving@groups.io
Subject: [kloving] ALPR

Good Morning All!

Is anyone aware of an ALPR (License plate reader) system that would date back pretty far? I have a missing person MIA since 2007 and an associated vehicle without any hits on an NCIC Offline search.

Thanks!

Detective Brianne Klingenberg #2226
Santa Clara County Sheriff's Office – Investigations Division
Missing Persons, Juvenile Crimes, Child Abuse (E/B)
55 West Younger Avenue; San Jose, CA 95110
408-808-4539 / 408-808-4545 Fax

Groups.io Links:

You receive all messages sent to this group.

View/Reply Online (#16763) | Reply To Group | Reply To Sender | Mute This Topic | New Topic
Your Subscription | Contact Group Owner | Unsubscribe [william.j.desantis@state.ma.us]

From: Babbin, Timothy (AGO)
To: Gallagher, David (POL)
Subject: RE: ALPR Accounts
Date: Tuesday, August 18, 2020 10:55:41 AM

Thank you, Sir.

From: Gallagher, David (POL) <david.gallagher3@MassMail.State.MA.US>
Sent: Tuesday, August 18, 2020 10:30 AM
To: Babbin, Timothy (AGO) <Timothy.G.Babbin@mass.gov>
Subject: Re: ALPR Accounts

I'll take care of that. I'll send you an updated password shortly.

David M. Gallagher

Major, Massachusetts State Police

Special Operations

508-820-2162

David.Gallagher3@MassMail.state.ma.us

From: Babbin, Timothy (AGO) <Timothy.G.Babbin@mass.gov>
Sent: Tuesday, August 18, 2020 10:03 AM

To: Gallagher, David (POL) <david.gallagher3@MassMail.State.MA.US>
Subject: RE: ALPR Accounts

Major-

Thank you for the prompt assistance with the ALPR.

Could you advise me who would handle password resets?

I had the ALPR when I was down at Plainville but have not had access since.

What (I thought) was my then password no longer works.

Thanks,

Tim

From: Gallagher, David (POL) <david.gallagher3@MassMail.State.MA.US>
Sent: Monday, August 17, 2020 7:44 PM
To: Babbin, Timothy (AGO) <Timothy.G.Babbin@mass.gov>
Subject: ALPR Accounts

DLT Babbin,

Sgt. Tirella reached out and requested I set up ALPR accounts for the following:

DLT Timothy Babbin #2120 *****

Lt. Michael Ahern #2486

Lt. Walter Foley #3110

Lt. Steven Connolly #2719 *****

Lt. Joseph Ross #2264

Lt. Michelle Sutherland #2466

Sgt. Michael Leo #2887

Sgt. Maura McCarthy #2759

Sgt. Patrick Johnson #3128

Sgt. Matthew Hannigan #3281

Sgt. Thomas Mahon #3146

Tpr. John MacDonald #3143

Tpr. Loming Chan #0741 *****

Tpr. Robert Noonan #3327

Tpr. Jose Cuevas #3237

Tpr. Carly Rose #3347

Tpr. Robert Soldani #3879

Tpr. Daniel Nunes #3674 *****

Tpr. Erin McLaughlin #3655

Tpr. Kevin Flynn #3791

Tpr. Christopher Andrade #3738 *****

Tpr. Martin Concannon #3409

Tpr. Shawn Murphy #3481

Tpr. Joshua Rucho #3704

Tpr. Nicholas Pellegrino #3684

Tpr. Shawn LeBlanc #3015

Tpr. Steven Grasso #3803

Tpr. Julio Barbosa #4074

***** Indicates that there is already account created.

I will send a separate email with user guide / link to download software.

Logon will be [redacted] [redacted]

Initial password will be [redacted] [redacted] [redacted]

They can change it after initial login.

If you can designate a single POC to address any issues, that would be greatly appreciated.

Lt's and Sgt's have advanced access. Tprs. have basic access.

Please let me know if you need any further assistance.

Respectfully,

David M. Gallagher

Major, Massachusetts State Police

Special Operations

508-820-2162

David.Gallagher3@MassMail.state.ma.us

From: Babbin, Timothy (AGO)
To: Gallagher, David (POL)
Subject: RE: ALPR Accounts
Date: Tuesday, August 18, 2020 10:03:34 AM

Major-

Thank you for the prompt assistance with the ALPR.

Could you advise me who would handle password resets?

I had the ALPR when I was down at Plainville but have not had access since.

What (I thought) was my then password no longer works.

Thanks,

Tim

From: Gallagher, David (POL) <david.gallagher3@MassMail.State.MA.US>
Sent: Monday, August 17, 2020 7:44 PM
To: Babbin, Timothy (AGO) <Timothy.G.Babbin@mass.gov>
Subject: ALPR Accounts

DLT Babbin,

Sgt. Tirella reached out and requested I set up ALPR accounts for the following:

DLT Timothy Babbin #2120 *****

Lt. Michael Ahern #2486

Lt. Walter Foley #3110

Lt. Steven Connolly #2719 *****

Lt. Joseph Ross #2264

Lt. Michelle Sutherland #2466

Sgt. Michael Leo #2887

Sgt. Maura McCarthy #2759

Sgt. Patrick Johnson #3128

Sgt. Matthew Hannigan #3281

Sgt. Thomas Mahon #3146

Tpr. John MacDonald #3143

Tpr. Loming Chan #0741 *****

Tpr. Robert Noonan #3327

Tpr. Jose Cuevas #3237

Tpr. Carly Rose #3347

Tpr. Robert Soldani #3879

Tpr. Daniel Nunes #3674 *****

Tpr. Erin McLaughlin #3655

Tpr. Kevin Flynn #3791

Tpr. Christopher Andrade #3738 *****

Tpr. Martin Concannon #3409

Tpr. Shawn Murphy #3481

Tpr. Joshua Rucho #3704

Tpr. Nicholas Pellegrino #3684

Tpr. Shawn LeBlanc #3015

Tpr. Steven Grasso #3803

Tpr. Julio Barbosa #4074

***** Indicates that there is already account created.

I will send a separate email with user guide / link to download software.

Logon will be [redacted]

Initial password will be [redacted]

They can change it after initial login.

If you can designate a single POC to address any issues, that would be greatly appreciated.

Lt's and Sgt's have advanced access. Tprs. have basic access.

Please let me know if you need any further assistance.

Respectfully,

David M. Gallagher

Major, Massachusetts State Police

Special Operations

508-820-2162

David.Gallagher3@MassMail.state.ma.us

From: Babbin, Timothy (AGO)
To: Gallagher, David (POL)
Subject: RE: ALPR Accounts
Date: Tuesday, August 18, 2020 11:04:30 AM

Thank you, Sir.
Can you resend that password info?
We had an IT issue here and I saw it briefly but it is no longer in my email.

Tim

From: Gallagher, David (POL) <david.gallagher3@MassMail.State.MA.US>
Sent: Tuesday, August 18, 2020 10:30 AM
To: Babbin, Timothy (AGO) <Timothy.G.Babbin@mass.gov>
Subject: Re: ALPR Accounts

I'll take care of that. I'll send you an updated password shortly.

David M. Gallagher

Major, Massachusetts State Police

Special Operations

508-820-2162

David.Gallagher3@MassMail.state.ma.us

From: Babbin, Timothy (AGO) <Timothy.G.Babbin@mass.gov>
Sent: Tuesday, August 18, 2020 10:03 AM
To: Gallagher, David (POL) <david.gallagher3@MassMail.State.MA.US>
Subject: RE: ALPR Accounts

Major-

Thank you for the prompt assistance with the ALPR.

Could you advise me who would handle password resets?

I had the ALPR when I was down at Plainville but have not had access since.

What (I thought) was my then password no longer works.

Thanks,

Tim

From: Gallagher, David (POL) <david.gallagher3@MassMail.State.MA.US>
Sent: Monday, August 17, 2020 7:44 PM
To: Babbin, Timothy (AGO) <Timothy.G.Babbin@mass.gov>
Subject: ALPR Accounts

DLT Babbin,

Sgt. Tirella reached out and requested I set up ALPR accounts for the following:

DLT Timothy Babbin #2120 *****

Lt. Michael Ahern #2486

Lt. Walter Foley #3110

Lt. Steven Connolly #2719 *****

Lt. Joseph Ross #2264

Lt. Michelle Sutherland #2466

Sgt. Michael Leo #2887

Sgt. Maura McCarthy #2759

Sgt. Patrick Johnson #3128

Sgt. Matthew Hannigan #3281

Sgt. Thomas Mahon #3146

Tpr. John MacDonald #3143

Tpr. Loming Chan #0741 *****

Tpr. Robert Noonan #3327

Tpr. Jose Cuevas #3237

Tpr. Carly Rose #3347

Tpr. Robert Soldani #3879

Tpr. Daniel Nunes #3674 *****

Tpr. Erin McLaughlin #3655

Tpr. Kevin Flynn #3791

Tpr. Christopher Andrade #3738 *****

Tpr. Martin Concannon #3409

Tpr. Shawn Murphy #3481

Tpr. Joshua Rucho #3704

Tpr. Nicholas Pellegrino #3684

Tpr. Shawn LeBlanc #3015

Tpr. Steven Grasso #3803

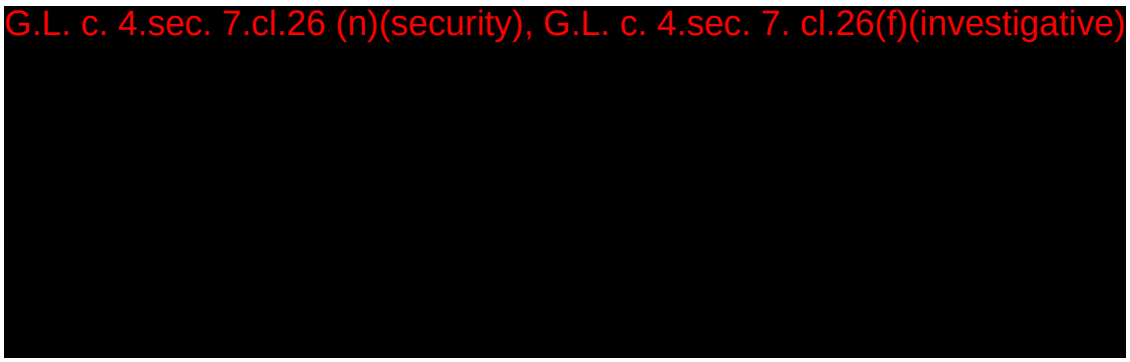
Tpr. Julio Barbosa #4074

***** Indicates that there is already account created.

I will

Logo

Initial



They can change it after initial login.

If you can designate a single POC to address any issues, that would be greatly appreciated.

Lt's and Sgt's have advanced access. Tprs. have basic access.

Please let me know if you need any further assistance.

Respectfully,

David M. Gallagher

Major, Massachusetts State Police

Special Operations

508-820-2162

David.Gallagher3@MassMail.state.ma.us

From: Egnitz, Brian (POL)
To: Peek, Brian T. (EOTSS)
Cc: Guerriero, Robert (EOTSS); Quinn, Dermot (POL); Hughes, Sean M. (EOTSS); Slater, James (CHS); Crouse, David (POL); Michalski, Maria (EPS)
Subject: RE: ALPR Cameras
Date: Thursday, May 14, 2020 10:09:00 AM

Hi Brian,

If possible, G.L. c. 4.sec. 7.cl.26 (n)(security) [redacted] It has recently been brought to our attention that a local Department's covert camera (running [redacted] was discovered and has been targeted by a reddit forum post and by members who appear to be actively looking for covert cameras. Are you available the first week in June for a meeting or should I direct this to someone else in TSS, I realize this would expand the scope.

Agenda could include:

- Overview of our long term goal to consolidate the current video management systems (BOSCH, View Commander, Vigilion, Genetec at the Watch, Genetec in Maynard) into the new Chelsea environment
- ALPR network – how to allow remote management and prepare for the cloud migration
- Covert Camera Network – how we currently handle cameras and could in the future. Can we bring in IPC to manage the TSU network?
- Can we build out one wireless MSP camera network, using sierra modems at the edge, VPN back to Chelsea and scale and store in the new environment.
- [redacted] cutover to the State Fiber (in discussions currently)
- Bandwidth, how much, what's currently in Maynard, what's available
- How we would access Evidence (video on disc)
- VMS networking limitations

Please let me know, Thanks Brian

Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
Phone: 978-451-3710 (Maynard) 508-988-7302 (GHQ)
Email: Brian.Egnitz@massmail.state.ma.us
Monday - Friday, 8 to 4

CONFIDENTIALITY NOTICE: *The information contained in this email and any attachment is privileged and confidential law enforcement information. If you have received this email in error, please call 978-451-3700 immediately. Thank you.*

From: Egnitz, Brian (POL)
Sent: Wednesday, May 6, 2020 8:52 AM
To: Peek, Brian T. (EOTSS)
Cc: Guerriero, Robert (EOTSS); Quinn, Dermot (POL); Hughes, Sean M. (EOTSS); Slater, James (CHS);

Crouse, David (POL)
Subject: Re: ALPR Cameras

A[G.L. c. 4.sec. 7.cl.26 (n)(security)] but would need support growth for [G.L. c. 4.sec. 7.cl.26 (n)(security)] next 2-3 years.

On May 6, 2020, at 8:42 AM, Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov> wrote:

Brian,

[G.L. c. 4.sec. 7.cl.26 (n)(security)] be looking to add to the network?

thanks
bp

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Tuesday, May 5, 2020 3:11 PM
To: Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>
Cc: Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>; Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Hughes, Sean M. (EOTSS) <sean.hughes@mass.gov>; Slater, James (CHS) <james.slater@mass.gov>; Crouse, David (POL) <david.crouse@pol.state.ma.us>
Subject: RE: ALPR Cameras

Hi Brian,

I will be cutting over MassPort cameras tomorrow. We have the MassPort modems, I've updated the firmware and double checked connectivity back to the BOSS server from the MassPort SIMS and there is no firewall work needed. For your records, I've included the details below of the modems and IPs/Accounts.

If possible, I would like to review with you or a member of the TSS network Team using the same solution now in place for the new DHS Livescans. We feel this is a good solution for all the MSP LPRS and it would allow us both the remote management needed for the project. If there are no objection, I can reach out to IPC for a quote, but I would prefer to get on a quick call to discuss. Please advise.

Thanks, Brian

<image001.png>

<image002.png>

<image003.png>
<image004.png>
<image005.png>
<image006.png>

From: Peek, Brian T. (EOTSS)
Sent: Tuesday, May 5, 2020 2:43 PM
To: Egnitz, Brian (POL)
Cc: Guerriero, Robert (EOTSS); Quinn, Dermot (POL); Hughes, Sean M. (EOTSS); Slater, James (CHS); Crouse, David (POL)
Subject: Re: ALPR Cameras

Hi Brian,

I just wanted to confirm that you are not waiting on us for anything? There are no network changes requested correct?

thanks
bp

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, April 17, 2020 10:51 AM
To: Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>
Cc: Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>; Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Hughes, Sean M. (EOTSS) <sean.hughes@mass.gov>; Slater, James (CHS) <james.slater@mass.gov>; Crouse, David (POL) <david.crouse@pol.state.ma.us>
Subject: Re: ALPR Cameras

You are the correct, the current plan is VZW, no network changes required. This is a new request to review if the below would be a better solution long term for ALPR.

On Apr 17, 2020, at 9:22 AM, Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov> wrote:

> Hi Brian,
>
> Is this different from the initial request? If I remember correctly the traffic was going to flow over the VZW network and no FW or Network configurations would need to be changed.
>
> Thanks
> Brian

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, April 17, 2020 6:56 AM
To: Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Hughes, Sean M. (EOTSS) <sean.hughes@mass.gov>; Slater, James (CHS) <james.slater@mass.gov>; Crouse, David (POL) <david.crouse@pol.state.ma.us>; Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>
Subject: ALPR Cameras

Hi Rob,

As you are probably aware the MassPort project to migrate their ALPR Cameras over to the MSP is moving forward over Verizon Wireless. We have identified modems, data plans and purchased the accessories needed for the project and hope to begin cutting over in the next 2-3 weeks.

I wanted to run something by you and the team to review; we just completed the Sierra MP70 VPN project with IPC and it went well (thanks for your teams help - BTW). Do you want to use the same approach (OneNetwork) for these ALPRS? I think it would give us the same functionality originally discussed by pushing the traffic over MassPorts network back to the core, but we would run it over Verizon.

A couple of thoughts;

This could be a good long term approach for all ALPRs we are hosting, we've begun to standardized on MP70s
This could give us much needed remote access to the cameras
If we moved to the Neology Hosted solution, we could do a split tunnel and pipe the traffic straight over the internet, but only allow remote management via the tunnel.
IPC was the prime on the sierra project and work would be minimal to expand, we also want to begin leveraging them more for our other wire/ covert/camera networks we run down the road (when Jim decides to retire).
If MassPort wants us off Verizon (since they are paying for the data plans), they could get us a straight internet route and connect to the MP70 (Our MP70 establishes internet via a LAN Port, Wifi and Cell, all establishing the VPN tunnel after connection).

Let me know what you think and if you want to get on a call to discuss. Otherwise, we can just get MassPort done with the normal static plan.

Thanks, Brian

Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
Phone: 978-451-3710 (Maynard) 508-988-7302 (GHQ)
Email: Brian.Egnitz@massmail.state.ma.us
Monday - Friday, 8 to 4

CONFIDENTIALITY NOTICE: *The information contained in this email and any attachment is privileged and confidential law enforcement information. If you have received this email in error, please call 978-451-3700 immediately. Thank you.*

From: brian.egnitz@pol.state.ma.us
To: Peek, Brian T. (EOTSS)
Cc: Guerriero, Robert (EOTSS); Quinn, Dermot (POL); Hughes, Sean M. (EOTSS); Slater, James (CHS); Crouse, David (POL)
Subject: Re: ALPR Cameras
Date: Wednesday, May 6, 2020 8:48:26 AM

Approximately

> On May 6, 2020, at 8:42 AM, Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov> wrote:
>
> Brian,
>
> How many MP70's would you be looking to add to the network?
>
> thanks
> bp
>
> ---
>
> **From:** Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Sent:** Tuesday, May 5, 2020 3:11 PM
> **To:** Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>
> **Cc:** Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>; Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Hughes, Sean M. (EOTSS) <sean.hughes@mass.gov>; Slater, James (CHS) <james.slater@mass.gov>; Crouse, David (POL) <david.crouse@pol.state.ma.us>
> **Subject:** RE: ALPR Cameras
>
> Hi Brian,
>
> I will be cutting over MassPort cameras tomorrow. We have the MassPort modems, I've updated the firmware and double checked connectivity back to the BOSS server from the MassPort SIMS and there is no firewall work needed. For your records, I've included the details below of the modems and IPs/Accounts.
>
> If possible, I would like to review with you or a member of the TSS network Team using the same solution now in place for the new DHS Livescans. We feel this is a good solution for all the MSP LPRS and it would allow us both the remote management needed for the project. If there are no objection, I can reach out to IPC for a quote, but I would prefer to get on a quick call to discuss. Please advise.
>
> Thanks, Brian

<image001.png>

<image002.png>

<image003.png>
<image004.png>
<image005.png>
<image006.png>

From: Peek, Brian T. (EOTSS)
Sent: Tuesday, May 5, 2020 2:43 PM
To: Egnitz, Brian (POL)
Cc: Guerriero, Robert (EOTSS); Quinn, Dermot (POL); Hughes, Sean M. (EOTSS); Slater, James (CHS); Crouse, David (POL)
Subject: Re: ALPR Cameras

Hi Brian,

I just wanted to confirm that you are not waiting on us for anything? There are no network changes requested correct?

thanks
bp

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, April 17, 2020 10:51 AM
To: Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>
Cc: Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>; Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Hughes, Sean M. (EOTSS) <sean.hughes@mass.gov>; Slater, James (CHS) <james.slater@mass.gov>; Crouse, David (POL) <david.crouse@pol.state.ma.us>
Subject: Re: ALPR Cameras

You are the correct, the current plan is VZW, no network changes required. This is a new request to review if the below would be a better solution long term for ALPR.

On Apr 17, 2020, at 9:22 AM, Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov> wrote:

> Hi Brian,
>
> Is this different from the initial request? If I remember correctly the traffic was going to flow over the VZW network and no FW or Network configurations would need to be changed.

Thanks
Brian

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, April 17, 2020 6:56 AM
To: Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Hughes, Sean M. (EOTSS) <sean.hughes@mass.gov>; Slater, James (CHS) <james.slater@mass.gov>; Crouse, David (POL) <david.crouse@pol.state.ma.us>; Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>
Subject: ALPR Cameras

Hi Rob,

As you are probably aware the MassPort project to migrate their ALPR Cameras over to the MSP is moving forward over Verizon Wireless. We have identified modems, data plans and purchased the accessories needed for the project and hope to begin cutting over in the next 2-3 weeks.

I wanted to run something by you and the team to review; we just completed the Sierra MP70 VPN project with IPC and it went well (thanks for your teams help - BTW). Do you want to use the same approach (OneNetwork) for these ALPRS? I think it would give us the same functionality originally discussed by pushing the traffic over MassPorts network back to the core, but we would run it over Verizon.

A couple of thoughts;

This could be a good long term approach for all ALPRs we are hosting, we've begun to standardized on MP70s
This could give us much needed remote access to the cameras
If we moved to the Neology Hosted solution, we could do a split tunnel and pipe the traffic straight over the internet, but only allow remote management via the tunnel.
IPC was the prime on the sierra project and work would be minimal to expand, we also want to begin leveraging them more for our other wire/ covert/camera networks we run down the road (when Jim decides to retire).
If MassPort wants us off Verizon (since they are paying for the data plans), they could get us a straight internet route and connect to the MP70 (Our MP70 establishes internet via a LAN Port, Wifi and Cell, all establishing the VPN tunnel after connection).

Let me know what you think and if you want to get on a call to discuss. Otherwise, we can just get MassPort done with the normal static plan.

Thanks, Brian

Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
Phone: 978-451-3710 (Maynard) 508-988-7302 (GHQ)
Email: Brian.Egnitz@massmail.state.ma.us
Monday - Friday, 8 to 4

CONFIDENTIALITY NOTICE: *The information contained in this email and any attachment is privileged and confidential law enforcement information. If you have received this email in error, please call 978-451-3700 immediately. Thank you.*

From: Peek, Brian T. (EOTSS)
To: Egnitz, Brian (POL)
Cc: Guerriero, Robert (EOTSS); Quinn, Dermot (POL); Hughes, Sean M. (EOTSS); Slater, James (CHS); Crouse, David (POL)
Subject: Re: ALPR Cameras
Date: Tuesday, May 5, 2020 2:42:32 PM

Hi Brian,

I just wanted to confirm that you are not waiting on us for anything? There are no network changes requested correct?

thanks
bp

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, April 17, 2020 10:51 AM
To: Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>
Cc: Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>; Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Hughes, Sean M. (EOTSS) <sean.hughes@mass.gov>; Slater, James (CHS) <james.slater@mass.gov>; Crouse, David (POL) <david.crouse@pol.state.ma.us>
Subject: Re: ALPR Cameras

You are the correct, the current plan is VZW, no network changes required. This is a new request to review if the below would be a better solution long term for ALPR.

> On Apr 17, 2020, at 9:22 AM, Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov> wrote:
>
> Hi Brian,
>
> Is this different from the initial request? If I remember correctly the traffic was going to flow over the VZW network and no FW or Network configurations would need to be changed.
>
> Thanks
> Brian
>
> ---
>
> **From:** Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Sent:** Friday, April 17, 2020 6:56 AM
> **To:** Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>
> **Cc:** Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Hughes, Sean M. (EOTSS) <sean.hughes@mass.gov>; Slater, James (CHS) <james.slater@mass.gov>; Crouse, David (POL) <david.crouse@pol.state.ma.us>; Peek, Brian T. (EOTSS)

<Brian.T.Peek@mass.gov>
Subject: ALPR Cameras

Hi Rob,

As you are probably aware the MassPort project to migrate their ALPR Cameras over to the MSP is moving forward over Verizon Wireless. We have identified modems, data plans and purchased the accessories needed for the project and hope to begin cutting over in the next 2-3 weeks.

I wanted to run something by you and the team to review; we just completed the Sierra MP70 VPN project with IPC and it went well (thanks for your teams help - BTW). Do you want to use the same approach (OneNetwork) for these ALPRS? I think it would give us the same functionality originally discussed by pushing the traffic over MassPorts network back to the core, but we would run it over Verizon.

A couple of thoughts;

This could be a good long term approach for all ALPRs we are hosting, we've begun to standardized on MP70s
This could give us much needed remote access to the cameras
If we moved to the Neology Hosted solution, we could do a split tunnel and pipe the traffic straight over the internet, but only allow remote management via the tunnel.
IPC was the prime on the sierra project and work would be minimal to expand, we also want to begin leveraging them more for our other wire/ covert/camera networks we run down the road (when Jim decides to retire).
If MassPort wants us off Verizon (since they are paying for the data plans), they could get us a straight internet route and connect to the MP70 (Our MP70 establishes internet via a LAN Port, Wifi and Cell, all establishing the VPN tunnel after connection).

Let me know what you think and if you want to get on a call to discuss. Otherwise, we can just get MassPort done with the normal static plan.

Thanks, Brian

Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
Phone: 978-451-3710 (Maynard) 508-988-7302 (GHQ)
Email: Brian.Egnitz@massmail.state.ma.us
Monday - Friday, 8 to 4

CONFIDENTIALITY NOTICE: *The information contained in this email and any attachment is privileged and confidential law enforcement information. If you have received this email in error, please call 978-451-3700 immediately. Thank you.*

From: Egnitz, Brian (POL)
To: Peek, Brian T. (EOTSS)
Cc: Guerriero, Robert (EOTSS); Quinn, Dermot (POL); Hughes, Sean M. (EOTSS); Slater, James (CHS); Crouse, David (POL)
Subject: Re: ALPR Cameras
Date: Friday, April 17, 2020 10:51:10 AM

You are the correct, the current plan is VZW, no network changes required. This is a new request to review if the below would be a better solution long term for ALPR.

> On Apr 17, 2020, at 9:22 AM, Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov> wrote:
>
> Hi Brian,
>
> Is this different from the initial request? If I remember correctly the traffic was going to flow over the VZW network and no FW or Network configurations would need to be changed.
>
> Thanks
> Brian
>
> ---
>
> **From:** Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Sent:** Friday, April 17, 2020 6:56 AM
> **To:** Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>
> **Cc:** Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Hughes, Sean M. (EOTSS) <sean.hughes@mass.gov>; Slater, James (CHS) <james.slater@mass.gov>; Crouse, David (POL) <david.crouse@pol.state.ma.us>; Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>
> **Subject:** ALPR Cameras
>
> Hi Rob,
>
> As you are probably aware the MassPort project to migrate their ALPR Cameras over to the MSP is moving forward over Verizon Wireless. We have identified modems, data plans and purchased the accessories needed for the project and hope to begin cutting over in the next 2-3 weeks.
>
> I wanted to run something by you and the team to review; we just completed the Sierra MP70 VPN project with IPC and it went well (thanks for your teams help - BTW). Do you want to use the same approach (OneNetwork) for these ALPRS? I think it would give us the same functionality originally discussed by pushing the traffic over MassPorts network back to the core, but we would run it over Verizon.

A couple of thoughts;

This could be a good long term approach for all ALPRs we are hosting, we've begun to standardized on MP70s
This could give us much needed remote access to the cameras
If we moved to the Neology Hosted solution, we could do a split tunnel and pipe the traffic straight over the internet, but only allow remote management via the tunnel.
IPC was the prime on the sierra project and work would be minimal to expand, we also want to begin leveraging them more for our other wire/ covert/camera networks we run down the road (when Jim decides to retire).
If MassPort wants us off Verizon (since they are paying for the data plans), they could get us a straight internet route and connect to the MP70 (Our MP70 establishes internet via a LAN Port, Wifi and Cell, all establishing the VPN tunnel after connection).

Let me know what you think and if you want to get on a call to discuss. Otherwise, we can just get MassPort done with the normal static plan.

Thanks, Brian

Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
Phone: 978-451-3710 (Maynard) 508-988-7302 (GHQ)
Email: Brian.Egnitz@massmail.state.ma.us
Monday - Friday, 8 to 4

CONFIDENTIALITY NOTICE: *The information contained in this email and any attachment is privileged and confidential law enforcement information. If you have received this email in error, please call 978-451-3700 immediately. Thank you.*

From: brian.egnitz@pol.state.ma.us
To: Peek, Brian T. (EOTSS)
Cc: Guerriero, Robert (EOTSS); Quinn, Dermot (POL); Hughes, Sean M. (EOTSS); Slater, James (CHS); Crouse, David (POL)
Subject: Re: ALPR Cameras
Date: Friday, April 17, 2020 10:51:09 AM

You are the correct, the current plan is VZW, no network changes required. This is a new request to review if the below would be a better solution long term for ALPR.

> On Apr 17, 2020, at 9:22 AM, Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov> wrote:
>
> Hi Brian,
>
> Is this different from the initial request? If I remember correctly the traffic was going to flow over the VZW network and no FW or Network configurations would need to be changed.
>
> Thanks
> Brian
>
> ---
>
> **From:** Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Sent:** Friday, April 17, 2020 6:56 AM
> **To:** Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>
> **Cc:** Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Hughes, Sean M. (EOTSS) <sean.hughes@mass.gov>; Slater, James (CHS) <james.slater@mass.gov>; Crouse, David (POL) <david.crouse@pol.state.ma.us>; Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>
> **Subject:** ALPR Cameras
>
> Hi Rob,
>
> As you are probably aware the MassPort project to migrate their ALPR Cameras over to the MSP is moving forward over Verizon Wireless. We have identified modems, data plans and purchased the accessories needed for the project and hope to begin cutting over in the next 2-3 weeks.
>
> I wanted to run something by you and the team to review; we just completed the Sierra MP70 VPN project with IPC and it went well (thanks for your teams help - BTW). Do you want to use the same approach (OneNetwork) for these ALPRS? I think it would give us the same functionality originally discussed by pushing the traffic over MassPorts network back to the core, but we would run it over Verizon.

A couple of thoughts;

This could be a good long term approach for all ALPRs we are hosting, we've begun to standardized on MP70s
This could give us much needed remote access to the cameras
If we moved to the Neology Hosted solution, we could do a split tunnel and pipe the traffic straight over the internet, but only allow remote management via the tunnel.
IPC was the prime on the sierra project and work would be minimal to expand, we also want to begin leveraging them more for our other wire/ covert/camera networks we run down the road (when Jim decides to retire).
If MassPort wants us off Verizon (since they are paying for the data plans), they could get us a straight internet route and connect to the MP70 (Our MP70 establishes internet via a LAN Port, Wifi and Cell, all establishing the VPN tunnel after connection).

Let me know what you think and if you want to get on a call to discuss. Otherwise, we can just get MassPort done with the normal static plan.

Thanks, Brian

Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
Phone: 978-451-3710 (Maynard) 508-988-7302 (GHQ)
Email: Brian.Egnitz@massmail.state.ma.us
Monday - Friday, 8 to 4

CONFIDENTIALITY NOTICE: *The information contained in this email and any attachment is privileged and confidential law enforcement information. If you have received this email in error, please call 978-451-3700 immediately. Thank you.*

From: brian.egnitz@pol.state.ma.us
To: Peek, Brian T. (EOTSS)
Cc: Guerriero, Robert (EOTSS); Quinn, Dermot (POL); Hughes, Sean M. (EOTSS); Slater, James (CHS); Crouse, David (POL)
Subject: Re: ALPR Cameras
Date: Friday, April 17, 2020 10:43:14 AM

You are the correct

> On Apr 17, 2020, at 9:22 AM, Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov> wrote:
>
> Hi Brian,
>
> Is this different from the initial request? If I remember correctly the traffic was going to flow over the VZW network and no FW or Network configurations would need to be changed.
>
> Thanks
> Brian
>
> ---
>
> **From:** Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Sent:** Friday, April 17, 2020 6:56 AM
> **To:** Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>
> **Cc:** Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Hughes, Sean M. (EOTSS) <sean.hughes@mass.gov>; Slater, James (CHS) <james.slater@mass.gov>; Crouse, David (POL) <david.crouse@pol.state.ma.us>; Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>
> **Subject:** ALPR Cameras
>
> Hi Rob,
>
> As you are probably aware the MassPort project to migrate their ALPR Cameras over to the MSP is moving forward over Verizon Wireless. We have identified modems, data plans and purchased the accessories needed for the project and hope to begin cutting over in the next 2-3 weeks.
>
> I wanted to run something by you and the team to review; we just completed the Sierra MP70 VPN project with IPC and it went well (thanks for your teams help - BTW). Do you want to use the same approach (OneNetwork) for these ALPRS? I think it would give us the same functionality originally discussed by pushing the traffic over MassPorts network back to the core, but we would run it over Verizon.
>
> A couple of thoughts;

This could be a good long term approach for all ALPRs we are hosting, we've begun to standardized on MP70s
This could give us much needed remote access to the cameras
If we moved to the Neology Hosted solution, we could do a split tunnel and pipe the traffic straight over the internet, but only allow remote management via the tunnel.
IPC was the prime on the sierra project and work would be minimal to expand, we also want to begin leveraging them more for our other wire/ covert/camera networks we run down the road (when Jim decides to retire).
If MassPort wants us off Verizon (since they are paying for the data plans), they could get us a straight internet route and connect to the MP70 (Our MP70 establishes internet via a LAN Port, Wifi and Cell, all establishing the VPN tunnel after connection).

Let me know what you think and if you want to get on a call to discuss. Otherwise, we can just get MassPort done with the normal static plan.

Thanks, Brian

Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
Phone: 978-451-3710 (Maynard) 508-988-7302 (GHQ)
Email: Brian.Egnitz@massmail.state.ma.us
Monday - Friday, 8 to 4

CONFIDENTIALITY NOTICE: *The information contained in this email and any attachment is privileged and confidential law enforcement information. If you have received this email in error, please call 978-451-3700 immediately. Thank you.*

From: brian.egnitz@pol.state.ma.us
To: Peek, Brian T. (EOTSS)
Cc: Guerriero, Robert (EOTSS); Quinn, Dermot (POL); Hughes, Sean M. (EOTSS); Slater, James (CHS); Crouse, David (POL)
Subject: Re: ALPR Cameras
Date: Friday, April 17, 2020 10:32:29 AM

You are the correct

> On Apr 17, 2020, at 9:22 AM, Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov> wrote:
>
> Hi Brian,
>
> Is this different from the initial request? If I remember correctly the traffic was going to flow over the VZW network and no FW or Network configurations would need to be changed.
>
> Thanks
> Brian
>
> ---
>
> **From:** Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Sent:** Friday, April 17, 2020 6:56 AM
> **To:** Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>
> **Cc:** Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Hughes, Sean M. (EOTSS) <sean.hughes@mass.gov>; Slater, James (CHS) <james.slater@mass.gov>; Crouse, David (POL) <david.crouse@pol.state.ma.us>; Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>
> **Subject:** ALPR Cameras
>
> Hi Rob,
>
> As you are probably aware the MassPort project to migrate their ALPR Cameras over to the MSP is moving forward over Verizon Wireless. We have identified modems, data plans and purchased the accessories needed for the project and hope to begin cutting over in the next 2-3 weeks.
>
> I wanted to run something by you and the team to review; we just completed the Sierra MP70 VPN project with IPC and it went well (thanks for your teams help - BTW). Do you want to use the same approach (OneNetwork) for these ALPRS? I think it would give us the same functionality originally discussed by pushing the traffic over MassPorts network back to the core, but we would run it over Verizon.
>
> A couple of thoughts;

This could be a good long term approach for all ALPRs we are hosting, we've begun to standardized on MP70s
This could give us much needed remote access to the cameras
If we moved to the Neology Hosted solution, we could do a split tunnel and pipe the traffic straight over the internet, but only allow remote management via the tunnel.
IPC was the prime on the sierra project and work would be minimal to expand, we also want to begin leveraging them more for our other wire/ covert/camera networks we run down the road (when Jim decides to retire).
If MassPort wants us off Verizon (since they are paying for the data plans), they could get us a straight internet route and connect to the MP70 (Our MP70 establishes internet via a LAN Port, Wifi and Cell, all establishing the VPN tunnel after connection).

Let me know what you think and if you want to get on a call to discuss. Otherwise, we can just get MassPort done with the normal static plan.

Thanks, Brian

Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
Phone: 978-451-3710 (Maynard) 508-988-7302 (GHQ)
Email: Brian.Egnitz@massmail.state.ma.us
Monday - Friday, 8 to 4

CONFIDENTIALITY NOTICE: *The information contained in this email and any attachment is privileged and confidential law enforcement information. If you have received this email in error, please call 978-451-3700 immediately. Thank you.*

From: brian.egnitz@pol.state.ma.us
To: Peek, Brian T. (EOTSS)
Cc: Guerriero, Robert (EOTSS); Quinn, Dermot (POL); Hughes, Sean M. (EOTSS); Slater, James (CHS); Crouse, David (POL)
Subject: Re: ALPR Cameras
Date: Friday, April 17, 2020 10:30:29 AM

You are the correct

> On Apr 17, 2020, at 9:22 AM, Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov> wrote:
>
> Hi Brian,
>
> Is this different from the initial request? If I remember correctly the traffic was going to flow over the VZW network and no FW or Network configurations would need to be changed.
>
> Thanks
> Brian
>
> ---
>
> **From:** Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Sent:** Friday, April 17, 2020 6:56 AM
> **To:** Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>
> **Cc:** Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Hughes, Sean M. (EOTSS) <sean.hughes@mass.gov>; Slater, James (CHS) <james.slater@mass.gov>; Crouse, David (POL) <david.crouse@pol.state.ma.us>; Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>
> **Subject:** ALPR Cameras
>
> Hi Rob,
>
> As you are probably aware the MassPort project to migrate their ALPR Cameras over to the MSP is moving forward over Verizon Wireless. We have identified modems, data plans and purchased the accessories needed for the project and hope to begin cutting over in the next 2-3 weeks.
>
> I wanted to run something by you and the team to review; we just completed the Sierra MP70 VPN project with IPC and it went well (thanks for your teams help - BTW). Do you want to use the same approach (OneNetwork) for these ALPRS? I think it would give us the same functionality originally discussed by pushing the traffic over MassPorts network back to the core, but we would run it over Verizon.
>
> A couple of thoughts;

This could be a good long term approach for all ALPRs we are hosting, we've begun to standardized on MP70s
This could give us much needed remote access to the cameras
If we moved to the Neology Hosted solution, we could do a split tunnel and pipe the traffic straight over the internet, but only allow remote management via the tunnel.
IPC was the prime on the sierra project and work would be minimal to expand, we also want to begin leveraging them more for our other wire/ covert/camera networks we run down the road (when Jim decides to retire).
If MassPort wants us off Verizon (since they are paying for the data plans), they could get us a straight internet route and connect to the MP70 (Our MP70 establishes internet via a LAN Port, Wifi and Cell, all establishing the VPN tunnel after connection).

Let me know what you think and if you want to get on a call to discuss. Otherwise, we can just get MassPort done with the normal static plan.

Thanks, Brian

Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
Phone: 978-451-3710 (Maynard) 508-988-7302 (GHQ)
Email: Brian.Egnitz@massmail.state.ma.us
Monday - Friday, 8 to 4

CONFIDENTIALITY NOTICE: *The information contained in this email and any attachment is privileged and confidential law enforcement information. If you have received this email in error, please call 978-451-3700 immediately. Thank you.*

From: Peek, Brian T. (EOTSS)
To: Egnitz, Brian (POL); Guerriero, Robert (EOTSS)
Cc: Quinn, Dermot (POL); Hughes, Sean M. (EOTSS); Slater, James (CHS); Crouse, David (POL)
Subject: Re: ALPR Cameras
Date: Friday, April 17, 2020 9:22:32 AM

Hi Brian,

Is this different from the initial request? If I remember correctly the traffic was going to flow over the VZW network and no FW or Network configurations would need to be changed.

Thanks
Brian

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, April 17, 2020 6:56 AM
To: Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Hughes, Sean M. (EOTSS) <sean.hughes@mass.gov>; Slater, James (CHS) <james.slater@mass.gov>; Crouse, David (POL) <david.crouse@pol.state.ma.us>; Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>
Subject: ALPR Cameras

Hi Rob,

As you are probably aware the MassPort project to migrate their ALPR Cameras over to the MSP is moving forward over Verizon Wireless. We have identified modems, data plans and purchased the accessories needed for the project and hope to begin cutting over in the next 2-3 weeks.

I wanted to run something by you and the team to review; we just completed the Sierra MP70 VPN project with IPC and it went well (thanks for your teams help - BTW). Do you want to use the same approach (OneNetwork) for these ALPRS? I think it would give us the same functionality originally discussed by pushing the traffic over MassPorts network back to the core, but we would run it over Verizon.

A couple of thoughts;

This could be a good long term approach for all ALPRs we are hosting, we've begun to standardized on MP70s
This could give us much needed remote access to the cameras
If we moved to the Neology Hosted solution, we could do a split tunnel and pipe the traffic straight over the internet, but only allow remote management via the tunnel.
IPC was the prime on the sierra project and work would be minimal to expand, we also want to begin leveraging them more for our other wire/ covert/camera networks we run down the road (when Jim decides to retire).
If MassPort wants us off Verizon (since they are paying for the data plans), they could get us a straight internet route and connect to the MP70 (Our MP70 establishes internet via a LAN Port, Wifi

and Cell, all establishing the VPN tunnel after connection).

Let me know what you think and if you want to get on a call to discuss. Otherwise, we can just get MassPort done with the normal static plan.

Thanks, Brian

Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
Phone: 978-451-3710 (Maynard) 508-988-7302 (GHQ)
Email: Brian.Egnitz@massmail.state.ma.us
Monday - Friday, 8 to 4

CONFIDENTIALITY NOTICE: *The information contained in this email and any attachment is privileged and confidential law enforcement information. If you have received this email in error, please call 978-451-3700 immediately. Thank you.*

From: Bryant, Michael
To: Griffin, Daniel (POL)
Subject: RE: ALPR Login
Date: Tuesday, February 18, 2020 3:56:42 PM

Afternoon, I never heard from Dan and my info still does not work, any luck on your end?

Thanks

Mike

From: Griffin, Daniel (POL) [mailto:daniel.griffin2@state.ma.us]
Sent: Wednesday, February 12, 2020 5:22 PM
To: Bryant, Michael <MBryant@yarmouth.ma.us>
Subject: Re: ALPR Login

Ok I'll forward it to him. Other option is our watch center.
I may still have access. Let me log in tonight and if I still have access I'll let you know and I'll reset it.

> On Feb 12, 2020, at 4:46 PM, Bryant, Michael <MBryant@yarmouth.ma.us> wrote:
>
> Dan, I tried sending it to david.gallagher@pol.state.ma.us and to david.gallagher@state.ma.us
>
> both e-mails got rejected?
>
> Mike
>
> ---
>
> **From:** Griffin, Daniel (POL) [mailto:daniel.griffin2@state.ma.us]
> **Sent:** Wednesday, February 12, 2020 4:14 PM
> **To:** Bryant, Michael <MBryant@yarmouth.ma.us>
> **Subject:** Re: ALPR Login
>
> Attention! This email originates outside of the organization. Do not open attachments or click links unless you are sure this email is from a known sender and you know the content is safe. Call the sender to verify if unsure. Otherwise delete this email.
>
> ---
>
> Sorry Mike
> I got transferred and no longer working with ALPR.
> CONTACT david.gallagher @pol.state.ma.us He can assist u. Sorry I missed your first

email. My apologies.

On Feb 12, 2020, at 4:03 PM, Bryant, Michael <MBryant@yarmouth.ma.us> wrote:

Lt I am just following up on my e-mail (see below) to see if you have had any time to look at my account.

Thank you,

Mike

From: Bryant, Michael
Sent: Wednesday, January 29, 2020 2:17 PM
To: 'daniel.griffin2@state.ma.us' <daniel.griffin2@state.ma.us>
Subject: RE: ALPR Login

Daniel, Det. Lundegren gave me the info to setup my account, I got as far as the Login screen but the password was rejected 3 times and it looks like it kicked me out?
I used [redacted] G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

Any help would be great.

Thank you

Mike

Lieutenant Michael A. Bryant
Yarmouth Police Department
One Brad Erickson Way
West Yarmouth Ma 02673
508-775-0445 Ext. 2122
Fax 508-775-0409

LAW ENFORCEMENT USE ONLY The document accompanying this email contains information from the Yarmouth Police Department that maybe CONFIDENTIAL and / or PRIVILEGED. The information is intended to be for the use of the individual or entity named on the email. If you are not the intended recipient, be aware that any misuse of this

information is strictly PROHIBITED.

From: Bryant, Michael
To: Griffin, Daniel (POL)
Subject: RE: ALPR Login
Date: Wednesday, February 12, 2020 4:46:18 PM

Dan, I tried sending it to david.gallagher@pol.state.ma.us and to david.gallagher@state.ma.us

both e-mails got rejected?

Mike

From: Griffin, Daniel (POL) [mailto:daniel.griffin2@state.ma.us]
Sent: Wednesday, February 12, 2020 4:14 PM
To: Bryant, Michael <MBryant@yarmouth.ma.us>
Subject: Re: ALPR Login

Attention! This email originates outside of the organization. Do not open attachments or click links unless you are sure this email is from a known sender and you know the content is safe. Call the sender to verify if unsure. Otherwise delete this email.

Sorry Mike
I got transferred and no longer working with ALPR.
CONTACT david.gallagher @pol.state.ma.us He can assist u. Sorry I missed your first email. My apologies.

> On Feb 12, 2020, at 4:03 PM, Bryant, Michael <MBryant@yarmouth.ma.us> wrote:
>
> Lt I am just following up on my e-mail (see below) to see if you have had any time to look at my account.
>
> Thank you,
>
> Mike
>
> **From:** Bryant, Michael
> **Sent:** Wednesday, January 29, 2020 2:17 PM
> **To:** 'daniel.griffin2@state.ma.us' <daniel.griffin2@state.ma.us>
> **Subject:** RE: ALPR Login
>
> Daniel, Det. Lundegren gave me the info to setup my account, I got as far as the Login screen but the password was rejected 3 times and it looks like it kicked me out?

[redacted] G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

Any help would be great.

Thank you

Mike

Lieutenant Michael A. Bryant
Yarmouth Police Department
One Brad Erickson Way
West Yarmouth Ma 02673
508-775-0445 Ext. 2122
Fax 508-775-0409

LAW ENFORCEMENT USE ONLY The document accompanying this email contains information from the Yarmouth Police Department that maybe CONFIDENTIAL and / or PRIVILEGED. The information is intended to be for the use of the individual or entity named on the email. If you are not the intended recipient, be aware that any misuse of this information is strictly PROHIBITED.

From: Bryant, Michael
To: Griffin, Daniel (POL)
Subject: RE: ALPR Login
Date: Wednesday, February 12, 2020 4:33:10 PM

No worries… thanks for the referral

Stay safe

Mike

From: Griffin, Daniel (POL) [mailto:daniel.griffin2@state.ma.us]
Sent: Wednesday, February 12, 2020 4:14 PM
To: Bryant, Michael <MBryant@yarmouth.ma.us>
Subject: Re: ALPR Login

Attention! This email originates outside of the organization. Do not open attachments or click links unless you are sure this email is from a known sender and you know the content is safe. Call the sender to verify if unsure. Otherwise delete this email.

Sorry Mike
I got transferred and no longer working with ALPR.
CONTACT david.gallagher @pol.state.ma.us He can assist u. Sorry I missed your first email. My apologies.

> On Feb 12, 2020, at 4:03 PM, Bryant, Michael <MBryant@yarmouth.ma.us> wrote:
>
> Lt I am just following up on my e-mail (see below) to see if you have had any time to look at my account.
>
> Thank you,
>
> Mike
>
> ---
>
> **From:** Bryant, Michael
> **Sent:** Wednesday, January 29, 2020 2:17 PM
> **To:** 'daniel.griffin2@state.ma.us' <daniel.griffin2@state.ma.us>
> **Subject:** RE: ALPR Login
>
> Daniel, Det. Lundegren gave me the info to setup my account, I got as far as the Login

screen but the password was rejected 3 times and it looks like it kicked me out?
I used [redacted]G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)[redacted].

Any help would be great.

Thank you

Mike

Lieutenant Michael A. Bryant
Yarmouth Police Department
One Brad Erickson Way
West Yarmouth Ma 02673
508-775-0445 Ext. 2122
Fax 508-775-0409

LAW ENFORCEMENT USE ONLY The document accompanying this email contains information from the Yarmouth Police Department that maybe CONFIDENTIAL and / or PRIVILEGED. The information is intended to be for the use of the individual or entity named on the email. If you are not the intended recipient, be aware that any misuse of this information is strictly PROHIBITED.

From: Bryant, Michael
To: Griffin, Daniel (POL)
Subject: RE: ALPR Login
Date: Wednesday, January 29, 2020 2:16:52 PM

Daniel, Det. Lundegren gave me the info to setup my account, I got as far as the Login screen but the password was rejected 3 times and it looks like it kicked me out?
I [redacted G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)].

Any help would be great.

Thank you

Mike

Lieutenant Michael A. Bryant
Yarmouth Police Department
One Brad Erickson Way
West Yarmouth Ma 02673
508-775-0445 Ext. 2122
Fax 508-775-0409

LAW ENFORCEMENT USE ONLY The document accompanying this email contains information from the Yarmouth Police Department that maybe CONFIDENTIAL and / or PRIVILEGED. The information is intended to be for the use of the individual or entity named on the email. If you are not the intended recipient, be aware that any misuse of this information is strictly PROHIBITED.

From: Bryant, Michael
To: Griffin, Daniel (POL)
Subject: RE: ALPR Login
Date: Monday, March 9, 2020 1:15:47 PM

Afternoon Dan,

FYI I have never received anything David and cannot access our system.

Any help would be great.

Thanks

Mike

From: Griffin, Daniel (POL) [mailto:daniel.griffin2@state.ma.us]
Sent: Wednesday, February 12, 2020 5:22 PM
To: Bryant, Michael <MBryant@yarmouth.ma.us>
Subject: Re: ALPR Login

Ok I'll forward it to him. Other option is our watch center.
I may still have access. Let me log in tonight and if I still have access I'll let you know and I'll reset it.

> On Feb 12, 2020, at 4:46 PM, Bryant, Michael <MBryant@yarmouth.ma.us> wrote:
>
> Dan, I tried sending it to david.gallagher@pol.state.ma.us and to david.gallagher@state.ma.us
>
> both e-mails got rejected?
>
> Mike
>
> ---
>
> **From:** Griffin, Daniel (POL) [mailto:daniel.griffin2@state.ma.us]
> **Sent:** Wednesday, February 12, 2020 4:14 PM
> **To:** Bryant, Michael <MBryant@yarmouth.ma.us>
> **Subject:** Re: ALPR Login
>
> Attention! This email originates outside of the organization. Do not open attachments or click links unless you are sure this email is from a known sender and you know the content is safe. Call the sender to verify if unsure. Otherwise delete this email.

Sorry Mike
I got transferred and no longer working with ALPR.
CONTACT david.gallagher @pol.state.ma.us He can assist u. Sorry I missed your first email. My apologies.

On Feb 12, 2020, at 4:03 PM, Bryant, Michael <MBryant@yarmouth.ma.us> wrote:

Lt I am just following up on my e-mail (see below) to see if you have had any time to look at my account.

Thank you,

Mike

From: Bryant, Michael
Sent: Wednesday, January 29, 2020 2:17 PM
To: 'daniel.griffin2@state.ma.us' <daniel.griffin2@state.ma.us>
Subject: RE: ALPR Login

Daniel, Det. Lundegren gave me the info to setup my account, I got as far as the Login screen but the password was rejected 3 times and it looks like it kicked me out?
I G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

Any help would be great.

Thank you

Mike

Lieutenant Michael A. Bryant
Yarmouth Police Department
One Brad Erickson Way
West Yarmouth Ma 02673
508-775-0445 Ext. 2122
Fax 508-775-0409

LAW ENFORCEMENT USE ONLY The document accompanying this email contains information from the Yarmouth Police Department

that maybe CONFIDENTIAL and / or PRIVILEGED. The information is intended to be for the use of the individual or entity named on the email. If you are not the intended recipient, be aware that any misuse of this information is strictly PROHIBITED.

To: Eric Weisz
Subject: RE: ALPR UPDATE
Date: Friday, September 25, 2020 11:37:48 AM

You at Rekford now?

From: Eric Weisz [mailto:eweisz@brekford.com]
Sent: Tuesday, February 26, 2019 12:12 PM
To: Egnitz, Brian (POL)
Subject: RE: ALPR UPDATE

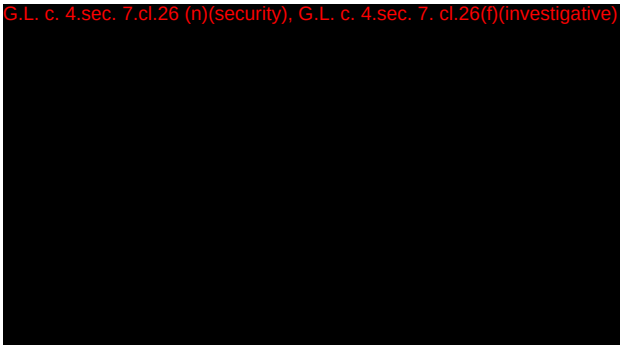
410.972.1987

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Tuesday, February 26, 2019 12:08 PM
To: Eric Weisz <eweisz@brekford.com>
Subject: Re: ALPR UPDATE

What's your phone?

On Feb 7, 2019, at 11:27 PM, Eric Weisz <eweisz@brekford.com> wrote:

> Brian and Dave, sorry for my delay, I'm just getting caught up on emails during my travel.
>
> We have Ryan, our engineer that developed the Finder software (and one that would be able to answer all your technical questions about the other parts of OpenALPR) slated to fly to Boston with Dave from MD with the test unit for you.
>
> If you could set aside a few min on Thursday, I assure you that's all it will take.
>
> Here are instructions for you to access the openalpr backend and all the reads we did.
>
> Attached are a brief explanation for how to do the SFTP hotlist upload and import. Here is the SFTP info for the finder:



> The hotlist format is exactly the same as the manual import. Here is the information about that. This is the same information that was in the original manual.

Hotlists must be formatted as follows:

plate,state,category,message

abc1234,us-md,stolen,stolen car

- *Plate*
  - *Required*
- *State*
  - *Optional*
  - *Must be formatted as country code – state abbreviation ex. us-md us-fl*
- *Category*
  - *Optional*
  - *Will be displayed in the Alert Notification Area. Recommended to use short words like stolen, repossess, amber alert*
  - *If left blank Alert Notification area will just display HOTLIST*
- *Message*
  - *Optional*

Attached as well are some samples.

For the backend here is the information:

Mass State Police -- M19F04

host: https://finderdemo4.brekford.com

user: demo@brekford.com



From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>

Sent: Wednesday, February 06, 2019 6:49 AM
To: Dave Brown <dave.brown@globalpublicsafety.us>
Cc: Eric Weisz <eweisz@brekford.com>
Subject: Re: ALPR UPDATE

No problem, thanks Dave

On Feb 5, 2019, at 4:29 PM, Dave Brown <dave.brown@globalpublicsafety.us> wrote:

> Hi Brian, I want to apologize for the demo yesterday. The unit was tested and trouble shot last night and today it was determined there was nothing wrong. The unit grab plates for the 20-30 minutes we were driving around. Eric has the plate info on the server and can explain how you can access the data.
>
> We were able to determine the issue was with the tablets wifi. The tablet kept trying to connect to the vehicle hotspot and therefore disconnecting from the reader, but the cameras were still recording plates the whole time.
>
> I am getting the unit back and will get it you as soon as I can.
>
> Thank you,
>
> <image001.png>Dave Brown
> Director Mobile Technology
> Global Publc Safety
> 240-904-4307
> Dave.brown@globalpublicsafety.us

<SFTP Hotlist Import.docx>

<frederick-speedtix.csv>

<hotlist.csv>

<Alpr Insrtructions.docx>

From: Tirella, Orlando (AGO)
To: Gallagher, David (POL)
Cc: timothy.babbin@MassMail.State.MA.US
Subject: Re: ALPR
Date: Wednesday, August 12, 2020 3:36:31 PM

Will do.

Thanks,

Sergeant Orlando Tirella #3187
Massachusetts State Police
Office of the Attorney General
One Ashburton Place
Boston, MA 02108
Phone: (617) 963-2190
Fax: (617) 727-5761

> On Aug 12, 2020, at 3:34 PM, Gallagher, David (POL) <david.gallagher3@massmail.state.ma.us> wrote:
>
> Please provide me the name and ID number for each member. I will send the list of the created accounts to DLT Babbin for distribution.
>
> Thank you
>
> Sent from my iPhone
>
> On Aug 12, 2020, at 15:24, Tirella, Orlando (AGO) <Orlando.N.Tirella@mass.gov> wrote:
>
> > Major, I spoke to DLT Babbin and he has approved every member of the AGO-SPDU to have access. I will compile a complete list of names and email addresses for you. If there is any other info you need other than names and email, please let me know.
> >
> > Respectfully,
> > Sgt. Tirella
> >
> > ---
> >
> > **From:** Gallagher, David (POL) <david.gallagher3@MassMail.State.MA.US>
> > **Sent:** Friday, August 7, 2020 1:56 PM
> > **To:** Tirella, Orlando (AGO) <Orlando.N.Tirella@mass.gov>
> > **Subject:** ALPR
> >
> > Sergeant,

MAKE SURE YOU ARE USING INTERNET EXPLORER 11

To download the software cut and paste the following into your browser http://[redacted]9988/publish.htm once loaded you will need to configure the port and perhaps the IP address. Click on the “Boss server” which will open the box below and make sure you have the correct server/port info. Once you connect to the server you won’t have to do it again.

Your login [redacted]

You can change it after you logon.

You have Advanced User status which means you can create hot lists. It also means you can change other information in other users lists so please be careful.

User guide is attached. I'll send you a separate email with some helpful shortcuts.

If there is anyone else in your office that could benefit from having an account, please forward me their information and I'll be happy to set it up.

Please reach out to me with any issues, sometimes the first attempt to login in isn't always successful .

Thank you,

David M. Gallagher

Major, Massachusetts State Police

Special Operations

508-820-2162

David.Gallagher3@MassMail.state.ma.us

From: Staples, Jennifer (POL)
To: Terrey, Susan (EPS); Koulouris, Agapi (CHS); Collins, Kerry (EPS); McGarry, Matthew (CHS); Lord, Spencer (EPS); Mullaney, Arielle (EPS)
Cc: Wark, Jake (EPS)
Subject: Re: ALPR
Date: Monday, December 21, 2020 1:59:08 PM

Looking now and will get back to you shortly. Brian says the following with regard to the shut down cameras:

That is correct. cruiser mounted cameras are not shut down. All fixed are shut down. Central server is off, preventing access to data and submissions of new data. Mobiles could be on, collecting locally but not getting updates (hot files). or submitting data.

From: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>
Sent: Monday, December 21, 2020 1:48 PM
To: Koulouris, Agapi (CHS) <agapi.koulouris@mass.gov>; Collins, Kerry (EPS) <Kerry.Collins@mass.gov>; Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>; McGarry, Matthew (CHS) <Matthew.McGarry@mass.gov>; Lord, Spencer (EPS) <spencer.b.lord@mass.gov>; Mullaney, Arielle (EPS) <Arielle.Mullaney@mass.gov>
Cc: Wark, Jake (EPS) <Jake.Wark@mass.gov>
Subject: RE: ALPR

Thanks Agapi. MSP can you let me know your thoughts when you get a chance

---

From: Koulouris, Agapi (CHS) <agapi.koulouris@mass.gov>
Sent: Monday, December 21, 2020 1:39 PM
To: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>; Collins, Kerry (EPS) <Kerry.Collins@mass.gov>; Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>; McGarry, Matthew (CHS) <Matthew.McGarry@mass.gov>; Lord, Spencer (EPS) <spencer.b.lord@mass.gov>; Mullaney, Arielle (EPS) <Arielle.Mullaney@mass.gov>
Subject: RE: ALPR

Good afternoon,

Attached please find the draft. I made one small change from DCJIS to the Public Safety Data Center to reflect location of the host server.

Thanks,
Agapi

From: Terrey, Susan (EPS) <Susan.W.Terrey@mass.gov>
Sent: Monday, December 21, 2020 12:56 PM
To: Collins, Kerry (EPS) <Kerry.Collins@mass.gov>; Staples, Jennifer (POL) <Jennifer.Staples@pol.state.ma.us>; Koulouris, Agapi (CHS) <agapi.koulouris@mass.gov>; McGarry, Matthew (CHS) <Matthew.McGarry@mass.gov>; Lord, Spencer (EPS) <spencer.b.lord@mass.gov>;

Mullaney, Arielle (EPS) <Arielle.Mullaney@mass.gov>
Subject: ALPR

Guys first run through by Gov's can you confirm my comments and changes. – Also double checking on the cameras that are shut down. Shut down cameras are the ALPR but not cruiser mounted cameras ?

Susan W. Terrey
General Counsel – Executive Office of Public Safety and Security
617-274-5522
G.L. c. 4.sec. 7.cl.26 (n)(security)

From: Powell, Timothy A (DSP)
To: Commonwealth Fusion Center (POL)
Subject: RE: Assistance with missing person for Delaware State Police
Date: Monday, May 4, 2020 12:32:30 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Good afternoon,

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

Thank you,
Det. Timothy Powell #1268
DSP Troop 4 Major Crimes
23652 Shortly Road
Georgetown, DE 19947
Desk- (302)752-3807
Fax- (302) 856-5080

From: Fusion (POL) [mailto:fusion@state.ma.us]
Sent: Monday, May 4, 2020 12:13 PM
To: Powell, Timothy A (DSP) <Timothy.Powell@delaware.gov>
Subject: Re: Assistance with missing person for Delaware State Police

Good Afternoon, Detective -

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

Respectfully,

Sean Bender
Intelligence Analyst

Massachusetts State Police | Commonwealth Fusion Center
470 Worcester Road | Framingham, MA 01702
Phone: (508) 820-2233

CONFIDENTIALITY NOTICE: The information contained in this email and any attachment is privileged and confidential law enforcement information. If you are not the intended recipient, you are hereby notified that any disclosure, dissemination, or copying of this communication is strictly prohibited. If you have received this email in error, please call (978) 451-3700 immediately.

From: Powell, Timothy A (DSP) <Timothy.Powell@delaware.gov>
Sent: Monday, May 4, 2020 11:39 AM
To: Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>
Subject: Assistance with missing person for Delaware State Police

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

[redacted]

-

Thank you,
Det. Timothy Powell #1268
DSP Troop 4 Major Crimes
23652 Shortly Road
Georgetown, DE 19947
Desk- (302)752-3807
Fax- (302) 856-5080

From: Egnitz, Brian (POL)
To: John Tedona; Peter Crary
Subject: RE: BOSS4 MSP Demo Instance
Date: Monday, June 29, 2020 8:19:00 AM

I can do tomorrow afternoon, around 2ish

From: John Tedona [mailto:jtedona@neology.net]
Sent: Wednesday, June 24, 2020 11:51 AM
To: Peter Crary; Egnitz, Brian (POL)
Subject: RE: BOSS4 MSP Demo Instance

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Brian. Does sometime today work for you?

John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: Peter Crary <pcrary@neology.net>
Sent: Tuesday, June 23, 2020 1:03 PM
To: John Tedona <jtedona@neology.net>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: BOSS4 MSP Demo Instance

Can we do this at or after 2pm tomorrow EDT?

-Peter Crary
Global R&D Director, ANPR/ALPR
(865) 386-3821 (m)

The information contained in this communication is confidential and intended only for the use of the recipient named and may also be legally privileged. If you are not the intended recipient (named addressee), you are hereby notified that any dissemination, distribution, copying or making use of this communication, or any of its contents, is strictly prohibited. Please notify the sender immediately by email and delete the original message and any copy of it from your computer system. The integrity, security of and absence of viruses in this message cannot be guaranteed on the internet. The sender therefore does not accept liability for any errors or omissions in the contents of this message, nor any damage caused, which arise as a result of e-mail transmission.

From: John Tedona <jtedona@neology.net>
Sent: Tuesday, 23 June, 2020 09:52
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Peter Crary <pcrary@neology.net>
Subject: Re: BOSS4 MSP Demo Instance

Now until 2pm est today or anytime tomorrow works for me.

Thank You

John Tedona
PIPS Technology
Mobile (201) 841-6237

On Jun 23, 2020, at 10:49 AM, Egnitz, Brian (POL) <brian.egnitz@state.ma.us> wrote:

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

We were looking at this week, let me know what works

From: John Tedona [mailto:jtedona@neology.net]
Sent: Tuesday, June 23, 2020 10:26 AM
To: Peter Crary
Cc: Egnitz, Brian (POL)
Subject: Re: BOSS4 MSP Demo Instance

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Guys, did I miss the conference call or did it not take place?

Thank You

John Tedona
PIPS Technology
Mobile (201) 841-6237

On Jun 16, 2020, at 5:51 PM, Peter Crary <pcrary@neology.net> wrote:

Anytime after 1400 EDT, ideal would be 1530 EDT.

-Peter Crary
Global R&D Director, ANPR/ALPR
(865) 386-3821 (m)

The information contained in this communication is confidential and intended only for the use of the recipient named and may also be legally privileged. If you are not the intended recipient (named addressee), you are hereby notified that any dissemination, distribution, copying or making use of this communication, or any of its contents, is strictly prohibited. Please notify the sender immediately by email and delete the original message and any copy of it from your computer system. The integrity, security of and absence of viruses in this message cannot be guaranteed on the internet. The sender therefore does not accept liability for any errors or omissions in the contents of this message, nor any damage caused, which arise as a result of e-mail transmission.

From: John Tedona <jtedona@neology.net>
Sent: Tuesday, 16 June, 2020 16:00
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Peter Crary <pcrary@neology.net>
Subject: RE: BOSS4 MSP Demo Instance

Anytime tomorrow works for me.

John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Tuesday, June 16, 2020 4:48 PM
To: Peter Crary <pcrary@neology.net>
Cc: John Tedona <jtedona@neology.net>
Subject: Re: BOSS4 MSP Demo Instance

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Absolutely, sometimes direct is just better let's get on a call and go over it. There's a lot of good stuff in there too, I think the result preview and the theme looked really good.

On Jun 16, 2020, at 4:32 PM, Peter Crary <pcrary@neology.net> wrote:

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Hey Brian,

Thanks for the input. I appreciate the honesty and want to see if you have time to review with John and I further. It's important to me that I hear it from you so I can relay those concerns to the team. Let me know when you'd be available this week or next.

Peter Crary
Global R&D Director, ALPR
PIPS Technology
(Sent from my iPhone)

On Jun 16, 2020, at 14:31, Egnitz, Brian (POL) <brian.egnitz@state.ma.us> wrote:

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize

the sender and know the content is safe.

Few comments;

- I received a number of errors during login, I sent John a few screenshots
- After successfully logging in using Edge, I can't re login using Edge and had to use Chrome
    - When I did login with chrome I had account error popups
- The naming conventions on filters is poor
    - Position should be simply location or address
    - Status, why would this be useful?
    - Hotlist, why would this be useful?
    - Users, why would this be useful? To search a device? why wouldn't I just search a device? is this mixing audit functions? If so, why isn't this contextual if it's for audits
    - No one knows or cares about brand name Mantis, this should have a more obvious title for vehicle description search
    - Remote server should not be a filter, if this section is to select reads from sharing sites its not a filter. It would be shown all the time and you would then filter it out, it appears opposite
    - To get the reads from the remote sever, it's not intuitive enough to have to run your search, then select the filter bubbles at the top of the page
        - If these are filters, then all results should be shown first and the filter bubbles would filter it
- The most important part is license plate search and the name is being truncated at the top (and I have a 30" monitor)
- Max export results is 5K, is this configurable, its not enough.
- On the date picker, "set" is unnecessary, should be one click
- When I logged back in using chrome, the page formatting is balled up and I cant search

Overall not impressed.

-----Original Message-----
From: John Tedona [mailto:jtedona@neology.net]
Sent: Friday, June 5, 2020 11:51 AM
To: Egnitz, Brian (POL)
Cc: Peter Crary; Michael Roth; Mark Windover
Subject: BOSS4 MSP Demo Instance

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Brian

A demo BOSS4 instance for MSP has been built and it's ready for use. Below are the details:

URL - https://urldefense.proofpoint.com/v2/url?u=https-3A__nam04.safelinks.protection.outlook.com_-3Furl-3Dhttps-253A-252F-252Fmsp.neology-2Dboss4.net-252Flogin-26amp-3Bdata-3D02-257C01-257Cjtedona-2540neology.net-257C14eb35fdc9344a6ba26208d808b008cc-257C01a7f7dd7222461580f6dddb58e158ef-257C1-257C0-257C637268899444957200-26amp-3Bsdata-3DKYTyQvASC-252FLO6L02XyUQ346y39lPF60MZfV8Qt22GQc-253D-26amp-3Breserved-3D0&d=DwIFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=qliXsWWPbAeXoKtkQsEuh_NAl0l8CIKw7Lu8EtEUU8w&s=JGuGWSXdrT_lW1qqAxMaJBM_qjVyxxXtB-avh1dSuu4&e=

Admin users (user : password)
brian.egnitz : Abcd1234.

VES & Pagis Static Public G.L. c. 4.sec. 7.cl.26 (n)(security)

Exporter & Hotlist Static G.L. c. 4.sec. 7.cl.26 (n)(security)

Since you do not have any cameras connected at this time we're giving you access to a test camera we have located in Nassau County, NY so you can "look" around the software. To access the Nassau County reads: Select READS on the title bar > SEARCH then select the green FILTER icon in the upper left. Select Remote Server on the left side under the Filter column and check the box for Nassau County in the pull down menu.

Give me a call when you access the software so I can give you a high-level run through.

PS -It's best to use CHROME

Regards,

John Tedona

PIPS TECHNOLOGY - A Neology Business
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: John Tedona
To: Peter Crary; Egnitz, Brian (POL)
Subject: RE: BOSS4 MSP Demo Instance
Date: Wednesday, June 24, 2020 11:51:33 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Brian. Does sometime today work for you?

John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: Peter Crary <pcrary@neology.net>
Sent: Tuesday, June 23, 2020 1:03 PM
To: John Tedona <jtedona@neology.net>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: BOSS4 MSP Demo Instance

Can we do this at or after 2pm tomorrow EDT?

-Peter Crary
Global R&D Director, ANPR/ALPR
(865) 386-3821 (m)

The information contained in this communication is confidential and intended only for the use of the recipient named and may also be legally privileged. If you are not the intended recipient (named addressee), you are hereby notified that any dissemination, distribution, copying or making use of this communication, or any of its contents, is strictly prohibited. Please notify the sender immediately by email and delete the original message and any copy of it from your computer system. The integrity, security of and absence of viruses in this message cannot be guaranteed on the internet. The sender therefore does not accept liability for any errors or omissions in the contents of this message, nor any damage caused, which arise as a result of e-mail transmission.

From: John Tedona <jtedona@neology.net>
Sent: Tuesday, 23 June, 2020 09:52
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Peter Crary <pcrary@neology.net>
Subject: Re: BOSS4 MSP Demo Instance

Now until 2pm est today or anytime tomorrow works for me.

Thank You

John Tedona
PIPS Technology
Mobile (201) 841-6237

> On Jun 23, 2020, at 10:49 AM, Egnitz, Brian (POL) <brian.egnitz@state.ma.us> wrote:
>
> **CAUTION:** This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>
> We were looking at this week, let me know what works
>
> ---
>
> **From:** John Tedona [mailto:jtedona@neology.net]
> **Sent:** Tuesday, June 23, 2020 10:26 AM
> **To:** Peter Crary
> **Cc:** Egnitz, Brian (POL)
> **Subject:** Re: BOSS4 MSP Demo Instance
>
> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>
> Guys, did I miss the conference call or did it not take place?
>
> Thank You
>
> John Tedona
> PIPS Technology
> Mobile (201) 841-6237

On Jun 16, 2020, at 5:51 PM, Peter Crary <pcrary@neology.net> wrote:

Anytime after 1400 EDT, ideal would be 1530 EDT.

-Peter Crary
Global R&D Director, ANPR/ALPR
(865) 386-3821 (m)

The information contained in this communication is confidential and intended only for the use of the recipient named and may also be legally privileged. If you are not the intended recipient (named addressee), you are hereby notified that any dissemination, distribution, copying or making use of this communication, or any of its contents, is strictly prohibited. Please notify the sender immediately by email and delete the original message and any copy of it from your computer system. The integrity, security of and absence of viruses in this message cannot be guaranteed on the internet. The sender therefore does not accept liability for any errors or omissions in the contents of this message, nor any damage caused, which arise as a result of e-mail transmission.

From: John Tedona <jtedona@neology.net>
Sent: Tuesday, 16 June, 2020 16:00
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Peter Crary <pcrary@neology.net>
Subject: RE: BOSS4 MSP Demo Instance

Anytime tomorrow works for me.

John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Tuesday, June 16, 2020 4:48 PM
To: Peter Crary <pcrary@neology.net>
Cc: John Tedona <jtedona@neology.net>
Subject: Re: BOSS4 MSP Demo Instance

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Absolutely, sometimes direct is just better let's get on a call and go over it. There's a lot of good stuff in there too, I think the result preview and the theme looked really good.

On Jun 16, 2020, at 4:32 PM, Peter Crary <pcrary@neology.net> wrote:

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Hey Brian,

Thanks for the input. I appreciate the honesty and want to see if you have time to review with John and I further. It's important to me that I hear it from you so I can relay those concerns to the team. Let me know when you'd be available this week or next.

Peter Crary
Global R&D Director, ALPR
PIPS Technology
(Sent from my iPhone)

On Jun 16, 2020, at 14:31, Egnitz, Brian (POL) <brian.egnitz@state.ma.us> wrote:

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Few comments;

- I received a number of errors during login, I sent John a few screenshots
- After successfully logging in using Edge, I can't re login using Edge and had to use Chrome
    - When I did login with chrome I had account error popups

- The naming conventions on filters is poor
    - Position should be simply location or address
    - Status, why would this be useful?
    - Hotlist, why would this be useful?
    - Users, why would this be useful? To search a device? why wouldn't I just search a device? is this mixing audit functions? If so, why isn't this contextual if it's for audits
    - No one knows or cares about brand name Mantis, this should have a more obvious title for vehicle description search
    - Remote server should not be a filter, if this section is to select reads from sharing sites its not a filter. It would be shown all the time and you would then filter it out, it appears opposite
    - To get the reads from the remote sever, it's not intuitive enough to have to run your search, then select the filter bubbles at the top of the page
        - If these are filters, then all results should be shown first and the filter bubbles would filter it
- The most important part is license plate search and the name is being truncated at the top (and I have a 30" monitor)
- Max export results is 5K, is this configurable, its not enough.
- On the date picker, "set" is unnecessary, should be one click
- When I logged back in using chrome, the page formatting is balled up and I cant search

Overall not impressed.

-----Original Message-----
From: John Tedona [mailto:jtedona@neology.net]
Sent: Friday, June 5, 2020 11:51 AM
To: Egnitz, Brian (POL)
Cc: Peter Crary; Michael Roth; Mark Windover
Subject: BOSS4 MSP Demo Instance

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Brian

A demo BOSS4 instance for MSP has been built and it's ready for use. Below are the details:

URL - https://urldefense.proofpoint.com/v2/url?u=https-3A__nam04.safelinks.protection.outlook.com_-3Furl-3Dhttps-253A-252F-252Fmsp.neology-2Dboss4.net-252Flogin-26amp-3Bdata-3D02-257C01-257Cjtedona-2540neology.net-257C14eb35fdc9344a6ba26208d808b008cc-257C01a7f7dd7222461580f6dddb58e158ef-257C1-257C0-257C637268899444957200-26amp-3Bsdata-3DKYTyQvASC-252FLO6L02XyUQ346y39lPF60MZfV8Qt22GQc-253D-26amp-3Breserved-3D0&d=DwIFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxl8vzFMhI&m=qliXsWWPbAeXoKtkQsEuh_NAl0l8CIKw7Lu8EtEUU8w&s=JGuGWSXdrT_lW1qqAxMaJBM_qjVyxxXtB-avh1dSuu4&e=

Admin users (user : password)
brian.egnitz : Abcd1234.

VES & Pagis Static Public IP: 54.147.16.2 VES Port: 10000 Pagis Port: 8092

Exporter & Hotlist Static Public IP : 54.237.29.234

Since you do not have any cameras connected at this time we're giving you access to a test camera we have located in Nassau County, NY so you can "look" around the software. To access the Nassau County reads: Select READS on the title bar > SEARCH then select the green FILTER icon in the upper left. Select Remote Server on the left side under the Filter column and check the box for Nassau County in the pull down menu.

Give me a call when you access the software so I can give you a high-level run through.

PS -It's best to use CHROME

Regards,

John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support

www.pipstechnology.com

From: Peter Crary
To: John Tedona; Egnitz, Brian (POL)
Subject: RE: BOSS4 MSP Demo Instance
Date: Tuesday, June 23, 2020 1:03:29 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Can we do this at or after 2pm tomorrow EDT?

-Peter Crary
Global R&D Director, ANPR/ALPR
(865) 386-3821 (m)

The information contained in this communication is confidential and intended only for the use of the recipient named and may also be legally privileged. If you are not the intended recipient (named addressee), you are hereby notified that any dissemination, distribution, copying or making use of this communication, or any of its contents, is strictly prohibited. Please notify the sender immediately by email and delete the original message and any copy of it from your computer system. The integrity, security of and absence of viruses in this message cannot be guaranteed on the internet. The sender therefore does not accept liability for any errors or omissions in the contents of this message, nor any damage caused, which arise as a result of e-mail transmission.

From: John Tedona <jtedona@neology.net>
Sent: Tuesday, 23 June, 2020 09:52
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Peter Crary <pcrary@neology.net>
Subject: Re: BOSS4 MSP Demo Instance

Now until 2pm est today or anytime tomorrow works for me.

Thank You

John Tedona
PIPS Technology
Mobile (201) 841-6237

On Jun 23, 2020, at 10:49 AM, Egnitz, Brian (POL) <brian.egnitz@state.ma.us> wrote:

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

We were looking at this week, let me know what works

From: John Tedona [mailto:jtedona@neology.net]
Sent: Tuesday, June 23, 2020 10:26 AM
To: Peter Crary
Cc: Egnitz, Brian (POL)
Subject: Re: BOSS4 MSP Demo Instance

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Guys, did I miss the conference call or did it not take place?

Thank You

John Tedona
PIPS Technology
Mobile (201) 841-6237

On Jun 16, 2020, at 5:51 PM, Peter Crary <pcrary@neology.net> wrote:

Anytime after 1400 EDT, ideal would be 1530 EDT.

-Peter Crary
Global R&D Director, ANPR/ALPR
(865) 386-3821 (m)

The information contained in this communication is confidential and intended only for the use of the recipient named and may also be legally privileged. If you are not the intended recipient (named addressee), you are hereby notified that any dissemination, distribution, copying or making use of this communication, or any of its contents, is strictly prohibited. Please notify the sender immediately by email and delete the original message and any copy of it from your computer system. The integrity, security of and absence of viruses in this message cannot be guaranteed on the internet. The sender therefore does not accept liability for any errors or omissions in the contents of this message, nor any damage caused, which arise as a result of e-mail transmission.

From: John Tedona <jtedona@neology.net>
Sent: Tuesday, 16 June, 2020 16:00
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Peter Crary <pcrary@neology.net>
Subject: RE: BOSS4 MSP Demo Instance

Anytime tomorrow works for me.

John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Tuesday, June 16, 2020 4:48 PM
To: Peter Crary <pcrary@neology.net>
Cc: John Tedona <jtedona@neology.net>
Subject: Re: BOSS4 MSP Demo Instance

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Absolutely, sometimes direct is just better let's get on a call and go over it. There's a lot of good stuff in there too, I think the result preview and the theme looked really good.

> On Jun 16, 2020, at 4:32 PM, Peter Crary <pcrary@neology.net> wrote:
>
> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>
> Hey Brian,
>
> Thanks for the input. I appreciate the honesty and want to see if you have time to review with John and I further. It's important to me that I hear it from you so I can relay those concerns to the team. Let me know when you'd be available this week or next.
>
> Peter Crary
> Global R&D Director, ALPR
> PIPS Technology
> (Sent from my iPhone)
>
> > On Jun 16, 2020, at 14:31, Egnitz, Brian (POL) <brian.egnitz@state.ma.us> wrote:
> >
> > **CAUTION:** This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
> >
> > Few comments;
> >
> > - I received a number of errors during login, I sent John a few screenshots
> > - After successfully logging in using Edge, I can't re login using Edge and had to use Chrome
> >   - When I did login with chrome I had account error popups
> > - The naming conventions on filters is poor
> >   - Position should be simply location or address
> >   - Status, why would this be useful?
> >   - Hotlist, why would this be useful?
> >   - Users, why would this be useful? To search a device? why wouldn't I just search a device? is this mixing audit functions? If so, why isn't this contextual if it's for audits
> >   - No one knows or cares about brand name Mantis, this should have a more obvious title for vehicle description search
> >   - Remote server should not be a filter, if this section is to select reads from sharing sites its not a filter. It would be shown all the time and you would then filter it out, it appears opposite
> >   - To get the reads from the remote sever, it's not intuitive enough to have to run your search, then select the filter bubbles at the top of the page
> >   - If these are filters, then all results should be shown first and the filter bubbles would filter it
> > - The most important part is license plate search and the name is being truncated at the top (and I have a 30" monitor)
> > - Max export results is 5K, is this configurable, its not enough.

On the date picker, “set” is unnecessary, should be one click
- When I logged back in using chrome, the page formatting is balled up and I cant search

Overall not impressed.

-----Original Message-----
From: John Tedona [mailto:jtedona@neology.net]
Sent: Friday, June 5, 2020 11:51 AM
To: Egnitz, Brian (POL)
Cc: Peter Crary; Michael Roth; Mark Windover
Subject: BOSS4 MSP Demo Instance

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system.
Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Brian

A demo BOSS4 instance for MSP has been built and it's ready for use. Below are the details:

URL - https://urldefense.proofpoint.com/v2/url?u=https-3A__nam04.safelinks.protection.outlook.com_-3Furl-3Dhttps-253A-252F-252Fmsp.neology-2Dboss4.net-252Flogin-26amp-3Bdata-3D02-257C01-257Cjtedona-2540neology.net-257C14eb35fdc9344a6ba26208d808b008cc-257C01a7f7dd7222461580f6dddb58e158ef-257C1-257C0-257C637268899444957200-26amp-3Bsdata-3DKYTyQvASC-252FLO6L02XyUQ346y39lPF60MZfV8Qt22GQc-253D-26amp-3Breserved-3D0&d=DwIFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=qliXsWWPbAeXoKtkQsEuh_NAl0l8CIKw7Lu8EtEUU8w&s=JGuGWSXdrT_lW1qqAxMaJBM_qjVyxxXtB-avh1dSuu4&e=

Admin users (user : password)
brian.egnitz : Abcd1234.

VES & Pagis Static Public IP: 54.147.16.2 VES Port: 10000 Pagis Port: 8092

Exporter & Hotlist Static Public IP : 54.237.29.234

Since you do not have any cameras connected at this time we're giving you access to a test camera we have located in Nassau County, NY so you can "look" around the software. To access the Nassau County reads: Select READS on the title bar > SEARCH then select the green FILTER icon in the upper left. Select Remote Server on the left side under the Filter column and check the box for Nassau County in the pull down menu.

Give me a call when you access the software so I can give you a high-level run through.

PS -It's best to use CHROME

Regards,

John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: Egnitz, Brian (POL)
To: Peter Crary; John Tedona
Subject: RE: BOSS4 MSP Demo Instance
Date: Tuesday, September 22, 2020 1:35:00 PM

Did the round trip stuff make it into the build?

From: Peter Crary [mailto:pcrary@neology.net]
Sent: Tuesday, June 23, 2020 1:03 PM
To: John Tedona; Egnitz, Brian (POL)
Subject: RE: BOSS4 MSP Demo Instance

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Can we do this at or after 2pm tomorrow EDT?

-Peter Crary
Global R&D Director, ANPR/ALPR
(865) 386-3821 (m)

The information contained in this communication is confidential and intended only for the use of the recipient named and may also be legally privileged. If you are not the intended recipient (named addressee), you are hereby notified that any dissemination, distribution, copying or making use of this communication, or any of its contents, is strictly prohibited. Please notify the sender immediately by email and delete the original message and any copy of it from your computer system. The integrity, security of and absence of viruses in this message cannot be guaranteed on the internet. The sender therefore does not accept liability for any errors or omissions in the contents of this message, nor any damage caused, which arise as a result of e-mail transmission.

From: John Tedona <jtedona@neology.net>
Sent: Tuesday, 23 June, 2020 09:52
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Peter Crary <pcrary@neology.net>
Subject: Re: BOSS4 MSP Demo Instance

Now until 2pm est today or anytime tomorrow works for me.

Thank You

John Tedona
PIPS Technology
Mobile (201) 841-6237

> On Jun 23, 2020, at 10:49 AM, Egnitz, Brian (POL) <brian.egnitz@state.ma.us> wrote:
>
> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>
> We were looking at this week, let me know what works
>
> **From:** John Tedona [mailto:jtedona@neology.net]
> **Sent:** Tuesday, June 23, 2020 10:26 AM
> **To:** Peter Crary
> **Cc:** Egnitz, Brian (POL)
> **Subject:** Re: BOSS4 MSP Demo Instance
>
> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>
> Guys, did I miss the conference call or did it not take place?
>
> Thank You
>
> John Tedona
> PIPS Technology
> Mobile (201) 841-6237
>
> On Jun 16, 2020, at 5:51 PM, Peter Crary <pcrary@neology.net> wrote:
>
> > Anytime after 1400 EDT, ideal would be 1530 EDT.
> >
> > -Peter Crary
> > Global R&D Director, ANPR/ALPR
> > (865) 386-3821 (m)
> >
> > The information contained in this communication is confidential and intended only for the use of the recipient named and may also be legally privileged. If you are not the intended recipient (named addressee), you are hereby notified that any dissemination, distribution, copying or making use of this communication, or any of its contents, is strictly prohibited. Please notify the sender immediately by email and delete the original message and any copy of it from your computer system. The integrity, security of and absence of viruses in this message cannot be guaranteed on the internet. The sender therefore does not accept liability for any errors or omissions in the contents of this message, nor any damage caused, which arise as a result

of e-mail transmission.

From: John Tedona <jtedona@neology.net>
Sent: Tuesday, 16 June, 2020 16:00
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Peter Crary <pcrary@neology.net>
Subject: RE: BOSS4 MSP Demo Instance

Anytime tomorrow works for me.

John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Tuesday, June 16, 2020 4:48 PM
To: Peter Crary <pcrary@neology.net>
Cc: John Tedona <jtedona@neology.net>
Subject: Re: BOSS4 MSP Demo Instance

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Absolutely, sometimes direct is just better let's get on a call and go over it. There's a lot of good stuff in there too, I think the result preview and the theme looked really good.

> On Jun 16, 2020, at 4:32 PM, Peter Crary <pcrary@neology.net> wrote:
>
> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>
> Hey Brian,
>
> Thanks for the input. I appreciate the honesty and want to see if you have time to review with John and I further. It's important to me that I hear it from you so I can relay those concerns to the team. Let me know when you'd be available this week or next.
>
> Peter Crary
> Global R&D Director, ALPR
> PIPS Technology
> (Sent from my iPhone)
>
> > On Jun 16, 2020, at 14:31, Egnitz, Brian (POL) <brian.egnitz@state.ma.us> wrote:
> >
> > **CAUTION:** This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
> >
> > Few comments;
> >
> > - I received a number of errors during login, I sent John a few screenshots
> > - After successfully logging in using Edge, I can't re login using Edge and had to use Chrome
> >   - When I did login with chrome I had account error popups
> > - The naming conventions on filters is poor
> >   - Position should be simply location or address
> >   - Status, why would this be useful?
> >   - Hotlist, why would this be useful?
> >   - Users, why would this be useful? To search a device? why wouldn't I just search a device? is this mixing audit functions? If so, why isn't this contextual if it's for audits
> >   - No one knows or cares about brand name Mantis, this should have a more obvious title for vehicle description search
> >   - Remote server should not be a filter, if this section is to select reads from sharing sites its not a filter. It would be shown all the time and you would then filter it out, it appears opposite
> >   - To get the reads from the remote sever, it's not intuitive enough to have to run your search, then

select the filter bubbles at the top of the page
    - If these are filters, then all results should be shown first and the filter bubbles would filter it
- The most important part is license plate search and the name is being truncated at the top (and I have a 30" monitor)
- Max export results is 5K, is this configurable, its not enough.
- On the date picker, "set" is unnecessary, should be one click
- When I logged back in using chrome, the page formatting is balled up and I cant search

Overall not impressed.

-----Original Message-----
From: John Tedona [mailto:jtedona@neology.net]
Sent: Friday, June 5, 2020 11:51 AM
To: Egnitz, Brian (POL)
Cc: Peter Crary; Michael Roth; Mark Windover
Subject: BOSS4 MSP Demo Instance

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system.
Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Brian

A demo BOSS4 instance for MSP has been built and it's ready for use. Below are the details:

URL - https://urldefense.proofpoint.com/v2/url?u=https-3A__nam04.safelinks.protection.outlook.com_-3Furl-3Dhttps-253A-252F-252Fmsp.neology-2Dboss4.net-252Flogin-26amp-3Bdata-3D02-257C01-257Cjtedona-2540neology.net-257C14eb35fdc9344a6ba26208d808b008cc-257C01a7f7dd7222461580f6dddb58e158ef-257C1-257C0-257C637268899444957200-26amp-3Bsdata-3DKYTyQvASC-252FLO6L02XyUQ346y39lPF60MZfV8Qt22GQc-253D-26amp-3Breserved-3D0&d=DwIFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4lX8nm64tlxI8vzFMhI&m=qliXsWWPbAeXoKtkQsEuh_NAl0l8ClKw7Lu8EtEUU8w&s=JGuGWSXdrT_lW1qqAxMaJBM_qjVyxxXtB-avh1dSuu4&e=

Admin users [redacted]
brian [redacted]

VES & Pagis Static [redacted]

Exporter & Hotlist Static [redacted]

Since you do not have any cameras connected at this time we're giving you access to a test camera we have located in Nassau County, NY so you can "look" around the software. To access the Nassau County reads: Select READS on the title bar > SEARCH then select the green FILTER icon in the upper left. Select Remote Server on the left side under the Filter column and check the box for Nassau County in the pull down menu.

Give me a call when you access the software so I can give you a high-level run through.

PS -It's best to use CHROME

Regards,

John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: steve.abramoski@pol.state.ma.us
To: E-All; D; James Pfeifer
Subject: Re: Case Update - ALPRs on Bourne/Sagamore Bridges not a search
Date: Tuesday, April 21, 2020 9:31:02 PM

Thanks. Good read. Throw my hands up is we have to starting writing for LPR s and Pole Cams in the future.

Trooper Jason P. Abramoski #3528
Massachusetts State Police
DHS - C.I.N.R.E.T
326 W Grove St. Middleboro, MA 02346
508-468-0502

On Apr 21, 2020, at 2:11 PM, Rudolph, James (POL) <James.Rudolph@pol.state.ma.us> wrote:

Case Law update.

Win for the good guys. Defense tried to mirror the Connolly case and suggest a S/W needed to check ALPRs. Court said no. But this could change if a case relied more heavily on ALPR info. Interesting read.

-rudy

RESPECTFULLY
LIEUTENANT JAMES D. RUDOLPH #2786
MASSACHUSETTS STATE POLICE, FRAMINGHAM, MA 01702
508 820-2213
<OUTLOOK-FEXBMUWE.PHD>

From: Grant Marguerite (NFK) <Marguerite.Grant@MassMail.State.MA.US>
Sent: Friday April 17 2020 5:33 PM



Chiefs
Commonwealth v. McCarthy (SJC 12750)€ click on that link to see the case
In this case the SJC ruled that police tracking D's car using 4 automatic license plate readers (ALPRs) at both ends of the Bourne and Sagamore Bridges was too limited to amount to a constitutional "search." The SJC declined to say exactly how detailed digital surveillance would have to be to constitute a search leaving that issue for future cases.

State Police maintain ALPRs including ones at both ends of the Bourne and Sagamore Bridges. (p.3) The ALPRs photograph vehicles' license plates; that data along with the date and time of the sighting is retained by EOPPS for a year. (p.3-4) Authorized users including police may put a license plate number on a "hot list" and receive an alert if that plate is sighted; reasons to put someone on the "hot list" include not only criminal investigations but also Amber alerts missing persons and BOLO alerts. (p. 3 25 n.13)

Through surveillance controlled buys and information from 4 Cis Barnstable police suspected that the co-D was se ling heroin out of his house in Barnstable. (p.4) Police saw a black Hyundai driven by D visit there briefly so they suspected that D was the co-D's supplier. Police put the Hyundai's license plate number on the State Police ALPR "hot list " so that they'd be notified whenever the Hyundai crossed one of the bridges. (p.5) After getting an alert that the Hyundai had crossed onto the Cape police followed both the Hyundai and the co-D to the buy location on a quiet residential street where D and co-D met for about 30 seconds but police could not see a physical exchange. (p.5) From the ALPR data police generated a spreadsheet showing that in mid-winter the Hyundai had crossed the bridges dozens of times sometimes more than once a day adding to police suspicion that D was the heroin supplier. (p.5-6) When police got a second alert that the Hyundai had crossed onto the Cape they again followed D and co-D to the buy location and saw a 30-second meeting but could not see any exchange. This time police stopped both cars handcuffed both co-D and D and read them Miranda. On co-D police found heroin; on D police found 2 cell phones and cash. (p.6-7) At the station police repeatedly told D he was "not under arrest " and D made statements.

D moved to suppress the ALPR data his statements and evidence obtained from the stop. A Superior Court judge found that the moment of arrest was when D and co-D were handcuffed at the scene of the traffic stop but denied the motion to suppress. (p.33) The SJC upheld the denial.

ALPRs and expectation of privacy in digital surveillance At some length the SJC discussed the constitutional issues raised by digital surveillance. (p.7-29) Police conduct amounts to a search if: (1) it intrudes on a D's expectation of privacy and (2) society is willing to recognize the expectation of privacy as reasonable. Here the SJC ruled D did have an expectation of privacy because D and co-D chose a buy location in a quiet residential area. (p.8 n.5) As to what expectation of privacy society recognizes as reasonable with regard to digital surveillance the SJC was guided by historical understandings of what was an unreasonable search and seizure when the U.S. and Mass. Constitutions were adopted in the late 1700s in reaction to redcoats' rummaging without restraint through colonists' homes. (p.8-10) New technologies like ALPRs raise difficult legal issues because they are easier and less expensive for police than traditional surveillance can be done secretly and permit police to search back in time for a vehicle's movements even before po ice suspicion arose. (p.12-14) Society does not recognize as reasonable an expectation of privacy in what someone knowingly exposes" to public view like a license plate – which by statute must be "displayed conspicuously." (p.15-16 & n.8) In older cases involving less advanced technology courts have held that a D did not have an expectation of privacy in contents of a phone conversation in a phone booth or a radio beeper" tracking a single journey. (p14-17) But technology like ALPRs GPS and CSLI are different because they may give police a **mosaic** of information where each piece may be public but when viewed together they create a picture that implicates someone's privacy interests like their political re igious or sexual associations. (p.17-21) The SJC was concerned that with enough ALPRs police could track someone's location everywhere which would be "creepy." (p.25) Exigent circumstances would likely justify using an ALPR in a situation involving an Amber alert or missing person. (p.25 n.13) The D urged the SJC to consider not just these four ALPRs on the Bourne and Sagamore Bridges but the hundreds of ALPRs across Massachusetts; the SJC declined to do so because that evidence is not in the record of this case. (p.26) The **limited number of cameras** here and their placements on the bridges was not enough to give D an expectation of privacy that society would recognize as reasonable. (p.26) The SJC declined to say how much digital surveillance would give such an expectation and admitted that its unwillingness to do so "**may bring some interim confusion**" until further cases develop the law on this issue. (p.28 n.15) Chief Justice Gants wrote a separate concurrence suggesting that one thing the SJC could do is to require police who want to search a vast amount of digital data to apply for a court order supported by an affidavit showing reasonable suspicion to do so. (concurrence p.3) This would be like a SW but with a lower standard than PC.

Written policy The SJC rejected D's argument that Barnstable PD should have had a written policy about ALPRs and the MSP policy on which Barnstable relied was not specific enough. (p.30) Written policies are required to justify certain exceptions to the SW requirement (like inventory searches and sobriety checkpoints) – they do not apply to the threshold question whether a search occurred in the first place. (p.31)

Miranda issues At the station police repeatedly told D that D was "not under arrest." But the motion judge found that the moment of arrest was when police handcuffed D at the traffic stop. (p.32) D argued that his statements should be suppressed because police tel ing him he was not under arrest amounted to "deceit or trickery" to get D to confess. The motion judge and the SJC rejected that argument saying that even if telling D he was not under arrest amounted to deceit or trickery it was just one factor to be used in determining voluntariness.

Bottom line: Police use of ALPRs at limited locations is not a constitutional search – but we don't know how many locations it'd have to be to amount to one. Using an ALPR in **exigent circumstances** like an Amber Alert is likely OK. Local police don't need a written policy to use ALPRs maintained by MSP. After a D has been handcuffed police should not tell D that D is "not under arrest" – po ice will likely be accused later of deceit and trickery.

A thought: There are news stories online that cell phones may be used to do contact tracing for people exposed to COVID-19. If lots of people willingly agree to let their cell phone data be used to track their whereabouts would that ever change courts' view of what society recognizes as a reasonable expectation of privacy? At some point if members of the public come to expect that they're being tracked should police be allowed to use that evidence too? Or at the very least should there be a jury instruction explaining that police have less access to the data than other entities (like software companies or public health agencies)?

As always email me with any questions. Wash your hands!

Marguerite

Marguerite T. Grant
General Counsel – Director of Training
Office of Norfolk District Attorney Michael W. Morrissey
45 Shawmut Road
Canton, MA 02021
781-830-4829

From: Grant, Marguerite (AG)
To: [redacted]
Cc: [redacted]
Subject: Comm v. McCarthy – scoring D's MV with ALPRs on Bourne/Sagamore Bridges not a "search"
Date: Friday, April 24, 2020 12:03:02 PM

https://reason.com/2020/04/22/automated-license-plate-readers-the-mosaic-theory-and-the-fourth-amendment/

Charli – this link is to a really interesting article by a University of California-Berkeley law professor analyzing (and disagreeing with) the SJC's opinion last week about ALPRs. The most interesting part:

> "This is a particularly challenging approach given the likely need for a warrant if a search is later found. *After* the data is collected the appellate courts will then look at the data figure out what it revealed and then say whether a warrant was needed *before* the government tried to collect it.
>
> Think of how it would work with a query into an existing database instead of a real-time query like the one in McCarthy. For example imagine the government wanted to know where McCarthy's car had been for the last 10 days. Maybe that query would reveal 10 hits from two cameras. Or maybe that query would reveal 1 000 hits from 300 cameras. If you're an officer you can't know whether your query wi l reveal a substantial picture of the defendant's public movements' until you know the results at which time you can find out if you needed a warrant before you ran the query you just finished. Or maybe more accurately you'll then have the information needed to ask a judge whether the judge finds the picture substantial' and therefore a search. Odd."

From: Grant Marguerite (NFK)
Sent: Friday April 17 2020 5:34 PM
To: 'jbukunt@avon-ma.gov' <jbukunt@avon-ma.gov>; 'mdubois@braintreema.gov' <mdubois@braintreema.gov>; 'mmorgan@brookline.ma.gov' <mmorgan@brookline.ma.gov>; Berkowitz Kenneth <kberkowitz@town.canton.ma.us>; 'mdeluca@cohasetpolice.com' <mdeluca@cohasetpo ice.com>; Lennon Gregory <glennon@cohasetpolice.com>; Quigley William <wquigley@cohasetpolice.com>; d'Entremont Michael <mdentremont@police.dedham-ma.gov>; McGowan Peter <pamcgowan@dovermapd.com>; Grace Michael <mgrace@foxboropolice.com>; 'Thomas L. Lynch (thynch@franklinpo ice.com)' <thynch@franklinpolice.com>; 'jmill@franklinpolice.com' <jmill@franklinpolice.com>; 'wsmith@holbrookpolice.com' <wsmith@holbrookpolice.com>; 'mguerette@medfield.net' <mguerette@medfield.net>; 'amringley@medwaypolice.com' <amringley@medwaypolice.com>; 'cwilfayer@mills.net' <cwilfayer@mi ls.net>; 'jking@mpdmilton.org' <jking@mpdm ilton.org>; 'jschlittler@bwedhamma.gov' <jschlittler@bwedhamma.gov>; 'cstone@norfolk.ma.us' <cstone@norfolk.ma.us>; Brooks William G. III <wbrooks@norwoodma.gov>; 'pkelly@norwoodma.gov' <pkelly@norwoodma.gov>; 'james Alfred (jalfred@police.plainville.ma.us)' <jalfred@police.plainville.ma.us>; Keenan Paul <pkeenan@quincyma.gov>; 'will sampaco@randolphmapolice.com' <willampaco@randolphmapolice.com>; 'jford@townofsharon.org' <jford@townofsharon.org>; 'dmcnamara@stoughton-ma.gov' <dmcnamara@stoughton-ma.gov>; 'jcarmichael@walpolepd.com' <jcarmichael@walpolepd.com>; jpilecki <jpilecki@wellesleyma.gov>; jpike@westwoodpd.org' <jpike@westwoodpd.org>; Grimes Richard C. <rgrimes@weymouth.ma.us>; 'chief@police.wrentham.ma.us' <chief@police.wrentham.ma.us>; Baker Chris (EA) <chris.baker@mass.gov>; 'jowernez@atl.edu' <jowernez@atl.edu>; 'jconnolly@suffolk.edu' <jconnolly@suffolk.edu>; 'jconnolly@suffolk.edu>; JMcAlkney Stephen (POL) <stOstephen.ctMullaney@pol.state.ma.us>; 'Matthew Reardon (mreardon@medwaypo ice.com)' <mreardon@medwaypolice.com>; 'mreardon@medwaypolice.com>; 'akingsbury@medwaypolice.com' <akingsbury@medwaypolice.com>; rwkingsbury@medwaypolice.com>; Hannon John <jhannon@foxboropolice.com>; Brewer Don <dbrewer@townofsharon.org>; Guerriero Michael (POL) <michael.guerriero@pol.state.ma.us>; 'Adams Jerry (pd334) (jadams@police.nantucket-ma.gov)' <jadams@police.nantucket-ma.gov>; Donoghue William (NOR) <Wilham.J.Donoghue@MassMail.State.MA.US>; Hunter Alan (MSI) <Alan.Hunter@MassMail.State.MA.US>; Fontes Steven M. (MSG) <steven.m.fontes@MassMail.State.MA.US>; Robert Connor (connor@bc.edu)' <connor@bc.edu>; Stanyanski Christopher <cstanyanski@gardner-ma.gov>; Solimini Ronald (POL) <ronald.solimini@pol.state.ma.us>; 'wawn@mpdmilton.org' <awawn@mpdmilton.org>; Viadoro@braintreema.gov' <jviadoro@braintreema.gov>; Goulding Michael L. <Goulding.M@westonmass.org>; Kennedy Kevin <dkennedy@lincolntown.org>; cchhs David (POL) <cdlaud.ccDfa@pol.state.ma.us>; David Faherty (fahertd@bc.edu)' <fahertd@bc.edu>; Moriarty Dan <daniel.moriarty.J@bc.edu>; 'cSullibur@gmail.com' <cSullibur@gmail.com>; Antoine Romere (POL) <romere.antoine@pol.state.ma.us>; Rudolph James (POL) <James.Rudolph@pol.state.ma.us>; 'mcollins@mpdmilton.org' <mcollins@mpdmilton.org>; Bulman Paul (NOR) <Paul.Bulman@MassMail.State.MA.US>; Pantazelos Keith (NFK) <keith.pantazelos@MassMail.State.MA.US>; Farioli Mark (NFK) <Mark.R.Farioli@MassMail.State.MA.US>; Sullivan Brian (POL) <Brian.Sullivan@pol.state.ma.us>; Lynch Dennis (NFK) <Dennis.M.Lynch@MassMail.State.MA.US>; Powers Meaghan (NFK) <meagn.powers@MassMail.State.MA.US>; Dicicco David M (POL) <David.M.Dicicco@pol.state.ma.us>; Bukhenik Yuriy (POL) <yuriy.bukhenik@pol.state.ma.us>; Dunne Matthew (POL) <Matthew.Dunne@pol.state.ma.us>; Nichol Kevin (POL) <kevin.nichol@pol.state.ma.us>; 'Matthew Murphy (mmurphy@brocktonpo ice.com)' <mmurphy@brocktonpolice.com>; 'shell@brocktonpolice.com' <shell@brocktonpolice.com>; 'arielly@hullpolice.org' <arielly@hullpolice.org>; Donovan Gerald (POL) <gerald.donovan@pol.state.ma.us>; 'dbrady@marblehead.org' <dbrady@marblehead.org>; 'matthew.kelch@jeff.gov' <matthew.kelch@jeff.gov>; 'jmclaughlin@wellesleyma.gov' <jmclaughlin@wellesleyma.gov>; 'juan.vasave@pd.boston.gov' <juan.vasave@pd.boston.gov>; Doiakow Peter <detectives@pawtucketpa.org>; Pack Noah (POL) <noah.pack@pol.state.ma.us>; O Brien Sean (NOR) <Sean.P.O Brien@MassMail.State.MA.US>; Delaney Mark (NOR) <mark.delaney1@MassMail.State.MA.US>; John Perchard <jperchard@weymouth.ma.us>; O'Neill Russ <roneill@brookline.ma.gov>; 'Shannon Ducharme' <ducharme@chicopeepolice.com>; 'Det. Lt. Melissa Greene' <melissagreene@randolphmapolice.com>; Bishop Kevin <kbishop@townofsharon.org>; 'jpenders@townofsharon.org' <jpenders@townofsharon.org>
Cc: Morrissey Michael (NFK) <Michael.W.Morrissey@MassMail.State.MA.US>; Doherty Denise (NFK) <Denise.M.Doherty@MassMail.State.MA.US>; Fanning John (NFK) <John.m.fanning@MassMail.State.MA.US>; Keefe Edward (NFK) <Edward.T.Keefe@MassMa i State.MA.US>; Mattallano Gerard (NFK) <Gerard.Mattallano@MassMail.State.MA.US>; 'Justin Fitzsimmons (justin@search.org)' <justin@search.org>; Quirk Sean (POL) <sean.quirk@pol.state.ma.us>; Tully Brian (NFK) <Brian.P.Tully@MassMail.State.MA.US>; NFK-DL-ADA-Superior-crt <NFK-DL-ADA-Superior-crt@MassMail.State.MA.US>; NFK-DL-ADA-District-crt <NFK-DL-ADA-District-crt@MassMail.State.MA.US>; NFK-DL-ADA- Appeals <NFK-DL-ADA-Appeals2@MassMail.State.MA.US>; Kelly Christopher (AGO) <christopher.kelly@mass.gov>
Subject: Comm v. McCarthy – scoring D's MV with ALPRs on Bourne/Sagamore Bridges not a "search"

[redacted]

Charli,
Commonwealth v. McCarthy (SJC-12750) ← click on that link to see the case
In this case the SJC ruled that police tracking D's car using 4 automatic license plate readers (ALPRs) at both ends of the Bourne and Sagamore Bridges was too limited to amount to a constitutional "search." The SJC declined to say exactly how detailed digital surveillance would have to be to constitute a search leaving that issue for future cases.

State Po ice maintain ALPRs including ones at both ends of the Bourne and Sagamore Bridges. (p.3) The ALPRs photograph vehicles' license plates; that data along with the date and time of the sighting is retained by EOPPS for a year. (p.3-4) Authorized users including police may put a license plate number on a "hot list " and receive an alert if that plate is sighted; reasons to put someone on the "hot list" include not only criminal investigations but also Amber alerts missing persons and BOLO alerts. (p. 3 25 n.13)

Through surveillance controlled buys and information from 4 Civ Barnstable police suspected that the co-D was selling heroin out of his house in Barnstable. (p.4) Police saw a black Hyundai driven by D visit there briefly so they suspected that D was the co-D's supplier. Police put the Hyundai's license plate number on the State Police ALPR "hot list " so that they'd be notified whenever the Hyundai crossed one of the bridges. (p.5) After getting an alert that the Hyundai had crossed onto the Cape police followed both the Hyundai and the co-D to the buy location on a quiet residential street where D and co-D met for about 30 seconds but police could not see a physical exchange. (p.5) From the ALPR data police generated a spreadsheet showing that in mid-winter the Hyundai had crossed the bridges dozens of times sometimes more than once a day adding to police suspicion that D was the heroin supplier. (p.5-6) When police got a second alert that the Hyundai had crossed onto the Cape they again followed D and co-D to the buy location and saw a 30-second meeting but could not see any exchange. This time police stopped both cars handcuffed both co-D and D and read them Miranda. On co-D police found heroin; on D police found 2 cell phones and cash. (p.6-7) At the station police repeatedly told D he was "not under arrest " and D made statements.

D moved to suppress the ALPR data his statements and evidence obtained from the stop. A Superior Court judge found that the moment of arrest was when D and co-D were handcuffed at the scene of the traffic stop but denied the motion to suppress. (p.33) The SJC upheld the denial.

ALPRs and expectation of privacy in digital surveillance At some length the SJC discussed the constitutional issues raised by digital surveillance. (p.7-29) Police conduct amounts to a search if: (1) it intrudes on a D's expectation of privacy and (2) society is willing to recognize the expectation of privacy as reasonable. Here the SJC ruled D did have an expectation of privacy because D and co-D chose a buy location in a quiet residential area. (p.8 n.5) As to what expectation of privacy society recognizes as reasonable with regard to digital surveillance the SJC was guided by historical understandings of what was an unreasonable search and seizure when the U.S. and Mass. Constitutions were adopted in the late 1700s in reaction to redcoats' rummaging without restraint through colonists' homes. (p.8-10) New technologies like ALPRs raise difficult legal issues because they are easier and less expensive for police than traditional surveillance can be done secretly and permit police to search back in time for a vehicle's movements even before police suspicion arose. (p.12-14) Society does not recognize as reasonable an expectation of privacy in what someone "knowingly exposes" to public view like a license plate – which by statute must be "displayed conspicuously." (p.15-16 & n.8) In older cases involving less advanced technology courts have held that a D did not have an expectation of privacy in contents of a phone conversation in a phone booth or a radio beeper" tracking a single journey. (p.14-17) But technology like ALPRs GPS and CSLI are different because they may give police a **mosaic** of information where each piece may be public but when viewed together they create a picture that implicates someone's privacy interests like their political religious or sexual associations. (p.17-21) The SJC was concerned that with enough ALPRs police could track someone's location everywhere which would be "creepy." (p.25) Exigent circumstances would likely justify using an ALPR in a situation involving an Amber alert or missing person. (p.25 n.13) The D urged the SJC to consider not just these four ALPRs on the Bourne and Sagamore Bridges but the hundreds of ALPRs across Massachusetts; the SJC declined to do so because that evidence is not in the record of this case. (p.26) The **limited number of cameras** here and their placements on the bridges was not enough to give D an expectation of privacy that society would recognize as reasonable. (p.28) The SJC declined to say how much digital surveillance would give such an expectation and admitted that its unwillingness to do so "**may bring some interim confusion**" until further cases develop the law on this issue. (p.28 n.15) Chief Justice Gants wrote a separate concurrence suggesting that one thing the SJC could do is to require police who want to search a vast amount of digital data to apply for a court order supported by an affidavit showing reasonable suspicion to do so. (concurrence p.3) This would be like a SW but with a lower standard than PC.

Written policy The SJC rejected D's argument that Barnstable PD should have had a written policy about ALPRs and the MSP policy on which Barnstable relied was not specific enough. (p.30) Written policies are required to justify certain exceptions to the SW requirement (like inventory searches and sobriety checkpoints) – they do not apply to the threshold question whether a search occurred in the first place. (p.31)

Miranda review At the station police repeatedly told D that D was "not under arrest." But the motion judge found that the moment of arrest was when police handcuffed D at the traffic stop. (p.33) D argued that his statements should be suppressed because police telling him he was not under arrest amounted to "deceit or trickery" to get D to confess. The motion judge and the SJC rejected that argument saying that even if telling D he was not under arrest amounted to deceit or trickery it was just one factor to be used in determining voluntariness.

Bottom line: Police use of ALPRs at limited locations is not a constitutional search – but we don't know how many locations it'd have to be to amount to one. Using an ALPR in **exigent circumstances** like an Amber Alert is likely OK. Local police don't need a written policy to use ALPRs maintained by MSP. After a D has been handcuffed police should not tell D that D is "not under arrest" – police will likely be accused later of deceit and trickery.

A thought: There are news stories online that cell phones may be used to do contact tracing for people exposed to COVID-19. If lots of people willingly agree to let their cell phone data be used to track their whereabouts would that ever change courts' view of what society recognizes as a reasonable expectation of privacy? At some point if members of the pub ic come to expect that they're being tracked should police be allowed to use that evidence too? Or at the very least should there be a jury instruction explaining that police have less access to the data than other entities (like software companies or public health agencies)?

As always email me with any questions. Wash your hands!

Marguerite

Marguerite T. Grant
General Counsel – Director of Training
Office of Norfolk District Attorney Michael W. Morrissey
45 Shawmut Road
Canton, MA 02021
781-830-4820

From: Grant, Marguerite (DA)
To: [redacted]
Cc: [redacted]
Subject: RE: Charles v. Norman - get a SW for ALL data if ELMO imposed as PTCOR
Date: Friday, June 26, 2020 3:24:41 PM

Charls

I've had a couple of questions about this case and I wanted to share with you the questions and my answers. The case seems to illustrate the mindset of some judges that technological advances like ELMO end up being an "unfair advantage" to police.

QUESTION #1: This illogical decision appears to create a set of circumstances where an unknown suspect's expectation of privacy cannot be known unt l after a search of ELMO data is completed which puts police in the position of not knowing whether it was reasonable or not until it's too late. It's reminiscent of the end of McCarthy where it was suggested that future LPR decisions may hinge on how much information comes back and not what was actually searched for.

However in light of this trend how would you expect a future case to play out where a suspect is not known (so it cannot be known if he has this new expectation of privacy) and po ice wish to query ELMO to develop a suspect. For example similar to Norman a home invasion occurs with no suspects po ice contact ELMO to query if any devices were in the area police learn that an ELMO bracelet was in the area police are given identity of suspect police attempt to determine whether suspect is wearing it as PTCOR or post-conviction police are given suspect's ELMO location history police investigate this new suspect. At what point would a search warrant likely be required?

Additionally do you think there is an avenue or benefit for probation to change the PTCOR form and procedure to specifically work in a suspect's voluntary consent?

ANSWER #1: Don't even get me started. The Norman case came down on March 17 the first day of the COVID lockdown and the irony is that that was right when the SJC was starting to tell judges to let more Ds out of jail on GPS bracelets. So we're going to let all of these people out on ELMO but then police can't search the ELMO data? And Ds will be out on ELMO on even more serious violent crimes in multiple cases?

I don't think it would help for probation to change the GPS consent form. What the SJC doesn't te l you in Norman is that the form says: "**Coordinates and other data related to your physical location while on GPS are recorded and may be shared with the court, probation, parole, attorneys and law enforcement. Data generated by GPS equipment assigned to you is not private and confidential.**" And in Norman D was represented by counsel when he signed it – how much more voluntary could it be?

The SJC's problem was that it did not think there was valid reason for GPS. The SJC pointed out (at fn.2) that the BMC arraignment had happened more than 4 years before and the transcript of it was no longer available. Since it's the Commonwealth's burden to prove D consented to GPS the SJC held that without the transcript the Comm couldn't prove it – D might've signed the consent form just to get out on bail. That seems like a stretch to me where D was represented by counsel. And it's annoying to read that fn.4 that says "there are some situations" where a D might consent to GPS but we're not going to tell you what they are. (I.ust like the ALPR in McCarthy) I am hopeful that in another situation with the arraignment transcript the Commonwealth would be able to prove that D did consent to GPS – from what I've seen defense attorneys beg for judges to put Ds on GPS rather than impose a higher bail especially because Ds don't want to go to jail because of COVID. But police aren't going to know all that when looking for the ELMO data.

We had a situation recently where police developed PC that a suspect was involved in a serious crime. On the suspect's BOP were open cases in several different courts with the abbreviation "PTCOR." A trooper called probation and they said the suspect is on ELMO and they'd send him the data without a SW. But because of Norman he got a SW. So I wanted to send this email around to warn police about the issue.

In general I would say that when police develop PC that a specific suspect was at the scene of the crime and they have reason to believe that the suspect was on ELMO as a PTCOR police should get a SW to search ELMO for the suspect's data. You're right that the tough situation is when police don't have a suspect. Maybe in a situation like a home invasion of a drug dealer's house police could write a SW affidavit for all ELMO data in the vicinity of the crime. (This would be kind of like a geofencing SW which authorizes a search for cell site location information for all phones that hit off cell towers at the specific time and the specific longitude/latitude of the crime scene.) It could say something like based on information that the Vs of this home invasion were involved in drug dealing there is PC that one or more persons in the area were wearing ELMO bracelets. Based on my training and experience I know that courts have increasingly been releasing defendants on pretrial conditions of release to wear ELMO including in drug-related crimes as a result of the COVID-19 pandemic." That is a stretch but if police have no other leads might be worth a try.

QUESTION #2: About the case you sent about Elmo information. I never ask about a specific person even if I have one in mind. As a matter of fact I had a B/E a few years ago and I just gave them time and location. I got a hit and it was not the guy I expected. My requests always say were there any Probationers in the vicinity of such location around this time? Does that sound like it would work? Sounds like enough or maybe if there answer is a pi:ctor then get warrant? I have told guys forever not to ask for specific person. No need and it limits you.

ANSWER #2: After this case if the suspect's BOP says "PTCOR " it is best to get a SW for the ELMO data. I hear you that it should be better for police to be open-minded and not specify a suspect. I suppose you could include in the SW affidavit the PC you have for suspect #1 and then ask for "data evidencing the presence of suspect #1 or any other probationer wearing an ELMO device in the vicinity of LOCATION on DATE at TIME." That way if the ELMO data comes back that it was someone other than your suspect you got that data pursuant to the SW – and data showing that suspect#2 was there would be evidence relevant to suspect#1 if it proves suspect#1 didn't do it.

Thanks for the questions – they help me figure out how much detail to put in my emails. Have a good weekend. –Marguerite

---

[redacted]

Charls

In this case the SJC ruled that electronic monitoring (ELMO) data placing D at the scene of a home invasion was properly suppressed because D did not consent to ELMO as a pretrial condition of release even though D signed a form agreeing to it. If you are seeking ELMO data from probation and ELMO was imposed as a pretrial condition of release get a SW.

In July 2015 D was arraigned in the BMC for possession of Class B and motor vehicle violations. As pretrial conditions of release (shown on a Mass. criminal record as "**PTCOR**") he was ordered to stay out of Boston and wear ELMO. D signed a form that said "I have read and understood the above conditions and **I agree to observe them**." A month later a home invasion and masked armed robbery occurred in Medford. Without any information linking D to those crimes police contacted probation to find out if any ELMO bracelets were at the Medford scene. They learned that D's ELMO bracelet was and immediately before and afterwards was at an address in Everett. Po lice got a SW for the Everett premises where they found evidence of the home invasion. A V of the home invasion ID'd D in a photo array.

A Superior Court judge allowed D's motion to suppress the ELMO data reasoning that D consented to ELMO only for the purposes of ensuring that D complied with the conditions of release (show up in court and stay out of Boston) not for general law enforcement purposes. The Commonwealth appealed. The SJC upheld the suppression. It ruled that because ELMO was imposed on D as a **pretrial condition,** D had a **greater** reasonable expectation of privacy than would a D who had it imposed after trial. The SJC ruled that "the only evidence of consent" was the fact that D signed the form agreeing to pretrial conditions of release and **D signing the form was not enough for the Commonwealth to meet its burden of proving D's consent**. The SJC noted that "there are some situations . . . where a pretrial condition of release would be justified by free and voluntary consent " but did not say what those would be. (fn.4) The SJC did not think there was a sufficient basis for imposing GPS at the BMC arraignment for drug and M/V crimes – GPS and the condition excluding D from Boston did not increase the likelihood of D showing up to court.

Bottom line: A D wearing ELMO as a pretrial condition of release has a reasonable expectation of privacy in the ELMO data. Before you get data from ELMO check to see f your suspect's BOP includes any open case with the abbreviation **PTCOR**. If so **get a SW** before obtaining any data from ELMO. Be forewarned the ELMO people may be perfectly willing to give you the data without a SW but after this case you need one if ELMO is imposed as a PTCOR. The situation may be different f D consented to ELMO by more than just signing the form or there's a stronger basis for ELMO than there was here – but usually you will have no way of knowing that. For example if a judge in a DV case imposed ELMO to enforce an order that D stay away from V and then D showed up at V's home there'd arguably be a much stronger basis for police to access ELMO – D's expectation of privacy would be less reasonable and often there'd be exigent circumstances for police to find D right away. If ELMO is imposed **after trial** it should be OK to search it. But most of the time you may not know much about why ELMO was imposed or how reasonable D's expectation of privacy was in agreeing to it. So if you see those five letters **PTCOR**" on the suspect's BOP get a SW for ELMO data.

As always email me with any questions. Wash your hands!

Marguerite

Marguerite T. Grant
General Counsel + Director of Training
Office of Norfolk District Attorney Michael W. Morrissey
45 Shawmut Road
Canton, MA 02021
781-830-4529

From: Pack, Marguerite (AGO)
To: [redacted]
Cc: [redacted]
Subject: RE: Cowles v. Norman - get a SW for ELMO anyway @ PTCOR
Date: Monday, June 29, 2020 3:26:26 PM

Chiefs – some more follow-up on the ELMO case I sent around last week. Trooper Noah Pack had a great suggestion about how to seek information from ELMO in an investigation where there is no PC for a specific suspect. I highlighted his suggestion in red below. This case is frustrating. Stay safe Marguerite

Hi Marguerite

Thanks for your reply and discussion on the matter. Today I read the decision in greater detail and I'm even more frustrated than I was before. They start the decision by saying that the imposition of GPS in the first place was unsupported so they don't need to address the issue of the search. (Until recently that would be the end of it...right?) Then they thoroughly and by their own words unnecessarily address the issue of the ELMO search by police. I won't comment further on that aside to again point to how they also did that with McCarthy.

More to the point I struggle to accept that ELMO is essentially gone as an investigative tool because the SJC thinks it's humiliating to defendants and unpopular with the judiciary. The distinction between PTCOR and probationary use is reasonably clear from the decision and your emails and I'm not sure we can do much with that. However I think that a search warrant for ELMO in a case without a suspect is a stretch. "Fishing expedition" is what the Springfield DC clerks will invariably te l us as they deny the application.

The SJC cites Moore in their final paragraph stating **For a warrantless search to be permissible under art. 14, the legitimate governmental interests must outweigh the level of intrusion.**" I think a reasonable way to balance the government's need to identify a suspect in a violent crime against the privacy interests of a GPS assigned individual would be the following:

(1) contact ELMO and ask if any signals were located in the area in question.
(2) If no: move on.
(3) If yes: go get a search warrant to identify the owner of the bracelet and his relevant travel.

I would argue that this procedure dramatically reduces the intrusion on the individual as his name and location information is not disclosed to the government until a search warrant is obtained. Officers have merely gained enough anonymized information to know that some unknown suspect was there and to establish PC to get the warrant to identify him.

Your thoughts?

Respectfully

Noah

Trooper Noah H. Pack
Massachusetts State Police Detective Unit
Office of the Hampden District Attorney
1500 Main Street 18th Floor
Springfield Massachusetts 01115

Chiefs
I've had a couple of questions about this case and I wanted to share with you the questions and my answers. The case seems to illustrate the mindset of some judges that technological advances like ELMO end up being an "unfair advantage" to police.

QUESTION #1: This illogical decision appears to create a set of circumstances where an unknown suspect's expectation of privacy cannot be known until after a search of ELMO data is completed which puts police in the position of not knowing whether it was reasonable or not until it's too late. It's reminiscent of the end of McCarthy where it was suggested that future LPR decisions may hinge on how much information comes back and not what was actually searched for. ever in light of this trend how would you expect a future case to play out where a suspect is not known (so it cannot be known if he has this new expectation of privacy) and police wish to query ELMO to develop a suspect. For example similar to Norman a home invasion occurs with no suspects police contact ELMO to query if any devices were in the area police learn that an ELMO bracelet was in the area police are given identity of suspect police attempt to determine whether suspect is wearing it as PTCOR or post-conviction police are given suspect's ELMO location history police investigate this new suspect. At what point would a search warrant likely be required?

Additionally do you think there is an avenue or benefit for probation to change the PTCOR form and procedure to specifically work in a suspect's voluntary consent?

ANSWER #1: Don't even get me started. The Norman case came down on March 17 the first day of the COVID lockdown and the irony is that that was right when the SJC was starting to tell judges to let more Ds out of jail on GPS bracelets. So we're going to let all of these people out on ELMO but then police can't search the ELMO data? And Ds will be out on ELMO on even more serious violent crimes in multiple cases?

I don't think it would help for probation to change the GPS consent form. What the SJC doesn't tell you in Norman is that the form says: "**Coordinates and other data related to your physical location while on GPS are recorded and may be shared with the court, probation, parole, attorneys and law enforcement. Data generated by GPS equipment assigned to you is not private and confidential.**" And in Norman D was represented by counsel when he signed it – how much more voluntary could it be?

The SJC's problem was that it did not think there was valid reason for GPS. The SJC pointed out (at fn.2) that the BMC arraignment had happened more than 4 years before and the transcript of it was no longer available. Since it's the Commonwealth's burden to prove D consented to GPS the SJC held that without the transcript the Comm couldn't prove it – D might've signed the consent form just to get out on bail. That seems like a stretch to me where D was represented by counsel. And it's annoying to read that fn.4 that says "there are some situations" where a D might consent to GPS but we're not going to tell you what they are. (Just like the AUN in McCarthy.) I am hopeful that in another situation with the arraignment transcript the Commonwealth would be able to prove that D did consent to GPS – from what I've seen defense attorneys beg for judges to put Ds on GPS rather than impose a higher bail especially because Ds don't want to go to jail because of COVID. But police aren't going to know all that when looking for the ELMO data.

We had a situation recently where police developed PC that a suspect was involved in a serious crime. On the suspect's BOP were open cases in several different courts with the abbreviation "PTCOR." A trooper called probation and they said the suspect is on ELMO and they'd send him the data without a SW. But because of Norman he got a SW. So I wanted to send this email around to warn police about the issue.

In general I would say that when police develop PC that a specific suspect was at the scene of the crime and they have reason to believe that the suspect was on ELMO as a PTCOR police should get a SW to search ELMO for the suspect's data. You're right that the tough situation is when police don't have a suspect. Maybe in a situation like a home invasion of a drug dealer's house police could write a SW affidavit for all ELMO data in the vicinity of the crime. (This would be kind of like a geofencing SW which authorizes a search for cell site location information for all phones that hit off cell towers at the specific time and the specific longitude/latitude of the crime scene.) It could say something like "based on information that the Vs of this home invasion were involved in drug dealing there is PC that one or more persons in the area were wearing ELMO bracelets. Based on my training and experience I know that courts have increasingly been releasing defendants on pretrial conditions of release to wear ELMO including in drug-related crimes as a result of the COVID-19 pandemic." That is a stretch but if police have no other leads might be worth a try.

QUESTION #2: About the case you sent about Elmo information. I never ask about a specific person even if I have one in mind. As a matter of fact I had a B/E a few years ago and I just gave them time and location. I got a hit and it was not the guy I expected. My requests always say were there any Probationers in the vicinity of such location around this time? Does that sound like it would work? Sounds like enough or maybe if there answer is a pricor then get warrant? I have told guys forever not to ask for specific person. No need and it limits you.

ANSWER #2: After this case if the suspect's BOP says "PTCOR " it is best to get a SW for the ELMO data. I hear you that it should be better for police to be open-minded and not specify a suspect. I suppose you could include in the SW affidavit the PC you have for suspect #1 and then ask for "data evidencing the presence of suspect #1 or any other probationer wearing an ELMO device in the vicinity of LOCATION on DATE at TIME." That way if the ELMO data comes back that it was someone other than your suspect you got that data pursuant to the SW – and data showing that suspect#2 was there would be evidence relevant to suspect#1 if it proves suspect#1 didn't do it.

Thanks for the questions – they help me figure out how much detail to put in my emails. Have a good weekend. –Marguerite

---

[redacted]

Chiefs

In this case the SJC ruled that electronic monitoring (ELMO) data placing D at the scene of a home invasion was properly suppressed because D did not consent to ELMO as a pretrial condition of release even though D signed a form agreeing to it. If you are seeking ELMO data from probation and ELMO was imposed as a pretrial condition of release get a SW.

In July 2015 D was arraigned in the BMC for possession of Class B and motor vehicle violations. As pretrial conditions of release (shown on a Mass. criminal record as "**PTCOR**") he was ordered to stay out of Boston and wear ELMO. D signed a form that said I have read and understood the above conditions and I **agree to observe them**." A month later a home invasion and masked armed robbery occurred in Medford. Without any information linking D to those crimes police contacted probation to find out if any ELMO bracelets were at the Medford scene. They learned that D's ELMO bracelet was and immediately before and afterwards was at an address in Everett. Police got a SW for the Everett premises where they found evidence of the home invasion. A V of the home invasion ID'd D in a photo array.

A Superior Court judge allowed D's motion to suppress the ELMO data reasoning that D consented to ELMO only for the purposes of ensuring that D complied with the conditions of release (show up in court and stay out of Boston) not for general law enforcement purposes. The Commonwealth appealed. The SJC upheld the suppression. It ruled that because ELMO was imposed on D as a **pretrial condition,** D had a **greater** reasonable expectation of privacy than would a D who had it imposed after trial. The SJC ruled that "the only evidence of consent" was the fact that D signed the form agreeing to pretrial conditions of release and **D signing the form was not enough for the Commonwealth to meet its burden of proving D's consent**. The SJC noted that "there are some situations . . . where a pretrial condition of release would be justified by free and voluntary consent " but did not say what those would be. (fn.4) The SJC did not think there was a sufficient basis for imposing GPS at the BMC arraignment for drug and MV crimes – GPS and the condition excluding D from Boston did not increase the likelihood of D showing up to court.

Bottom line: A D wearing ELMO as a pretrial condition of release has a reasonable expectation of privacy in the ELMO data. Before you get data from ELMO check to see if your suspect's BOP includes any open case with the abbreviation **PTCOR**. If so **get a SW** before obtaining any data from ELMO. Be forewarned: the ELMO people may be perfectly willing to give you the data without a SW but after this case you need one if ELMO is imposed as a PTCOR. The situation may be different if D consented to ELMO by more than just signing the form or there's a stronger basis for ELMO than there was here – but usually you will have no way of knowing that. For example if a judge in a DV case imposed ELMO to enforce an order that D stay away from V and then D showed up at V's home there'd arguably be a much stronger basis for police to access ELMO – D's expectation of privacy would be less reasonable and often there'd be exigent circumstances for police to find D right away. If ELMO is imposed **after trial** it should be OK to search it. But most of the time you may not know much about why ELMO was imposed or how reasonable D's expectation of privacy was in agreeing to it. So if you see those five letters **"PTCOR"** on the suspect's BOP get a SW for ELMO data.

As always email me with any questions. Wash your hands!

Marguerite

Marguerite T. Grace
General Counsel + Director of Training
Office of Norfolk District Attorney Michael W. Morrissey
45 Shawmut Road
Canton, MA 02021
781-830-4150

From: Halpin, Michael (POL)
To: Mason, Christopher (POL)
Subject: RE: Commonwealth v McCarthy - SJC Decision (the Sagamore bridge cam case)
Date: Thursday, April 16, 2020 1:05:02 PM

Good outcome and an interesting read. However, I fear the decision will encourage and produce more defense motions (and public record requests) for the specific number, location, and capabilities of MSP and municipal ALPR systems (not only in specific cases but as an entire network).

-----Original Message-----
From: Mason, Christopher (POL) <Chris.Mason@pol.state.ma.us>
Sent: Thursday, April 16, 2020 10:54 AM
To: Halpin, Michael (POL) <michael.halpin@pol.state.ma.us>
Subject: FW: Commonwealth v McCarthy - SJC Decision (the Sagamore bridge cam case)

FYI

-----Original Message-----
From: Thibeault, Sharon (CPI)
Sent: Thursday, April 16, 2020 10:23 AM
To: Mason, Christopher (POL) <Chris.Mason@pol.state.ma.us>
Subject: Commonwealth v McCarthy - SJC Decision (the Sagamore bridge cam case)

https://www.mass.gov/files/documents/2020/04/16/e12750.pdf

Good morning Colonel,

It is nice to share some good news for a change.
I know the Bridge cam case has wide State Police implications. Thought you would like to give it a read.
Another win for the Cape!
Stay healthy.

Sharon Thibeault

From: daniel.griffin@pol.state.ma.us
To: Nardone, Andrea (DAA)
Subject: Re: Court Decision - April 16, 2020
Date: Thursday, April 16, 2020 12:49:17 PM

Good news. Thanks

> On Apr 16, 2020, at 11:15 AM, Nardone, Andrea (DAA) <Andrea.Nardone@massmail.state.ma.us> wrote:
>
> ***<image001.png>***
>
> ***Commonwealth v. McCarthy***
> Supreme Judicial Court, April 16, 2020
> (Search and Seizure/Automatic License Plate Readers)
>
> *The use of four automatic license plate reader cameras, placed at two fixed locations on the ends of the Bourne and Sagamore bridges and used to "hit" on the defendant's license when he drove over either bridge,, does not constitute a search within the meaning of either art. 14 or the Fourth Amendment.*
>
> "While we recognize that the widespread use of ALPRs in the Commonwealth could implicate constitutional protections against unreasonable searches, the limited use of the technology in this case does not."
>
> Note:
> The Court did not find error in the fact that the Bourne Police Department did not have a separate policy, apart from State Police TRF-11, regarding ALPRs.
>
> Additionally, the Court ruled that the government's use of ALPR data is not subject to the Stored Communication Act nor the Electronic Communications Privacy Act
>
> See attached opinion.
>
> *For other recent case law decisions, go to the MDAA website at www.mass.gov/mdaa*
>
> <Commonwealth v. McCarthy - opinion.pdf>

To: Harney, Michael
Cc: Quinn, Dermot (POL); O'Leary, John F; Burke, Kevin (POL); Alexander Chute (abchute@gmail.com); Slater, James (CHS)
Subject: RE: data
Date: Monday, March 9, 2020 10:21:00 AM

Hi Mike,

As you may be aware, the MSP and MassPort have been actively working towards migrating the MassPort ALPR cameras into the EOPSS BOSS server. The original plan was to physically network the cameras through F Troop's TSS infrastructure and into the new BOSS system. However, the new BOSS system has been delayed for a number of reasons. In an effort to move this project along I would like to cannibalize 6 cruisers MP70's identified from the below and push the ALPR data wirelessly to the data center. I consider this a phased approach and once the new BOSS system is up and running, we would then move forward with the original TSS networking and cut the ALPR off VZW. I have spoken with Alex at MassPort and with approval, we'd like to begin identifying the camera sectors to cut over. Please advise if you are ok the above approach and if you can assist in scheduling the removal of the devices by the Technical Services Unit.

Thanks, Brian

Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
Phone: 978-451-3710 (Maynard) 508-988-7302 (GHQ)
Email: Brian.Egnitz@massmail.state.ma.us
Monday - Friday, 8 to 4

CONFIDENTIALITY NOTICE: *The information contained in this email and any attachment is privileged and confidential law enforcement information. If you have received this email in error, please call 978-451-3700 immediately. Thank you.*

From: Burke, Kevin [mailto:KBurke@massport.com]
Sent: Wednesday, February 26, 2020 2:49 PM
To: Harney, Michael
Cc: Quinn, Dermot (POL); Egnitz, Brian (POL); O'Leary, John F
Subject: RE: data

Sirs,
Troop F installed [redacted] AVL in marked vehicles that did not have lap tops. These same vehicles are also equipped with the GeoTab system.
Respectfully,
Kevin

Sgt. Kevin Burke

From: Harney, Michael
Sent: Wednesday, February 26, 2020 8:37 AM
To: Burke, Kevin
Cc: Quinn, Dermot (POL); 'Egnitz, Brian (POL)'
Subject: RE: data

Sgt Burke,
Kevin could see the email below and find the answers for Brian about the cruiser please.

Thanks,
Michael

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Wednesday, February 26, 2020 8:01 AM
To: Harney, Michael
Cc: Quinn, Dermot (POL)
Subject: Re: data

Hi Mike,

We were wondering if you could help answer a question. Do you know how many Massport cruisers had the Sierra wireless AVL installed but did not have a laptop? I trying to find out if there are any cars with both Sierra modems and geotab installed, but with no laptop or need for the Sierra device.

Thanks, Brian

On Jul 23, 2019, at 9:55 AM, Harney, Michael <MHarney@massport.com> wrote:

> I have been taken out of the loop on that and Steph is handling all of that.
>
> He should have all of what you are looking for.
>
> Thanks,
> Michael
>
> ---
>
> **From:** Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
> **Sent:** Tuesday, July 23, 2019 9:54 AM
> **To:** Harney, Michael
> **Cc:** Quinn, Dermot (POL)
> **Subject:** RE: data
>
> Ok, I'll forward to Steph.
>
> Can you please send me the drop tables from Orion that you are sending to RAMS?
> Also, do you have a Unit table with rolls or duty assignments?
>
> Thanks, Brian

From: Harney, Michael [mailto:MHarney@massport.com]
Sent: Tuesday, July 23, 2019 9:42 AM
To: Egnitz, Brian (POL)
Cc: Quinn, Dermot (POL)
Subject: RE: data

Brian,
Stephe Weldon would be the best person to get you that. I don't have access to the full roster table.

Hope that helps,
Michael

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Monday, July 22, 2019 4:57 PM
To: Harney, Michael
Cc: Quinn, Dermot (POL)
Subject: data

Hi Mike,

Can you please send me a few examples of the run roster and code tables for assignments or rolls/duty assignments from RAMS?

Thanks, Brian

Brian Egnitz
Commonwealth Fusion Center
Massachusetts State Police
Phone: 978-451-3710 (Maynard) 508-988-7302 (GHQ)
Email: Brian.Egnitz@massmail.state.ma.us
Monday - Friday, 8 to 4

CONFIDENTIALITY NOTICE: *The information contained in this email and any attachment is privileged and confidential law enforcement information. If you have received this email in error, please call 978-451-3700 immediately. Thank you.*

From: Connolly, Kevin
To: Egnitz, Brian (POL)
Subject: RE: Elsag ALPR / Barnstable MA Police ; 2020 JAG edward-byrne-memorial Grant for Massachusetts Police agencies
Date: Friday, July 24, 2020 9:27:26 AM

Great, I'll see how it is and talk to you monday

Kevin A. Connolly
Sergeant
Barnstable Police Department
USSS Electronic Crimes Task Force
508-958-6522
connollyk@barnstablepolice.com

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Friday, July 24, 2020 9:25 AM
To: Connolly, Kevin <connollyk@barnstablepolice.com>
Subject: Re: Elsag ALPR / Barnstable MA Police ; 2020 JAG edward-byrne-memorial Grant for Massachusetts Police agencies

I can do it Monday, let's see how many we get so we don't know up your phone. VIP The email account t if you have an iPhone and it will act the same as text. You'll also get RMV stuff (not insurance violations) and Northern NCIS.

> On Jul 24, 2020, at 9:21 AM, Connolly, Kevin <connollyk@barnstablepolice.com> wrote:
>
> I got 2 already thins morning, want to add 5089586522@vtext.com as
> well, I usually get text and that alerts me to check my email
>
>
> Kevin A. Connolly
> Sergeant
> Barnstable Police Department
> USSS Electronic Crimes Task Force
> 508-958-6522
> connollyk@barnstablepolice.com
>
>
>
> -----Original Message-----
> From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
> Sent: Friday, July 24, 2020 8:37 AM
> To: Connolly, Kevin <connollyk@barnstablepolice.com>
> Subject: RE: Elsag ALPR / Barnstable MA Police ; 2020 JAG
> edward-byrne-memorial Grant for Massachusetts Police agencies
>
> I'm testing a new WMS hotlist workflow and setup your account to get emails. Can you test it out and let me know what you think? Its WMS matched with active registrations. I setup both your readers to relay to your email.
>
> -----Original Message-----
> From: Connolly, Kevin [mailto:connollyk@barnstablepolice.com]
> Sent: Thursday, July 23, 2020 1:39 PM
> To: Egnitz, Brian (POL)
> Subject: Re: Elsag ALPR / Barnstable MA Police ; 2020 JAG
> edward-byrne-memorial Grant for Massachusetts Police agencies
>
> Yes I can.
>
> We have got to get more around town, we had a Great b&e with good side shot of car but no plate. They would have went right [redacted]. I've had 4 detectives checking addresses in 3 towns last 2 days crossing off possible vehicles. No doubt these things save time/money.
>
> Kevin A. Connolly
> Sergeant
> Barnstable Police Department
> USSS
> 508-958-6522<tel:508-958-6522>
> connollyk@barnstablepolice.com<mailto:connollyk@barnstablepolice.com>
> [bpd-patch small]
>
>
> On Jul 23, 2020, at 12:47 PM, Egnitz, Brian (POL) <brian.egnitz@state.ma.us> wrote:
>
> Thanks, but free market we are always looking for a cheaper and better mouse trap. EOPSS/EOTSS need to get their act together and support open lpr, making data sharing a non-issue. BTW - Bourne is back online and I may have a box for you. I'll know more in a week or so. Can you still get a dataplan?
>
> -----Original Message-----
> From: Connolly, Kevin [mailto:connollyk@barnstablepolice.com]
> Sent: Thursday, July 23, 2020 12:43 PM
> To: Egnitz, Brian (POL)
> Subject: Re: Elsag ALPR / Barnstable MA Police ; 2020 JAG

> edward-byrne-memorial Grant for Massachusetts Police agencies
>
> Not at all, that is just who sent is the heads up. I will NOT buy anything unless we talk to you first. Foolish to buy something that won't work with MSP system.
>
> Kevin A. Connolly
> Sergeant
> Barnstable Police Department
> USSS
> 508-958-6522<tel:508-958-6522>
> connollyk@barnstablepolice.com<mailto:connollyk@barnstablepolice.com>
> [bpd-patch small]
>
>
> On Jul 23, 2020, at 12:38 PM, Egnitz, Brian (POL) <brian.egnitz@state.ma.us> wrote:
>
>
> Tks, you guys looking to go Elsag? I'm not sure how they will submit to the backend and share data.
>
> From: Connolly, Kevin [mailto:connollyk@barnstablepolice.com]
> Sent: Thursday, July 23, 2020 10:28 AM
> To: Egnitz, Brian (POL)
> Subject: FW: Elsag ALPR / Barnstable MA Police ; 2020 JAG
> edward-byrne-memorial Grant for Massachusetts Police agencies
>
> Brian,
> I don't see the MSP on here, but there is a list of city's
> that you may be abel to share with. It looks like these funds can be
> used for ALPR's
>
> Kevin A. Connolly
> Sergeant
> Barnstable Police Department
> USSS Electronic Crimes Task Force
> 508-958-6522
> connollyk@barnstablepolice.com<mailto:connollyk@barnstablepolice.com>
> <image001.jpg>
> <image002.jpg>
>
>
> From: Hurwitz, Craig <hurwitzc@barnstablepolice.com>
> Sent: Thursday, July 23, 2020 8:33 AM
> To: Connolly, Kevin <connollyk@barnstablepolice.com>
> Subject: FW: Elsag ALPR / Barnstable MA Police ; 2020 JAG
> edward-byrne-memorial Grant for Massachusetts Police agencies
>
>
> _____
> From: Ben Miller [ben.miller@leonardocompany-us.com]
> Sent: Wednesday, July 22, 2020 3:48 PM
> To: Hurwitz, Craig
> Subject: Elsag ALPR / Barnstable MA Police ; 2020 JAG
> edward-byrne-memorial Grant for Massachusetts Police agencies Hi
> Craig,
>
> Good to catch up with you last week. As discussed, I found a grant that might help with your goal to get a Mobile ALPR system for Barnstable Police ….
>
> If you click on this link from Bureau of Justice https://urldefense.proofpoint.com/v2/url?u=https-3A__bja.ojp.gov_program_jag_fy-2D2020-2Dallocations-2Dand-2Ddisparate-2Dinformation&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=nF3oiRzulLrcME0WA8EOYnD2tlx-8Kssb0278nyA9-w&s=S06RkEFSSJzE8BFB0rFBtHkFEQhVqDi1cAgLM952omM&e=
<https://urldefense.proofpoint.com/v2/url?u=https-3A__bja.ojp.gov_program_jag_fy-2D2020-2Dallocations-2Dand-2Ddisparate-2Dinformation&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=zYal0qbp2-8p_jJR5qj65DmQRm9xooNTRXV_ZD9cvus&e=> , click on the Massachusetts button and look on this list, you will see that Barnstable is eligible to apply for $15,240.00.
>
> Our attached new MPH M7 system is $11,500 including all hardware and
> software. We could fully install it for you on one of your vehicles
> for $1250, so the total cost would be $12,750, well within the
> eligible grant of $15,240.00
>
>
> * The Program overview link is : https://urldefense.proofpoint.com/v2/url?u=https-3A__bja.ojp.gov_funding_opportunities_bja-2D2020-2D17276&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=nF3oiRzulLrcME0WA8EOYnD2tlx-8Kssb0278nyA9-w&s=0URU95vtxRgZxAFjcJXMsEEo1j4rie4BCG9MvQl046c&e=
<https://urldefense.proofpoint.com/v2/url?u=https-3A__bja.ojp.gov_funding_opportunities_bja-2D2020-2D17276&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=1W2-HkI_cz1jsQ3etfDe56uRHgnXuQyhGFluXeNQ6jk&e=>
> * RFP: https://urldefense.proofpoint.com/v2/url?u=https-3A__bja.ojp.gov_sites_g_files_xyckuh186_files_media_document_bja-2D2020-2D17276.pdf&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=nF3oiRzulLrcME0WA8EOYnD2tlx-8Kssb0278nyA9-w&s=OesK2QQMHJfDif8U78cIRJirP-80eWpWGOOQ8xKFwyY&e=
<https://urldefense.proofpoint.com/v2/url?u=https-3A__bja.ojp.gov_sites_g_files_xyckuh186_files_media_document_bja-2D2020-2D17276.pdf&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=fb8ZDct9yj0YL7wRFQkY8ROhfITB-

r0mFaaJUTo3fqE&e=>
>
> * I suggest reviewing page 16-17 of RFP – the application checklist
>
> * Deadline: August 19th at 11:59 PM EDT
> * Administrative requirements: SAM.gov registration<https://urldefense.proofpoint.com/v2/url?u=https-3A__sam.gov_SAM_pages_public_index.jsf&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=e6dKFPtxucVTAvX0gXxt3c53fH8Vy4V2nzKdl5Ce8Ms&e=>, DUNS number<https://urldefense.proofpoint.com/v2/url?u=https-3A__www.dnb.com_duns-2Dnumber.html&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=wc7Vf9Hi2y1EvIM_A5X7cg-utlW-NIqRPzSaEQ2orJ8&e=>, GMS registration<https://urldefense.proofpoint.com/v2/url?u=https-3A__grants.ojp.usdoj.gov_gmsexternal_&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=T2bnfgMz1eVG6XA-WSxFz4bnW6iVgYd-U-ApHvkl-6I&e=> & SF-424 form<https://urldefense.proofpoint.com/v2/url?u=https-3A__www.ojp.gov_funding_apply_ojp-2Dgrant-2Dapplication-2Dresource-2Dguide-23completeApplication&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=NvE2xAM6-IZSDEkhr4lcxKx1VVKB9mwCbXcSKs2GYU0&e=>
> * Category 1 under this solicitation allows for requests under $25,000 and allows for regional and single projects.
> * No cost match required.
>
> For this application, you, as a sworn agency, have to fill out the forms on-line directly with BJA OJP, but we can help you if you have questions about it. We also have a grant writing service who can give you direct assistance free of charge if you need that.
>
> Please let me know if this is interesting for you to follow up on.
>
> Best Regards, Ben
>
> Ben Miller
> Operations Director New England
> Selex ES Inc., a Leonardo Company
> ELSAG® ALPR Plate Recognition Technology Proudly Made in the USA
> 4221 Tudor Lane
> Greensboro, North Carolina 27410 USA
> ben.miller@leonardocompany-us.com<mailto:ben.miller@leonardocompany-us
> .com>
> Cell: +1 845 [redacted]
> www.elsag.com<https://urldefense.proofpoint.com/v2/url?u=http-3A__www.
> elsag.com_&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hN
> TkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikB
> h_wo2MFBsZE8SsyzY&s=_yNIVENVm0CtK8KY0fqz7R3d84RxEspYO2WuK_5-eMs&e=>
>
>
>
>
>
> From: Ben Miller
> Sent: Tuesday, March 10, 2020 7:44 PM
> To:
> hurwitzc@barnstablepolice.com<mailto:hurwitzc@barnstablepolice.com>
> Subject: Elsag ALPR / Barnstable MA Police ; Massachusetts Homeland
> Security Grant
>
> To : Craig Hurwitz, Director of Information Systems, Barnstable
> Police Department
>
> Hello Craig,
>
> Good to speak with you today. As discussed, I went searching for a possible Grant for your Department to use for funding of an ALPR Automatic License Plate Recognition system and found this one :
>
> Massachusetts Homeland Security Grant Program State (SHSP) Shared
> Funds Save Download Grant Tips
>
> Please note: This is an estimated deadline based on the previous year grant schedule. We recommend adding this grant to your alert list to be notified of any release date updates.
>
> Program Area
> Criminal Justice & Law Enforcement, Intelligence, Emergency Response &
> Public Safety, Hazmat & CBRNE Response, Disaster Planning/Assistance,
> Emergency Management Administering Authority
>
> Massachusetts Executive Office of Public Safety and Security
>
> Funder
>
> State
>
> Administering State
>
> MA
>
> Location

>
> MA
>
> Who Can Apply?
>
> Non-Profit, Institution of Higher Education, State Government
>
> Letter of Intent?
>
> No
>
> Deadline
>
> 04/25/2020
> Application Deadline
>
> Last Updated
>
> 03/04/2020
>
> Summary
>
> Overview: Through this announcement of the Availability of Grant Funds (AGF), the Massachusetts Executive Office of Public Safety and Security (EOPSS) is making a portion of the twenty-percent (20%) state-share of the U.S. Department of Homeland Security (DHS) FFY 2016 Homeland Security Grant Program (HSGP) funding available to eligible applicants. It is anticipated that up to approximately $2.0 million may be made available.
>
> In general, eighty-percent (80%) of the HSGP funding allocated to Massachusetts is distributed to municipalities through the five Regional Homeland Security Advisory Councils. The remaining 20% is used to fund state priorities and administrative costs.
> Eligibility: Massachusetts state government agencies and authorities, state institutions of higher education and non-profit organizations that support state homeland security needs and Sheriff's Offices. Municipalities are not eligible to apply for this funding.
> Projects funded through this AGF must address:
> * at least one capability target in the Massachusetts Threat and
> Hazard Identification and Risk Assessment (THIRA);
> * a capability gap in the 2016 Massachusetts State Preparedness Report
> (SPR);
> * an implementation step in the State Homeland Security Strategy
> (SHSS); and
> * align with a Massachusetts HSGP State Priority.
> Links
>
> Please note: This is an estimated deadline based on the previous year grant schedule. We recommend you review the grant guidance and instructions from the previous grant cycle so you can prepare in advance for this grant to open.
> Program Link
> <https://www.mass.gov/how-to/apply-for-a-state-share-grant>
> Announcement or Guideline Link
> <https://www.mass.gov/files/documents/2019/04/22/FFY2019%20State-Share
> %20NOFO-revised.pdf> Application Link
> <https://www.mass.gov/doc/ffy2019-state-share-application/download>
> Matching Requirement
>
> No
>
> Program Contact
> stateshare.pc@mass.gov<mailto:stateshare.pc@mass.gov>
> (617) 933-3529<tel:6179333529>
>
>
> I called the 617 933 3529 number and left a voicemail for Nick Danald(sp?) of the Homeland Security Grant program this afternoon, but I have a feeling that if you called or emailed from a sworn Massachusetts agency, you might get a quicker response ….
>
> What I believe you would be interested in is a Mobile ALPR system (our MPH (Mobile Plate Hunter) M7 (7th generation) technical data sheet is attached. I would think that Barnstable being situated right in the middle of the Cape with access to G.L. c. 4 sec. 7 cl.26 (n)(security), G.L. c. 4 sec. 7 cl.26(f)(investigative) If you have any questions about other deployments that Elsag has with Homeland Security around the country that you want to ask me before you make the enquiry, please call my cell on + 1 845 G.L. c. 4 sec. 7
>
> Best Regards, Ben
>
> Ben Miller
> Operations Director New England
> Selex ES Inc., a Leonardo Company
> ELSAG® ALPR Plate Recognition Technology Proudly Made in the USA
> 4221 Tudor Lane
> Greensboro, North Carolina 27410 USA
> ben.miller@elsag.com<mailto:ben.miller@elsag.com>
> Cell: +1 845 G.L. c. 4 sec. 7
> www.elsag.com<https://urldefense.proofpoint.com/v2/url?u=http-3A__www.
> elsag.com_&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hN
> TkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7M11ikB
> h_wo2MFBsZE8SsyzY&s=_yNIVENVm0CtK8KY0fqz7R3d84RxEspYO2WuK_5-eMs&e=>
>
>
>
> The content of this email is confidential and intended for the recipient specified in message only. It is strictly forbidden to share any part of this message with any third

party, without a written consent of the sender. If you received this message by mistake, please reply to this message and follow with its deletion, so that we can ensure such a mistake does not occur in the future.
>
>
>
> Confidentiality Notice | This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential, proprietary, legally privileged and/or CORI information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient or have received this email in error, immediately contact the sender by reply e-mail and destroy all copies of the original message. This email message may be monitored by the Barnstable Police Department.
>
> Confidentiality Notice | This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential, proprietary, legally privileged and/or CORI information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient or have received this email in error, immediately contact the sender by reply e-mail and destroy all copies of the original message. This email message may be monitored by the Barnstable Police Department.
>
> Confidentiality Notice | This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential, proprietary, legally privileged and/or CORI information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient or have received this email in error, immediately contact the sender by reply e-mail and destroy all copies of the original message. This email message may be monitored by the Barnstable Police Department.
> Confidentiality Notice | This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential, proprietary, legally privileged and/or CORI information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient or have received this email in error, immediately contact the sender by reply e-mail and destroy all copies of the original message. This email message may be monitored by the Barnstable Police Department.
Confidentiality Notice | This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential, proprietary, legally privileged and/or CORI information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient or have received this email in error, immediately contact the sender by reply e-mail and destroy all copies of the original message. This email message may be monitored by the Barnstable Police Department.

From: Connolly, Kevin
To: Egnitz, Brian (POL)
Subject: RE: Elsag ALPR / Barnstable MA Police ; 2020 JAG edward-byrne-memorial Grant for Massachusetts Police agencies
Date: Friday, July 24, 2020 9:21:36 AM

I got 2 already thins morning, want to add [redacted]text.com as well, I usually get text and that alerts me to check my email

Kevin A. Connolly
Sergeant
Barnstable Police Department
USSS Electronic Crimes Task Force
508-958-6522
connollyk@barnstablepolice.com

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Friday, July 24, 2020 8:37 AM
To: Connolly, Kevin <connollyk@barnstablepolice.com>
Subject: RE: Elsag ALPR / Barnstable MA Police ; 2020 JAG edward-byrne-memorial Grant for Massachusetts Police agencies

I'm testing a new WMS hotlist workflow and setup your account to get emails. Can you test it out and let me know what you think? Its WMS matched with active registrations. I setup both your readers to relay to your email.

-----Original Message-----
From: Connolly, Kevin [mailto:connollyk@barnstablepolice.com]
Sent: Thursday, July 23, 2020 1:39 PM
To: Egnitz, Brian (POL)
Subject: Re: Elsag ALPR / Barnstable MA Police ; 2020 JAG edward-byrne-memorial Grant for Massachusetts Police agencies

Yes I can.

We have got to get more around town, we had a Great b&e with good side shot of car but no plate. They would have went right by [redacted]. I've had 4 detectives checking addresses in 3 towns last 2 days crossing off possible vehicles. No doubt these things save time/money.

Kevin A. Connolly
Sergeant
Barnstable Police Department
USSS
508-958-6522<tel:508-958-6522>
connollyk@barnstablepolice.com<mailto:connollyk@barnstablepolice.com>
[bpd-patch small]

On Jul 23, 2020, at 12:47 PM, Egnitz, Brian (POL) <brian.egnitz@state.ma.us> wrote:

Thanks, but free market we are always looking for a cheaper and better mouse trap. EOPSS/EOTSS need to get their act together and support open lpr, making data sharing a non-issue. BTW - Bourne is back online and I may have a box for you. I'll know more in a week or so. Can you still get a dataplan?

-----Original Message-----
From: Connolly, Kevin [mailto:connollyk@barnstablepolice.com]
Sent: Thursday, July 23, 2020 12:43 PM
To: Egnitz, Brian (POL)
Subject: Re: Elsag ALPR / Barnstable MA Police ; 2020 JAG edward-byrne-memorial Grant for Massachusetts Police agencies

Not at all, that is just who sent is the heads up. I will NOT buy anything unless we talk to you first. Foolish to buy something that won't work with MSP system.

Kevin A. Connolly
Sergeant
Barnstable Police Department
USSS
508-958-6522<tel:508-958-6522>
connollyk@barnstablepolice.com<mailto:connollyk@barnstablepolice.com>
[bpd-patch small]

On Jul 23, 2020, at 12:38 PM, Egnitz, Brian (POL) <brian.egnitz@state.ma.us> wrote:

Tks, you guys looking to go Elsag? I'm not sure how they will submit to the backend and share data.

From: Connolly, Kevin [mailto:connollyk@barnstablepolice.com]
Sent: Thursday, July 23, 2020 10:28 AM
To: Egnitz, Brian (POL)
Subject: FW: Elsag ALPR / Barnstable MA Police ; 2020 JAG edward-byrne-memorial Grant for Massachusetts Police agencies

Brian,
I don't see the MSP on here, but there is a list of city's that you may be abel to share with. It looks like these funds can be used for ALPR's

Kevin A. Connolly
Sergeant
Barnstable Police Department
USSS Electronic Crimes Task Force
508-958-6522
connollyk@barnstablepolice.com<mailto:connollyk@barnstablepolice.com>

From: Hurwitz, Craig <hurwitzc@barnstablepolice.com>
Sent: Thursday, July 23, 2020 8:33 AM
To: Connolly, Kevin <connollyk@barnstablepolice.com>
Subject: FW: Elsag ALPR / Barnstable MA Police ; 2020 JAG edward-byrne-memorial Grant for Massachusetts Police agencies

_____
From: Ben Miller [ben.miller@leonardocompany-us.com]
Sent: Wednesday, July 22, 2020 3:48 PM
To: Hurwitz, Craig
Subject: Elsag ALPR / Barnstable MA Police ; 2020 JAG edward-byrne-memorial Grant for Massachusetts Police agencies Hi Craig,

Good to catch up with you last week. As discussed, I found a grant that might help with your goal to get a Mobile ALPR system for Barnstable Police ….

If you click on this link from Bureau of Justice https://urldefense.proofpoint.com/v2/url?u=https-3A__bja.ojp.gov_program_jag_fy-2D2020-2Dallocations-2Dand-2Ddisparate-2Dinformation&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=nF3oiRzulLrcME0WA8EOYnD2tlx-8Kssb0278nyA9-w&s=S06RkEFSSJzE8BFB0rFBtHkFEQhVqDi1cAgLM952omM&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__bja.ojp.gov_program_jag_fy-2D2020-2Dallocations-2Dand-2Ddisparate-2Dinformation&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=zYal0qbp2-8p_jJR5qj65DmQRm9xooNTRXV_ZD9cvus&e=> , click on the Massachusetts button and look on this list, you will see that Barnstable is eligible to apply for $15,240.00.

Our attached new MPH M7 system is $11,500 including all hardware and software. We could fully install it for you on one of your vehicles for $1250, so the total cost would be $12,750, well within the eligible grant of $15,240.00

* The Program overview link is : https://urldefense.proofpoint.com/v2/url?u=https-3A__bja.ojp.gov_funding_opportunities_bja-2D2020-2D17276&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=nF3oiRzulLrcME0WA8EOYnD2tlx-8Kssb0278nyA9-w&s=0URU95vtxRgZxAFjcJXMsEEo1j4rie4BCG9MvQl046c&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__bja.ojp.gov_funding_opportunities_bja-2D2020-2D17276&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=1W2-HkI_cz1jsQ3etfDe56uRHgnXuQyhGFluXeNQ6jk&e=>
* RFP: https://urldefense.proofpoint.com/v2/url?u=https-3A__bja.ojp.gov_sites_g_files_xyckuh186_files_media_document_bja-2D2020-2D17276.pdf&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=nF3oiRzulLrcME0WA8EOYnD2tlx-8Kssb0278nyA9-w&s=OesK2QQMHJfDif8U78cIRJirP-80eWpWGOOQ8xKFwyY&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__bja.ojp.gov_sites_g_files_xyckuh186_files_media_document_bja-2D2020-2D17276.pdf&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=fb8ZDct9yj0YL7wRFQkY8ROhfITB-r0mFaaJUTo3fqE&e=>

* I suggest reviewing page 16-17 of RFP – the application checklist

* Deadline: August 19th at 11:59 PM EDT
* Administrative requirements: SAM.gov registration<https://urldefense.proofpoint.com/v2/url?u=https-3A__sam.gov_SAM_pages_public_index.jsf&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=e6dKFPtxucVTAvX0gXxt3c53fH8Vy4V2nzKdl5Ce8Ms&e=>, DUNS number<https://urldefense.proofpoint.com/v2/url?u=https-3A__www.dnb.com_duns-2Dnumber.html&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=wc7Vf9Hi2y1EvIM_A5X7cg-utlW-NIqRPzSaEQ2orJ8&e=>, GMS registration<https://urldefense.proofpoint.com/v2/url?u=https-3A__grants.ojp.usdoj.gov_gmsexternal_&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=T2bnfgMz1eVG6XA-WSxFz4bnW6iVgYd-U-ApHvkl-6I&e=> & SF-424 form<https://urldefense.proofpoint.com/v2/url?u=https-3A__www.ojp.gov_funding_apply_ojp-2Dgrant-2Dapplication-2Dresource-2Dguide-23completeApplication&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=NvE2xAM6-IZSDEkhr4lcxKx1VVKB9mwCbXcSKs2GYU0&e=>
* Category 1 under this solicitation allows for requests under $25,000 and allows for regional and single projects.
* No cost match required.

For this application, you, as a sworn agency, have to fill out the forms on-line directly with BJA OJP, but we can help you if you have questions about it. We also have a grant writing service who can give you direct assistance free of charge if you need that.

Please let me know if this is interesting for you to follow up on.

Best Regards, Ben

Ben Miller
Operations Director New England
Selex ES Inc., a Leonardo Company
ELSAG® ALPR Plate Recognition Technology Proudly Made in the USA
4221 Tudor Lane
Greensboro, North Carolina 27410 USA

ben.miller@leonardocompany-us.com<mailto:ben.miller@leonardocompany-us.com>
Cell: +1 845 [redacted]
www.elsag.com<https://urldefense.proofpoint.com/v2/url?u=http-3A__www.elsag.com_&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=_yNIVENVm0CtK8KY0fqz7R3d84RxEspYO2WuK_5-eMs&e=>

From: Ben Miller
Sent: Tuesday, March 10, 2020 7:44 PM
To: hurwitzc@barnstablepolice.com<mailto:hurwitzc@barnstablepolice.com>
Subject: Elsag ALPR / Barnstable MA Police ; Massachusetts Homeland Security Grant

To : Craig Hurwitz, Director of Information Systems, Barnstable Police Department

Hello Craig,

Good to speak with you today. As discussed, I went searching for a possible Grant for your Department to use for funding of an ALPR Automatic License Plate Recognition system and found this one :

Massachusetts Homeland Security Grant Program State (SHSP) Shared Funds Save Download Grant Tips

Please note: This is an estimated deadline based on the previous year grant schedule. We recommend adding this grant to your alert list to be notified of any release date updates.

Program Area
Criminal Justice & Law Enforcement, Intelligence, Emergency Response & Public Safety, Hazmat & CBRNE Response, Disaster Planning/Assistance, Emergency Management Administering Authority

Massachusetts Executive Office of Public Safety and Security

Funder

State

Administering State

MA

Location

MA

Who Can Apply?

Non-Profit, Institution of Higher Education, State Government

Letter of Intent?

No

Deadline

04/25/2020
Application Deadline

Last Updated

03/04/2020

Summary

Overview: Through this announcement of the Availability of Grant Funds (AGF), the Massachusetts Executive Office of Public Safety and Security (EOPSS) is making a portion of the twenty-percent (20%) state-share of the U.S. Department of Homeland Security (DHS) FFY 2016 Homeland Security Grant Program (HSGP) funding available to eligible applicants. It is anticipated that up to approximately $2.0 million may be made available.

In general, eighty-percent (80%) of the HSGP funding allocated to Massachusetts is distributed to municipalities through the five Regional Homeland Security Advisory Councils. The remaining 20% is used to fund state priorities and administrative costs.
Eligibility: Massachusetts state government agencies and authorities, state institutions of higher education and non-profit organizations that support state homeland security needs and Sheriff's Offices. Municipalities are not eligible to apply for this funding.
Projects funded through this AGF must address:
* at least one capability target in the Massachusetts Threat and Hazard Identification and Risk Assessment (THIRA);
* a capability gap in the 2016 Massachusetts State Preparedness Report (SPR);
* an implementation step in the State Homeland Security Strategy (SHSS); and
* align with a Massachusetts HSGP State Priority.
Links

Please note: This is an estimated deadline based on the previous year grant schedule. We recommend you review the grant guidance and instructions from the previous grant cycle so you can prepare in advance for this grant to open.
Program Link <https://www.mass.gov/how-to/apply-for-a-state-share-grant>

Announcement or Guideline Link <https://www.mass.gov/files/documents/2019/04/22/FFY2019%20State-Share%20NOFO-revised.pdf>
Application Link <https://www.mass.gov/doc/ffy2019-state-share-application/download>
Matching Requirement

No

Program Contact
stateshare.pc@mass.gov<mailto:stateshare.pc@mass.gov>
(617) 933-3529<tel:6179333529>

I called the 617 933 3529 number and left a voicemail for Nick Danald(sp?) of the Homeland Security Grant program this afternoon, but I have a feeling that if you called or emailed from a sworn Massachusetts agency, you might get a quicker response ….

What I believe you would be interested in is a Mobile ALPR system (our MPH (Mobile Plate Hunter) M7 (7th generation) technical data sheet is attached. I would think that Barnstable being situated right in the middle of the Cape with G.L. c. 2G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative) If you have any questions about other deployments that Elsag has with Homeland Security around the country that you want to ask me before you make the enquiry, please call my cell on + 1 845 G.L. c. 4.sec. 7

Best Regards, Ben

Ben Miller
Operations Director New England
Selex ES Inc., a Leonardo Company
ELSAG® ALPR Plate Recognition Technology Proudly Made in the USA
4221 Tudor Lane
Greensboro, North Carolina 27410 USA
ben.miller@elsag.com<mailto:ben.miller@elsag.com>
Cell: +1 845 G.L. c. 4.sec. 7
www.elsag.com<https://urldefense.proofpoint.com/v2/url?u=http-3A__www.elsag.com_&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=_yNIVENVm0CtK8KY0fqz7R3d84RxEspYO2WuK_5-eMs&e=>

The content of this email is confidential and intended for the recipient specified in message only. It is strictly forbidden to share any part of this message with any third party, without a written consent of the sender. If you received this message by mistake, please reply to this message and follow with its deletion, so that we can ensure such a mistake does not occur in the future.

Confidentiality Notice | This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential, proprietary, legally privileged and/or CORI information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient or have received this email in error, immediately contact the sender by reply e-mail and destroy all copies of the original message. This email message may be monitored by the Barnstable Police Department.

Confidentiality Notice | This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential, proprietary, legally privileged and/or CORI information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient or have received this email in error, immediately contact the sender by reply e-mail and destroy all copies of the original message. This email message may be monitored by the Barnstable Police Department.

Confidentiality Notice | This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential, proprietary, legally privileged and/or CORI information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient or have received this email in error, immediately contact the sender by reply e-mail and destroy all copies of the original message. This email message may be monitored by the Barnstable Police Department.
Confidentiality Notice | This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential, proprietary, legally privileged and/or CORI information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient or have received this email in error, immediately contact the sender by reply e-mail and destroy all copies of the original message. This email message may be monitored by the Barnstable Police Department.

From: Egnitz, Brian (POL)
To: Connolly, Kevin
Subject: RE: Elsag ALPR / Barnstable MA Police ; 2020 JAG edward-byrne-memorial Grant for Massachusetts Police agencies
Date: Friday, July 24, 2020 8:36:00 AM

I'm testing a new WMS hotlist workflow and setup your account to get emails. Can you test it out and let me know what you think? Its WMS matched with active registrations. I setup both your readers to relay to your email.

-----Original Message-----
From: Connolly, Kevin [mailto:connollyk@barnstablepolice.com]
Sent: Thursday, July 23, 2020 1:39 PM
To: Egnitz, Brian (POL)
Subject: Re: Elsag ALPR / Barnstable MA Police ; 2020 JAG edward-byrne-memorial Grant for Massachusetts Police agencies

Yes I can.

We have got to get more around town, we had a Great b&e with good side shot of car but no plate. They would have went right by reader on 28 if we had one. I've had 4 detectives checking addresses in 3 towns last 2 days crossing off possible vehicles. No doubt these things save time/money.

Kevin A. Connolly
Sergeant
Barnstable Police Department
USSS
508-958-6522<tel:508-958-6522>
connollyk@barnstablepolice.com<mailto:connollyk@barnstablepolice.com>
[bpd-patch small]

On Jul 23, 2020, at 12:47 PM, Egnitz, Brian (POL) <brian.egnitz@state.ma.us> wrote:

Thanks, but free market we are always looking for a cheaper and better mouse trap. EOPSS/EOTSS need to get their act together and support open lpr, making data sharing a non-issue. BTW - Bourne is back online and I may have a box for you. I'll know more in a week or so. Can you still get a dataplan?

-----Original Message-----
From: Connolly, Kevin [mailto:connollyk@barnstablepolice.com]
Sent: Thursday, July 23, 2020 12:43 PM
To: Egnitz, Brian (POL)
Subject: Re: Elsag ALPR / Barnstable MA Police ; 2020 JAG edward-byrne-memorial Grant for Massachusetts Police agencies

Not at all, that is just who sent is the heads up. I will NOT buy anything unless we talk to you first. Foolish to buy something that won't work with MSP system.

Kevin A. Connolly
Sergeant
Barnstable Police Department
USSS
508-958-6522<tel:508-958-6522>
connollyk@barnstablepolice.com<mailto:connollyk@barnstablepolice.com>
[bpd-patch small]

On Jul 23, 2020, at 12:38 PM, Egnitz, Brian (POL) <brian.egnitz@state.ma.us> wrote:

Tks, you guys looking to go Elsag? I'm not sure how they will submit to the backend and share data.

From: Connolly, Kevin [mailto:connollyk@barnstablepolice.com]
Sent: Thursday, July 23, 2020 10:28 AM
To: Egnitz, Brian (POL)
Subject: FW: Elsag ALPR / Barnstable MA Police ; 2020 JAG edward-byrne-memorial Grant for Massachusetts Police agencies

Brian,
I don't see the MSP on here, but there is a list of city's that you may be abel to share with. It looks like these funds can be used for ALPR's

Kevin A. Connolly
Sergeant
Barnstable Police Department
USSS Electronic Crimes Task Force
508-958-6522
connollyk@barnstablepolice.com<mailto:connollyk@barnstablepolice.com>
<image001.jpg>
<image002.jpg>

From: Hurwitz, Craig <hurwitzc@barnstablepolice.com>
Sent: Thursday, July 23, 2020 8:33 AM
To: Connolly, Kevin <connollyk@barnstablepolice.com>
Subject: FW: Elsag ALPR / Barnstable MA Police ; 2020 JAG edward-byrne-memorial Grant for Massachusetts Police agencies

---

From: Ben Miller [ben.miller@leonardocompany-us.com]

Sent: Wednesday, July 22, 2020 3:48 PM
To: Hurwitz, Craig
Subject: Elsag ALPR / Barnstable MA Police ; 2020 JAG edward-byrne-memorial Grant for Massachusetts Police agencies Hi Craig,

Good to catch up with you last week. As discussed, I found a grant that might help with your goal to get a Mobile ALPR system for Barnstable Police ….

If you click on this link from Bureau of Justice https://urldefense.proofpoint.com/v2/url?u=https-3A__bja.ojp.gov_program_jag_fy-2D2020-2Dallocations-2Dand-2Ddisparate-2Dinformation&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=nF3oiRzulLrcME0WA8EOYnD2tlx-8Kssb0278nyA9-w&s=S06RkEFSSJzE8BFB0rFBtHkFEQhVqDi1cAgLM952omM&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__bja.ojp.gov_program_jag_fy-2D2020-2Dallocations-2Dand-2Ddisparate-2Dinformation&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=zYal0qbp2-8p_jJR5qj65DmQRm9xooNTRXV_ZD9cvus&e=> , click on the Massachusetts button and look on this list, you will see that Barnstable is eligible to apply for $15,240.00.

Our attached new MPH M7 system is $11,500 including all hardware and software. We could fully install it for you on one of your vehicles for $1250, so the total cost would be $12,750, well within the eligible grant of $15,240.00

* The Program overview link is : https://urldefense.proofpoint.com/v2/url?u=https-3A__bja.ojp.gov_funding_opportunities_bja-2D2020-2D17276&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=nF3oiRzulLrcME0WA8EOYnD2tlx-8Kssb0278nyA9-w&s=0URU95vtxRgZxAFjcJXMsEEo1j4rie4BCG9MvQl046c&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__bja.ojp.gov_funding_opportunities_bja-2D2020-2D17276&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=1W2-HkI_cz1jsQ3etfDe56uRHgnXuQyhGFluXeNQ6jk&e=>
* RFP: https://urldefense.proofpoint.com/v2/url?u=https-3A__bja.ojp.gov_sites_g_files_xyckuh186_files_media_document_bja-2D2020-2D17276.pdf&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=nF3oiRzulLrcME0WA8EOYnD2tlx-8Kssb0278nyA9-w&s=OesK2QQMHJfDif8U78cIRJirP-80eWpWGOOQ8xKFwyY&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__bja.ojp.gov_sites_g_files_xyckuh186_files_media_document_bja-2D2020-2D17276.pdf&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=fb8ZDct9yj0YL7wRFQkY8ROhfITB-r0mFaaJUTo3fqE&e=>

* I suggest reviewing page 16-17 of RFP – the application checklist

* Deadline: August 19th at 11:59 PM EDT
* Administrative requirements: SAM.gov registration<https://urldefense.proofpoint.com/v2/url?u=https-3A__sam.gov_SAM_pages_public_index.jsf&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=e6dKFPtxucVTAvX0gXxt3c53fH8Vy4V2nzKdl5Ce8Ms&e=>, DUNS number<https://urldefense.proofpoint.com/v2/url?u=https-3A__www.dnb.com_duns-2Dnumber.html&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=wc7Vf9Hi2y1EvIM_A5X7cg-utlW-NIqRPzSaEQ2orJ8&e=>, GMS registration<https://urldefense.proofpoint.com/v2/url?u=https-3A__grants.ojp.usdoj.gov_gmsexternal_&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=T2bnfgMz1eVG6XA-WSxFz4bnW6iVgYd-U-ApHvkl-6I&e=> & SF-424 form<https://urldefense.proofpoint.com/v2/url?u=https-3A__www.ojp.gov_funding_apply_ojp-2Dgrant-2Dapplication-2Dresource-2Dguide-23completeApplication&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=NvE2xAM6-IZSDEkhr4lcxKx1VVKB9mwCbXcSKs2GYU0&e=>
* Category 1 under this solicitation allows for requests under $25,000 and allows for regional and single projects.
* No cost match required.

For this application, you, as a sworn agency, have to fill out the forms on-line directly with BJA OJP, but we can help you if you have questions about it. We also have a grant writing service who can give you direct assistance free of charge if you need that.

Please let me know if this is interesting for you to follow up on.

Best Regards, Ben

Ben Miller
Operations Director New England
Selex ES Inc., a Leonardo Company
ELSAG® ALPR Plate Recognition Technology Proudly Made in the USA
4221 Tudor Lane
Greensboro, North Carolina 27410 USA
ben.miller@leonardocompany-us.com<mailto:ben.miller@leonardocompany-us.com>
Cell: +1 845 [redacted]
www.elsag.com<https://urldefense.proofpoint.com/v2/url?u=http-3A__www.elsag.com_&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=_yNIVENVm0CtK8KY0fqz7R3d84RxEspYO2WuK_5-eMs&e=>

From: Ben Miller
Sent: Tuesday, March 10, 2020 7:44 PM
To: hurwitzc@barnstablepolice.com<mailto:hurwitzc@barnstablepolice.com>
Subject: Elsag ALPR / Barnstable MA Police ; Massachusetts Homeland Security Grant

To : Craig Hurwitz, Director of Information Systems, Barnstable Police Department

Hello Craig,

Good to speak with you today. As discussed, I went searching for a possible Grant for your Department to use for funding of an ALPR Automatic License Plate Recognition system and found this one :

Massachusetts Homeland Security Grant Program State (SHSP) Shared Funds Save Download Grant Tips

Please note: This is an estimated deadline based on the previous year grant schedule. We recommend adding this grant to your alert list to be notified of any release date updates.

Program Area
Criminal Justice & Law Enforcement, Intelligence, Emergency Response & Public Safety, Hazmat & CBRNE Response, Disaster Planning/Assistance, Emergency Management Administering Authority

Massachusetts Executive Office of Public Safety and Security

Funder

State

Administering State

MA

Location

MA

Who Can Apply?

Non-Profit, Institution of Higher Education, State Government

Letter of Intent?

No

Deadline

04/25/2020
Application Deadline

Last Updated

03/04/2020

Summary

Overview: Through this announcement of the Availability of Grant Funds (AGF), the Massachusetts Executive Office of Public Safety and Security (EOPSS) is making a portion of the twenty-percent (20%) state-share of the U.S. Department of Homeland Security (DHS) FFY 2016 Homeland Security Grant Program (HSGP) funding available to eligible applicants. It is anticipated that up to approximately $2.0 million may be made available.

In general, eighty-percent (80%) of the HSGP funding allocated to Massachusetts is distributed to municipalities through the five Regional Homeland Security Advisory Councils. The remaining 20% is used to fund state priorities and administrative costs.
Eligibility: Massachusetts state government agencies and authorities, state institutions of higher education and non-profit organizations that support state homeland security needs and Sheriff's Offices. Municipalities are not eligible to apply for this funding.
Projects funded through this AGF must address:
* at least one capability target in the Massachusetts Threat and Hazard Identification and Risk Assessment (THIRA);
* a capability gap in the 2016 Massachusetts State Preparedness Report (SPR);
* an implementation step in the State Homeland Security Strategy (SHSS); and
* align with a Massachusetts HSGP State Priority.
Links

Please note: This is an estimated deadline based on the previous year grant schedule. We recommend you review the grant guidance and instructions from the previous grant cycle so you can prepare in advance for this grant to open.
Program Link <https://www.mass.gov/how-to/apply-for-a-state-share-grant>
Announcement or Guideline Link <https://www.mass.gov/files/documents/2019/04/22/FFY2019%20State-Share%20NOFO-revised.pdf>
Application Link <https://www.mass.gov/doc/ffy2019-state-share-application/download>
Matching Requirement

No

Program Contact
stateshare.pc@mass.gov<mailto:stateshare.pc@mass.gov>
(617) 933-3529<tel:6179333529>

I called the 617 933 3529 number and left a voicemail for Nick Danald(sp?) of the Homeland Security Grant program this afternoon, but I have a feeling that if you called or emailed from a sworn Massachusetts agency, you might get a quicker response ….

What I believe you would be interested in is a Mobile ALPR system (our MPH (Mobile Plate Hunter) M7 (7th generation) technical data sheet is attached. I would think that Barnstable being situated right in the middle of the Cape with access G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7 G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7, cl.26(f)(investigat If you have any questions about other deployments that Elsag has with Homeland Security around the country that you want to ask me before you make the enquiry, please call my cell on + 1 845 G.L. c. 4.sec. 7

Best Regards, Ben

Ben Miller
Operations Director New England
Selex ES Inc., a Leonardo Company
ELSAG® ALPR Plate Recognition Technology Proudly Made in the USA
4221 Tudor Lane
Greensboro, North Carolina 27410 USA
ben.miller@elsag.com<mailto:ben.miller@elsag.com>
Cell: +1 845 [redacted]
www.elsag.com<https://urldefense.proofpoint.com/v2/url?u=http-3A__www.elsag.com_&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=_yNIVENVm0CtK8KY0fqz7R3d84RxEspYO2WuK_5-eMs&e=>

The content of this email is confidential and intended for the recipient specified in message only. It is strictly forbidden to share any part of this message with any third party, without a written consent of the sender. If you received this message by mistake, please reply to this message and follow with its deletion, so that we can ensure such a mistake does not occur in the future.

Confidentiality Notice | This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential, proprietary, legally privileged and/or CORI information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient or have received this email in error, immediately contact the sender by reply e-mail and destroy all copies of the original message. This email message may be monitored by the Barnstable Police Department.

Confidentiality Notice | This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential, proprietary, legally privileged and/or CORI information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient or have received this email in error, immediately contact the sender by reply e-mail and destroy all copies of the original message. This email message may be monitored by the Barnstable Police Department.

Confidentiality Notice | This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential, proprietary, legally privileged and/or CORI information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient or have received this email in error, immediately contact the sender by reply e-mail and destroy all copies of the original message. This email message may be monitored by the Barnstable Police Department.

From: Egnitz, Brian (POL)
To: Connolly, Kevin
Subject: RE: Elsag ALPR / Barnstable MA Police ; 2020 JAG edward-byrne-memorial Grant for Massachusetts Police agencies
Date: Thursday, July 23, 2020 12:47:00 PM

Thanks, but free market we are always looking for a cheaper and better mouse trap. EOPSS/EOTSS need to get their act together and support open lpr, making data sharing a non-issue. BTW - Bourne is back online and I may have a box for you. I'll know more in a week or so. Can you still get a dataplan?

-----Original Message-----
From: Connolly, Kevin [mailto:connollyk@barnstablepolice.com]
Sent: Thursday, July 23, 2020 12:43 PM
To: Egnitz, Brian (POL)
Subject: Re: Elsag ALPR / Barnstable MA Police ; 2020 JAG edward-byrne-memorial Grant for Massachusetts Police agencies

Not at all, that is just who sent is the heads up. I will NOT buy anything unless we talk to you first. Foolish to buy something that won't work with MSP system.

Kevin A. Connolly
Sergeant
Barnstable Police Department
USSS
508-958-6522<tel:508-958-6522>
connollyk@barnstablepolice.com<mailto:connollyk@barnstablepolice.com>
[bpd-patch small]

On Jul 23, 2020, at 12:38 PM, Egnitz, Brian (POL) <brian.egnitz@state.ma.us> wrote:

Tks, you guys looking to go Elsag? I'm not sure how they will submit to the backend and share data.

From: Connolly, Kevin [mailto:connollyk@barnstablepolice.com]
Sent: Thursday, July 23, 2020 10:28 AM
To: Egnitz, Brian (POL)
Subject: FW: Elsag ALPR / Barnstable MA Police ; 2020 JAG edward-byrne-memorial Grant for Massachusetts Police agencies

Brian,
I don't see the MSP on here, but there is a list of city's that you may be abel to share with. It looks like these funds can be used for ALPR's

Kevin A. Connolly
Sergeant
Barnstable Police Department
USSS Electronic Crimes Task Force
508-958-6522
connollyk@barnstablepolice.com<mailto:connollyk@barnstablepolice.com>
<image001.jpg>
<image002.jpg>

From: Hurwitz, Craig <hurwitzc@barnstablepolice.com>
Sent: Thursday, July 23, 2020 8:33 AM
To: Connolly, Kevin <connollyk@barnstablepolice.com>
Subject: FW: Elsag ALPR / Barnstable MA Police ; 2020 JAG edward-byrne-memorial Grant for Massachusetts Police agencies

---

From: Ben Miller [ben.miller@leonardocompany-us.com]
Sent: Wednesday, July 22, 2020 3:48 PM
To: Hurwitz, Craig
Subject: Elsag ALPR / Barnstable MA Police ; 2020 JAG edward-byrne-memorial Grant for Massachusetts Police agencies Hi Craig,

Good to catch up with you last week. As discussed, I found a grant that might help with your goal to get a Mobile ALPR system for Barnstable Police ….

If you click on this link from Bureau of Justice https://urldefense.proofpoint.com/v2/url?u=https-3A__bja.ojp.gov_program_jag_fy-2D2020-2Dallocations-2Dand-2Ddisparate-2Dinformation&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=nF3oiRzulLrcME0WA8EOYnD2tlx-8Kssb0278nyA9-w&s=S06RkEFSSJzE8BFB0rFBtHkFEQhVqDi1cAgLM952omM&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__bja.ojp.gov_program_jag_fy-2D2020-2Dallocations-2Dand-2Ddisparate-2Dinformation&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=zYal0qbp2-8p_jJR5qj65DmQRm9xooNTRXV_ZD9cvus&e=> , click on the Massachusetts button and look on this list, you will see that Barnstable is eligible to apply for $15,240.00.

Our attached new MPH M7 system is $11,500 including all hardware and software. We could fully install it for you on one of your vehicles for $1250, so the total cost would be $12,750, well within the eligible grant of $15,240.00

* The Program overview link is : https://urldefense.proofpoint.com/v2/url?u=https-3A__bja.ojp.gov_funding_opportunities_bja-2D2020-2D17276&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=nF3oiRzulLrcME0WA8EOYnD2tlx-8Kssb0278nyA9-w&s=0URU95vtxRgZxAFjcJXMsEEo1j4rie4BCG9MvQl046c&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__bja.ojp.gov_funding_opportunities_bja-2D2020-2D17276&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=1W2-HkI_cz1jsQ3etfDe56uRHgnXuQyhGFluXeNQ6jk&e=>

* RFP: https://urldefense.proofpoint.com/v2/url?u=https-3A__bja.ojp.gov_sites_g_files_xyckuh186_files_media_document_bja-2D2020-2D17276.pdf&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=nF3oiRzulLrcME0WA8EOYnD2tlx-8Kssb0278nyA9-w&s=OesK2QQMHJfDif8U78cIRJirP-80eWpWGOOQ8xKFwyY&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__bja.ojp.gov_sites_g_files_xyckuh186_files_media_document_bja-2D2020-2D17276.pdf&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=fb8ZDct9yj0YL7wRFQkY8ROhfITB-r0mFaaJUTo3fqE&e=>

* I suggest reviewing page 16-17 of RFP – the application checklist

* Deadline: August 19th at 11:59 PM EDT
* Administrative requirements: SAM.gov registration<https://urldefense.proofpoint.com/v2/url?u=https-3A__sam.gov_SAM_pages_public_index.jsf&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=e6dKFPtxucVTAvX0gXxt3c53fH8Vy4V2nzKdl5Ce8Ms&e=>, DUNS number<https://urldefense.proofpoint.com/v2/url?u=https-3A__www.dnb.com_duns-2Dnumber.html&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=wc7Vf9Hi2y1EvIM_A5X7cg-utlW-NIqRPzSaEQ2orJ8&e=>, GMS registration<https://urldefense.proofpoint.com/v2/url?u=https-3A__grants.ojp.usdoj.gov_gmsexternal_&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=T2bnfgMz1eVG6XA-WSxFz4bnW6iVgYd-U-ApHvkl-6I&e=> & SF-424 form<https://urldefense.proofpoint.com/v2/url?u=https-3A__www.ojp.gov_funding_apply_ojp-2Dgrant-2Dapplication-2Dresource-2Dguide-23completeApplication&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=NvE2xAM6-IZSDEkhr4lcxKx1VVKB9mwCbXcSKs2GYU0&e=>
* Category 1 under this solicitation allows for requests under $25,000 and allows for regional and single projects.
* No cost match required.

For this application, you, as a sworn agency, have to fill out the forms on-line directly with BJA OJP, but we can help you if you have questions about it. We also have a grant writing service who can give you direct assistance free of charge if you need that.

Please let me know if this is interesting for you to follow up on.

Best Regards, Ben

Ben Miller
Operations Director New England
Selex ES Inc., a Leonardo Company
ELSAG® ALPR Plate Recognition Technology Proudly Made in the USA
4221 Tudor Lane
Greensboro, North Carolina 27410 USA
ben.miller@leonardocompany-us.com<mailto:ben.miller@leonardocompany-us.com>
Cell: +1 845[redacted]
www.elsag.com<https://urldefense.proofpoint.com/v2/url?u=http-3A__www.elsag.com_&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=_yNIVENVm0CtK8KY0fqz7R3d84RxEspYO2WuK_5-eMs&e=>

From: Ben Miller
Sent: Tuesday, March 10, 2020 7:44 PM
To: hurwitzc@barnstablepolice.com<mailto:hurwitzc@barnstablepolice.com>
Subject: Elsag ALPR / Barnstable MA Police ; Massachusetts Homeland Security Grant

To : Craig Hurwitz, Director of Information Systems, Barnstable Police Department

Hello Craig,

Good to speak with you today. As discussed, I went searching for a possible Grant for your Department to use for funding of an ALPR Automatic License Plate Recognition system and found this one :

Massachusetts Homeland Security Grant Program State (SHSP) Shared Funds Save Download Grant Tips

Please note: This is an estimated deadline based on the previous year grant schedule. We recommend adding this grant to your alert list to be notified of any release date updates.

Program Area
Criminal Justice & Law Enforcement, Intelligence, Emergency Response & Public Safety, Hazmat & CBRNE Response, Disaster Planning/Assistance, Emergency Management Administering Authority

Massachusetts Executive Office of Public Safety and Security

Funder

State

Administering State

MA

Location

MA

Who Can Apply?

Non-Profit, Institution of Higher Education, State Government

Letter of Intent?

No

Deadline

04/25/2020
Application Deadline

Last Updated

03/04/2020

Summary

Overview: Through this announcement of the Availability of Grant Funds (AGF), the Massachusetts Executive Office of Public Safety and Security (EOPSS) is making a portion of the twenty-percent (20%) state-share of the U.S. Department of Homeland Security (DHS) FFY 2016 Homeland Security Grant Program (HSGP) funding available to eligible applicants. It is anticipated that up to approximately $2.0 million may be made available.

In general, eighty-percent (80%) of the HSGP funding allocated to Massachusetts is distributed to municipalities through the five Regional Homeland Security Advisory Councils. The remaining 20% is used to fund state priorities and administrative costs.
Eligibility: Massachusetts state government agencies and authorities, state institutions of higher education and non-profit organizations that support state homeland security needs and Sheriff's Offices. Municipalities are not eligible to apply for this funding.
Projects funded through this AGF must address:
* at least one capability target in the Massachusetts Threat and Hazard Identification and Risk Assessment (THIRA);
* a capability gap in the 2016 Massachusetts State Preparedness Report (SPR);
* an implementation step in the State Homeland Security Strategy (SHSS); and
* align with a Massachusetts HSGP State Priority.
Links

Please note: This is an estimated deadline based on the previous year grant schedule. We recommend you review the grant guidance and instructions from the previous grant cycle so you can prepare in advance for this grant to open.
Program Link <https://www.mass.gov/how-to/apply-for-a-state-share-grant>
Announcement or Guideline Link <https://www.mass.gov/files/documents/2019/04/22/FFY2019%20State-Share%20NOFO-revised.pdf>
Application Link <https://www.mass.gov/doc/ffy2019-state-share-application/download>
Matching Requirement

No

Program Contact
stateshare.pc@mass.gov<mailto:stateshare.pc@mass.gov>
(617) 933-3529<tel:6179333529>

I called the 617 933 3529 number and left a voicemail for Nick Danald(sp?) of the Homeland Security Grant program this afternoon, but I have a feeling that if you called or emailed from a sworn Massachusetts agency, you might get a quicker response ….

What I believe you would be interested in is a Mobile ALPR system (our MPH (Mobile Plate Hunter) M7 (7th generation) technical data sheet is attached. I would think that Barnstable being situated right in the middle of the Cape with access to G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative) If you have any questions about other deployments that Elsag has with Homeland Security around the country that you want to ask me before you make the enquiry, please call my cell on + 1 845 G.L. c. 4.sec. 7

Best Regards, Ben

Ben Miller
Operations Director New England
Selex ES Inc., a Leonardo Company
ELSAG® ALPR Plate Recognition Technology Proudly Made in the USA
4221 Tudor Lane
Greensboro, North Carolina 27410 USA
ben.miller@elsag.com<mailto:ben.miller@elsag.com>
Cell: +1 845 G.L. c. 4.sec. 7
www.elsag.com<https://urldefense.proofpoint.com/v2/url?u=http-3A__www.elsag.com_&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=_yNIVENVm0CtK8KY0fqz7R3d84RxEspYO2WuK_5-eMs&e=>

The content of this email is confidential and intended for the recipient specified in message only. It is strictly forbidden to share any part of this message with any third party, without a written consent of the sender. If you received this message by mistake, please reply to this message and follow with its deletion, so that we can ensure such a mistake does not occur in the future.

Confidentiality Notice | This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential, proprietary, legally

privileged and/or CORI information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient or have received this email in error, immediately contact the sender by reply e-mail and destroy all copies of the original message. This email message may be monitored by the Barnstable Police Department.

Confidentiality Notice | This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential, proprietary, legally privileged and/or CORI information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient or have received this email in error, immediately contact the sender by reply e-mail and destroy all copies of the original message. This email message may be monitored by the Barnstable Police Department.

From:	Egnitz, Brian (POL)
To:	Connolly, Kevin
Subject:	RE: Elsag ALPR / Barnstable MA Police ; 2020 JAG edward-byrne-memorial Grant for Massachusetts Police agencies
Date:	Thursday, July 23, 2020 12:37:00 PM

Tks, you guys looking to go Elsag? I'm not sure how they will submit to the backend and share data.

From: Connolly, Kevin [mailto:connollyk@barnstablepolice.com]
Sent: Thursday, July 23, 2020 10:28 AM
To: Egnitz, Brian (POL)
Subject: FW: Elsag ALPR / Barnstable MA Police ; 2020 JAG edward-byrne-memorial Grant for Massachusetts Police agencies

Brian,

I don't see the MSP on here, but there is a list of city's that you may be abel to share with. It looks like these funds can be used for ALPR's

Kevin A. Connolly
Sergeant
Barnstable Police Department
USSS Electronic Crimes Task Force
508-958-6522
connollyk@barnstablepolice.com

From: Hurwitz, Craig <hurwitzc@barnstablepolice.com>
Sent: Thursday, July 23, 2020 8:33 AM
To: Connolly, Kevin <connollyk@barnstablepolice.com>
Subject: FW: Elsag ALPR / Barnstable MA Police ; 2020 JAG edward-byrne-memorial Grant for Massachusetts Police agencies

---

From: Ben Miller [ben.miller@leonardocompany-us.com]
Sent: Wednesday, July 22, 2020 3:48 PM
To: Hurwitz, Craig
Subject: Elsag ALPR / Barnstable MA Police ; 2020 JAG edward-byrne-memorial Grant for Massachusetts Police agencies

Hi Craig,

Good to catch up with you last week. As discussed, I found a grant that might help with your goal to get a Mobile ALPR system for Barnstable Police ….

If you click on this link from Bureau of Justice https://bja.ojp.gov/program/jag/fy-2020-allocations-and-disparate-information , click on the Massachusetts button and look on this list, you will see that Barnstable is eligible to apply for $15,240.00.

Our attached new MPH M7 system is $11,500 including all hardware and software. We could fully install it for you on one of your vehicles for $1250, so the total cost would be $12,750, well within the eligible grant of $15,240.00

- The Program overview link is : https://bja.ojp.gov/funding/opportunities/bja-2020-17276
- RFP: https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/bja-2020-17276.pdf
    - I suggest reviewing page 16-17 of RFP – the application checklist
- Deadline: **August 19th** at 11:59 PM EDT
- Administrative requirements: SAM.gov registration, DUNS number, GMS registration & SF-424 form
- Category 1 under this solicitation allows for requests under $25,000 and allows for regional and single projects.
- No cost match required.

For this application, you, as a sworn agency, have to fill out the forms on-line directly with BJA OJP, but we can help you if you have questions about it. We also have a grant writing service who can give you direct assistance free of charge if you need that.

Please let me know if this is interesting for you to follow up on.

Best Regards, Ben

Ben Miller
Operations Director New England
Selex ES Inc., a Leonardo Company
ELSAG® ALPR Plate Recognition Technology
Proudly Made in the USA
4221 Tudor Lane
Greensboro, North Carolina 27410 USA
ben.miller@leonardocompany-us.com
Cell: +1 845 [redacted]
www.elsag.com

From: Ben Miller
Sent: Tuesday, March 10, 2020 7:44 PM

To: hurwitzc@barnstablepolice.com
Subject: Elsag ALPR / Barnstable MA Police ; Massachusetts Homeland Security Grant

To : Craig Hurwitz, Director of Information Systems, Barnstable Police Department

Hello Craig,

Good to speak with you today. As discussed, I went searching for a possible Grant for your Department to use for funding of an ALPR Automatic License Plate Recognition system and found this one :

Massachusetts Homeland Security Grant Program State (SHSP) Shared Funds

Save Download Grant Tips

Please note: This is an estimated deadline based on the previous year grant schedule. We recommend adding this grant to your alert list to be notified of any release date updates.

Program Area

Criminal Justice & Law Enforcement, Intelligence, Emergency Response & Public Safety, Hazmat & CBRNE Response, Disaster Planning/Assistance, Emergency Management

Administering Authority

Massachusetts Executive Office of Public Safety and Security

Funder

State

Administering State

MA

Location

MA

Who Can Apply?

Non-Profit, Institution of Higher Education, State Government

Letter of Intent?

No

Deadline

04/25/2020
Application Deadline

Last Updated

03/04/2020

Summary

Overview: Through this announcement of the Availability of Grant Funds (AGF), the Massachusetts Executive Office of Public Safety and Security (EOPSS) is making a portion of the twenty-percent (20%) state-share of the U.S. Department of Homeland Security (DHS) FFY 2016 Homeland Security Grant Program (HSGP) funding available to eligible applicants. It is anticipated that up to approximately $2.0 million may be made available.

In general, eighty-percent (80%) of the HSGP funding allocated to Massachusetts is distributed to municipalities through the five Regional Homeland Security Advisory Councils. The remaining 20% is used to fund state priorities and administrative costs.

Eligibility: Massachusetts state government agencies and authorities, state institutions of higher education and non-profit organizations that support state homeland security needs and Sheriff's Offices. Municipalities are not eligible to apply for this funding.

Projects funded through this AGF must address:
* at least one capability target in the Massachusetts Threat and Hazard Identification and Risk Assessment (THIRA);
* a capability gap in the 2016 Massachusetts State Preparedness Report (SPR);
* an implementation step in the State Homeland Security Strategy (SHSS); and
* align with a Massachusetts HSGP State Priority.

Links

Please note: This is an estimated deadline based on the previous year grant schedule. We recommend you review the grant guidance and instructions from the previous grant cycle so you can prepare in advance for this grant to open.

Program Link
Announcement or Guideline Link
Application Link

Matching Requirement

No

Program Contact

stateshare.pc@mass.gov
(617) 933-3529

I called the 617 933 3529 number and left a voicemail for Nick Danald(sp?) of the Homeland Security Grant program this afternoon, but I have a feeling that if you called or emailed from a sworn Massachusetts agency, you might get a quicker response ….

What I believe you would be interested in is a Mobile ALPR system (our MPH (Mobile Plate Hunter) M7 (7th generation) technical data sheet is attached. I would think that Barnstable being situated right in the middle of the Cape with access to G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative) [redacted] If you have any questions about other deployments that Elsag has with Homeland Security around the country that you want to ask me before you make the enquiry, please call my cell on + 1 845 [redacted]

Best Regards, Ben

Ben Miller
Operations Director New England
Selex ES Inc., a Leonardo Company
ELSAG® ALPR Plate Recognition Technology
Proudly Made in the USA
4221 Tudor Lane
Greensboro, North Carolina 27410 USA
ben.miller@elsag.com
Cell: +1 845 [redacted]
www.elsag.com

The content of this email is confidential and intended for the recipient specified in message only. It is strictly forbidden to share any part of this message with any third party, without a written consent of the sender. If you received this message by mistake, please reply to this message and follow with its deletion, so that we can ensure such a mistake does not occur in the future.

Confidentiality Notice | This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential, proprietary, legally privileged and/or CORI information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient or have received this email in error, immediately contact the sender by reply e-mail and destroy all copies of the original message. This email message may be monitored by the Barnstable Police Department.

From: Egnitz, Brian (POL)
To: Connolly, Kevin
Subject: RE: Elsag ALPR / Barnstable MA Police ; 2020 JAG edward-byrne-memorial Grant for Massachusetts Police agencies
Date: Tuesday, July 28, 2020 9:20:00 AM

I've added the cell

-----Original Message-----
From: Connolly, Kevin [mailto:connollyk@barnstablepolice.com]
Sent: Friday, July 24, 2020 9:27 AM
To: Egnitz, Brian (POL)
Subject: RE: Elsag ALPR / Barnstable MA Police ; 2020 JAG edward-byrne-memorial Grant for Massachusetts Police agencies

Great, I'll see how it is and talk to you monday

Kevin A. Connolly
Sergeant
Barnstable Police Department
USSS Electronic Crimes Task Force
508-958-6522
connollyk@barnstablepolice.com

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Friday, July 24, 2020 9:25 AM
To: Connolly, Kevin <connollyk@barnstablepolice.com>
Subject: Re: Elsag ALPR / Barnstable MA Police ; 2020 JAG edward-byrne-memorial Grant for Massachusetts Police agencies

I can do it Monday, let's see how many we get so we don't know up your phone. VIP The email account t if you have an iPhone and it will act the same as text. You'll also get RMV stuff (not insurance violations) and Northern NCIS.

> On Jul 24, 2020, at 9:21 AM, Connolly, Kevin <connollyk@barnstablepolice.com> wrote:
>
> I got 2 already thins morning, want to add 5089586522@vtext.com as
> well, I usually get text and that alerts me to check my email
>
>
> Kevin A. Connolly
> Sergeant
> Barnstable Police Department
> USSS Electronic Crimes Task Force
> 508-958-6522
> connollyk@barnstablepolice.com
>
>
>
> -----Original Message-----
> From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
> Sent: Friday, July 24, 2020 8:37 AM
> To: Connolly, Kevin <connollyk@barnstablepolice.com>
> Subject: RE: Elsag ALPR / Barnstable MA Police ; 2020 JAG
> edward-byrne-memorial Grant for Massachusetts Police agencies
>
> I'm testing a new WMS hotlist workflow and setup your account to get emails. Can you test it out and let me know what you think? Its WMS matched with active registrations. I setup both your readers to relay to your email.
>
> -----Original Message-----
> From: Connolly, Kevin [mailto:connollyk@barnstablepolice.com]
> Sent: Thursday, July 23, 2020 1:39 PM
> To: Egnitz, Brian (POL)
> Subject: Re: Elsag ALPR / Barnstable MA Police ; 2020 JAG
> edward-byrne-memorial Grant for Massachusetts Police agencies
>
> Yes I can.
>
> We have got to get more around town, we had a Great b&e with good side shot of car but no plate. They would have went right by reader on 28 if we had one. I've had 4 detectives checking addresses in 3 towns last 2 days crossing off possible vehicles. No doubt these things save time/money.
>
> Kevin A. Connolly
> Sergeant
> Barnstable Police Department
> USSS
> 508-958-6522<tel:508-958-6522>
> connollyk@barnstablepolice.com<mailto:connollyk@barnstablepolice.com>
> [bpd-patch small]
>
>
> On Jul 23, 2020, at 12:47 PM, Egnitz, Brian (POL) <brian.egnitz@state.ma.us> wrote:
>

> Thanks, but free market we are always looking for a cheaper and better mouse trap. EOPSS/EOTSS need to get their act together and support open lpr, making data sharing a non-issue. BTW - Bourne is back online and I may have a box for you. I'll know more in a week or so. Can you still get a dataplan?
>
> -----Original Message-----
> From: Connolly, Kevin [mailto:connollyk@barnstablepolice.com]
> Sent: Thursday, July 23, 2020 12:43 PM
> To: Egnitz, Brian (POL)
> Subject: Re: Elsag ALPR / Barnstable MA Police ; 2020 JAG
> edward-byrne-memorial Grant for Massachusetts Police agencies
>
> Not at all, that is just who sent is the heads up. I will NOT buy anything unless we talk to you first. Foolish to buy something that won't work with MSP system.
>
> Kevin A. Connolly
> Sergeant
> Barnstable Police Department
> USSS
> 508-958-6522<tel:508-958-6522>
> connollyk@barnstablepolice.com<mailto:connollyk@barnstablepolice.com>
> [bpd-patch small]
>
>
> On Jul 23, 2020, at 12:38 PM, Egnitz, Brian (POL) <brian.egnitz@state.ma.us> wrote:
>
>
> Tks, you guys looking to go Elsag? I'm not sure how they will submit to the backend and share data.
>
> From: Connolly, Kevin [mailto:connollyk@barnstablepolice.com]
> Sent: Thursday, July 23, 2020 10:28 AM
> To: Egnitz, Brian (POL)
> Subject: FW: Elsag ALPR / Barnstable MA Police ; 2020 JAG
> edward-byrne-memorial Grant for Massachusetts Police agencies
>
> Brian,
> I don't see the MSP on here, but there is a list of city's
> that you may be abel to share with. It looks like these funds can be
> used for ALPR's
>
> Kevin A. Connolly
> Sergeant
> Barnstable Police Department
> USSS Electronic Crimes Task Force
> 508-958-6522
> connollyk@barnstablepolice.com<mailto:connollyk@barnstablepolice.com>
> <image001.jpg>
> <image002.jpg>
>
>
> From: Hurwitz, Craig <hurwitzc@barnstablepolice.com>
> Sent: Thursday, July 23, 2020 8:33 AM
> To: Connolly, Kevin <connollyk@barnstablepolice.com>
> Subject: FW: Elsag ALPR / Barnstable MA Police ; 2020 JAG
> edward-byrne-memorial Grant for Massachusetts Police agencies
>
>
> _____
> From: Ben Miller [ben.miller@leonardocompany-us.com]
> Sent: Wednesday, July 22, 2020 3:48 PM
> To: Hurwitz, Craig
> Subject: Elsag ALPR / Barnstable MA Police ; 2020 JAG
> edward-byrne-memorial Grant for Massachusetts Police agencies Hi
> Craig,
>
> Good to catch up with you last week. As discussed, I found a grant that might help with your goal to get a Mobile ALPR system for Barnstable Police ….
>
> If you click on this link from Bureau of Justice https://urldefense.proofpoint.com/v2/url?u=https-3A__bja.ojp.gov_program_jag_fy-2D2020-2Dallocations-2Dand-2Ddisparate-2Dinformation&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=nF3oiRzulLrcME0WA8EOYnD2tlx-8Kssb0278nyA9-w&s=S06RkEFSSJzE8BFB0rFBtHkFEQhVqDi1cAgLM952omM&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__bja.ojp.gov_program_jag_fy-2D2020-2Dallocations-2Dand-2Ddisparate-2Dinformation&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=zYal0qbp2-8p_jJR5qj65DmQRm9xooNTRXV_ZD9cvus&e=> , click on the Massachusetts button and look on this list, you will see that Barnstable is eligible to apply for $15,240.00.
>
> Our attached new MPH M7 system is $11,500 including all hardware and
> software. We could fully install it for you on one of your vehicles
> for $1250, so the total cost would be $12,750, well within the
> eligible grant of $15,240.00
>
>
> * The Program overview link is : https://urldefense.proofpoint.com/v2/url?u=https-3A__bja.ojp.gov_funding_opportunities_bja-2D2020-2D17276&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=nF3oiRzulLrcME0WA8EOYnD2tlx-8Kssb0278nyA9-w&s=0URU95vtxRgZxAFjcJXMsEEo1j4rie4BCG9MvQl046c&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__bja.ojp.gov_funding_opportunities_bja-2D2020-2D17276&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-

fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=1W2-HkI_cz1jsQ3etfDe56uRHgnXuQyhGFluXeNQ6jk&e=>
> * RFP: https://urldefense.proofpoint.com/v2/url?u=https-3A__bja.ojp.gov_sites_g_files_xyckuh186_files_media_document_bja-2D2020-2D17276.pdf&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=nF3oiRzulLrcME0WA8EOYnD2tlx-8Kssb0278nyA9-w&s=OesK2QQMHJfDif8U78cIRJirP-80eWpWGOOQ8xKFwyY&e=
<https://urldefense.proofpoint.com/v2/url?u=https-3A__bja.ojp.gov_sites_g_files_xyckuh186_files_media_document_bja-2D2020-2D17276.pdf&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=fb8ZDct9yj0YL7wRFQkY8ROhfITB-r0mFaaJUTo3fqE&e=>
>
> * I suggest reviewing page 16-17 of RFP – the application checklist
>
> * Deadline: August 19th at 11:59 PM EDT
> * Administrative requirements: SAM.gov registration<https://urldefense.proofpoint.com/v2/url?u=https-3A__sam.gov_SAM_pages_public_index.jsf&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=e6dKFPtxucVTAvX0gXxt3c53fH8Vy4V2nzKdl5Ce8Ms&e=>, DUNS number<https://urldefense.proofpoint.com/v2/url?u=https-3A__www.dnb.com_duns-2Dnumber.html&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=wc7Vf9Hi2y1EvIM_A5X7cg-utlW-NIqRPzSaEQ2orJ8&e=>, GMS registration<https://urldefense.proofpoint.com/v2/url?u=https-3A__grants.ojp.usdoj.gov_gmsexternal_&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=T2bnfgMz1eVG6XA-WSxFz4bnW6iVgYd-U-ApHvkl-6I&e=> & SF-424 form<https://urldefense.proofpoint.com/v2/url?u=https-3A__www.ojp.gov_funding_apply_ojp-2Dgrant-2Dapplication-2Dresource-2Dguide-23completeApplication&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikBh_wo2MFBsZE8SsyzY&s=NvE2xAM6-IZSDEkhr4lcxKx1VVKB9mwCbXcSKs2GYU0&e=>
> * Category 1 under this solicitation allows for requests under $25,000 and allows for regional and single projects.
> * No cost match required.
>
> For this application, you, as a sworn agency, have to fill out the forms on-line directly with BJA OJP, but we can help you if you have questions about it. We also have a grant writing service who can give you direct assistance free of charge if you need that.
>
> Please let me know if this is interesting for you to follow up on.
>
> Best Regards, Ben
>
> Ben Miller
> Operations Director New England
> Selex ES Inc., a Leonardo Company
> ELSAG® ALPR Plate Recognition Technology Proudly Made in the USA
> 4221 Tudor Lane
> Greensboro, North Carolina 27410 USA
> ben.miller@leonardocompany-us.com<mailto:ben.miller@leonardocompany-us
> .com>
> Cell: +1 845 [redacted]
> www.elsag.com<https://urldefense.proofpoint.com/v2/url?u=http-3A__www.
> elsag.com_&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hN
> TkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikB
> h_wo2MFBsZE8SsyzY&s=_yNIVENVm0CtK8KY0fqz7R3d84RxEspYO2WuK_5-eMs&e=>
>
>
>
>
>
> From: Ben Miller
> Sent: Tuesday, March 10, 2020 7:44 PM
> To:
> hurwitzc@barnstablepolice.com<mailto:hurwitzc@barnstablepolice.com>
> Subject: Elsag ALPR / Barnstable MA Police ; Massachusetts Homeland
> Security Grant
>
> To : Craig Hurwitz, Director of Information Systems, Barnstable
> Police Department
>
> Hello Craig,
>
> Good to speak with you today. As discussed, I went searching for a possible Grant for your Department to use for funding of an ALPR Automatic License Plate Recognition system and found this one :
>
> Massachusetts Homeland Security Grant Program State (SHSP) Shared
> Funds Save Download Grant Tips
>
> Please note: This is an estimated deadline based on the previous year grant schedule. We recommend adding this grant to your alert list to be notified of any release date updates.
>
> Program Area
> Criminal Justice & Law Enforcement, Intelligence, Emergency Response &
> Public Safety, Hazmat & CBRNE Response, Disaster Planning/Assistance,
> Emergency Management Administering Authority
>
> Massachusetts Executive Office of Public Safety and Security
>
> Funder

>
> State
>
> Administering State
>
> MA
>
> Location
>
> MA
>
> Who Can Apply?
>
> Non-Profit, Institution of Higher Education, State Government
>
> Letter of Intent?
>
> No
>
> Deadline
>
> 04/25/2020
> Application Deadline
>
> Last Updated
>
> 03/04/2020
>
> Summary
>
> Overview: Through this announcement of the Availability of Grant Funds (AGF), the Massachusetts Executive Office of Public Safety and Security (EOPSS) is making a portion of the twenty-percent (20%) state-share of the U.S. Department of Homeland Security (DHS) FFY 2016 Homeland Security Grant Program (HSGP) funding available to eligible applicants. It is anticipated that up to approximately $2.0 million may be made available.
>
> In general, eighty-percent (80%) of the HSGP funding allocated to Massachusetts is distributed to municipalities through the five Regional Homeland Security Advisory Councils. The remaining 20% is used to fund state priorities and administrative costs.
> Eligibility: Massachusetts state government agencies and authorities, state institutions of higher education and non-profit organizations that support state homeland security needs and Sheriff's Offices. Municipalities are not eligible to apply for this funding.
> Projects funded through this AGF must address:
> * at least one capability target in the Massachusetts Threat and
> Hazard Identification and Risk Assessment (THIRA);
> * a capability gap in the 2016 Massachusetts State Preparedness Report
> (SPR);
> * an implementation step in the State Homeland Security Strategy
> (SHSS); and
> * align with a Massachusetts HSGP State Priority.
> Links
>
> Please note: This is an estimated deadline based on the previous year grant schedule. We recommend you review the grant guidance and instructions from the previous grant cycle so you can prepare in advance for this grant to open.
> Program Link
> <https://www.mass.gov/how-to/apply-for-a-state-share-grant>
> Announcement or Guideline Link
> <https://www.mass.gov/files/documents/2019/04/22/FFY2019%20State-Share
> %20NOFO-revised.pdf> Application Link
> <https://www.mass.gov/doc/ffy2019-state-share-application/download>
> Matching Requirement
>
> No
>
> Program Contact
> stateshare.pc@mass.gov<mailto:stateshare.pc@mass.gov>
> (617) 933-3529<tel:6179333529>
>
>
> I called the 617 933 3529 number and left a voicemail for Nick Danald(sp?) of the Homeland Security Grant program this afternoon, but I have a feeling that if you called or emailed from a sworn Massachusetts agency, you might get a quicker response ….
>
> What I believe you would be interested in is a Mobile ALPR system (our MPH (Mobile Plate Hunter) M7 (7th generation) technical data sheet is attached. I would think that Barnstable being situated right in the middle of the Cape with access to G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative) If you have any questions about other deployments that Elsag has with Homeland Security around the country that you want to ask me before you make the enquiry, please call my cell on + 1 845 G.L. c. 4.sec. 7
>
> Best Regards, Ben
>
> Ben Miller
> Operations Director New England
> Selex ES Inc., a Leonardo Company
> ELSAG® ALPR Plate Recognition Technology Proudly Made in the USA
> 4221 Tudor Lane
> Greensboro, North Carolina 27410 USA
> ben.miller@elsag.com<mailto:ben.miller@elsag.com>
> Cell: +1 845 G.L. c. 4.sec. 7

> www.elsag.com<https://urldefense.proofpoint.com/v2/url?u=http-3A__www.
> elsag.com_&d=DwMFAg&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hN
> TkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=oQvnXYpsTMAHiOFEUyG7Ml1ikB
> h_wo2MFBsZE8SsyzY&s=_yNIVENVm0CtK8KY0fqz7R3d84RxEspYO2WuK_5-eMs&e=>
>
>
>
> The content of this email is confidential and intended for the recipient specified in message only. It is strictly forbidden to share any part of this message with any third party, without a written consent of the sender. If you received this message by mistake, please reply to this message and follow with its deletion, so that we can ensure such a mistake does not occur in the future.
>
>
>
> Confidentiality Notice | This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential, proprietary, legally privileged and/or CORI information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient or have received this email in error, immediately contact the sender by reply e-mail and destroy all copies of the original message. This email message may be monitored by the Barnstable Police Department.
>
> Confidentiality Notice | This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential, proprietary, legally privileged and/or CORI information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient or have received this email in error, immediately contact the sender by reply e-mail and destroy all copies of the original message. This email message may be monitored by the Barnstable Police Department.
>
> Confidentiality Notice | This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential, proprietary, legally privileged and/or CORI information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient or have received this email in error, immediately contact the sender by reply e-mail and destroy all copies of the original message. This email message may be monitored by the Barnstable Police Department.
> Confidentiality Notice | This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential, proprietary, legally privileged and/or CORI information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient or have received this email in error, immediately contact the sender by reply e-mail and destroy all copies of the original message. This email message may be monitored by the Barnstable Police Department.
Confidentiality Notice | This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential, proprietary, legally privileged and/or CORI information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient or have received this email in error, immediately contact the sender by reply e-mail and destroy all copies of the original message. This email message may be monitored by the Barnstable Police Department.

From: brian.egnitz@pol.state.ma.us
To: Griffin, Robert
Subject: Re: Flock LPRs to State DB
Date: Tuesday, October 20, 2020 9:17:20 AM

Hi Ron,

Can you check to see if your vendor has an adapter to Rekor's open ALPR?

Tks, Brian

> On Jul 7, 2020, at 5:19 PM, Griffin, Robert <rgriffin@chelseama.gov> wrote:
>
> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>
> Brian,
>
> Last time we spoke, I know you were involved with the LPRs. We just went live with G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative) Quincy. At a minimum, I'd like to give you access. But I would also like to work with the state police and see if we can use Flock's API somehow to transfer the data to the State's LPR database. I believe you guys are still using PIPS?
>
> Rob
> 617-438-7331

From: Egnitz, Brian (POL)
To: Griffin, Robert
Subject: Re: Flock LPRs to State DB
Date: Tuesday, October 20, 2020 9:17:21 AM

Hi Ron,

Can you check to see if your vendor has an adapter to Rekor's open ALPR?

Tks, Brian

> On Jul 7, 2020, at 5:19 PM, Griffin, Robert <rgriffin@chelseama.gov> wrote:
>
> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>
> Brian,
>
> Last time we spoke, I know you were involved with the LPRs. We just went live with G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative) Quincy. At a minimum, I'd like to give you access. But I would also like to work with the state police and see if we can use Flock's API somehow to transfer the data to the State's LPR database. I believe you guys are still using PIPS?
>
> Rob
> 617-438-7331

From: Liam Hawkins
To: Scott, William (POL)
Subject: Re: LPR Case Support request BPD I#202093583
Date: Sunday, December 27, 2020 12:26:13 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Thanks for the reply. I'll reach out again during the week if need be. Stay safe.

On Sat, Dec 26, 2020 at 23:57 Fusion (POL) <fusion@state.ma.us> wrote:

> Good Morning,
>
> Unfortunately, our ALPR system is down for maintenance and is not operational. We do not have a time frame for when it will be operational. If you still need the information please resubmit this request next week. We apologize for the inconvenience.
>
> **Lt. William T. Scott**
>
> **Division of Homeland Security and Preparedness**
>
> **Commonwealth Fusion Center**
>
> **Massachusetts State Police**
>
> **470 Worcester Road**
>
> **Framingham, MA 01702**
>
> **Work: 508-820-2233**
>
> **Fax: 508-820-2150**
>
> **William.t.scott@pol.state.ma.us**
>
> ---
>
> **From:** Liam Hawkins <liam.hawkins@pd.boston.gov>

Sent: Saturday, December 26, 2020 11:16 PM
To: Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>
Subject: LPR Case Support [redacted]

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Ma'am/Sir:

[redacted]

Any questions, concerns or clarifications can be directed to me via this email or my department cell phone [redacted]. Thank you.

--

Respectfully,

Detective Liam P. Hawkins

B*oston* ***P****olice* ***D****epartment*

B*ureau of* ***I****nvestigative* ***S****ervices*

District E-5 *(West Roxbury/Roslindale)*

1708 Centre Street

West Roxbury, MA 02132-1536

Detectives Main Office line: 617-343-4595

Direct Extension/Voicemail: 617-343-9854

Department Cell: 6[redacted]

> Fax: 617-343-4817
>
> Email: Liam.Hawkins@pd.boston.gov
>
> CRIMESTOPPERS 1-800-494-TIPS or TEXT the word "TIP" to 27463
>
> ***IF THE READER OF THIS MESSAGE IS NOT THE INTENDED RECIPIENT, YOU ARE HEREBY NOTIFIED THAT ANY DISSEMINATION, DISTRIBUTION, OR COPYING OF THIS COMMUNICATION IS STRICTLY PROHIBITED.***
>
> ***Please consider the environment before printing this message.***

--

Respectfully,

Detective Liam P. Hawkins

Boston Police Department
Bureau of Investigative Services
District E-5 (West Roxbury/Roslindale)
1708 Centre Street
West Roxbury, MA 02132-1536
Detectives Main Office line: 617-343-4595
Direct Extension/Voicemail: 617-343-9854
Department Cell: [redacted] M.G.L. c. 4,sec. 7,cl.26 (n)(security)
Fax: 617-343-4817
Email: Liam.Hawkins@pd.boston.gov

CRIMESTOPPERS 1-800-494-TIPS or TEXT the word "TIP" to 27463

IF THE READER OF THIS MESSAGE IS NOT THE INTENDED RECIPIENT, YOU ARE HEREBY NOTIFIED THAT ANY DISSEMINATION, DISTRIBUTION, OR COPYING OF THIS COMMUNICATION IS STRICTLY PROHIBITED.

Please consider the environment before printing this message.

This message was sent from a mobile device, please excuse any typographical errors as it was not authored with a full-size keyboard.

From: Chris.Mason@pol.state.ma.us
To: Quinn, Dermot (POL)
Subject: Re: LPR
Date: Monday, February 10, 2020 10:10:54 AM

Can't hurt. Thank you.

Colonel Christopher Mason
Superintendent
Massachusetts State Police

On Feb 10, 2020, at 10:08 AM, Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us> wrote:

What do you think about copying Secretary Wood?

From: Mason, Christopher (POL) <Chris.Mason@pol.state.ma.us>
Sent: Monday, February 10, 2020 10:08 AM
To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Cc: Warmington, Scott (POL) <Scott.Warmington@pol.state.ma.us>
Subject: Re: LPR

Sir,

This looks good. Thank you.

Colonel Christopher Mason
Superintendent
Massachusetts State Police

On Feb 10, 2020, at 9:34 AM, Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us> wrote:

Sirs,

Are you ok with this email? I would like to send to EOPSS and EOTSS and Massport teams.

Respectfully,

DJQ

Good Morning,

I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.

Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.

Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.

MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.

I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.

To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.

I can't overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security's technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.

Respectfully,

Lieutenant Colonel Dermot J. Quinn #1765
Division Commander
Division of Homeland Security & Preparedness
Massachusetts State Police
<image001.png>

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, January 17, 2020 1:10 PM
To: Slater, James (CHS) <james.slater@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>; Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; John Tedona <jtedona@neology.net>; Chute, Alexander <AChute@massport.com>; Peter Crary <pcrary@neology.net>; Michalski, Maria (EPS) <maria.michalski@mass.gov>
Subject: RE: MassPort LPR Cameras

Hi Jim,

BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.

-Brian

From: Egnitz, Brian (POL)
Sent: Monday, January 6, 2020 1:33 PM
To: Slater, James (CHS)
Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter Crary
Subject: RE: MassPort LPR Cameras

Hi Jim,

We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?

Thanks Brian

From: John Tedona [mailto:jtedona@neology.net]
Sent: Monday, December 9, 2019 4:55 PM
To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); Slater, James (CHS)
Subject: RE: MassPort LPR Cameras

Alex,

I can be available most anytime tomorrow for a call.

Regards,

John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager

12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: Chute, Alexander <AChute@massport.com>
Sent: Monday, December 9, 2019 4:38 PM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; John Tedona <jtedona@neology.net>; Peter Crary <pcrary@neology.net>
Cc: Guerriero, Robert (MASSIT) <robert.guerriero@state.ma.us>; Peek, Brian T. (EOTSS) <brian.t.peek@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Slater III, James F (CHS) <james.slater@state.ma.us>
Subject: RE: MassPort LPR Cameras

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Hello All,

I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.

Respectfully,

~Alex

<image002.png>

Alexander B. Chute
Program Manager, Public Safety Systems
Massachusetts Port Authority
Cell: [redacted]
Office: 617.568.5942
achute@massport.com

WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons

without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Monday, November 18, 2019 3:26 PM
To: John Tedona (jtedona@neology.net); pcrary@neology.net
Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
Subject: RE: MassPort LPR Cameras

Hi John, Peter

Any issues with moving Massports cameras to the Chelsea DB?

Using the Boss calculator, I estimate that we would need 9-10 TB of storage.

The current app server
<image003.png>

Current DB server

<image004.png>
<image005.png>

Our current reads by month for about [redacted]

Year	Month	Day	Month Name	Reads Count
2019	11	1	November	495,113
2019	11	2	November	472,907
2019	11	3	November	384,409
2019	11	4	November	411,440
2019	11	5	November	434,085
2019	11	6	November	495,537
2019	11	7	November	444,123
2019	11	8	November	542,492

2019	11	9	November	443,463
2019	11	10	November	389,514
2019	11	11	November	362,548
2019	11	12	November	236,539

From: Chute, Alexander [mailto:AChute@massport.com]
Sent: Wednesday, November 13, 2019 2:49 PM
To: Egnitz, Brian (POL)
Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
Subject: RE: MassPort LPR Cameras

These stats are from the [redacted] we have in the system for this month:

<image006.png>

~Alex

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Tuesday, November 12, 2019 5:28 PM
To: Chute, Alexander
Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
Subject: RE: MassPort LPR Cameras

Hi Alex,

Can you please provide the updated reads per day? Previously you were interested in sharing [redacted] at approximately 75,000 reads per day.

Here is [redacted] I mentioned.

Set hos
Set ima
Set nu
Set Pin
Set udp
Set pin
Set sec

[redacted]

I've looped in the network and server team from TSS on the thread.
Maybe we can schedule a call in the next week.
For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.

-Brian

From: Chute, Alexander [mailto:AChute@massport.com]
Sent: Tuesday, November 12, 2019 2:08 PM
To: Egnitz, Brian (POL)
Subject: MassPort LPR Cameras

Brian,

Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to approximately [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.

Respectfully,

~Alex

<image002.png>

Alexander B. Chute
Program Manager, Public Safety Systems
Massachusetts Port Authority
Cell: [redacted]
Office: 617.568.5942
achute@massport.com

WARNING: This record may contain Sensitive Security Information that is controlled

under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

Lieutenant Colonel Dermot J. Quinn #1765
Division Commander
Division of Investigative Services
Massachusetts State Police


From: Chris.Mason@pol.state.ma.us
To: Quinn, Dermot (POL)
Cc: Warmington, Scott (POL)
Subject: Re: LPR
Date: Monday, February 10, 2020 10:07:33 AM

Sir,

This looks good. Thank you.

Colonel Christopher Mason
Superintendent
Massachusetts State Police

On Feb 10, 2020, at 9:34 AM, Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us> wrote:

Sirs,

Are you ok with this email? I would like to send to EOPSS and EOTSS and Massport teams.

Respectfully,

DJQ

Good Morning,

I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.

Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to

make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.

Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as "BOSS" and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport's cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.

MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.

I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.

To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.

I can't overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security's technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.

Respectfully,

Lieutenant Colonel Dermot J. Quinn #1765
Division Commander
Division of Homeland Security & Preparedness
Massachusetts State Police
<image001.png>

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, January 17, 2020 1:10 PM
To: Slater, James (CHS) <james.slater@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>; Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; John Tedona <jtedona@neology.net>; Chute, Alexander <AChute@massport.com>; Peter Crary <pcrary@neology.net>; Michalski, Maria (EPS) <maria.michalski@mass.gov>
Subject: RE: MassPort LPR Cameras

Hi Jim,

BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.

-Brian

From: Egnitz, Brian (POL)
Sent: Monday, January 6, 2020 1:33 PM
To: Slater, James (CHS)
Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter Crary
Subject: RE: MassPort LPR Cameras

Hi Jim,

We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?

Thanks Brian

From: John Tedona [mailto:jtedona@neology.net]
Sent: Monday, December 9, 2019 4:55 PM
To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); Slater, James (CHS)

Subject: RE: MassPort LPR Cameras

Alex,

I can be available most anytime tomorrow for a call.

Regards,

John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: Chute, Alexander <AChute@massport.com>
Sent: Monday, December 9, 2019 4:38 PM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; John Tedona <jtedona@neology.net>; Peter Crary <pcrary@neology.net>
Cc: Guerriero, Robert (MASSIT) <robert.guerriero@state.ma.us>; Peek, Brian T. (EOTSS) <brian.t.peek@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Slater III, James F (CHS) <james.slater@state.ma.us>
Subject: RE: MassPort LPR Cameras

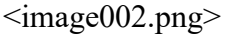
CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Hello All,

I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.

Respectfully,

~Alex



Alexander B. Chute
Program Manager, Public Safety Systems
Massachusetts Port Authority
Cell: [redacted]
Office: 617.568.5942
achute@massport.com

WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Monday, November 18, 2019 3:26 PM
To: John Tedona (jtedona@neology.net); pcrary@neology.net
Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
Subject: RE: MassPort LPR Cameras

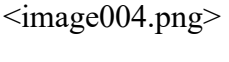
Hi John, Peter

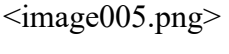
Any issues with moving Massports cameras to the Chelsea DB?

Using the Boss calculator, I estimate that we would need 9-10 TB of storage.

The current app server


Current DB server





Our current reads by month for about [redacted]

Month	Reads

Year	Month	Day	Name	Count
2019	11	1	November	495,113
2019	11	2	November	472,907
2019	11	3	November	384,409
2019	11	4	November	411,440
2019	11	5	November	434,085
2019	11	6	November	495,537
2019	11	7	November	444,123
2019	11	8	November	542,492
2019	11	9	November	443,463
2019	11	10	November	389,514
2019	11	11	November	362,548
2019	11	12	November	236,539

From: Chute, Alexander [mailto:AChute@massport.com]
Sent: Wednesday, November 13, 2019 2:49 PM
To: Egnitz, Brian (POL)
Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
Subject: RE: MassPort LPR Cameras

These stats are from the G.L. c. 4.sec. 7.cl.26 (n)(security) we have in the system for this month:

<image006.png>

~Alex

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Tuesday, November 12, 2019 5:28 PM
To: Chute, Alexander
Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
Subject: RE: MassPort LPR Cameras

Hi Alex,

Can you please provide the updated reads per day? Previously you were interested in

sharing [redacted] at approximately 75,000 reads per day.

Here is the [redacted] confi I mentioned.

Set host to boss [redacted]
Set image [redacted]
Set numb [redacted]
Set Ping [redacted]
Set udp p [redacted]
Set ping [redacted]
Set secur [redacted]

I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.

-Brian

From: Chute, Alexander [mailto:AChute@massport.com]
Sent: Tuesday, November 12, 2019 2:08 PM
To: Egnitz, Brian (POL)
Subject: MassPort LPR Cameras

Brian,

Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to approximately [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.

Respectfully,

~Alex

<image002.png>

Alexander B. Chute
Program Manager, Public Safety Systems
Massachusetts Port Authority
Cell: [redacted]
Office: 617.568.5942
achute@massport.com

WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

Lieutenant Colonel Dermot J. Quinn #1765
Division Commander
Division of Investigative Services
Massachusetts State Police
<image001.png>

From: Mason, Christopher (POL)
To: Quinn, Dermot (POL)
Subject: Re: LPR
Date: Monday, February 10, 2020 10:10:55 AM

Can't hurt. Thank you.

Colonel Christopher Mason
Superintendent
Massachusetts State Police

> On Feb 10, 2020, at 10:08 AM, Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us> wrote:
>
> What do you think about copying Secretary Wood?
>
> ---
>
> **From:** Mason, Christopher (POL) <Chris.Mason@pol.state.ma.us>
> **Sent:** Monday, February 10, 2020 10:08 AM
> **To:** Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
> **Cc:** Warmington, Scott (POL) <Scott.Warmington@pol.state.ma.us>
> **Subject:** Re: LPR
>
> Sir,
>
> This looks good. Thank you.
>
> Colonel Christopher Mason
> Superintendent
> Massachusetts State Police
>
> > On Feb 10, 2020, at 9:34 AM, Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us> wrote:

Sirs,

Are you ok with this email? I would like to send to EOPSS and EOTSS and Massport teams.

Respectfully,

DJQ

Good Morning,

I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.

Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.

Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.

MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.

I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.

To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.

I can't overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security's technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.

Respectfully,

Lieutenant Colonel Dermot J. Quinn #1765
Division Commander
Division of Homeland Security & Preparedness
Massachusetts State Police
<image001.png>

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, January 17, 2020 1:10 PM
To: Slater, James (CHS) <james.slater@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>; Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; John Tedona <jtedona@neology.net>; Chute, Alexander <AChute@massport.com>; Peter Crary <pcrary@neology.net>; Michalski, Maria (EPS) <maria.michalski@mass.gov>
Subject: RE: MassPort LPR Cameras

Hi Jim,

BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.

-Brian

From: Egnitz, Brian (POL)
Sent: Monday, January 6, 2020 1:33 PM
To: Slater, James (CHS)
Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter Crary
Subject: RE: MassPort LPR Cameras

Hi Jim,

We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?

Thanks Brian

From: John Tedona [mailto:jtedona@neology.net]
Sent: Monday, December 9, 2019 4:55 PM
To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); Slater, James (CHS)
Subject: RE: MassPort LPR Cameras

Alex,

I can be available most anytime tomorrow for a call.

Regards,

John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager

12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: Chute, Alexander <AChute@massport.com>
Sent: Monday, December 9, 2019 4:38 PM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; John Tedona <jtedona@neology.net>; Peter Crary <pcrary@neology.net>
Cc: Guerriero, Robert (MASSIT) <robert.guerriero@state.ma.us>; Peek, Brian T. (EOTSS) <brian.t.peek@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Slater III, James F (CHS) <james.slater@state.ma.us>
Subject: RE: MassPort LPR Cameras

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Hello All,

I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.

Respectfully,

~Alex

<image002.png>

Alexander B. Chute
Program Manager, Public Safety Systems
Massachusetts Port Authority
Cell: [redacted]
Office: 617.568.5942
achute@massport.com

WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons

without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Monday, November 18, 2019 3:26 PM
To: John Tedona (jtedona@neology.net); pcrary@neology.net
Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
Subject: RE: MassPort LPR Cameras

Hi John, Peter

Any issues with moving Massports cameras to the Chelsea DB?

Using the Boss calculator, I estimate that we would need 9-10 TB of storage.

The current app server
<image003.png>

Current DB server

<image004.png>
<image005.png>

Our current reads by month for about [redacted]

Year	Month	Day	Month Name	Reads Count
2019	11	1	November	495,113
2019	11	2	November	472,907
2019	11	3	November	384,409
2019	11	4	November	411,440
2019	11	5	November	434,085
2019	11	6	November	495,537
2019	11	7	November	444,123
2019	11	8	November	542,492

2019	11	9	November	443,463
2019	11	10	November	389,514
2019	11	11	November	362,548
2019	11	12	November	236,539

From: Chute, Alexander [mailto:AChute@massport.com]
Sent: Wednesday, November 13, 2019 2:49 PM
To: Egnitz, Brian (POL)
Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
Subject: RE: MassPort LPR Cameras

These stats are from the G.L. c. 4.sec. 7.cl.26 (n)(security) we have in the system for this month:

<image006.png>

~Alex

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Tuesday, November 12, 2019 5:28 PM
To: Chute, Alexander
Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
Subject: RE: MassPort LPR Cameras

Hi Alex,

Can you please provide the updated reads per day? Previously you were interested in sharing G.L. c. 4.sec. 7.cl.26 (n)(s at approximately 75,000 reads per day.

Here is the G.L. c. 4.sec confi I mentioned.

Set host to boss G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c.
Set image G.L. c. 4.sec. 7.cl.26 (n)(s
Set number of G.L. c. 4.sec. 7.cl.26 (n)(security
Set Ping G.L. c. 4.sec. 7.cl.26 (n)(security),
Set udp ping G.L. c. 4.sec. 7.cl.26 (n)(s
Set ping G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.se
Set security G.L. c. 4.sec. 7.cl.26 (n)

I've looped in the network and server team from TSS on the thread.
Maybe we can schedule a call in the next week.
For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.

-Brian

From: Chute, Alexander [mailto:AChute@massport.com]
Sent: Tuesday, November 12, 2019 2:08 PM
To: Egnitz, Brian (POL)
Subject: MassPort LPR Cameras

Brian,

Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to approximately [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.

Respectfully,

~Alex

<image002.png>

Alexander B. Chute
Program Manager, Public Safety Systems
Massachusetts Port Authority
Cell: [redacted]
Office: 617.568.5942
achute@massport.com

WARNING: This record may contain Sensitive Security Information that is controlled

under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

Lieutenant Colonel Dermot J. Quinn #1765
Division Commander
Division of Investigative Services
Massachusetts State Police
<image001.png>

From: brian.egnitz@pol.state.ma.us
To: Brian Kruger
Subject: Re: LRP network ideas?
Date: Thursday, February 20, 2020 10:29:13 AM

There isn't one that I'm aware of.

> On Feb 20, 2020, at 9:47 AM, Brian Kruger <bkruger@forensiclogic.com> wrote:
>
> Brian,
> This is the last email from John. It looks like we are missing a XSD file for the name space. I reached out just on the side to xfact to see if they have the XSD but haven't heard back.
>
> Regards,
>
> <image001.png>
> **Brian Kruger**
> Operations and Support Manager
> **Forensic Logic / COPLINK**
> Office: 520.367.2775
> Mobile: 520.488.1603
> bkruger@forensiclogic.com
> www.forensiclogic.com
>
> ***CONFIDENTIALITY:*** *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*
>
> **From:** Ouellette, John (EPS) <john.ouellette@state.ma.us>
> **Sent:** Wednesday, February 12, 2020 8:37 AM
> **To:** Samson Dunatunga <mdunatunga@forensiclogic.com>
> **Cc:** Billy Moore <bmoore@forensiclogic.com>; Brian Kruger <bkruger@forensiclogic.com>
> **Subject:** RE: LRP network ideas?
>
> Hi Samson,
>
> All of the xsd files are in the package and that is the only dev package we have.
> Some of these namespaces were developed some time ago and are still in use.
>
> John Ouellette | Massachusetts Executive Office of Public Safety and Security
> Office of Technology and Information Services
> Enterprise Application and Database Services
> Application Support and Management
> 200 Arlington Street Suite 2200
> Chelsea, MA 02150
> john.ouellette@state.ma.us | http://www.mass.gov/eops
>
> **From:** Samson Dunatunga <mdunatunga@forensiclogic.com>
> **Sent:** Tuesday, February 11, 2020 11:23 AM
> **To:** Ouellette, John (EPS) <john.ouellette@mass.gov>
> **Cc:** Billy Moore <bmoore@forensiclogic.com>; Brian Kruger <bkruger@forensiclogic.com>
> **Subject:** RE: LRP network ideas?
>
> Got all three packages extracted. I still don't see the XSD file for http://www.xfact.com/schemas/eopss/dcjis/cjx/3.0
> I see XSD file (CJISBroker_2016-03-24.zip\CJISBroker_2016-03-24\CJISBroker\transactions\core\xsd\dcjis\1.0\dcjis.xsd) for http://www.xfact.com/schemas/eopss/dcjis/1.0 within the package CJISBroker_2016-03-24.zip
>
> Do you have any other dev packages that includes above XSD files?
> Thanks,
> -Samson
>
> **From:** Ouellette, John (EPS)
> **Sent:** Tuesday, February 11, 2020 6:37 AM
> **To:** Samson Dunatunga
> **Cc:** Billy Moore; Brian Kruger
> **Subject:** RE: LRP network ideas?
>
> HI Samson,
>
> Attached are the dev packages. They are zipped up, let me know if you don't get them.
>
> John Ouellette | Massachusetts Executive Office of Public Safety and Security
> Office of Technology and Information Services
> Enterprise Application and Database Services
> Application Support and Management
> 200 Arlington Street Suite 2200
> Chelsea, MA 02150
> john.ouellette@state.ma.us | http://www.mass.gov/eops
>
> **From:** Samson Dunatunga <mdunatunga@forensiclogic.com>
> **Sent:** Monday, February 10, 2020 4:11 PM
> **To:** Ouellette, John (EPS) <john.ouellette@mass.gov>; Brian Kruger <bkruger@forensiclogic.com>
> **Cc:** Billy Moore <bmoore@forensiclogic.com>
> **Subject:** RE: LRP network ideas?
>
> Hi John,
> Thank you for the reply. The sample you have attached is a bit different from the sample I have. Where can I get the development package with the sample file you sent? It looks like I have been using an older implementation development package to generate the request. I don't have any class files related to dcjis schema in the development package I have.
>
> Thanks,
> -Samson
>
> **From:** Ouellette, John (EPS)
> **Sent:** Friday, February 7, 2020 2:39 PM
> **To:** Samson Dunatunga; Brian Kruger
> **Cc:** Billy Moore
> **Subject:** RE: LRP network ideas?
>
> Your namespaces should be:
> xmlns:dcjis="http://www.xfact.com/schemas/eopss/dcjis/1.0" xmlns:cjx="http://www.xfact.com/schemas/eopss/dcjis/cjx/3.0"
> xmlns:j="http://www.it.ojp.gov/jxdm/3.0"
> xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
>
> Attached is a sample R1 request.
>
> John Ouellette | Massachusetts Executive Office of Public Safety and Security
> Office of Technology and Information Services

Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Samson Dunatunga <mdunatunga@forensiclogic.com>
Sent: Friday, February 7, 2020 4:26 PM
To: Brian Kruger <bkruger@forensiclogic.com>; Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Billy Moore <bmoore@forensiclogic.com>
Subject: RE: LRP network ideas?

Hi John,
I compared the XML we are sending with the sample XML in the development package. I don't see any structural differences in them, but we are still getting reply indicating XML is not valid. Any help you can provide is appreciated.
Here is the XML we are sending for transaction type R1.
Thanks,
-Samson

---request begin----

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns1:CJISRequestTransaction xmlns:ns2="http://www.it.ojp.gov/jxdm/3.0" xmlns:ns1="http://www.xfact.com/schemas/chsb/cjis/2.0">
  <ns1:CJISRequestHeader>
    <ns1:UUID>S.L. c. 4 sec. 7 cl.26893d578-1867-4332-b278-b71a2c72f5b3</ns1:UUID>
    <ns1:CreateDateTime>2020-02-07T16:08:03.123-05:00</ns1:CreateDateTime>
    <ns1:TransactionSource>COPLINK</ns1:TransactionSource>
    <ns1:UserID>TEST</ns1:UserID>
    <ns2:OrganizationORIID>
      <ns2:ID>MAMSP0000</ns2:ID>
    </ns2:OrganizationORIID>
    <ns1:TimeToLive>unlimited</ns1:TimeToLive>
    <ns1:SchemaVersion>2.0</ns1:SchemaVersion>
    <ns1:ApplicationVersion>2.0</ns1:ApplicationVersion>
    <ns1:ResponseMechanism>Wait</ns1:ResponseMechanism>
    <ns1:RespondTo>http://S.L. c. 4 sec. 7 cl.2:6060/CHSBReceiver/CHSBService</ns1:RespondTo>
    <ns1:CJISUserID>
      <ns2:ID>TEST</ns2:ID>
    </ns1:CJISUserID>
    <ns1:CJISUserPassword>password</ns1:CJISUserPassword>
    <ns1:CJISQueryAuthorizer>
      <ns2:PersonFullName>Joe Authorizer</ns2:PersonFullName>
    </ns1:CJISQueryAuthorizer>
    <ns1:CJISQueryOperator>
      <ns2:PersonFullName>Jane Authorizer</ns2:PersonFullName>
    </ns1:CJISQueryOperator>
    <ns1:CJISQueryRequester>
      <ns2:PersonFullName>Jane Requester</ns2:PersonFullName>
    </ns1:CJISQueryRequester>
    <ns1:CJISQueryPurposeCode>C</ns1:CJISQueryPurposeCode>
  </ns1:CJISRequestHeader>
  <ns1:CJISRequestBody>
    <ns1:R1QueryInput>
      <ns1:CJISMessageKey>R1</ns1:CJISMessageKey>
      <ns2:DriverAuthorization xsi:type="ns1:DriverAuthorizationType" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <ns2:DriverAuthorizationID>
          <ns2:ID>S32935254</ns2:ID>
        </ns2:DriverAuthorizationID>
      </ns2:DriverAuthorization>
    </ns1:R1QueryInput>
  </ns1:CJISRequestBody>
</ns1:CJISRequestTransaction>
```

--- request end ----

Here is the sample XML provided to us.

```
<?xml version="1.0" encoding="UTF-8"?>
<cjx:CJISRequestTransaction xmlns:cjx="http://www.xfact.com/schemas/chsb/cjis/2.0" xmlns:j="http://www.it.ojp.gov/jxdm/3.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <cjx:CJISRequestHeader>
    <cjx:UUID>192.168.0.18/1237228378953.1.12</cjx:UUID>
    <cjx:CreateDateTime>2009-03-16T14:32:58-04:00</cjx:CreateDateTime>
    <cjx:TransactionSource>192.168.1.137 / CHSB</cjx:TransactionSource>
    <cjx:UserID>joe_user</cjx:UserID>
    <j:OrganizationORIID>
      <j:ID>MACJIS0M0</j:ID>
    </j:OrganizationORIID>
    <cjx:DeviceAddress></cjx:DeviceAddress>
    <cjx:UserContexts></cjx:UserContexts>
    <cjx:TimeToLive>unlimited</cjx:TimeToLive>
    <cjx:SchemaVersion>2.0</cjx:SchemaVersion>
    <cjx:ApplicationVersion>2.0</cjx:ApplicationVersion>
    <cjx:ResponseMechanism>Wait</cjx:ResponseMechanism>
    <cjx:RespondTo>http://192.168.0.30:6060/public/CHSBService.asmx</cjx:RespondTo>
    <cjx:CJISUserID>
      <j:ID>cjis_user</j:ID>
    </cjx:CJISUserID>
    <cjx:CJISUserPassword>password</cjx:CJISUserPassword>
    <cjx:CJISQueryAuthorizer>
      <j:PersonFullName>Joe Authorizer</j:PersonFullName>
    </cjx:CJISQueryAuthorizer>
    <cjx:CJISQueryOperator>
      <j:PersonFullName>Jane Operator</j:PersonFullName>
    </cjx:CJISQueryOperator>
    <cjx:CJISQueryRequester>
      <j:PersonFullName>Jane Requester</j:PersonFullName>
    </cjx:CJISQueryRequester>
    <cjx:CJISQueryPurposeCode>C</cjx:CJISQueryPurposeCode>
  </cjx:CJISRequestHeader>
  <cjx:CJISRequestBody>
    <cjx:R1QueryInput>
      <cjx:CJISMessageKey>R1</cjx:CJISMessageKey>
      <j:DriverAuthorization xsi:type="cjx:DriverAuthorizationType">
        <j:DriverAuthorizationID>
          <j:ID>900000035</j:ID>
        </j:DriverAuthorizationID>
      </j:DriverAuthorization>
    </cjx:R1QueryInput>
  </cjx:CJISRequestBody>
</cjx:CJISRequestTransaction>
```

Here is the reply we got for the XML we sent.

imagebroker.ImageBrokerREST.getEncodedImage result of service call: <?xml version="1.0" encoding="UTF-8"?>
<dcjis:DataExchange xmlns:dcjis="http://www.xfact.com/schemas/eopss/dcjis/1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><dcjis:Acknowledgment><dcjis:AcknowledgmentHeader>
<dcjis:UUID>ERROR</dcjis:UUID><dcjis:CreateDateTime>2020-02-07T16:08:18-0500</dcjis:CreateDateTime><dcjis:TransactionSource>ERROR</dcjis:TransactionSource>
<dcjis:TransactionMessageKey>ERROR</dcjis:TransactionMessageKey><dcjis:TransactionOrganizationID><dcjis:ID>ERROR</dcjis:ID></dcjis:TransactionOrganizationID><dcjis:UserContexts /><dcjis:DeviceAddress />
<dcjis:SchemaVersion>1.0</dcjis:SchemaVersion><dcjis:ApplicationVersion>2.0</dcjis:ApplicationVersion><dcjis:CJISUserID><dcjis:ID>ERROR</dcjis:ID></dcjis:CJISUserID><dcjis:CJISUserPassword>ERROR</dcjis:CJISUserPassword>
<dcjis:CJISQueryAuthorizer><dcjis:PersonFullName>ERROR</dcjis:PersonFullName></dcjis:CJISQueryAuthorizer><dcjis:CJISQueryOperator><dcjis:PersonFullName>ERROR</dcjis:PersonFullName></dcjis:CJISQueryOperator>
<dcjis:CJISQueryRequester><dcjis:PersonFullName>ERROR</dcjis:PersonFullName></dcjis:CJISQueryRequester><dcjis:CJISQueryPurposeCode>ERROR</dcjis:CJISQueryPurposeCode><dcjis:Transaction>
<dcjis:TransactionStatus>-903</dcjis:TransactionStatus><dcjis:TransactionDescription>Transaction failed schema validation</dcjis:TransactionDescription></dcjis:Transaction></dcjis:AcknowledgmentHeader>
<dcjis:AcknowledgmentBody /></dcjis:Acknowledgment></dcjis:DataExchange>

From: Brian Kruger
Sent: Tuesday, January 28, 2020 3:23 PM
To: Ouellette, John (EPS); Samson Dunatunga
Subject: RE: LRP network ideas?

Samson,
Did you get what you needed?

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Thursday, January 23, 2020 9:25 AM
To: Samson Dunatunga <mdunatunga@forensiclogic.com>
Cc: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hi Samson,

Do you have the dev package? There are example xml documents in there.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Samson Dunatunga <mdunatunga@forensiclogic.com>
Sent: Thursday, January 23, 2020 11:00 AM
To: Brian Kruger <bkruger@forensiclogic.com>; Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
Here is the XML sent from our server to retrieve relevant data. The CJISMessageKey is set to R1. The response we got indicates the XML sent is invalid. Can you point me to what is not valid in the XML? By the way, I checked the XML syntax with an online XML validation tool which indicates the syntax is good.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<ns1:CJISRequestTransaction xmlns:ns2="http://www.it.ojp.gov/jxdm/3.0" xmlns:ns1="http://www.xfact.com/schemas/chsb/cjis/2.0">
  <ns1:CJISRequestHeader>
    <ns1:UUID>S.L. c. 4.sec. 7.cl.2487fc738-d2fa-4b4f-8841-067b2d85e636</ns1:UUID>
    <ns1:CreateDateTime>2020-01-22T10:47:23.216-05:00</ns1:CreateDateTime>
    <ns1:TransactionSource>COPLINK</ns1:TransactionSource>
    <ns1:UserID>TEST</ns1:UserID>
    <ns2:OrganizationORIID>
      <ns2:ID>MAMSP0000</ns2:ID>
    </ns2:OrganizationORIID>
    <ns1:TimeToLive>unlimited</ns1:TimeToLive>
    <ns1:SchemaVersion>2.0</ns1:SchemaVersion>
    <ns1:ApplicationVersion>2.0</ns1:ApplicationVersion>
    <ns1:ResponseMechanism>Wait</ns1:ResponseMechanism>
    <ns1:RespondTo>http://S.L. c. 4.sec. 7.cl.2:6060/CHSBReceiver/CHSBService</ns1:RespondTo>
    <ns1:CJISUserID>
      <ns2:ID>TEST</ns2:ID>
    </ns1:CJISUserID>
    <ns1:CJISUserPassword>password</ns1:CJISUserPassword>
    <ns1:CJISQueryAuthorizer>
      <ns2:PersonFullName>Joe Authorizer</ns2:PersonFullName>
    </ns1:CJISQueryAuthorizer>
    <ns1:CJISQueryOperator>
      <ns2:PersonFullName>Jane Authorizer</ns2:PersonFullName>
    </ns1:CJISQueryOperator>
    <ns1:CJISQueryRequester>
      <ns2:PersonFullName>Jane Requester</ns2:PersonFullName>
    </ns1:CJISQueryRequester>
    <ns1:CJISQueryPurposeCode>C</ns1:CJISQueryPurposeCode>
  </ns1:CJISRequestHeader>
  <ns1:CJISRequestBody>
    <ns1:R1QueryInput>
      <ns1:CJISMessageKey>R1</ns1:CJISMessageKey>
      <ns2:DriverAuthorization xsi:type="ns1:DriverAuthorizationType" ns2:id="S32935254" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"/>
    </ns1:R1QueryInput>
  </ns1:CJISRequestBody>
</ns1:CJISRequestTransaction>
```

Thank you,
-Samson

From: Brian Kruger
Sent: Wednesday, January 22, 2020 1:39 PM
To: Ouellette, John (EPS); Samson Dunatunga
Subject: RE: LRP network ideas?

John,
I am adding Samson on this thread.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Wednesday, January 22, 2020 1:35 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hi Brian,

The only namespaces I can find are:
xmlns:dcjis="http://www.xfact.com/schemas/eopss/dcjis/1.0"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:cjx="http://www.xfact.com/schemas/eopss/dcjis/cjx/3.0"
xmlns:j="http://www.it.ojp.gov/jxdm/3.0">

Which message key are you trying to run?

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Wednesday, January 22, 2020 2:57 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
I have been putting out new versions of our Broker on this build Samson noticed that we are using xml namespace 2.0 which doesn't work. Do you know what version we should be running.

From: Samson Dunatunga <mdunatunga@forensiclogic.com>
Sent: Wednesday, January 22, 2020 11:28 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE:

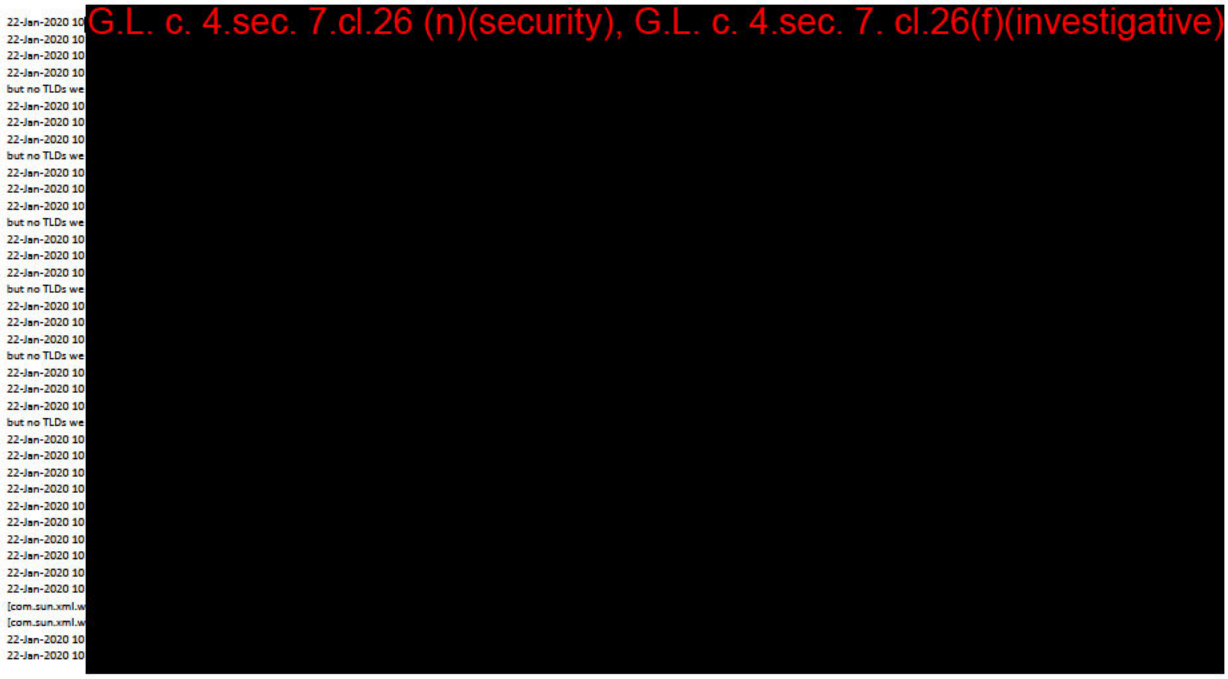
Looks like the XML namespace xmlns:ns1="http://www.xfact.com/schemas/chsb/cjis/2.0"
is no longer available. Can you find out what we are supposed to use?

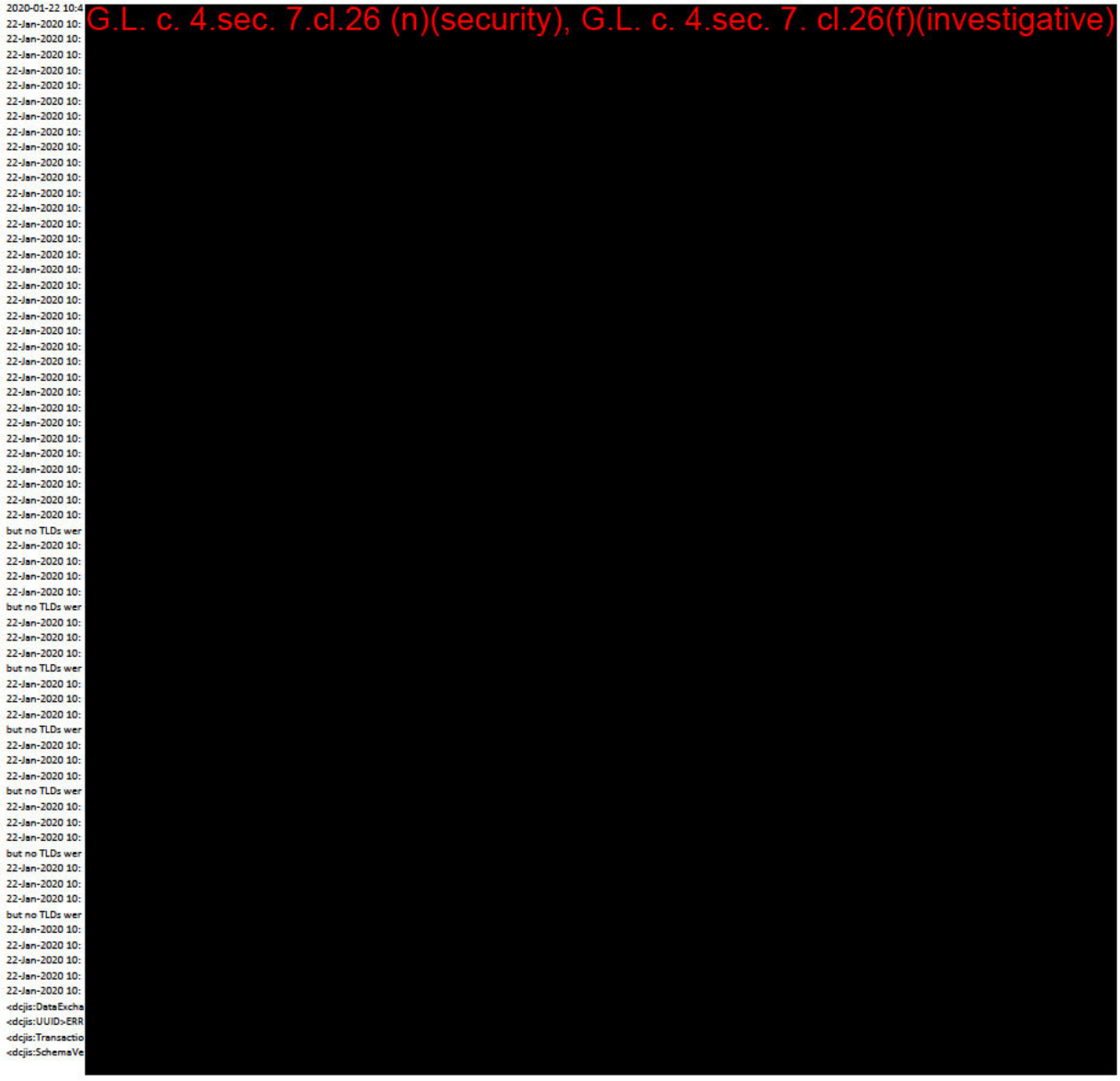
Thanks,
-Samson

From: Brian Kruger
Sent: Wednesday, January 22, 2020 8:56 AM
To: Samson Dunatunga
Subject:

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

2020-01-22 10:43:39 Commons Daem
22-Jan-2020 10:43:42.362 INFO [main
22-Jan-2020 10:43:42.362 INFO [main
22-Jan-2020 10:43:42.362 INFO [main


G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)


G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

<dcjis:CJISQueryAuthorizer><dcjis:PersonFullName>ERROR</dcjis:PersonFullName></dcjis:CJISQueryAuthorizer><dcjis:CJISQueryOperator><dcjis:PersonFullName>ERROR</dcjis:PersonFullName></dcjis:CJISQueryOperator>
<dcjis:CJISQueryRequester><dcjis:PersonFullName>ERROR</dcjis:PersonFullName></dcjis:CJISQueryRequester><dcjis:CJISQueryPurposeCode>ERROR</dcjis:CJISQueryPurposeCode><dcjis:Transaction>
<dcjis:TransactionStatus>-903</dcjis:TransactionStatus><dcjis:TransactionDescription>Transaction failed schema validation</dcjis:TransactionDescription></dcjis:Transaction></dcjis:AcknowledgmentHeader>
<dcjis:AcknowledgmentBody /></dcjis:Acknowledgment></dcjis:DataExchange>

Regards,

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, December 6, 2019 9:45 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hey Brian,

Can we change the subject to Broker?
LPR is the license plate reader.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, December 6, 2019 11:31 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Samson Dunatunga <mdunatunga@forensiclogic.com>; Billy Moore <bmoore@forensiclogic.com>; Rhonda Fromm <rfromm@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

Billy,
Please let the group know when this will be available. I will work with John to get it deployed and tested as soon as we have it released.

Regards,

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Tuesday, November 26, 2019 1:17 PM
To: 'Ouellette, John (EPS)' <john.ouellette@state.ma.us>; 'Egnitz, Brian (POL)' <brian.egnitz@state.ma.us>; Samson Dunatunga <mdunatunga@forensiclogic.com>; Billy Moore <bmoore@forensiclogic.com>
Cc: 'Dunne, Michaela (CHS)' <michaela.dunne@state.ma.us>; 'Dunn-CHS, William (CHS)' <william.dunn-chs@state.ma.us>; 'Mitchell, Timothy (EPS)' <timothy.mitchell@state.ma.us>; 'Ramsay, Christopher (EPS)' <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

John,
Thank you for the information on the call this afternoon.

Samson/Billy,
We need to add some additional debug code into our service so we can see the full communication path and what is being sent and received. John is also in the process to check and make sure their three servers can reach back into our [redacted] I have also reattached the IP wireshark I did this morning.

Regards,

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Tuesday, November 26, 2019 8:29 AM
To: Ouellette, John (EPS) <john.ouellette@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

John,
Give me a few minutes and I will give you a call. Here is the CSV file from wireshark. I had to repull it. I don't see any actually log details in our tomcat instance. In the wireshark though I see a bunch of event code errors like below:

Event: <Unknown eventcode 72>, <Unknown eventcode 111>, <Unknown eventcode 116>, <Unknown eventcode 121>, <Unknown eventcode 110>, <Unknown eventcode 45>, <Unknown eventcode 112>, <Unknown eventcode 110>, <Unknown eventcode 114>, <Unknown eventcode 115>, <Unknown eventcode 47>, <Unknown eventcode 110>, <Unknown eventcode 111>, <Unknown eventcode 118>, <Unknown eventcode 110>, <Unknown eventcode 111>, <Unknown eventcode 47>, ColormapNotify, <Unknown eventcode 97>, <Unknown eventcode 120>, <Unknown eventcode 58>, <Unknown eventcode 46>, <Unknown eventcode 104>, <Unknown eventcode 46>, <Unknown eventcode 117>, <Unknown eventcode 97>, <Unknown eventcode 47>, <Unknown eventcode 62>, <Unknown eventcode 114>, <Unknown eventcode 114>, <Unknown eventcode 82>, <Unknown eventcode 120>, <Unknown

eventcode 101>, MappingNotify, <Unknown eventcode 109>, <Unknown eventcode 98>, <Unknown eventcode 47>, <Unknown eventcode 119>, <Unknown eventcode 62>, <Unknown eventcode 114>, ColormapNotify, <Unknown eventcode 62>, <Unknown eventcode 115>, MappingNotify, <Unknown eventcode 110>

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Tuesday, November 26, 2019 7:29 AM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Hey Brian,

You can call me at 617-660-4775

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Monday, November 25, 2019 7:53 PM
To: Brian Kruger <bkruger@forensiclogic.com>; Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: Re: LRP network ideas?

Does it make sense to schedule a call and work through it in real time?

> On Nov 22, 2019, at 4:00 PM, Ouellette, John (EPS) <john.ouellette@mass.gov> wrote:
>
> Hi Brian,
>
> I do not see any requests for your ORI. Can you review the acknowledgements that the broker sends back as a return value? There may be error information in there.
>
> John Ouellette | Massachusetts Executive Office of Public Safety and Security
> Office of Technology and Information Services
> Enterprise Application and Database Services
> Application Support and Management
> 200 Arlington Street Suite 2200
> Chelsea, MA 02150
> john.ouellette@state.ma.us | http://www.mass.gov/eops
>
> ---
>
> **From:** Brian Kruger <bkruger@forensiclogic.com>
> **Sent:** Friday, November 22, 2019 3:47 PM
> **To:** Ouellette, John (EPS) <john.ouellette@mass.gov>
> **Cc:** Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
> **Subject:** RE: LRP network ideas?
>
> John,
> Can you check again and see if there is a request coming into the .154 server. I ran a packet capture and I do see data sent from the .171 to the .154 server.
>
> <image001.png>
>
> Regards,
>
>
>
> **Brian Kruger**
> Operations and Support Manager
> **Forensic Logic / COPLINK**
> Office: 520.367.2775
> Mobile: 520.488.1603
> bkruger@forensiclogic.com
> www.forensiclogic.com
>
> ***CONFIDENTIALITY:*** *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*
>
> ---
>
> **From:** Ouellette, John (EPS) <john.ouellette@state.ma.us>
> **Sent:** Friday, November 22, 2019 12:26 PM
> **To:** Brian Kruger <bkruger@forensiclogic.com>
> **Cc:** Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
> **Subject:** RE: LRP network ideas?
>
> Hi Brian,
>
> I'm not sure if 224.154 is a load balancer. I don't believe it is though. It doesn't matter though, that is where you will send requests. You will receive a synchronous response called an acknowledgement. That will let you know if your request was accepted or rejected.
>
> Later, an asynchronous response will be sent from G.L. c. 4,sec. 7,cl2or G.L. c. 4,sec. 7,cl2to your web service.
>
> John Ouellette | Massachusetts Executive Office of Public Safety and Security
> Office of Technology and Information Services
> Enterprise Application and Database Services

Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 22, 2019 2:19 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
The 154 address is a load balancer for the services correct. As far as I know there should be no blocked traffic to the .171 but let me include Chris and Tim on this thread.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 22, 2019 9:36 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

I didn't find any submitted requests.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Ouellette, John (EPS)
Sent: Friday, November 22, 2019 11:34 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

I can check.

The broker will send responses from[redacted] Make sure you are allowing that traffic.

When you send in a request you will receive an xml document as the return value. The documents lists if the request was accepted and if it wasn't, why it wasn't. You should be checking those.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 22, 2019 11:28 AM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

Bill,
I have the service send back a no data found so it looks like we are connecting. Can you check your logs to see if our request actually made it into your system.

I am sending the following test cycle from the[redacted] web server to our FR server

http:/[redacted]6060/CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=S32935254

Just so everybody is clear, this the is the connection path

[redacted] →[redacted]→[redacted]

Return path

[redacted]→[redacted]→[redacted]

Log of request:

2019-11-22 11:16:13,982 main DEBUG LoggerContext[name=MassLPRServlet, org.apache.logging.log4j.core.LoggerContext@59303963] started OK with configuration org.apache.logging.log4j.core.config.properties.PropertiesConfiguration@61e86192.
2019-11-22 11:16:13,982 main DEBUG Log4jServletContextListener ensuring that Log4j starts up properly.
2019-11-22 11:16:13,982 main DEBUG Log4jServletFilter initialized.
driversLicense=S32935254
remote host=[redacted]
remote port=60194
remote addr=[redacted]
scheme =http
scheme =HTTP/1.1
local addr =[redacted]
local name =EPS-CLFACEMATCH
context path = /CHSBReceiver
Init parameter1 =Value1
Current UUID : f3837e1f-0e40-4af6-8587-203e99240d92
javax.xml.bind.JAXBElement@227d5180

Request UUID:[redacted] f3837e1f-0e40-4af6-8587-203e99240d92

Rest response file contains:
no data found.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Thursday, November 21, 2019 2:11 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Ouellette, John (EPS) <john.ouellette@state.ma.us>
Subject: RE: LRP network ideas?

Thanks Bill!

It looks like we are close on this.

-Brian

From: Dunn-CHS, William (CHS)
Sent: Tuesday, November 19, 2019 7:50 AM
To: Brian Kruger; Ouellette, John (EPS)
Cc: Dunne, Michaela (CHS); Egnitz, Brian (POL); Dunn-CHS, William (CHS)
Subject: RE: LRP network ideas?

I think I see what might be part of the problem.

The R1 is either OLN or SSN, you can not send both at the same time.

There is No TEST SSN inquiry, use someone from MSP who is working on your project or if you have a developer who is from MA
The TEST OLN is S32935254

From: Brian Kruger [mailto:bkruger@forensiclogic.com]
Sent: Monday, November 18, 2019 6:33 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
Dev confirmed they are sending XML in the request. Do you have a valid License number in the test data I can try.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 15, 2019 11:16 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

The broker is a web service. You need to create a client to connect. Requests are made by sending in an xml document.

Did I forget to send you the broker documentation? Let me know.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 1:10 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
I ran two queries through IE I don't see an acknowledge me in the logs. Below is what I am seeing. Do we have a valid Lic number that is in the system I can try, or valid SSN.

My test URLs are:"
http://[redacted]6060/CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=987654321

http://[redacted]6060/CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=987654321

In my access log I see a 200:

G.L. c. 4.sec. 7.cl.2- - [15/Nov/2019:13:02:50 -0500] "GET /CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=987654321 HTTP/1.1" 200 -
G.L. c. 4.sec. 7.cl.2- - [15/Nov/2019:13:03:05 -0500] "GET /CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=987654321 HTTP/1.1" 200 –

In my log stdout log I see this:

2019-11-15 13:0 G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)
2019-11-15 13:0 /log4j2.properties
2019-11-15 13:0
org.apache.loggi
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0 cript, javascript, ECMAScript,
ecmascript], fact
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0 rtiesConfig), Filter=null)
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0 ull", alwaysWriteExceptions="null",
disableAnsi="nul
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0 npCompressedFilePattern="null",
Configuration(Pr
2019-11-15 13:0
2019-11-15 13:0 ppend="null", locking="null",
Policies(Composi
DefaultRolloverS null", fileGroup="null",
bufferedIo="null), Filter=null)
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
SizeBasedTrigger
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0
2019-11-15 13:0

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

15-Nov-2019 13:02:34.4
15-Nov-2019 13:02:34.4
15-Nov-2019 13:02:34.4
15-Nov-2019 13:02:34.4
15-Nov-2019 13:02:34.4
15-Nov-2019 13:02:34.4
15-Nov-2019 13:02:34.4
15-Nov-2019 13:02:34.4
15-Nov-2019 13:02:34.4
15-Nov-2019 13:02:34.4
15-Nov-2019 13:02:34.4
15-Nov-2019 13:02:34.4
15-Nov-2019 13:02:34.4
15-Nov-2019 13:02:34.4
15-Nov-2019 13:02:34.4
15-Nov-2019 13:02:34.4
15-Nov-2019 13:02:34.4
15-Nov-2019 13:02:34.4
15-Nov-2019 13:02:34.4
15-Nov-2019 13:02:34.4
15-Nov-2019 13:02:34.4
15-Nov-2019 13:02:34.4
15-Nov-2019 13:02:34.4
15-Nov-2019 13:02:34.4
15-Nov-2019 13:02:34.4
15-Nov-2019 13:02:34.7
15-Nov-2019 13:02:34.9
15-Nov-2019 13:02:34.9
15-Nov-2019 13:02:34.9
15-Nov-2019 13:02:34.9
15-Nov-2019 13:02:35.0
15-Nov-2019 13:02:38.8
15-Nov-2019 13:02:38.9
were scanned but no TLD
15-Nov-2019 13:02:38.9
15-Nov-2019 13:02:38.9
ms
15-Nov-2019 13:02:38.9
15-Nov-2019 13:02:39.2
were scanned but no TLD
15-Nov-2019 13:02:40.0
ms
15-Nov-2019 13:02:40.0
15-Nov-2019 13:02:40.2
were scanned but no TLD
15-Nov-2019 13:02:40.2
15-Nov-2019 13:02:40.2
15-Nov-2019 13:02:40.6
were scanned but no TLD
15-Nov-2019 13:02:40.6
15-Nov-2019 13:02:40.6
15-Nov-2019 13:02:40.8
were scanned but no TLD
15-Nov-2019 13:02:40.9
ms
15-Nov-2019 13:02:40.9
15-Nov-2019 13:02:41.1
were scanned but no TLD
15-Nov-2019 13:02:41.1
15-Nov-2019 13:02:41.1
15-Nov-2019 13:02:41.5
were scanned but no TLD
15-Nov-2019 13:02:41.5
15-Nov-2019 13:02:41.5
15-Nov-2019 13:02:41.5
15-Nov-2019 13:02:41.5

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 15, 2019 9:54 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hey Brian,

When you send in a request, the return to that call is an acknowledgement. That is an xml document that will state if your request was accepted or not; and if it is not, what the reason is.

Are you seeing any acknowledgements?

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 11:49 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
According to dev the message that is coming back: remote host not allowed. ignoring request. They are stating is a response from your system telling us we are not allowed. Is there anyway you and I can get on the

phone, I can try and send some responses and see if you see anything in your log files. I am wondering if they are forming the response to you correctly.

As for the WSDL this is what I see from the 184.171 server.

<image003.png>

Full WSDL [G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)]

<?xml version="1.
- <wsdl:definitions
xmlns:soap="http:
- <wsdl:types>
- <xsd:schema xml
targetNamespace=
<xsd:element nam
<xsd:element nam
<xsd:element nam
<xsd:element nam
</xsd:schema>
</wsdl:types>
- <wsdl:message n
<wsdl:part elemen
</wsdl:message>
- <wsdl:message n
<wsdl:part elemen
</wsdl:message>
<wsdl:message na
+ <wsdl:message n
<wsdl:part elemen
</wsdl:message>
- <wsdl:message n
<wsdl:part elemen
</wsdl:message>
- <wsdl:message n
<wsdl:part elemen
</wsdl:message>
- <wsdl:message n
<wsdl:part elemen
</wsdl:message>
- <wsdl:message n
<wsdl:part elemen
</wsdl:message>
- <wsdl:portType n
- <wsdl:operation
<wsdl:input messa
<wsdl:output mess
</wsdl:operation>
- <wsdl:operation
<wsdl:input messa
<wsdl:output mess
</wsdl:operation>
- <wsdl:operation
<wsdl:input messa
<wsdl:output mess
</wsdl:operation>
- <wsdl:operation
<wsdl:input messa
<wsdl:output mess
</wsdl:operation>
</wsdl:portType>
- <wsdl:binding na
<soap:binding styl
- <wsdl:operation
<soap:operation s
- <wsdl:input nam
<soap:body use="l
</wsdl:input>
- <wsdl:output na
<soap:body use="l
</wsdl:output>
</wsdl:operation>
- <wsdl:operation
<soap:operation s
- <wsdl:input nam
<soap:body use="l
</wsdl:input>
- <wsdl:output na
<soap:body use="l
</wsdl:output>
</wsdl:operation>
- <wsdl:operation
<soap:operation s
- <wsdl:input nam
<soap:body use="l
</wsdl:input>
- <wsdl:output na
<soap:body use="l
</wsdl:output>
</wsdl:operation>
- <wsdl:operation
<soap:operation s
- <wsdl:input nam
<soap:body use="l
</wsdl:input>
- <wsdl:output na
<soap:body use="l
</wsdl:output>
</wsdl:operation>
</wsdl:binding>
- <wsdl:service na
- <wsdl:port bindin
<soap:address loca
</wsdl:port>
</wsdl:service>
</wsdl:definitions>

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 15, 2019 9:36 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

If you are able to telnet, then you should be able to send in a request.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 11:06 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
This is all from the 184.171 server.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 15, 2019 8:41 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Are you doing the ping and telnet from[redacted]

Your error message from earlier seems to be your network not allowing the access.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 10:37 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
I am reaching out to the[redacted]on[redacted] I can ping the IP and also hit the port.
<image004.png>

<image005.png>

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 15, 2019 8:26 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

What is the ip address you are trying to connect to?
Are you able to ping that machine?

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 10:22 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

Brian,
Thank you for checking in, sorry for the delay. I had the email together but it was in my draft. I tested the connection again today.

John,
I am still getting the remote Host not allowed. This is the error below:

2019-11-15 10:15:45,808 main DEBUG Log4jServletFilter initialized.
driversLicense=987654321
remote host=S-L-c-4-sec-7-cl-2
remote port=61799
remote addr=S-L-c-4-sec-7-cl-2
scheme =http
scheme =HTTP/1.1
local addr =S-L-c-4-sec-7-cl-2
local name =EPS-CLFACEMATCH
context path = /CHSBReceiver
Init parameter1 =Value1
remote host not allowed. ignoring request.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Friday, November 8, 2019 1:17 PM
To: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

John,
Thank you, I will work on testing the connection and let you know the results. According to Dev the other queries we will be running on the R1 and RI.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 8, 2019 12:18 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

I have added your configuration on the test broker for R1 and RI.
Are there more queries/transactions you'd like to test? Michaela may have requirements for other queries.

The ORI is MAMSPF022
Your requests come from S-L-c-4-sec-7-cl-2 and responses will be sent back to http://S-L-c-4-sec-7-cl-2:6060/CHSBReceiver/CHSBService

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Ouellette, John (EPS)
Sent: Tuesday, November 5, 2019 12:54 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>
Subject: RE: LRP network ideas?

Hi Brian,

I think Bill needs to have more information on your project to assign an ORI to use on the test broker.

Is there a project name on your side?

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Monday, November 4, 2019 3:30 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
Any luck on this.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Tuesday, October 22, 2019 12:32 PM
To: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Subject: RE: LRP network ideas?

John,
Yea we should be sending the XML packet with the service that we have created. Do you know if that IP is natted to [redacted] The server that we have our service on is the [redacted] Face match server. I don't have any servers in the [redacted] IP range unless it is getting natted somehow.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Tuesday, October 22, 2019 12:21 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hay Brian,

That won't work. The broker accepts an xml document containing the request, as well as other information.
Attached is a sample R1 request.

By the way, I have your requests coming from [redacted]

In order to get responses, you need a web service on your end to receive the responses and I'll need to configure it on the broker side.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Monday, October 21, 2019 5:04 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
Can you provide me with a DL that should work. From the .82 server this is what we are running:

http:/[redacted]6060/CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=987654321

I just need to update the drivers license number and hopefully it will work

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Tuesday, September 24, 2019 8:07 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

So, just R1 and RI?

I'll start configuring the test broker.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Tuesday, September 24, 2019 10:59 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
For the queries that we will using this is what I got back from Dev… let me know if this helps

…Attachments\CJISBroker_2016-03-24[13247].zip\CJISBroker_2016-03-24\CJISBroker\transactions\queries\rmv\r1\xml

…Attachments\CJISBroker_2016-03-24[13247].zip\CJISBroker_2016-03-24\CJISBroker\transactions\queries\rmv\ri\xml

The rest is correct, for testing the ORI list will grow once we go to production.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Tuesday, September 24, 2019 6:39 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hi Brian,

I haven't added your configuration to the test broker yet. Can you confirm the following:
For broker connections, we need the following:
IP Address for requests: [redacted]
URL for responses: http://[redacted]6060/CHSBReceiver/CHSBService
ORI: MAMSP0000
Queries: I need the list of queries/transactions you will be testing

You will submit to http://[redacted]6060/CJISService This call will return a synchronous acknowledgment.

Responses will come back from [redacted] You need to return a synchronous acknowledgement for each response.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Monday, September 23, 2019 7:53 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
I have deployed a new package, but I see this in the log.

2019-09-23 19:48
2019-09-23 19:48
2019-09-23 19:48 [redacted] G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative) on
org.apache.loggin
2019-09-23 19:48
2019-09-23 19:48
driversLicense=98
remote host=0:0:
remote port=6514
remote addr=0:0:
scheme =http
scheme =HTTP/
local addr =0:0:0:
local name =EPS-C
context path = /C
Init parameter1 =
remote host not a

can you check and make sure this machine has access:

EPS-CLFACEMATCH
Connection-specific DNS Suffix . :
IPv4 Address. . . . . : [redacted]
Subnet Mask . . . . . : 255.255.255.128
Default Gateway . . . . . : [redacted]

C:\Users\msp_user>
Regards,

<image002.png>

Brian Kruger
Operations and Support Manager

orensic Logic / COPLINK
20.488.1603
k er@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, September 6, 2019 6:15 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hey Brian,

I'm not sure what is in the test system either. I believe a dl of 987654321 will work; at least it used to.
Try to find something in test CJISWeb.

Remember that all queries will send in an xml document and will receive a return acknowledgement stating success or failure. If the request failed, the reason will be in the acknowledgement.

At a later time, seconds or less, the response will be returned to your web service. You must return an acknowledgement to that also to let the system know that the response was received and the next response can be sent.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Thursday, September 5, 2019 5:17 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
Not yet, I don't know what is in the test system… are they actually dls or fake ones.

Our query against our service is going to look something like, that will translate to yours.

http://[redacted]6060/CHSBReceiver/CHSBService?ori=REM000001&username=TEST&ssn=123123123&driversLicense=AZ67676767

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Thursday, September 5, 2019 1:09 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Have you tried your DL and SSN?

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Thursday, September 5, 2019 2:36 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
Do you have a sample DL and ssn, we can try passing through the service to see if we can pull an image. According to dev we are just utilizing the XML out of R1 and Ri.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, August 9, 2019 7:04 AM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Brian Kruger <bkruger@forensiclogic.com>; Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

All of the broker queries use the same method and accept an xml document. The contents of the xml direct what action the system should take. I have attached documentation for the broker. It's a 5 MB zip file.

If you can't accept zip files or 5 MB files let me know how to send the file.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, August 9, 2019 9:39 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Brian Kruger <bkruger@forensiclogic.com>; Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>
Subject: Re: LRP network ideas?

Thanks John, I'll defer to Brian Kruger to respond regarding where he's sending the query. Are you able to answer his question below?

"

> I can pull back the WSDL but want to send an image request to it to see if it actually pulls the image. I am looking for something like /GetPhoto?dl_num=20180061903&ss_num=2&type=M, the actually call method

"

On Aug 9, 2019, at 9:04 AM, Ouellette, John (EPS) <john.ouellette@mass.gov> wrote:

> Hi Brian,
>
> For broker connections to test, we need the following:
> IP Address for request: [redacted]
> URL for responses: http://[redacted]6060/CHSBReceiver/CHSBService
> ORI: MAMSP0000
> Queries:
>
> Can you confirm this information and send the list of queries you would like to run?
> Please remember that this system would only be used for test. Another system would need to be used when you move to production.
>
> John Ouellette | Massachusetts Executive Office of Public Safety and Security
> Office of Technology and Information Services
> Enterprise Application and Database Services
> Application Support and Management
> 200 Arlington Street Suite 2200
> Chelsea, MA 02150
> john.ouellette@state.ma.us | http://www.mass.gov/eops
>
> ---
>
> **From:** Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Sent:** Friday, August 9, 2019 8:54 AM
> **To:** Brian Kruger <bkruger@forensiclogic.com>
> **Cc:** Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Ouellette, John (EPS) <john.ouellette@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>
> **Subject:** Re: LRP network ideas?
>
> Hi Brian,
>
> are we testing on this yet?
>
> On Jul 22, 2019, at 1:37 PM, Brian Kruger <bkruger@forensiclogic.com> wrote:
>
> > Tim,
> > Attached is the full list of agencies and ORI that we currently have in the admin DB.
> >
> > Regards,
> >
> > <image001.png>
> > **Brian Kruger**
> > Operations and Support Manager
> > **Forensic Logic / COPLINK**
> > 520.488.1603
> > bkruger@forensiclogic.com
> > www.forensiclogic.com
> >
> > ***CONFIDENTIALITY:*** *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*
> >
> > ---
> >
> > **From:** Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
> > **Sent:** Monday, July 22, 2019 8:37 AM
> > **To:** Brian Kruger <bkruger@forensiclogic.com>
> > **Cc:** Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Ouellette, John (EPS) <john.ouellette@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
> > **Subject:** RE: LRP network ideas?
> >
> > Any update on this from dev, do you still need a sample RI url? Can you make sure you are also sending the CopLink user name in the UserID parameter.
> >
> > Tks, Brian
> >
> > ---
> >
> > **From:** Brian Kruger [mailto:bkruger@forensiclogic.com]
> > **Sent:** Thursday, July 18, 2019 5:19 PM
> > **To:** Mitchell, Timothy (EPS)
> > **Cc:** Ramsay, Christopher (EPS); Egnitz, Brian (POL); Ouellette, John (EPS)
> > **Subject:** RE: LRP network ideas?
> >
> > Tim,
> > I am still pending an answer back from dev on how they are going to pull the ORI. For now can we use `MAMSP0000. That is actually in our systems as MSP.`
> >
> > Regards,
> >
> > <image001.png>
> > **Brian Kruger**
> > Operations and Support Manager
> > **Forensic Logic / COPLINK**
> > 520.488.1603
> > bkruger@forensiclogic.com
> > www.forensiclogic.com
> >
> > ***CONFIDENTIALITY:*** *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
Sent: Tuesday, July 16, 2019 4:07 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Ouellette, John (EPS) <john.ouellette@state.ma.us>
Subject: RE: LRP network ideas?

Brian
What is the ORI that you are using for this setup? There is some configuration work that needs to be done on the broker side to allow your service to run transactions.
Thanks
Tim

Timothy Mitchell
Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise and Field Services Support Division
Public Safety Data Center
200 Arlington St., Suite 2200
Chelsea, MA 02150
(P) 617.660.4665
(F) 617.884.4601
(E) timothy.mitchell@state.ma.us
http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Monday, July 15, 2019 7:05 PM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

Folks,
For the RMV pull, does anybody have an example image we can try and run through. All the connectivity looks good, I have tried a few ways to pull an image without success.

Our service
http://[redacted]6060/CHSBReceiver/CHSBService?wsdl refers to http://[redacted]6060/CJISService?wsdl

I can pull back the WSDL but want to send an image request to it to see if it actually pulls the image. I am looking for something like /GetPhoto?dl_num=20180061903&ss_num=2&type=M, the actually call method

To pull back the WSDL
<?xml version="1
- <wsdl:definition
xmlns:soap="htt
- <wsdl:types>
- <xsd:schema xm
targetNamespac
<xsd:element na
<xsd:element na
<xsd:element na
<xsd:element na
</xsd:schema>
</wsdl:types>
- <wsdl:message
<wsdl:part eleme
</wsdl:message>
- <wsdl:message
<wsdl:part eleme
</wsdl:message>
<wsdl:message n
- <wsdl:message
<wsdl:part eleme
</wsdl:message>
- <wsdl:message
<wsdl:part eleme
</wsdl:message>
- <wsdl:message
<wsdl:part eleme
</wsdl:message>
- <wsdl:message
<wsdl:part eleme
</wsdl:message>
- <wsdl:message
<wsdl:part eleme
</wsdl:message>
- <wsdl:portType
- <wsdl:operatio
<wsdl:input mess
<wsdl:output me
</wsdl:operation
- <wsdl:operatio
<wsdl:input mess
<wsdl:output me
</wsdl:operation
- <wsdl:operatio
<wsdl:input mess
<wsdl:output me
</wsdl:operation
- <wsdl:operatio
<wsdl:input mess
<wsdl:output me
</wsdl:operation
</wsdl:portType
- <wsdl:binding n
<soap:binding st
- <wsdl:operatio
<soap:operation
- <wsdl:input na
<soap:body use=
</wsdl:input>
- <wsdl:output n
<soap:body use=
</wsdl:output>
</wsdl:operation
- <wsdl:operatio
<soap:operation
- <wsdl:input nam

[redacted]
G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

<soap:body
</wsdl:inpu
. <wsdl:out
<soap:body
</wsdl:out
</wsdl:ope
. <wsdl:ope
<soap:oper
. <wsdl:inp
<soap:body
</wsdl:inpu
. <wsdl:out
<soap:body
</wsdl:out
</wsdl:ope
. <wsdl:ope
<soap:oper
. <wsdl:inp
<soap:body
</wsdl:inpu
. <wsdl:out
<soap:body
</wsdl:out
</wsdl:ope
</wsdl:bind
. <wsdl:ser
. <wsdl:por
<soap:addr
</wsdl:port
</wsdl:serv
</wsdl:defi

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
Sent: Wednesday, May 8, 2019 5:52 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: Re: LRP network ideas?

Brian
Can you test the connectivity again?
Thanks

Sent from my iPhone

On May 7, 2019, at 10:43 AM, Brian Kruger <bkruger@forensiclogic.com> wrote:

> Tim,
> Thank you sir, sorry this fell off my radar. I was working on reallocation for Dan.
>
> Regards,
>
> <image001.png>
>
> **Brian Kruger**
> Operations and Support Manager
> **Forensic Logic / COPLINK**
> 520.488.1603
> bkruger@forensiclogic.com
> www.forensiclogic.com
>
> ***CONFIDENTIALITY:*** *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*
>
> ---
>
> **From:** Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
> **Sent:** Tuesday, May 7, 2019 7:42 AM
> **To:** Brian Kruger <bkruger@forensiclogic.com>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
> **Subject:** RE: LRP network ideas?
>
> Brian
> Yes you will need to run the transactions across to the test server first and DCJIS will need to approve it before you can run to the production server. I will check out the firewall rules today and let you know.
> Thanks
>
> Timothy Mitchell
> Massachusetts Executive Office of Public Safety and Security
> Office of Technology and Information Services
> Enterprise and Field Services Support Division
> Public Safety Data Center
> 200 Arlington St., Suite 2200
> Chelsea, MA 02150
> (P) 617.660.4665
> (F) 617.884.4601
> (E) timothy.mitchell@state.ma.us
> http://www.mass.gov/eops
>
> ---
>
> **From:** Brian Kruger <bkruger@forensiclogic.com>
> **Sent:** Tuesday, May 07, 2019 10:40 AM
> **To:** Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> **Subject:** RE: LRP network ideas?
>
> Chris,
> I am guessing test first, that way we can validate the broker, unless the route is setup already for production and I can switch it out to that.

Brian E.,
Your thoughts?

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Sent: Tuesday, May 7, 2019 7:18 AM
To: Brian Kruger <bkruger@forensiclogic.com>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Brian,

G.L. c. 4.sec. 7.cl.2is the TEST cjis broker system. Is the test system what you're looking to use?

-Chris

Christopher Ramsay | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Division of Enterprise & Field Services Support | Enterprise Systems

200 Arlington St. Suite 2200
Chelsea, MA 02150
p. 617.660.4720 | f. 617.660.4613
christopher.ramsay@mass.gov | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Tuesday, May 7, 2019 1:49 AM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

Tim,
I was checking the cjis broker service and I can't get to theG.L. c. 4.sec. 7.cl.2on 6060 from the FR server atG.L. c. 4.sec. 7.cl.2 I was going through old email and just checking the status of the connections. TheG.L. c. 4.sec. 7.cl.2is what I received from Dev. Let me know if this is not correct.

<image003.jpg>

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
Sent: Friday, March 1, 2019 1:28 PM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Brian Kruger <bkruger@forensiclogic.com>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Hi folks
The CJIS broker transactions will need to useG.L. c. 4.sec as that is what they have been configured for in the past.

We have discussed the LPR port request and we think that going with a higher port seems to be more acceptable to EOTSS to allow through their public access firewall. Would port 56446 (https) work? We will need to open a ticket with EOTSS to have them allow this port through.

Thanks

Timothy Mitchell
Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise and Field Services Support Division
Public Safety Data Center
200 Arlington St., Suite 2200
Chelsea, MA 02150
(P) 617.660.4665
(F) 617.884.4601
(E) timothy.mitchell@state.ma.us
http://www.mass.gov/eops

From: Egnitz, Brian (POL)
Sent: Friday, March 01, 2019 12:44 PM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Brian Kruger <bkruger@forensiclogic.com>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

Hi Tim,

I spoke with Brian Kruger and he wants the RI image CJIS Broker return to go to the same port as the ALPR image results, are there any issues with that? If not, is your team picking the port or is CopLink? I've included his email request. It sounds like they want to use the same web service to simplify the two integrations (LPR & RMV Images).

Tks, Brian

From: Mitchell, Timothy (EPS)
Sent: Friday, February 15, 2019 9:39 AM
To: Brian Kruger; Egnitz, Brian (POL); Ramsay, Christopher (EPS)
Subject: RE: LRP network ideas?

Brian
We are in receipt and reviewing on this side. I will get back to you next week.

Thanks

Timothy Mitchell
Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise and Field Services Support Division
Public Safety Data Center
200 Arlington St., Suite 2200
Chelsea, MA 02150
(P) 617.660.4665
(F) 617.884.4601
(E) timothy.mitchell@state.ma.us
http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Tuesday, February 12, 2019 2:46 PM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

Tim,
Here you go.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
Sent: Tuesday, February 12, 2019 8:19 AM
To: Brian Kruger <bkruger@forensiclogic.com>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian
Did you send over a diagram for review? If yes, can you resend as I can't come across it? We need to review this before providing any additional ports.
Thanks

Timothy Mitchell
Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise and Field Services Support Division
Public Safety Data Center
200 Arlington St., Suite 2200
Chelsea, MA 02150
(P) 617.660.4665
(F) 617.884.4601
(E) timothy.mitchell@state.ma.us
http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Tuesday, February 12, 2019 12:00 AM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

Tim/Brian,
We are ready to start up the LPR ingest again, however I still need to assign a port to Tomcat on the FR server that will be accessible from both application servers. Is there any port range that we can shoot for. I would like to get the LPR data flowing as soon as possible.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Thursday, February 7, 2019 1:47 PM
To: 'Mitchell, Timothy (EPS)' <timothy.mitchell@state.ma.us>; 'Egnitz, Brian (POL)' <brian.egnitz@state.ma.us>; 'Ramsay, Christopher (EPS)' <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Tim,
Do you have any ports you send me that would be allowed for the connection from the app servers. I can update the diagram for approval that will work on the FR server. I will need two, one for Tomcat and one for LEXSR TR.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Thursday, February 7, 2019 8:50 AM
To: 'Mitchell, Timothy (EPS)' <timothy.mitchell@state.ma.us>; 'Egnitz, Brian (POL)' <brian.egnitz@state.ma.us>; 'Ramsay, Christopher (EPS)' <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Tim/Brian,
I was thinking last night and would actually like to move the new Image service to the FR server S.L. c. 4 sec. 7 cl 26We have a route in place already from both PAA and Internal web to that server. I would just need to know what port to run tomcat on. This would also work for the Thompson Reuters adapter as well. Let me know what you guys think.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Monday, February 4, 2019 11:17 AM
To: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: LRP network ideas?

Brian/Tim,
Nick is almost done with the new LPR service that will remove the images from the database and have a tomcat app that host the images for a return to the UI. What I need to know:

<!--
[if
!supportLists]-
-
>1.
<!-
-
[endif]-
-
>The
Migration
will
sit
on
the
migration
server
and
needs
access
to
the
LPR
database
to
pull
out
the
metadata
and
create
the
URL
for
the
Image
links.
<!--
[if
!supportLists]-
-
>2.
<!-
-
[endif]-
-
>The
new
service
is
going
to
be
hosted
in
Tomcat,
so
this
service
will
need
access
to
the
LPR
database
for
images
and
both
application
servers
need
to
be
able
to

query this tomcat instance. I just need to know where to put it, I can host it on both severs or if we can set it up on the internal server and have a firewall rule that will allow the DMZ server to talk to the internal server. Let me know if you would like to have a call on this. I have attached a rough network diagram for visual reference.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

<MSP agency ORI.xlsx>

From: Egnitz, Brian (POL)
To: Brian Kruger
Cc: Rhonda Fromm
Subject: Re: LRP network ideas?
Date: Tuesday, January 7, 2020 3:05:10 PM

Thanks

> On Jan 7, 2020, at 10:10 AM, Brian Kruger <bkruger@forensiclogic.com> wrote:
>
> Brian,
> We have dropped three builds in the last 2 weeks out there. They are still having connection code issues with the debug code in place. I am expecting to have another build either today or tomorrow. The last one was deployed yesterday.
>
> Regards,
>
> <image001.png>
> **Brian Kruger**
> Operations and Support Manager
> **Forensic Logic / COPLINK**
> Office: 520.367.2775
> Mobile: 520.488.1603
> bkruger@forensiclogic.com
> www.forensiclogic.com
>
> ***CONFIDENTIALITY:*** *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*
>
> ---
>
> **From:** Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
> **Sent:** Tuesday, January 7, 2020 7:11 AM
> **To:** Brian Kruger <bkruger@forensiclogic.com>
> **Cc:** Rhonda Fromm <rfromm@forensiclogic.com>
> **Subject:** Re: LRP network ideas?
>
> How are we making out on RMV?
>
> > On Dec 6, 2019, at 11:31 AM, Brian Kruger <bkruger@forensiclogic.com> wrote:
> >
> > Billy,
> > Please let the group know when this will be available. I will work with John to get it deployed and tested as soon as we have it released.
> >
> > Regards,
> >
> > **Brian Kruger**
> > Operations and Support Manager



Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Tuesday, November 26, 2019 1:17 PM
To: 'Ouellette, John (EPS)' <john.ouellette@state.ma.us>; 'Egnitz, Brian (POL)' <brian.egnitz@state.ma.us>; Samson Dunatunga <mdunatunga@forensiclogic.com>; Billy Moore <bmoore@forensiclogic.com>
Cc: 'Dunne, Michaela (CHS)' <michaela.dunne@state.ma.us>; 'Dunn-CHS, William (CHS)' <william.dunn-chs@state.ma.us>; 'Mitchell, Timothy (EPS)' <timothy.mitchell@state.ma.us>; 'Ramsay, Christopher (EPS)' <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

John,
Thank you for the information on the call this afternoon.

Samson/Billy,
We need to add some additional debug code into our service so we can see the full communication path and what is being sent and received. John is also in the process to check and make sure their three servers can reach back into our [redacted] I have also reattached the IP wireshark I did this morning.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Tuesday, November 26, 2019 8:29 AM
To: Ouellette, John (EPS) <john.ouellette@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

John,
Give me a few minutes and I will give you a call. Here is the CSV file from wireshark. I had to repull it. I don't see any actually log details in our tomcat instance. In the wireshark though I see a bunch of event code errors like below:

Event: <Unknown eventcode 72>, <Unknown eventcode 111>, <Unknown eventcode 116>, <Unknown eventcode 121>, <Unknown eventcode 110>, <Unknown eventcode 45>, <Unknown eventcode 112>, <Unknown eventcode 110>, <Unknown eventcode 114>, <Unknown eventcode 115>, <Unknown eventcode 47>, <Unknown eventcode 110>, <Unknown eventcode 111>, <Unknown eventcode 118>, <Unknown eventcode 110>, <Unknown eventcode 111>, <Unknown eventcode 47>, ColormapNotify, <Unknown eventcode 97>, <Unknown eventcode 120>, <Unknown eventcode 58>, <Unknown eventcode 46>, <Unknown eventcode 104>, <Unknown eventcode 46>, <Unknown eventcode 117>, <Unknown eventcode 97>, <Unknown eventcode 47>, <Unknown eventcode 62>, <Unknown eventcode 114>, <Unknown eventcode 114>, <Unknown eventcode 82>, <Unknown eventcode 120>, <Unknown eventcode 101>, MappingNotify, <Unknown eventcode 109>, <Unknown eventcode 98>, <Unknown eventcode 47>, <Unknown eventcode 119>, <Unknown eventcode 62>, <Unknown eventcode 114>, ColormapNotify, <Unknown eventcode 62>, <Unknown eventcode 115>, MappingNotify, <Unknown eventcode 110>

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Tuesday, November 26, 2019 7:29 AM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Hey Brian,

You can call me at 617-[redacted]

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Monday, November 25, 2019 7:53 PM
To: Brian Kruger <bkruger@forensiclogic.com>; Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: Re: LRP network ideas?

Does it make sense to schedule a call and work through it in real time?

> On Nov 22, 2019, at 4:00 PM, Ouellette, John (EPS) <john.ouellette@mass.gov> wrote:
>
> Hi Brian,
>
> I do not see any requests for your ORI. Can you review the acknowledgements that the broker sends back as a return value? There may be error information in there.
>
> John Ouellette | Massachusetts Executive Office of Public Safety and Security
> Office of Technology and Information Services
> Enterprise Application and Database Services
> Application Support and Management
> 200 Arlington Street Suite 2200
> Chelsea, MA 02150
> john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 22, 2019 3:47 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

John,
Can you check again and see if there is a request coming into the [redacted] server. I ran a packet capture and I do see data sent from the [redacted] to the [redacted] server.

<image001.png>

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 22, 2019 12:26 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

I'm not sure if [redacted] is a load balancer. I don't believe it is though. It doesn't matter though, that is where you will send requests. You will receive a synchronous response called an acknowledgement. That will let you know if your request was accepted or rejected.

Later, an asynchronous response will be sent from [redacted] or [redacted] to your web service.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 22, 2019 2:19 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
The [redacted] is a load balancer for the services correct. As far as I know there should be no blocked traffic to the [redacted] but let me include Chris and Tim on this thread.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 22, 2019 9:36 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

I didn't find any submitted requests.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Ouellette, John (EPS)
Sent: Friday, November 22, 2019 11:34 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

I can check.

The broker will send responses from [redacted] or [redacted] on [redacted] Make sure you are allowing that traffic.

When you send in a request you will receive an xml document as the return value. The documents lists if the request was accepted and if it wasn't, why it wasn't. You should be checking those.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 22, 2019 11:28 AM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

Bill,

I have the service send back a no data found so it looks like we are connecting. Can you check your logs to see if our request actually made it into your system.

I am sending the following test cycle from the [redacted] web server to our FR server

http://[redacted]6060/CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=S32935254

Just so everybody is clear, this the is the connection path

[redacted] → [redacted] [redacted] → [redacted]

Return path

[redacted] → [redacted] → [redacted]

Log of request:

2019-11-22 11:16:13,982 main DEBUG LoggerContext[name=MassLPRServlet, org.apache.logging.log4j.core.LoggerContext@59303963] started OK with configuration org.apache.logging.log4j.core.config.properties.PropertiesConfiguration@61e86192.
2019-11-22 11:16:13,982 main DEBUG Log4jServletContextListener ensuring that Log4j starts up properly.
2019-11-22 11:16:13,982 main DEBUG Log4jServletFilter initialized.
driversLicense=S32935254
remote host=[redacted]
remote port=60194
remote addr=[redacted]
scheme =http
scheme =HTTP/1.1
local addr =[redacted]
local name =EPS-CLFACEMATCH
context path = /CHSBReceiver
Init parameter1 =Value1
Current UUID : f3837e1f-0e40-4af6-8587-203e99240d92
javax.xml.bind.JAXBElement@227d5180
Request UUID:[redacted]f3837e1f-0e40-4af6-8587-203e99240d92

Rest response file contains:
no data found.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Thursday, November 21, 2019 2:11 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Ouellette, John (EPS) <john.ouellette@state.ma.us>
Subject: RE: LRP network ideas?

Thanks Bill!

It looks like we are close on this.

-Brian

From: Dunn-CHS, William (CHS)
Sent: Tuesday, November 19, 2019 7:50 AM
To: Brian Kruger; Ouellette, John (EPS)
Cc: Dunne, Michaela (CHS); Egnitz, Brian (POL); Dunn-CHS, William (CHS)
Subject: RE: LRP network ideas?

I think I see what might be part of the problem.

The R1 is either OLN or SSN, you can not send both at the same time.

There is No TEST SSN inquiry, use someone from MSP who is working on your project or if you have a developer who is from MA
The TEST [redacted]

From: Brian Kruger [mailto:bkruger@forensiclogic.com]
Sent: Monday, November 18, 2019 6:33 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
Dev confirmed they are sending XML in the request. Do you have a valid License number in the test data I can try.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 15, 2019 11:16 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

The broker is a web service. You need to create a client to connect. Requests are made by sending in an xml document.

Did I forget to send you the broker documentation? Let me know.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 1:10 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>

Subject: RE: LRP network ideas?

John,
I ran two queries through IE I don't see an acknowledge me in the logs.
Below is what I am seeing. Do we have a valid Lic number that is in the system I can try, or valid SSN.

My test URLs are:"
http://[redacted]6060/CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=987654321

http://[redacted]6060/CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=987654321

In my access log I see a 200:

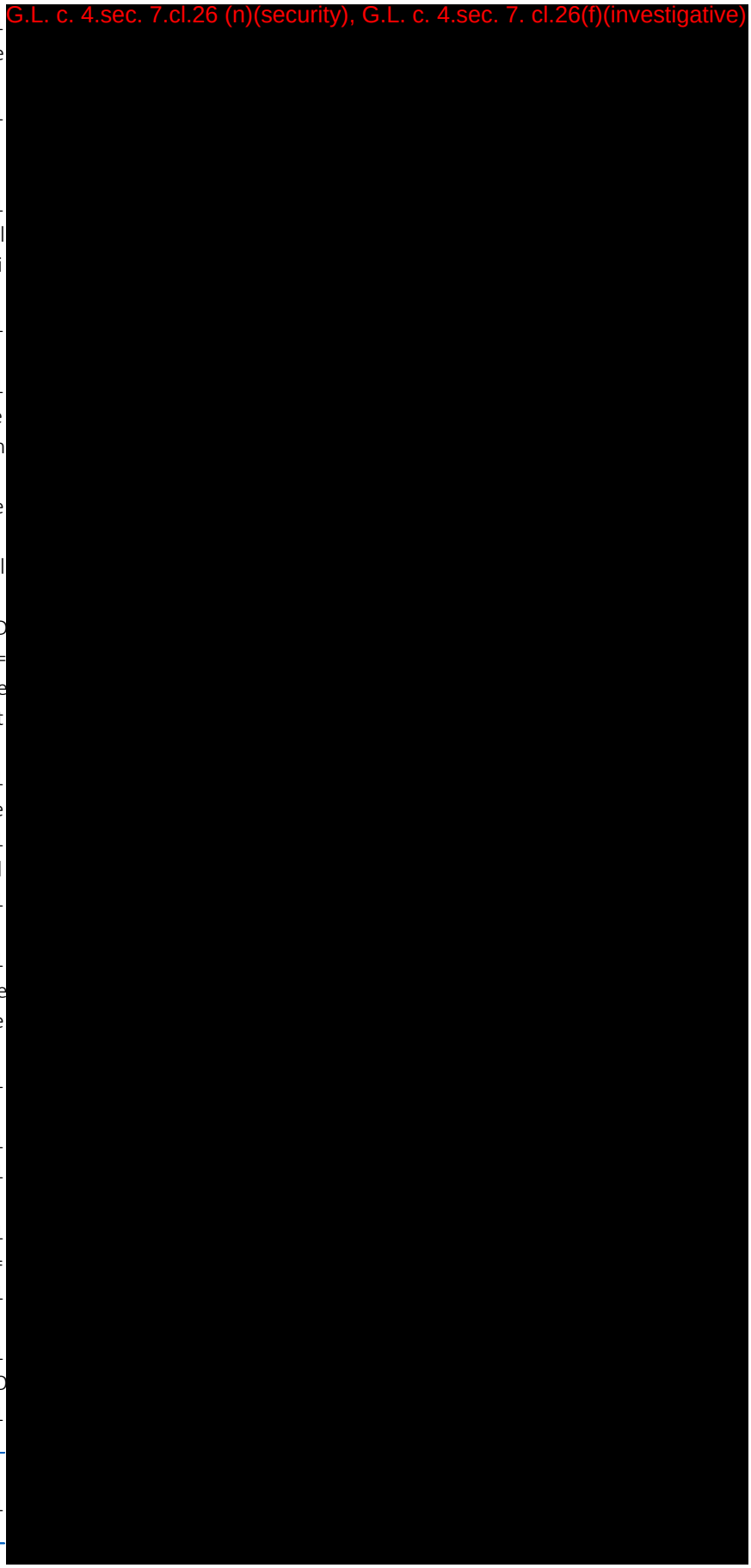
[redacted] - - [15/Nov/2019:13:02:50 -0500] "GET /CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=987654321 HTTP/1.1" 200 -
[redacted] - - [15/Nov/2019:13:03:05 -0500] "GET /CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=987654321 HTTP/1.1" 200 –

In my log stdout log I see this:

2019 G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative) [redacted]

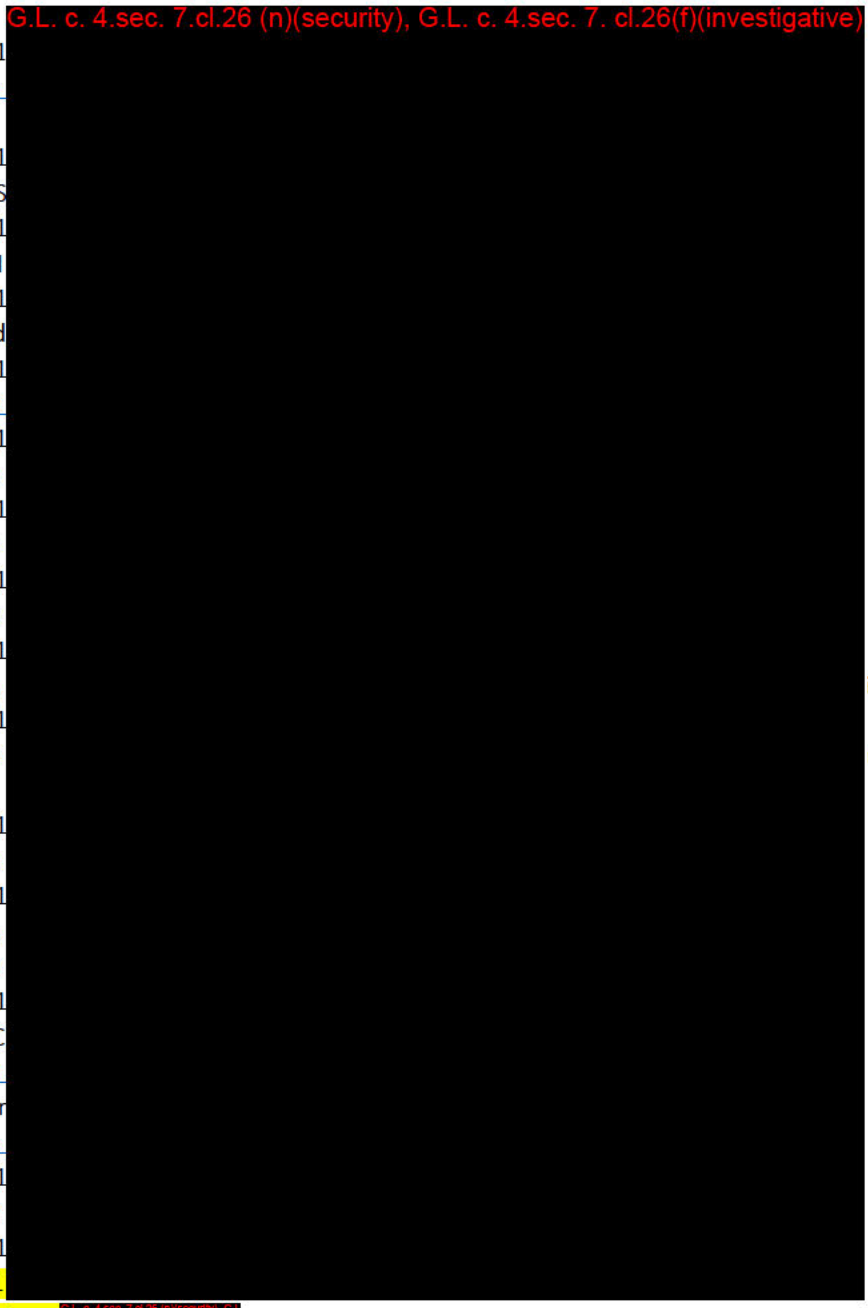

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)



2019-11-1
{TimeBase
modulate
2019-11-1
Plugin[na
class=org.
2019-11-1
DefaultRol
compressi
tempCom
2019-11-1
class=org.
2019-11-1
RollingFile
filePattern
append="
[TimeBase
modulate
DefaultRol
useMax=t
createOnD
fileGroup=
immediate
%C{1.} [%t
Filter=null
2019-11-1
C:\Apache
2019-11-1
found 2 pl
2019-11-1
07T17:27:
2019-11-1
Composite
[TimeBase
modulate
2019-11-1
class=org.
2019-11-1
2019-11-1
class=org.
2019-11-1
onMatch=
2019-11-1
creating d
2019-11-1
SYSTEM_O
2019-11-1
org.apach
initialized
2019-11-1
org.apach

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)



2019-11
org.apa
OK.
2019-11
OutputS
2019-11
SYSTEM
2019-11
stopped
2019-11
org.apa
2019-11
org.apa
2019-11
org.apa
2019-11
org.apa
2019-11
org.apa
2019-11
org.apa
2
2019-11
org.apa
2019-11
org.apa
timesta
2019-11
LoggerC
org.apa
configur
org.apa
2019-11
ensurin
2019-11
driversL
remote host=
remote port=62034
remote addr=
scheme =http
scheme =HTTP/1.1
local addr =
local name =EPS-CLFACEMATCH
context path = /CHSBReceiver
Init parameter1 =Value1
remote host not allowed. ignoring request.
driversLicense=987654321
remote host=
remote port=62034
remote addr=
scheme =http

images

nsole-

scheme =HTTP/1.1
local addr = [redacted]
local name =EPS-CLFACEMATCH
context path = /CHSBReceiver
Init parameter1 =Value1
remote host not allowed. ignoring request.

My stderr log

[redacted]

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

15-Nov-2019 1
org.apache.cat
argument: -Dig
9.0.14\endorse
15-Nov-2019 1
org.apache.cat
argument: -Dja
15-Nov-2019 1
org.apache.cat
argument: -
Djava.util.loggi
15-Nov-2019 1
org.apache.cat
argument: -Dja
9.0.14\conf\log
15-Nov-2019 1
org.apache.cat
argument: exit
15-Nov-2019 1
org.apache.cat
argument: abor
15-Nov-2019 1
org.apache.cat
argument: -Xm
15-Nov-2019 1
org.apache.cat
argument: -Xm
15-Nov-2019 1
org.apache.cat
based Apache T
15-Nov-2019 1
org.apache.cat
capabilities: IPv
15-Nov-2019 1
org.apache.cat
configuration:
15-Nov-2019 1
org.apache.cat
successfully init
15-Nov-2019 1
org.apache.coy
nio-6060"]
15-Nov-2019 1
org.apache.coy
nio-8009"]
15-Nov-2019 1
org.apache.cat
milliseconds
15-Nov-2019 1
org.apache.cat
[Catalina]

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

15-Nov-2019 13:02:
org.apache.catalina.
engine: [Apache Tom
15-Nov-2019 13:02:
org.apache.catalina.s
application archive [
9.0.14\webapps\CHS
15-Nov-2019 13:02:
com.sun.xml.ws.tran
WSSERVLET14: JAX-
15-Nov-2019 13:02:
org.apache.jasper.se
scanned for TLDs yet
logger for a complet
found in them. Skipp
startup time and JSP
15-Nov-2019 13:02:
com.sun.xml.ws.tran
WSSERVLET12: JAX-
15-Nov-2019 13:02:
org.apache.catalina.s
application archive [
9.0.14\webapps\CHS
15-Nov-2019 13:02:
org.apache.catalina.s
application archive [
9.0.14\webapps\Ima
15-Nov-2019 13:02:
org.apache.jasper.se
scanned for TLDs yet
logger for a complet
found in them. Skipp
startup time and JSP
15-Nov-2019 13:02:
org.apache.catalina.s
application archive [
9.0.14\webapps\Ima
15-Nov-2019 13:02:
org.apache.catalina.s
application directory
15-Nov-2019 13:02:
org.apache.jasper.se
scanned for TLDs yet
logger for a complet
found in them. Skipp
startup time and JSP
15-Nov-2019 13:02:
org.apache.catalina.s
web application dire
9.0.14\webapps\doc
15-Nov-2019 13:02:

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

[redacted]

```
org.apache.catalina.sta
application directory [D
9.0.14\webapps\exam
15-Nov-2019 13:02:40.
org.apache.jasper.servl
scanned for TLDs yet co
logger for a complete li
found in them. Skippin
startup time and JSP co
15-Nov-2019 13:02:40.
org.apache.catalina.sta
web application directo
9.0.14\webapps\exam
15-Nov-2019 13:02:40.
org.apache.catalina.sta
application directory [D
manager]
15-Nov-2019 13:02:40.
org.apache.jasper.servl
scanned for TLDs yet co
logger for a complete li
found in them. Skippin
startup time and JSP co
15-Nov-2019 13:02:40.
org.apache.catalina.sta
web application directo
9.0.14\webapps\host-
15-Nov-2019 13:02:40.
org.apache.catalina.sta
application directory [D
9.0.14\webapps\mana
15-Nov-2019 13:02:41.
org.apache.jasper.servl
scanned for TLDs yet co
logger for a complete li
found in them. Skippin
startup time and JSP co
15-Nov-2019 13:02:41.
org.apache.catalina.sta
web application directo
9.0.14\webapps\mana
15-Nov-2019 13:02:41.
org.apache.catalina.sta
application directory [D
15-Nov-2019 13:02:41.
org.apache.jasper.servl
scanned for TLDs yet co
logger for a complete li
found in them. Skippin
startup time and JSP co
15-Nov-2019 13:02:41.
```

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

org.apach
web appli
9.0.14\w
15-Nov-2
org.apach
nio-6060"
15-Nov-2
org.apach
nio-8009"
15-Nov-2
org.apach
millisecon

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 15, 2019 9:54 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hey Brian,

When you send in a request, the return to that call is an acknowledgement. That is an xml document that will state if your request was accepted or not; and if it is not, what the reason is.

Are you seeing any acknowledgements?

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management

200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 11:49 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
According to dev the message that is coming back: remote host not allowed. ignoring request. They are stating is a response from your system telling us we are not allowed. Is there anyway you and I can get on the phone, I can try and send some responses and see if you see anything in your log files. I am wondering if they are forming the response to you correctly.

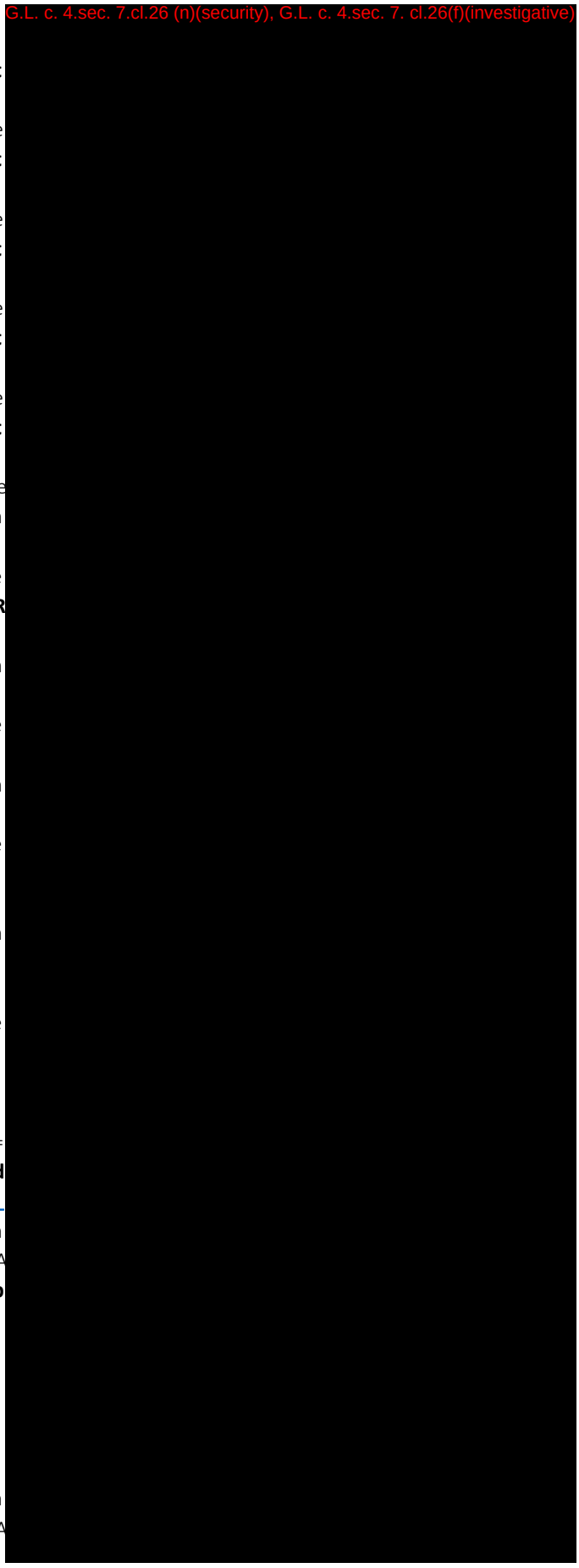
As for the WSDL this is what I see from the 184.171 server.

<image003.png>

Full WSDL
<?xml version=
- <wsdl:definiti
xmlns:wsdl="ht
xmlns:tns="htt
xmlns:soap="ht
xmlns:ns1="htt
targetNamespa
- <wsdl:types>
- <xsd:schema x
xmlns:tns="htt
attributeFormD
targetNamespa
<xsd:element n
<xsd:element n
<xsd:element n
<xsd:element n
</xsd:schema>
</wsdl:types>
- <wsdl:messag
<wsdl:part elem
</wsdl:messag
- <wsdl:messag
<wsdl:part elem
</wsdl:messag
<wsdl:message

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)



+ <wsdl:message nam
<wsdl:part element="**t**
</wsdl:message>
- <wsdl:message name
<wsdl:part element="**t**
</wsdl:message>
- <wsdl:message name
<wsdl:part element="**t**
</wsdl:message>
- <wsdl:message name
<wsdl:part element="**t**
</wsdl:message>
- <wsdl:message name
<wsdl:part element="**t**
</wsdl:message>
- <wsdl:portType name
- <wsdl:operation nam
<wsdl:input message=
<wsdl:output message
name="**processEventR**
</wsdl:operation>
- <wsdl:operation nam
<wsdl:input message=
<wsdl:output message
</wsdl:operation>
- <wsdl:operation nam
<wsdl:input message=
<wsdl:output message
name="**processReque**
</wsdl:operation>
- <wsdl:operation nam
<wsdl:input message=
/>
<wsdl:output message
name="**processRespo**
</wsdl:operation>
</wsdl:portType>
- <wsdl:binding name=
<soap:binding style="**d**
transport="**http://sch**
- <wsdl:operation nam
<soap:operation soapA
- <wsdl:input name="**p**
<soap:body use="**liter**
</wsdl:input>
- <wsdl:output name=
<soap:body use="**liter**
</wsdl:output>
</wsdl:operation>
- <wsdl:operation nam
<soap:operation soapA

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

[redacted]

- <wsdl:input name="**ve**
<soap:body use="**literal**
</wsdl:input>
- <wsdl:output name="
<soap:body use="**literal**
</wsdl:output>
</wsdl:operation>
- <wsdl:operation name
<soap:operation soapA
- <wsdl:input name="**pr**
<soap:body use="**literal**
</wsdl:input>
- <wsdl:output name="
<soap:body use="**literal**
</wsdl:output>
</wsdl:operation>
- <wsdl:operation name
<soap:operation soapA
- <wsdl:input name="**pr**
<soap:body use="**literal**
</wsdl:input>
- <wsdl:output name="
<soap:body use="**literal**
</wsdl:output>
</wsdl:operation>
</wsdl:binding>
- <wsdl:service name="
- <wsdl:port binding="**t**
name="**CJISServiceCXF**
<soap:address location
</wsdl:port>
</wsdl:service>
</wsdl:definitions>

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please*

notify the sender and delete this e-mail from your system.

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 15, 2019 9:36 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

If you are able to telnet, then you should be able to send in a request.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 11:06 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
This is all from the 184.171 server.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 15, 2019 8:41 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Are you doing the ping and telnet from [redacted]

Your error message from earlier seems to be your network not allowing the access.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 10:37 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
I am reaching out to the [redacted] on [redacted] I can ping the IP and also hit the port.
<image004.png>

<image005.png>

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please*

notify the sender and delete this e-mail from your system.

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 15, 2019 8:26 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

What is the ip address you are trying to connect to?
Are you able to ping that machine?

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 10:22 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

Brian,
Thank you for checking in, sorry for the delay. I had the email together but it was in my draft. I tested the connection again today.

John,
I am still getting the remote Host not allowed. This is the error below:

2019-11-15 10:15:45,808 main DEBUG Log4jServletFilter initialized.
driversLicense=987654321
remote host=[redacted]
remote port=61799
remote addr=[redacted]
scheme =http
scheme =HTTP/1.1
local addr =[redacted]
local name =EPS-CLFACEMATCH

context path = /CHSBReceiver
Init parameter1 =Value1
remote host not allowed. ignoring request.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Friday, November 8, 2019 1:17 PM
To: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

John,
Thank you, I will work on testing the connection and let you know the results. According to Dev the other queries we will be running on the R1 and RI.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>

Sent: Friday, November 8, 2019 12:18 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

I have added your configuration on the test broker for R1 and RI.
Are there more queries/transactions you'd like to test? Michaela may have requirements for other queries.

The ORI is MAMSPF022
Your requests come from [redacted] and responses will be sent back to http://[redacted]6060/CHSBReceiver/CHSBService

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Ouellette, John (EPS)
Sent: Tuesday, November 5, 2019 12:54 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>
Subject: RE: LRP network ideas?

Hi Brian,

I think Bill needs to have more information on your project to assign an ORI to use on the test broker.
Is there a project name on your side?

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Monday, November 4, 2019 3:30 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>

Subject: RE: LRP network ideas?

John,
Any luck on this.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Tuesday, October 22, 2019 12:32 PM
To: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Subject: RE: LRP network ideas?

John,
Yea we should be sending the XML packet with the service that we have created. Do you know if that IP is natted to [redacted] The server that we have our service on is the [redacted] Face match server. I don't have any servers in the [redacted] x IP range unless it is getting natted somehow.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Tuesday, October 22, 2019 12:21 PM

To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hay Brian,

That won't work. The broker accepts an xml document containing the request, as well as other information.
Attached is a sample R1 request.

By the way, I have your requests coming from [redacted]

In order to get responses, you need a web service on your end to receive the responses and I'll need to configure it on the broker side.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Monday, October 21, 2019 5:04 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
Can you provide me with a DL that should work. From the .82 server this is what we are running:

http://[redacted]6060/CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=987654321

I just need to update the drivers license number and hopefully it will work

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please*

notify the sender and delete this e-mail from your system.

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Tuesday, September 24, 2019 8:07 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

So, just R1 and RI?

I'll start configuring the test broker.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Tuesday, September 24, 2019 10:59 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
For the queries that we will using this is what I got back from Dev… let me know if this helps

…Attachments\CJISBroker_2016-03-24[13247].zip\CJISBroker_2016-03-24\CJISBroker\transactions\queries\rmv\r1\xml

…Attachments\CJISBroker_2016-03-24[13247].zip\CJISBroker_2016-03-24\CJISBroker\transactions\queries\rmv\ri\xml

The rest is correct, for testing the ORI list will grow once we go to production.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized*

disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Tuesday, September 24, 2019 6:39 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hi Brian,

I haven't added your configuration to the test broker yet. Can you confirm the following:
For broker connections, we need the following:
IP Address for request: [redacted]
URL for responses:
http://[redacted]6060/CHSBReceiver/CHSBService
ORI: MAMSP0000
Queries: I need the list of queries/transactions you will be testing

You will submit to http://[redacted]6060/CJISService This call will return a synchronous acknowledgment.

Responses will come back from [redacted] or [redacted] on [redacted] You need to return a synchronous acknowledgement for each response.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Monday, September 23, 2019 7:53 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
I have deployed a new package, but I see this in the log.

2019-09-23 19:48:37,297 main DEBUG Registering MBean org.apache.logging.log4j2:type=MassLPRServlet,component=Appenders,name=RollingFile
2019-09-23 19:48:37,304 main DEBUG org.apache.logging.log4j.core.util.SystemClock does not support precise timestamps.
2019-09-23 19:48:37,305 main DEBUG

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

LoggerContext[n
org.apache.loggi
configuration
org.apache.loggi
2019-09-23 19:4
ensuring that Log
2019-09-23 19:4
driversLicense=9
remote host=0:0
remote port=651
remote addr=0:0
scheme =http
scheme =HTTP
local addr =0:0:0:
local name =EPS-
context path = /C
Init parameter1 =
remote host not

can you check and make sure this machine has access:

EPS-CLFACEMATCH
Connection-specific DNS Suffix . :
IPv4 Address. . . . . : G.L. c. 4.sec. 7.cl.26 (n)(security), G.L
Subnet Mask . . . . . : 255.255.255.128
Default Gateway . . . . . : G.L. c. 4.sec. 7.cl.26 (n)(security), G.L

C:\Users\msp_user>
Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, September 6, 2019 6:15 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hey Brian,

I'm not sure what is in the test system either. I believe a [redacted] will work; at least it used to.
Try to find something in test CJISWeb.

Remember that all queries will send in an xml document and will receive a return acknowledgement stating success or failure. If the request failed, the reason will be in the acknowledgement.

At a later time, seconds or less, the response will be returned to your web service. You must return an acknowledgement to that also to let the system know that the response was received and the next response can be sent.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Thursday, September 5, 2019 5:17 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
Not yet, I don't know what is in the test system… are they actually dls or fake ones.

Our query against our service is going to look something like, that will translate to yours.

http://[redacted]6060/CHSBReceiver/CHSBService?ori=REM000001&username=TEST&ssn=123123123&driversLicense=AZ67676767

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain*

confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Thursday, September 5, 2019 1:09 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

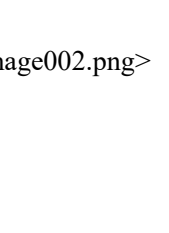
Have you tried your DL and SSN?

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Thursday, September 5, 2019 2:36 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
Do you have a sample DL and ssn, we can try passing through the service to see if we can pull an image. According to dev we are just utilizing the XML out of R1 and Ri.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, August 9, 2019 7:04 AM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Brian Kruger

<bkruger@forensiclogic.com>; Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

All of the broker queries use the same method and accept an xml document. The contents of the xml direct what action the system should take. I have attached documentation for the broker. It's a 5 MB zip file.

If you can't accept zip files or 5 MB files let me know how to send the file.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, August 9, 2019 9:39 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Brian Kruger <bkruger@forensiclogic.com>; Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>
Subject: Re: LRP network ideas?

Thanks John, I'll defer to Brian Kruger to respond regarding where he's sending the query. Are you able to answer his question below?

"

> I can pull back the WSDL but want to send an image request to it to see if it actually pulls the image. I am looking for something like /GetPhoto?dl_num=20180061903&ss_num=2&type=M, the actually call method

"

On Aug 9, 2019, at 9:04 AM, Ouellette, John (EPS) <john.ouellette@mass.gov> wrote:

Hi Brian,

For broker connections to test, we need the following:
IP Address for request: [redacted]
URL for responses:
http://[redacted]6060/CHSBReceiver/CHSBService
ORI: MAMSP0000
Queries:

Can you confirm this information and send the list of queries you would like to run?
Please remember that this system would only be used for test. Another system would need to be used when you move to production.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, August 9, 2019 8:54 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Ouellette, John (EPS) <john.ouellette@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>
Subject: Re: LRP network ideas?

Hi Brian,

are we testing on this yet?

On Jul 22, 2019, at 1:37 PM, Brian Kruger <bkruger@forensiclogic.com> wrote:

> Tim,
> Attached is the full list of agencies and ORI that we currently have in the admin DB.
>
> Regards,
>
> <image001.png>
> **Brian Kruger**
> Operations and Support Manager
> **Forensic Logic / COPLINK**

520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Monday, July 22, 2019 8:37 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Ouellette, John (EPS) <john.ouellette@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
Subject: RE: LRP network ideas?

Any update on this from dev, do you still need a sample RI url? Can you make sure you are also sending the CopLink user name in the UserID parameter.

Tks, Brian

From: Brian Kruger [mailto:bkruger@forensiclogic.com]
Sent: Thursday, July 18, 2019 5:19 PM
To: Mitchell, Timothy (EPS)
Cc: Ramsay, Christopher (EPS); Egnitz, Brian (POL); Ouellette, John (EPS)
Subject: RE: LRP network ideas?

Tim,
I am still pending an answer back from dev on how they are going to pull the ORI. For now can we use M[redacted] That is actually in our S[redacted] MSP.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com

www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
Sent: Tuesday, July 16, 2019 4:07 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Ouellette, John (EPS) <john.ouellette@state.ma.us>
Subject: RE: LRP network ideas?

Brian
What is the ORI that you are using for this setup? There is some configuration work that needs to be done on the broker side to allow your service to run transactions.
Thanks
Tim

Timothy Mitchell
Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise and Field Services Support Division
Public Safety Data Center
200 Arlington St., Suite 2200
Chelsea, MA 02150
(P) 617.660.4665
(F) 617.884.4601
(E) timothy.mitchell@state.ma.us
http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Monday, July 15, 2019 7:05 PM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>

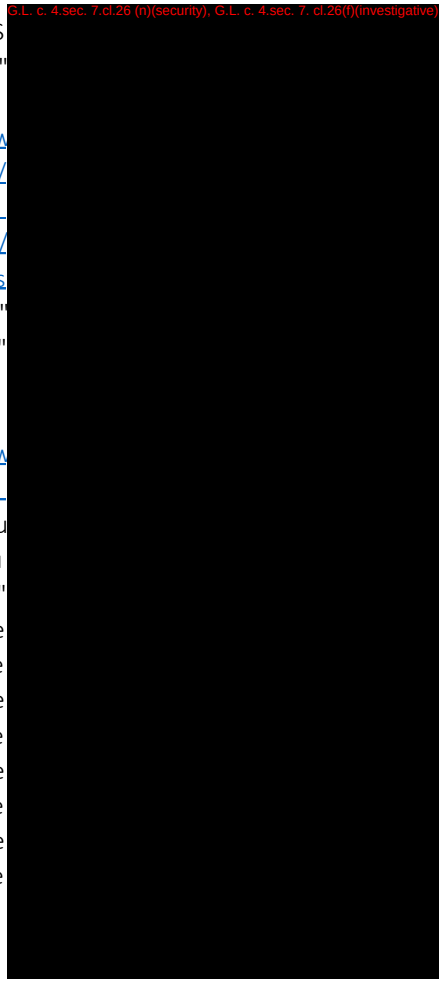
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

Folks,
For the RMV pull, does anybody have an example image we can try and run through. All the connectivity looks good, I have tried a few ways to pull an image without success.

Our service http://[redacted]6060/CHSBReceiver/CHSBService?wsdl refers to http://[redacted]6060/CJISService?wsdl

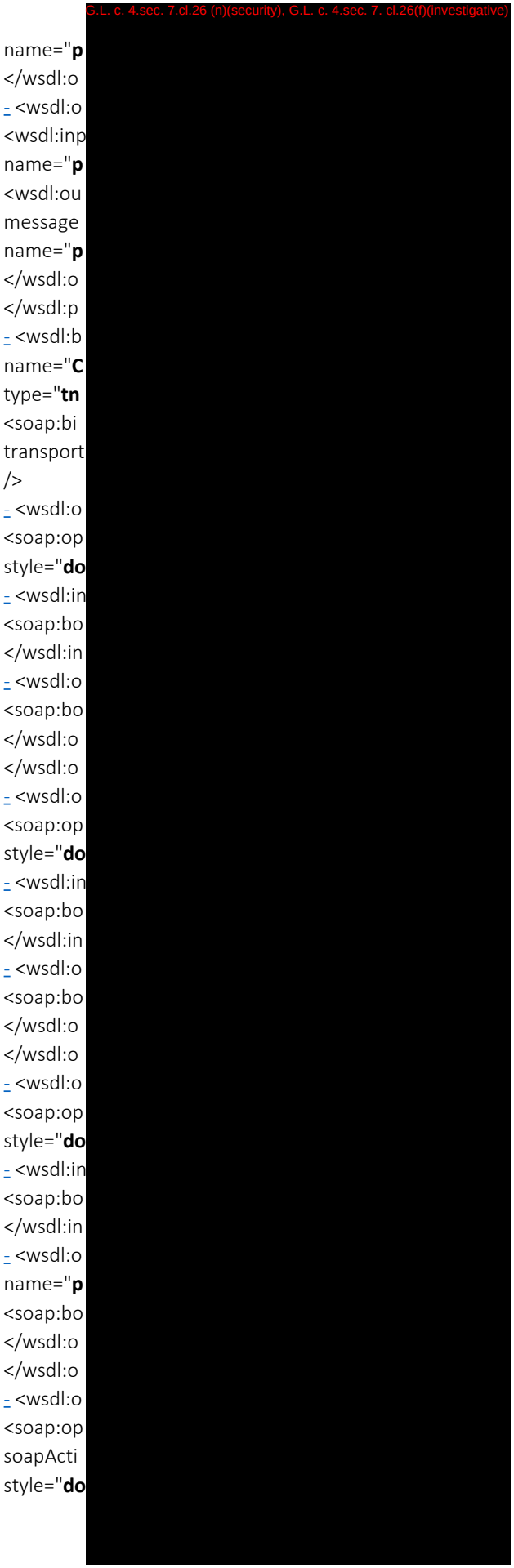
I can pull back the WSDL but want to send an image request to it to see if it actually pulls the image. I am looking for something like /GetPhoto?dl_num=20180061903&ss_num=2&type=M, the actually call method

To pull back the WS
<?xml version="1.0"
- <wsdl:definitions
xmlns:xsd="http://w
xmlns:wsdl="http://
xmlns:tns="http://s
xmlns:soap="http://
xmlns:ns1="http://s
name="**CJISService**"
targetNamespace="
- <wsdl:types>
- <xsd:schema
xmlns:xsd="http://w
xmlns:tns="http://s
attributeFormDefau
elementFormDefau
targetNamespace="
<xsd:element name
nillable="**true**" type
<xsd:element name
nillable="**true**" type
<xsd:element name
nillable="**true**" type
<xsd:element name
nillable="**true**" type
</xsd:schema>
</wsdl:types>





- <wsdl:mess
<wsdl:part el
name="**strEv**
</wsdl:mess
- <wsdl:mess
<wsdl:part el
name="**strRe**
</wsdl:mess
<wsdl:messa
- <wsdl:mess
<wsdl:part el
name="**strRe**
</wsdl:mess
- <wsdl:mess
name="**proc**
<wsdl:part el
name="**strRe**
</wsdl:mess
- <wsdl:mess
<wsdl:part el
name="**strRe**
</wsdl:mess
- <wsdl:mess
name="**proc**
<wsdl:part el
name="**strRe**
</wsdl:mess
- <wsdl:mess
name="**proc**
<wsdl:part el
name="**strRe**
</wsdl:mess
- <wsdl:portT
- <wsdl:oper
<wsdl:input
name="**proc**
<wsdl:outpu
message="**tn**
name="**proc**
</wsdl:opera
- <wsdl:oper
<wsdl:input
name="**verif**
<wsdl:outpu
name="**verif**
</wsdl:opera
- <wsdl:oper
<wsdl:input
name="**proc**
<wsdl:outpu
message="**tn**



name="**p**
</wsdl:o
- <wsdl:o
<wsdl:inp
name="**p**
<wsdl:ou
message
name="**p**
</wsdl:o
</wsdl:p
- <wsdl:b
name="**C**
type="**tn**
<soap:bi
transport
/>
- <wsdl:o
<soap:op
style="**do**
- <wsdl:in
<soap:bo
</wsdl:in
- <wsdl:o
<soap:bo
</wsdl:o
</wsdl:o
- <wsdl:o
<soap:op
style="**do**
- <wsdl:in
<soap:bo
</wsdl:in
- <wsdl:o
<soap:bo
</wsdl:o
</wsdl:o
- <wsdl:o
<soap:op
style="**do**
- <wsdl:in
<soap:bo
</wsdl:in
- <wsdl:o
name="**p**
<soap:bo
</wsdl:o
</wsdl:o
- <wsdl:o
<soap:op
soapActi
style="**do**

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

- <wsdl:in
<soap:bo
</wsdl:in
- <wsdl:o
name="**pr**
<soap:bo
</wsdl:ou
</wsdl:op
</wsdl:bi
- <wsdl:se
- <wsdl:p
binding="
name="**CJ**
<soap:ad
</wsdl:po
</wsdl:se
</wsdl:de

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
Sent: Wednesday, May 8, 2019 5:52 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: Re: LRP network ideas?

Brian
Can you test the connectivity again?
Thanks

Sent from my iPhone

On May 7, 2019, at 10:43 AM, Brian Kruger <bkruger@forensiclogic.com> wrote:

Tim,
Thank you sir, sorry this fell off my radar. I was working on reallocation for Dan.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
Sent: Tuesday, May 7, 2019 7:42 AM
To: Brian Kruger <bkruger@forensiclogic.com>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Brian
Yes you will need to run the transactions across to the test server first and DCJIS will need to approve it before you can run to the production server. I will check out the firewall rules today and let you know.
Thanks

Timothy Mitchell
Massachusetts Executive Office of
Public Safety and Security
Office of Technology and
Information Services
Enterprise and Field Services
Support Division
Public Safety Data Center
200 Arlington St., Suite 2200
Chelsea, MA 02150
(P) 617.660.4665
(F) 617.884.4601
(E) timothy.mitchell@state.ma.us
http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Tuesday, May 07, 2019 10:40 AM
To: Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

Chris,
I am guessing test first, that way we can validate the broker, unless the route is setup already for production and I can switch it out to that.

Brian E.,
Your thoughts?

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may*

contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.

From: Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Sent: Tuesday, May 7, 2019 7:18 AM
To: Brian Kruger <bkruger@forensiclogic.com>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Brian,

[redacted] is the TEST cjis broker system. Is the test system what you're looking to use?

-Chris

Christopher Ramsay |
Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Division of Enterprise & Field Services Support | Enterprise Systems

200 Arlington St. Suite 2200
Chelsea, MA 02150
p. 617.660.4720 | f. 617.660.4613
christopher.ramsay@mass.gov |
http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Tuesday, May 7, 2019 1:49 AM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>

Subject: RE: LRP network ideas?

Tim,
I was checking the cjis broker service and I can't get to the [redacted] on 6060 from the FR server at [redacted] I was going through old email and just checking the status of the connections. The [redacted] is what I received from Dev. Let me know if this is not correct.

<image003.jpg>

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
Sent: Friday, March 1, 2019 1:28 PM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Brian Kruger <bkruger@forensiclogic.com>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Hi folks
The CJIS broker transactions will need to use [redacted] as that is

what they have been configured for in the past.

We have discussed the LPR port request and we think that going with a higher port seems to be more acceptable to EOTSS to allow through their public access firewall. Would [redacted] work? We will need to open a ticket with EOTSS to have them allow this port through.

Thanks

Timothy Mitchell
Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise and Field Services Support Division
Public Safety Data Center
200 Arlington St., Suite 2200
Chelsea, MA 02150
(P) 617.660.4665
(F) 617.884.4601
(E) timothy.mitchell@state.ma.us
http://www.mass.gov/eops

From: Egnitz, Brian (POL)
Sent: Friday, March 01, 2019 12:44 PM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Brian Kruger <bkruger@forensiclogic.com>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

Hi Tim,

I spoke with Brian Kruger and he wants the RI image CJIS Broker return to go to the same port as the ALPR image results, are there any issues with that? If not, is your

team picking the port or is CopLink? I've included his email request. It sounds like they want to use the same web service to simplify the two integrations (LPR & RMV Images).

Tks, Brian

From: Mitchell, Timothy (EPS)
Sent: Friday, February 15, 2019 9:39 AM
To: Brian Kruger; Egnitz, Brian (POL); Ramsay, Christopher (EPS)
Subject: RE: LRP network ideas?

Brian
We are in receipt and reviewing on this side. I will get back to you next week.
Thanks

Timothy Mitchell
Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise and Field Services Support Division
Public Safety Data Center
200 Arlington St., Suite 2200
Chelsea, MA 02150
(P) 617.660.4665
(F) 617.884.4601
(E) timothy.mitchell@state.ma.us
http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Tuesday, February 12, 2019 2:46 PM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

Tim,
Here you go.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
Sent: Tuesday, February 12, 2019 8:19 AM
To: Brian Kruger <bkruger@forensiclogic.com>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian
Did you send over a diagram for review? If yes, can you resend as I can't come across it? We need to review this before providing any additional ports.
Thanks

Timothy Mitchell
Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services

Enterprise and Field Services
Support Division
Public Safety Data Center
200 Arlington St., Suite 2200
Chelsea, MA 02150
(P) 617.660.4665
(F) 617.884.4601
(E) timothy.mitchell@state.ma.us
http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Tuesday, February 12, 2019 12:00 AM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

Tim/Brian,
We are ready to start up the LPR ingest again, however I still need to assign a port to Tomcat on the FR server that will be accessible from both application servers. Is there any port range that we can shoot for. I would like to get the LPR data flowing as soon as possible.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Thursday, February 7, 2019 1:47 PM
To: 'Mitchell, Timothy (EPS)' <timothy.mitchell@state.ma.us>; 'Egnitz, Brian (POL)' <brian.egnitz@state.ma.us>; 'Ramsay, Christopher (EPS)' <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Tim,
Do you have any ports you send me that would be allowed for the connection from the app servers. I can update the diagram for approval that will work on the FR server. I will need two, one for Tomcat and one for LEXSR TR.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Thursday, February 7, 2019 8:50 AM
To: 'Mitchell, Timothy (EPS)' <timothy.mitchell@state.ma.us>; 'Egnitz, Brian (POL)' <brian.egnitz@state.ma.us>; 'Ramsay, Christopher (EPS)' <christopher.ramsay@state.ma.us>

Subject: RE: LRP network ideas?

Tim/Brian,
I was thinking last night and would actually like to move the new Image service to the FR server([redacted]) We have a route in place already from both PAA and Internal web to that server. I would just need to know what port to run tomcat on. This would also work for the Thompson Reuters adapter as well. Let me know what you guys think.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Monday, February 4, 2019 11:17 AM
To: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: LRP network ideas?

Brian/Tim,
Nick is almost done with the new LPR service that will remove the images from the database and have a tomcat app that host the

images for a return to the UI. What I need to know:

1. The Migration will sit on the migration server and needs access to the LPR database to pull out the metadata and create the URL for the Image links.
2. The new service is going to be hosted in Tomcat, so this service will need access to the LPR database for images and both application servers need to be able to query this tomcat instance. I just need to know where to put it, I can host it on both severs or if we can set it up on the internal server and have a firewall rule that will allow the DMZ server to talk to the internal server. Let me know if you would like to have a call on this. I have attached a rough network diagram for visual reference.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

<MSP agency ORI.xlsx>

From: Egnitz, Brian (POL)
To: Brian Kruger
Cc: Rhonda Fromm
Subject: Re: LRP network ideas?
Date: Tuesday, January 7, 2020 9:10:47 AM

How are we making out on RMV?

> On Dec 6, 2019, at 11:31 AM, Brian Kruger <bkruger@forensiclogic.com> wrote:
>
> Billy,
> Please let the group know when this will be available. I will work with John to get it deployed and tested as soon as we have it released.
>
> Regards,
>
> <image001.png>
>
> **Brian Kruger**
> Operations and Support Manager
> **Forensic Logic / COPLINK**
> Office: 520.367.2775
> Mobile: 520.488.1603
> bkruger@forensiclogic.com
> www.forensiclogic.com
>
> ***CONFIDENTIALITY:*** *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*
>
> ---
>
> **From:** Brian Kruger
> **Sent:** Tuesday, November 26, 2019 1:17 PM
> **To:** 'Ouellette, John (EPS)' <john.ouellette@state.ma.us>; 'Egnitz, Brian (POL)' <brian.egnitz@state.ma.us>; Samson Dunatunga <mdunatunga@forensiclogic.com>; Billy Moore <bmoore@forensiclogic.com>
> **Cc:** 'Dunne, Michaela (CHS)' <michaela.dunne@state.ma.us>; 'Dunn-CHS, William (CHS)' <william.dunn-chs@state.ma.us>; 'Mitchell, Timothy (EPS)' <timothy.mitchell@state.ma.us>; 'Ramsay, Christopher (EPS)' <christopher.ramsay@state.ma.us>
> **Subject:** RE: LRP network ideas?
>
> John,
> Thank you for the information on the call this afternoon.
>
> Samson/Billy,
> We need to add some additional debug code into our service so we can see the full communication path and what is being sent and received. John is also in the process to check and make sure their three servers can reach back into our 184.171 on [redacted] I have also

reattached the IP wireshark I did this morning.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Tuesday, November 26, 2019 8:29 AM
To: Ouellette, John (EPS) <john.ouellette@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

John,
Give me a few minutes and I will give you a call. Here is the CSV file from wireshark. I had to repull it. I don't see any actually log details in our tomcat instance. In the wireshark though I see a bunch of event code errors like below:

Event: <Unkno
<Unknown even
<Unknown even
<Unknown even
<Unknown even
<Unknown even
97>, <Unknown
<Unknown even
<Unknown even
eventcode 114>
eventcode 120>
<Unknown even
eventcode 62>,
<Unknown even

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Tuesday, November 26, 2019 7:29 AM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Hey Brian,

You can call me at 617-660-4775

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Monday, November 25, 2019 7:53 PM
To: Brian Kruger <bkruger@forensiclogic.com>; Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: Re: LRP network ideas?

Does it make sense to schedule a call and work through it in real time?

On Nov 22, 2019, at 4:00 PM, Ouellette, John (EPS) <john.ouellette@mass.gov> wrote:

Hi Brian,

I do not see any requests for your ORI. Can you review the acknowledgements that the broker sends back as a return value? There may be error information in there.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 22, 2019 3:47 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

John,
Can you check again and see if there is a request coming into the .154 server. I ran a packet capture and I do see data sent from the .171 to the .154 server.

<image001.png>

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure*

or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 22, 2019 12:26 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

I'm not sure if [redacted] balancer. I don't believe it is though. It doesn't matter though, that is where you will send requests. You will receive a synchronous response called an acknowledgement. That will let you know if your request was accepted or rejected.

Later, an asynchronous response will be sent from [redacted] or [redacted] to your web service.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 22, 2019 2:19 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
[redacted] is a load balancer for the services correct. As far as I know there should be no blocked traffic to the .171 but let me include Chris and Tim on this thread.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 22, 2019 9:36 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

I didn't find any submitted requests.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Ouellette, John (EPS)
Sent: Friday, November 22, 2019 11:34 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

I can check.

The broker will send responses from [redacted] or [redacted] on [redacted] Make sure you are allowing that traffic.

When you send in a request you will receive an xml document as the return value. The documents lists if the request was accepted and if it wasn't, why it wasn't. You should be checking those.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 22, 2019 11:28 AM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

Bill,
I have the service send back a no data found so it looks like we are connecting. Can you check your logs to see if our request actually made it into your system.

I am sending the following test cycle from the [redacted] web server to our FR server

http://[redacted]6060/CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=S32935254

Just so everybody is clear, this the is the connection path

[redacted] → [redacted] → [redacted]

Return path

[redacted] → [redacted] → [redacted]

Log of request:

2019-11-22 11:16:13,982 main DEBUG LoggerContext[name=MassLPRServlet, org.apache.logging.log4j.core.LoggerContext@59303963] started OK with configuration org.apache.logging.log4j.core.config.properties.PropertiesConfiguration@61e86192.
2019-11-22 11:16:13,982 main DEBUG Log4jServletContextListener ensuring that Log4j starts up properly.

2019-11-22 11:16:13,982 main DEBUG Log4jServletFilter initialized.
driversLicense=S32935254
remote host=[redacted]
remote port=60194
remote addr=[redacted]
scheme =http
scheme =HTTP/1.1
local addr =[redacted]
local name =EPS-CLFACEMATCH
context path = /CHSBReceiver
Init parameter1 =Value1
Current UUID : f3837e1f-0e40-4af6-8587-203e99240d92
javax.xml.bind.JAXBElement@227d5180
Request UUID: [redacted]f3837e1f-0e40-4af6-8587-203e99240d92

Rest response file contains:
no data found.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Thursday, November 21, 2019 2:11 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Ouellette, John (EPS) <john.ouellette@state.ma.us>
Subject: RE: LRP network ideas?

Thanks Bill!

It looks like we are close on this.

-Brian

From: Dunn-CHS, William (CHS)
Sent: Tuesday, November 19, 2019 7:50 AM
To: Brian Kruger; Ouellette, John (EPS)
Cc: Dunne, Michaela (CHS); Egnitz, Brian (POL); Dunn-CHS, William (CHS)
Subject: RE: LRP network ideas?

I think I see what might be part of the problem.

The R1 is either OLN or SSN, you can not send both at the same time.

There is No TEST SSN inquiry, use someone from MSP who is working on your project or if you have a developer who is from MA
The TEST OLN [redacted]

From: Brian Kruger [mailto:bkruger@forensiclogic.com]
Sent: Monday, November 18, 2019 6:33 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
Dev confirmed they are sending XML in the request. Do you have a valid License number in the test data I can try.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 15, 2019 11:16 AM

To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

The broker is a web service. You need to create a client to connect. Requests are made by sending in an xml document.

Did I forget to send you the broker documentation? Let me know.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 1:10 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
I ran two queries through IE I don't see an acknowledge me in the logs. Below is what I am seeing. Do we have a valid Lic number that is in the system I can try, or valid SSN.

My test URLs are:"
http://[redacted]6060/CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=987654321

http://[redacted]6060/CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=987654321

In my access log I see a 200:

[redacted] - - [15/Nov/2019:13:02:50 -0500] "GET /CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=987654321 HTTP/1.1" 200 -

[redacted] - - [15/Nov/2019:13:03:05 -0500] "GET /CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=987654321 HTTP/1.1" 200 –

In my log stdout log I see this:

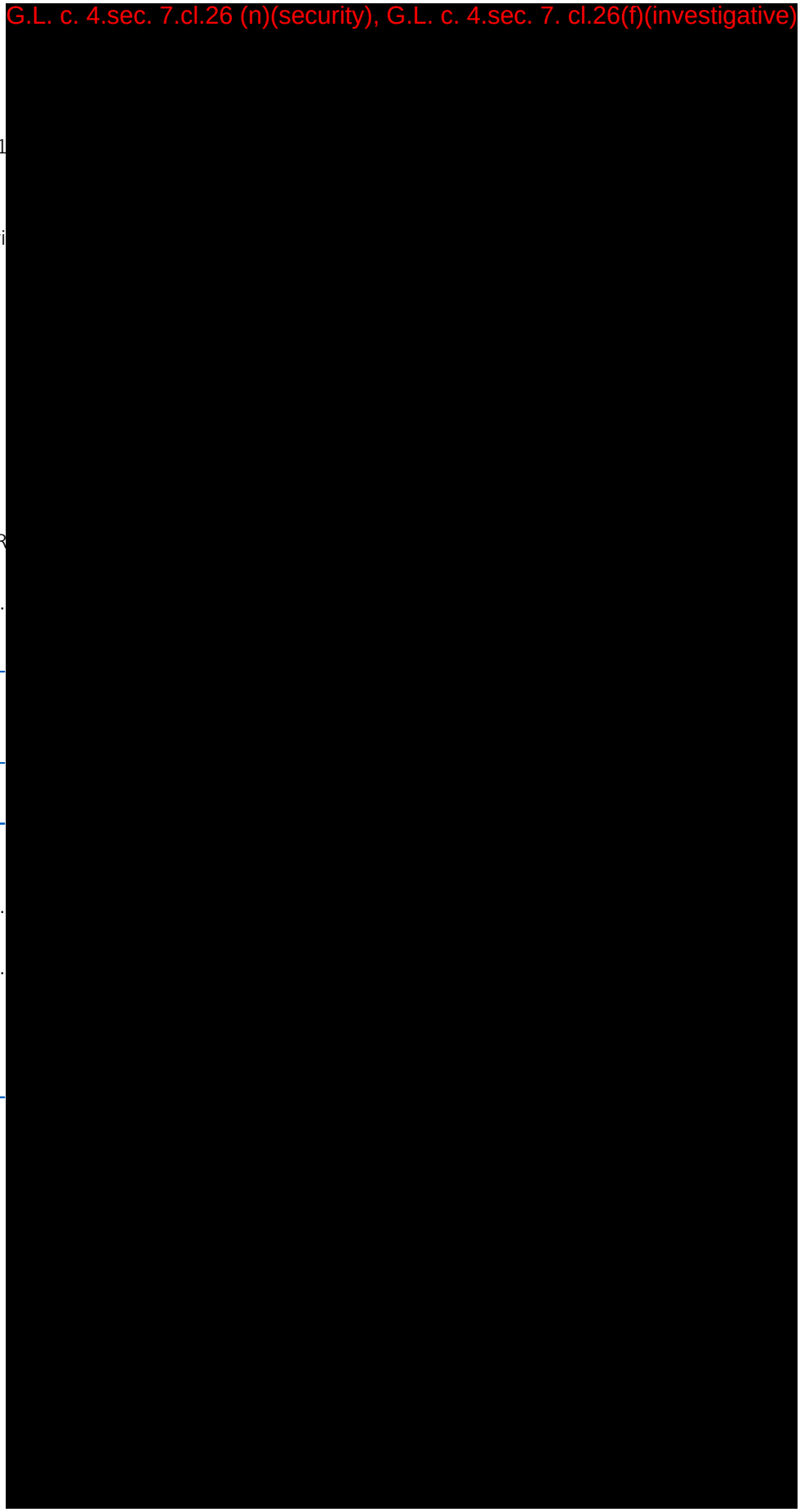
G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

[redacted]

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)



G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)



G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

2019-11-15 [redacted]
org.apache.l
timestamps.
2019-11-15
org.apache.l
configuratio
org.apache.l 0.
2019-11-15
Log4j starts
2019-11-15
driversLicen
remote host [redacted]
remote port=62034
remote addr=[redacted]
scheme =http
scheme =HTTP/1.1
local addr =[redacted]
local name =EPS-CLFACEMATCH
context path = /CHSBReceiver
Init parameter1 =Value1
remote host not allowed. ignoring request.
driversLicense=987654321
remote host=[redacted]
remote port=62034
remote addr=[redacted]
scheme =http
scheme =HTTP/1.1
local addr =[redacted]
local name =EPS-CLFACEMATCH
context path = /CHSBReceiver
Init parameter1 =Value1
remote host not allowed. ignoring request.

My stderr log

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

2019-11-15 13:02:33 [redacted]
15-Nov-2019 13:02:
org.apache.catalina.s
Apache Tomcat/9.0.
15-Nov-2019 13:02:
org.apache.catalina.s
2018 21:13:53 UTC
15-Nov-2019 13:02:
org.apache.catalina.s
9.0.14.0
15-Nov-2019 13:02:
org.apache.catalina.s


G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

[redacted]

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

[redacted]

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

org.apac
applicati
15-Nov-
org.apac
TLDs yet
list of JA
unneede
time.
15-Nov-
org.apac
applicati
finished
15-Nov-
org.apac
applicati
15-Nov-
org.apac
TLDs yet
list of JA
unneede
time.
15-Nov-
org.apac
applicati
finished
15-Nov-
Starting
15-Nov-
Starting
15-Nov-
Server st

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 15, 2019 9:54 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hey Brian,

When you send in a request, the return to that call is an acknowledgement. That is an xml document that will state if your request was accepted or not; and if it is not, what the reason is.

Are you seeing any acknowledgements?

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 11:49 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
According to dev the message that is coming back: remote host not allowed. ignoring request. They are stating is a response from your system telling us we are not allowed. Is there anyway you and I can get on the phone, I can try and send some responses and see if you see anything in your log files. I am wondering if they are forming the response to you correctly.

As for the WSDL this is what I see from the 184.171 server.

<image003.png>

Full WSDL
<?xml version="1.0" encoding="UTF-8" ?>
- <wsdl:definitions xmlns:xsd="http://www.w3.org/2001/XMLSchema"

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

</wsdl:
- <wsdl:
- <wsdl:
name="
<soap:a
</wsdl:
</wsdl:
</wsdl:

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 15, 2019 9:36 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

If you are able to telnet, then you should be able to send in a request.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 11:06 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
This is all from the 184.171 server.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 15, 2019 8:41 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Are you doing the ping and telnet from [redacted]

Your error message from earlier seems to be your network not allowing the access.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 10:37 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

John,
I am reaching out to the [redacted] on [redacted] I can ping the IP and also hit the port.
<image004.png>

<image005.png>

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 15, 2019 8:26 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

What is the ip address you are trying to connect to?
Are you able to ping that machine?

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services

Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Friday, November 15, 2019 10:22 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

Brian,
Thank you for checking in, sorry for the delay. I had the email together but it was in my draft. I tested the connection again today.

John,
I am still getting the remote Host not allowed. This is the error below:

2019-11-15 10:15:45,808 main DEBUG Log4jServletFilter initialized.
driversLicense=987654321
remote host=[redacted]
remote port=61799
remote addr=[redacted]
scheme =http
scheme =HTTP/1.1
local addr =[redacted]
local name =EPS-CLFACEMATCH
context path = /CHSBReceiver
Init parameter1 =Value1
remote host not allowed. ignoring request.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure*

or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.

From: Brian Kruger
Sent: Friday, November 8, 2019 1:17 PM
To: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

John,
Thank you, I will work on testing the connection and let you know the results. According to Dev the other queries we will be running on the R1 and RI.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, November 8, 2019 12:18 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

I have added your configuration on the test broker for R1 and RI.
Are there more queries/transactions you'd like to test? Michaela may have requirements for other queries.

The ORI is MAMSPF022
Your requests come from [redacted] and responses will be sent back to http://[redacted]6060/CHSBReceiver/CHSBService

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Ouellette, John (EPS)
Sent: Tuesday, November 5, 2019 12:54 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>
Subject: RE: LRP network ideas?

Hi Brian,

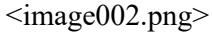
I think Bill needs to have more information on your project to assign an ORI to use on the test broker.
Is there a project name on your side?

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Monday, November 4, 2019 3:30 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
Any luck on this.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
Office: 520.367.2775
Mobile: 520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Tuesday, October 22, 2019 12:32 PM
To: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Subject: RE: LRP network ideas?

John,
Yea we should be sending the XML packet with the service that we have created. Do you know if that IP is natted to [redacted] The server that we have our service on is the [redacted] Face match server. I don't have any servers in the [redacted]x IP range unless it is getting natted somehow.

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Tuesday, October 22, 2019 12:21 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hay Brian,

That won't work. The broker accepts an xml document containing the request, as well as other information.
Attached is a sample R1 request.

By the way, I have your requests coming from [redacted]

In order to get responses, you need a web service on your end to receive the responses and I'll need to configure it on the broker side.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Monday, October 21, 2019 5:04 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
Can you provide me with a DL that should work. From the .82 server this is what we are running:

http://[redacted]6060/CHSBReceiver/rest?ori=MAMSP0000&username=TEST&ssn=123123123&driversLicense=987654321

I just need to update the drivers license number and hopefully it will work

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Tuesday, September 24, 2019 8:07 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

So, just R1 and RI?

I'll start configuring the test broker.

John Ouellette | Massachusetts Executive Office of Public Safety and Security

Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Tuesday, September 24, 2019 10:59 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
For the queries that we will using this is what I got back from Dev… let me know if this helps

…Attachments\CJISBroker_2016-03-24[13247].zip\CJISBroker_2016-03-24\CJISBroker\transactions\queries\rmv\r1\xml

…Attachments\CJISBroker_2016-03-24[13247].zip\CJISBroker_2016-03-24\CJISBroker\transactions\queries\rmv\ri\xml

The rest is correct, for testing the ORI list will grow once we go to production.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Tuesday, September 24, 2019 6:39 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hi Brian,

I haven't added your configuration to the test broker yet. Can you confirm the

following:
For broker connections, we need the following:
IP Address for request: [redacted]
URL for responses: http://[redacted]6060/CHSBReceiver/CHSBService
ORI: MAMSP0000
Queries: I need the list of queries/transactions you will be testing

You will submit to http://[redacted]6060/CJISService This call will return a synchronous acknowledgment.

Responses will come back from [redacted] or [redacted] on [redacted] You need to return a synchronous acknowledgement for each response.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

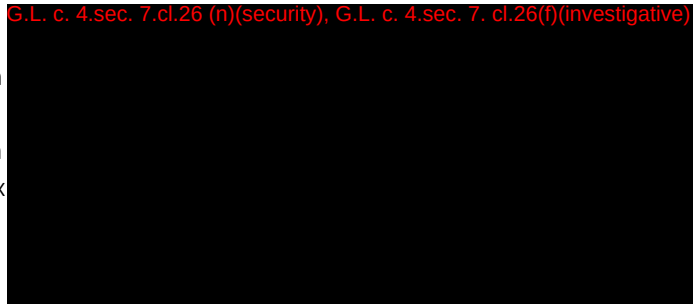
From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Monday, September 23, 2019 7:53 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
I have deployed a new package, but I see this in the log.

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

[redacted]

schem
local a
local n
contex
Init pa
remot



can you check and make sure this machine has access:

EPS-CLFACEMATCH
Connection-specific DNS Suffix . :
IPv4 Address. . . . . : [redacted]
Subnet Mask . . . . . : 255.255.255.128
Default Gateway . . . . . : [redacted]

C:\Users\msp_user>
Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, September 6, 2019 6:15 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Hey Brian,

I'm not sure what is in the test system either. I believe a dl of 987654321 will work; at least it used to.
Try to find something in test CJISWeb.

Remember that all queries will send in an xml document and will receive a return acknowledgement stating success or failure. If the request failed, the reason will be in the acknowledgement.

At a later time, seconds or less, the response will be returned to your web

service. You must return an acknowledgement to that also to let the system know that the response was received and the next response can be sent.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Thursday, September 5, 2019 5:17 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
Not yet, I don't know what is in the test system… are they actually dls or fake ones.

Our query against our service is going to look something like, that will translate to yours.

http://[G.L. c. 4,sec. 7,cl.26 (n)(security); G.L. c. 4][redacted]6060/CHSBReceiver/CHSBService?ori=REM000001&username=TEST&ssn=123123123&driversLicense=AZ67676767

Regards,

<image002.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Thursday, September 5, 2019 1:09 PM
To: Brian Kruger <bkruger@forensiclogic.com>
Subject: RE: LRP network ideas?

Have you tried your DL and SSN?

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Thursday, September 5, 2019 2:36 PM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Subject: RE: LRP network ideas?

John,
Do you have a sample DL and ssn, we can try passing through the service to see if we can pull an image. According to dev we are just utilizing the XML out of R1 and Ri.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ouellette, John (EPS) <john.ouellette@state.ma.us>
Sent: Friday, August 9, 2019 7:04 AM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Brian Kruger <bkruger@forensiclogic.com>; Dunne, Michaela (CHS) <michaela.dunne@state.ma.us>; Dunn-CHS, William (CHS) <william.dunn-chs@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian,

All of the broker queries use the same method and accept an xml document. The contents of the xml direct what action the system should take. I have attached documentation for the broker. It's a 5 MB zip file.

If you can't accept zip files or 5 MB files let me know how to send the file.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, August 9, 2019 9:39 AM
To: Ouellette, John (EPS) <john.ouellette@mass.gov>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Brian Kruger <bkruger@forensiclogic.com>; Dunne, Michaela (CHS) <michaela.dunne@mass.gov>; Dunn-CHS, William (CHS) <William.Dunn-CHS@mass.gov>
Subject: Re: LRP network ideas?

Thanks John, I'll defer to Brian Kruger to respond regarding where he's sending the query. Are you able to answer his question below?

"

> I can pull back the WSDL but want to send an image request to it to see if it actually pulls the image. I am looking for something like /GetPhoto?dl_num=20180061903&ss_num=2&type=M, the actually call method

"

On Aug 9, 2019, at 9:04 AM, Ouellette, John (EPS) <john.ouellette@mass.gov> wrote:

> Hi Brian,
>
> For broker connections to test, we need the following:
> IP Address for request: [redacted]
> URL for responses:

http://[redacted]6060/CHSBReceiver/CHSBService
ORI: MAMSP0000
Queries:

Can you confirm this information and send the list of queries you would like to run?
Please remember that this system would only be used for test. Another system would need to be used when you move to production.

John Ouellette | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise Application and Database Services
Application Support and Management
200 Arlington Street Suite 2200
Chelsea, MA 02150
john.ouellette@state.ma.us | http://www.mass.gov/eops

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, August 9, 2019 8:54 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Ouellette, John (EPS) <john.ouellette@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>
Subject: Re: LRP network ideas?

Hi Brian,

are we testing on this yet?

On Jul 22, 2019, at 1:37 PM, Brian Kruger <bkruger@forensiclogic.com> wrote:

> Tim,
> Attached is the full list of agencies and ORI that we currently have in the admin DB.
>
> Regards,
>
> <image001.png>
>
> **Brian Kruger**
> Operations and Support Manager
> **Forensic Logic / COPLINK**
> 520.488.1603
> bkruger@forensiclogic.com
> www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Monday, July 22, 2019 8:37 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Ouellette, John (EPS) <john.ouellette@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
Subject: RE: LRP network ideas?

Any update on this from dev, do you still need a sample RI url? Can you make sure you are also sending the CopLink user name in the UserID parameter.

Tks, Brian

From: Brian Kruger [mailto:bkruger@forensiclogic.com]
Sent: Thursday, July 18, 2019 5:19 PM
To: Mitchell, Timothy (EPS)
Cc: Ramsay, Christopher (EPS); Egnitz, Brian (POL); Ouellette, John (EPS)
Subject: RE: LRP network ideas?

Tim,

I am still pending an answer back from dev on how they are going to pull the ORI. For now can we use [redacted]
That is actually in our syst [redacted].

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or*

use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.

From: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
Sent: Tuesday, July 16, 2019 4:07 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Ouellette, John (EPS) <john.ouellette@state.ma.us>
Subject: RE: LRP network ideas?

Brian
What is the ORI that you are using for this setup? There is some configuration work that needs to be done on the broker side to allow your service to run transactions.
Thanks
Tim

Timothy Mitchell
Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise and Field Services Support Division
Public Safety Data Center
200 Arlington St., Suite 2200
Chelsea, MA 02150
(P) 617.660.4665
(F) 617.884.4601
(E) timothy.mitchell@state.ma.us
http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Monday, July 15, 2019 7:05 PM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

Folks,

For the RMV pull, does anybody have an example image we can try and run through. All the connectivity looks good, I have tried a few ways to pull an image without success.

Our service http://[redacted]6060/CHSBReceiver/CHSBService?wsdl refers to http://[redacted]6060/CJISService?wsdl

I can pull back the WSDL but want to send an image request to it to see if it actually pulls the image. I am looking for something like /GetPhoto?dl_num=20180061903&ss_num=2&type=M, the actually call method

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

To pull
<?xml v
- <wsdl
xmlns:x
xmlns:
xmlns:t
xmlns:s
xmlns:n
name=
targetN
- <wsdl
- <xsd:s
xmlns:x
xmlns:t
attribut
elemen
targetN
<xsd:el
type="x
<xsd:el
type="x
<xsd:el
type="x
<xsd:el
type="x
</xsd:s
</wsdl:
- <wsdl
<wsdl:p
name=
</wsdl:
- <wsdl

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)



G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

[redacted]
</wsdl:
</wsdl:
- <wsdl:
type="**t**
<soap:b
transpo
/>
- <wsdl:
<soap:o
style="**d**
- <wsdl:
<soap:b
</wsdl:i
- <wsdl:
<soap:b
</wsdl:
</wsdl:
- <wsdl:
<soap:o
style="**d**
- <wsdl:
<soap:b
</wsdl:i
- <wsdl:
<soap:b
</wsdl:
</wsdl:
- <wsdl:
<soap:o
style="**d**
- <wsdl:
<soap:b
</wsdl:i
- <wsdl:
<soap:b
</wsdl:
</wsdl:
- <wsdl:
<soap:o
style="**d**
- <wsdl:
<soap:b
</wsdl:i
- <wsdl:
<soap:b
</wsdl:
</wsdl:
</wsdl:

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

- <wsdl:ser
- <wsdl:po
name="**CJI**
<soap:add
</wsdl:por
</wsdl:ser
</wsdl:defi

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
Sent: Wednesday, May 8, 2019 5:52 AM
To: Brian Kruger <bkruger@forensiclogic.com>
Cc: Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: Re: LRP network ideas?

Brian
Can you test the connectivity again?
Thanks

Sent from my iPhone

On May 7, 2019, at 10:43 AM, Brian Kruger <bkruger@forensiclogic.com> wrote:

> Tim,
> Thank you sir, sorry this fell off my radar. I was working on reallocation for Dan.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
Sent: Tuesday, May 7, 2019 7:42 AM
To: Brian Kruger <bkruger@forensiclogic.com>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Brian
Yes you will need to run the transactions across to the test server first and DCJIS will need to approve it before you can run to the production server. I will check out the firewall rules today and let you know.
Thanks

Timothy Mitchell
Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise and Field Services Support Division
Public Safety Data Center

200 Arlington St., Suite 2200
Chelsea, MA 02150
(P) 617.660.4665
(F) 617.884.4601
(E) timothy.mitchell@state.ma.us
http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Tuesday, May 07, 2019 10:40 AM
To: Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Subject: RE: LRP network ideas?

Chris,
I am guessing test first, that way we can validate the broker, unless the route is setup already for production and I can switch it out to that.

Brian E.,
Your thoughts?

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Sent: Tuesday, May 7, 2019 7:18 AM

To: Brian Kruger <bkruger@forensiclogic.com>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Subject: RE: LRP network ideas?

Brian,

[redacted] is the TEST cjis broker system. Is the test system what you're looking to use?

-Chris

Christopher Ramsay | Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Division of Enterprise & Field Services
Support | Enterprise Systems

200 Arlington St. Suite 2200
Chelsea, MA 02150
p. 617.660.4720 | f. 617.660.4613
christopher.ramsay@mass.gov |
http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Tuesday, May 7, 2019 1:49 AM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

Tim,
I was checking the cjis broker service and I can't get to the [redacted] on 6060 from the FR server at [redacted] I was going through old email and just checking the status of the connections. The [redacted] is what I received from Dev. Let me know if this is not correct.

<image003.jpg>

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
Sent: Friday, March 1, 2019 1:28 PM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Brian Kruger <bkruger@forensiclogic.com>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Hi folks
The CJIS broker transactions will need to use [redacted] as that is what they have been configured for in the past.

We have discussed the LPR port request and we think that going with a higher port seems to be more acceptable to EOTSS to allow through their public access firewall. Would port 56446 (https) work? We will need to open a ticket with EOTSS to have them allow this port through.

Thanks

Timothy Mitchell
Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise and Field Services Support Division
Public Safety Data Center
200 Arlington St., Suite 2200
Chelsea, MA 02150
(P) 617.660.4665
(F) 617.884.4601
(E) timothy.mitchell@state.ma.us
http://www.mass.gov/eops

From: Egnitz, Brian (POL)
Sent: Friday, March 01, 2019 12:44 PM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Brian Kruger <bkruger@forensiclogic.com>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

Hi Tim,

I spoke with Brian Kruger and he wants the RI image CJIS Broker return to go to the same port as the ALPR image results, are there any issues with that? If not, is your team picking the port or is CopLink? I've included his email request. It sounds like they want to use the same web service to simplify the two integrations (LPR & RMV Images).

Tks, Brian

From: Mitchell, Timothy (EPS)
Sent: Friday, February 15, 2019 9:39 AM
To: Brian Kruger; Egnitz, Brian (POL); Ramsay, Christopher (EPS)
Subject: RE: LRP network ideas?

Brian
We are in receipt and reviewing on this side. I will get back to you next week.
Thanks

Timothy Mitchell
Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise and Field Services Support Division
Public Safety Data Center
200 Arlington St., Suite 2200
Chelsea, MA 02150
(P) 617.660.4665
(F) 617.884.4601
(E) timothy.mitchell@state.ma.us
http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Tuesday, February 12, 2019 2:46 PM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

Tim,
Here you go.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure*

or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.

From: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>
Sent: Tuesday, February 12, 2019 8:19 AM
To: Brian Kruger <bkruger@forensiclogic.com>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Hi Brian
Did you send over a diagram for review? If yes, can you resend as I can't come across it? We need to review this before providing any additional ports.
Thanks

Timothy Mitchell
Massachusetts Executive Office of Public Safety and Security
Office of Technology and Information Services
Enterprise and Field Services Support Division
Public Safety Data Center
200 Arlington St., Suite 2200
Chelsea, MA 02150
(P) 617.660.4665
(F) 617.884.4601
(E) timothy.mitchell@state.ma.us
http://www.mass.gov/eops

From: Brian Kruger <bkruger@forensiclogic.com>
Sent: Tuesday, February 12, 2019 12:00 AM
To: Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Ramsay,

Christopher (EPS)
<christopher.ramsay@mass.gov>
Subject: RE: LRP network ideas?

Tim/Brian,
We are ready to start up the LPR ingest again, however I still need to assign a port to Tomcat on the FR server that will be accessible from both application servers. Is there any port range that we can shoot for. I would like to get the LPR data flowing as soon as possible.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Thursday, February 7, 2019 1:47 PM
To: 'Mitchell, Timothy (EPS)' <timothy.mitchell@state.ma.us>; 'Egnitz, Brian (POL)' <brian.egnitz@state.ma.us>; 'Ramsay, Christopher (EPS)' <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Tim,
Do you have any ports you send me that would be allowed for the connection from the app servers. I can update the diagram for approval that will work on the FR server. I will need two, one for Tomcat and one for LEXSR TR.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Thursday, February 7, 2019 8:50 AM
To: 'Mitchell, Timothy (EPS)' <timothy.mitchell@state.ma.us>; 'Egnitz, Brian (POL)' <brian.egnitz@state.ma.us>; 'Ramsay, Christopher (EPS)' <christopher.ramsay@state.ma.us>
Subject: RE: LRP network ideas?

Tim/Brian,
I was thinking last night and would actually like to move the new Image service to the FR server([redacted]) We have a route in place already from both PAA and Internal web to that server. I would just need to know what port to run tomcat on. This would also work for the Thompson Reuters adapter as well. Let me know what you guys think.

Regards,

<image001.png>

Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

From: Brian Kruger
Sent: Monday, February 4, 2019 11:17 AM
To: Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Ramsay, Christopher (EPS) <christopher.ramsay@state.ma.us>
Subject: LRP network ideas?

Brian/Tim,
Nick is almost done with the new LPR service that will remove the images from the database and have a tomcat app that host the images for a return to the UI. What I need to know:

1. The Migration will sit on the migration server and needs access to the LPR database to pull out the metadata and create the URL for the Image links.
2. The new service is going to be hosted in Tomcat, so this service will need access to the LPR database for images and both application servers need to be able to query this tomcat instance. I just need to know where to put it, I can host it on both severs or if we can set it up on the internal server and have a firewall rule that will allow the DMZ server to talk to the internal server. Let me know if you would like to have a call on this. I have attached a rough network diagram for visual reference.

Regards,



Brian Kruger
Operations and Support Manager
Forensic Logic / COPLINK
520.488.1603
bkruger@forensiclogic.com
www.forensiclogic.com

CONFIDENTIALITY: *This e-mail (including any attachments) may contain confidential, proprietary and privileged information, and unauthorized disclosure or use is prohibited. If you received this e-mail in error, please notify the sender and delete this e-mail from your system.*

<MSP agency ORI.xlsx>

From: Shaw, Harold
To: Mason, Christopher (POL)
Cc: Egnitz, Brian (POL); Warmington, Scott (POL); Quinn, Dermot (POL); Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Warren, Rosemary (POL); Ryan, Deborah (POL); Ball, Richard (POL); Crouse, David (POL); Chen, Kwang; Haverty, Robert; Gallant, Edward; Freni, Edward
Subject: Re: MassPort LPR Cameras
Date: Tuesday, August 18, 2020 7:37:48 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Great job. Thanks very much for all of your support and assistance.

Hank

Harold H. Shaw
Chief Security Officer
Massachusetts Port Authority
617-568-3173 (w)
347-582-9976 (c)

> On Aug 18, 2020, at 7:20 PM, Mason, Chris (POL) <chris.mason@state.ma.us> wrote:
>
> Outstanding work by the team!
>
> I know this data will aid In future investigations and all should be proud of the work done to get this project across the finish line.
>
> Colonel Christopher Mason
> Superintendent
> Massachusetts State Police
>
>
>
>
>
>
>> On Aug 18, 2020, at 7:08 PM, Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us> wrote:
>>
>> The Technical Service Unit and I have completed cutting over all of the Massport LPR cameras and they are reporting back to boss and Chelsea.
>>
>> Brian
>>
>>>>>> On May 6, 2020, at 6:57 PM, Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us> wrote:
>>>
>>>> Hi Sirs,
>>>
>>>> We have begun cutting over the MassPort LPR Cameras into the EOPSS BOSS LPR Server. Today, [redacted] at Airport Road arrivals were migrated and are now writing data to Chelsea. I will continue to cut the remaining cameras over in the next few days and weeks. I will advise when the project is complete.
>>>
>>>> - Brian

>>>
>>> -----Original Message-----
>>> From: Warmington, Scott (POL)
>>> Sent: Tuesday, March 10, 2020 11:36 AM
>>> To: Quinn, Dermot (POL)
>>> Cc: Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Mason, Christopher (POL); Egnitz, Brian (POL); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL)
>>> Subject: Re: MassPort LPR Cameras
>>>
>>> What is the cost?
>>>
>>> Sent from my iPhone
>>>
>>>>>> On Mar 10, 2020, at 11:28 AM, Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us> wrote:
>>>> Michelle and Kyra,
>>>> This purchase request is for equipment to allow Mass Port Sierra Wireless modems to communicate directly with the existing ALPR Boss server in Chelsea. This is the fastest way to bring the Massport LPR cameras on line. EOTSS and EOPSS are OK with this solution as is Major Deb Ryan, the CO at Troop F.
>>>> As you can see from the thread, this has been going on for some time. I think we can close it out with this small purchase.
>>>> This does not resolve the replacement of the existing ALPR equipment that we discussed at Command Staff yesterday. That is a different issue.
>>>> Thanks
>>>> Lieutenant Colonel Dermot J. Quinn #1765
>>>> Division Commander
>>>> Division of Homeland Security & Preparedness
>>>> Massachusetts State Police
>>>> -----Original Message-----
>>>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>>>> Sent: Tuesday, March 10, 2020 10:52 AM
>>>> To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>>>> Subject: FW: MassPort LPR Cameras
>>>> Hi LTC.,
>>>> Can we order this equipment for the MassPort project?
>>>> Thanks, Brian
>>>> -----Original Message-----
>>>> From: Slater, James (CHS)
>>>> Sent: Tuesday, March 10, 2020 10:26 AM
>>>> To: Egnitz, Brian (POL)
>>>> Subject: RE: MassPort LPR Cameras
>>>> Hi, Brian!
>>>> This needs to go through MSP fiscal. They need to enter the purchase in OPAS.
>>>> Jim
>>>> -----Original Message-----
>>>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>>>> Sent: Tuesday, March 10, 2020 08:06
>>>> To: Slater, James (CHS) <james.slater@mass.gov>
>>>> Subject: RE: MassPort LPR Cameras
>>>> Is this something you can order or does it need to go through MSP?
>>>> -----Original Message-----
>>>> From: Slater, James (CHS)
>>>> Sent: Monday, March 9, 2020 10:36 AM
>>>> To: Egnitz, Brian (POL)
>>>> Subject: RE: MassPort LPR Cameras
>>>> Thanks, Brian...I will check with TSS.
>>>> Jim
>>>> -----Original Message-----

>>>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>>>> Sent: Monday, March 9, 2020 10:29
>>>> To: Slater, James (CHS) <james.slater@mass.gov>
>>>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>>>> Subject: RE: MassPort LPR Cameras
>>>> Thanks Jim,
>>>> I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need [redacted] wireless AC adapters and [redacted] I have reached out to BCM for a quote.
>>>> I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.
>>>> I plan to cut one sector [redacted] over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?
>>>> -Brian
>>>> -----Original Message-----
>>>> From: Slater, James (CHS)
>>>> Sent: Friday, March 6, 2020 1:43 PM
>>>> To: Egnitz, Brian (POL)
>>>> Cc: Quinn, Dermot (POL)
>>>> Subject: RE: MassPort LPR Cameras
>>>> Hi, Brian!
>>>> I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.
>>>> So, assuming you move forward with this, who would actually make this happen?
>>>> Thanks.
>>>> Jim
>>>> -----Original Message-----
>>>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>>>> Sent: Wednesday, March 4, 2020 17:53
>>>> To: Slater, James (CHS) <james.slater@mass.gov>
>>>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>>>> Subject: Re: MassPort LPR Cameras
>>>> Hi Jim,
>>>> Regarding the Massport cameras; in the early days of AVL we installed [redacted] modem's in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don't we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn't have to do any firewall work either because they have a 166. and communicate like all of the MDT's . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.
>>>> We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.
>>>> Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.
>>>>>> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>>>>> Thank you sir
>>>>> Major Charles W. Atchison III
>>>>> Troop F Commander
>>>>> Massachusetts State Police
>>>>> Director of Aviation Security
>>>>> 2 Service Road
>>>>> East Boston, Ma 02128
>>>>> Office: 617-568-7555
>>>>> Cell: [redacted]
[redacted] 11:28 AM, Wood, Curtis (MASSIT)

<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>>>>> All,
>>>>> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>>>>> Thanks
>>>>> CW
>>>>> From: Quinn, Dermot (POL)
>>>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
>>>>> Sent: Monday, February 10, 2020 10:31 AM
>>>>> To: Egnitz, Brian (POL)
>>>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
>>>>> Slater, James (CHS)
>>>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
>>>>> Robert (EOTSS)
>>>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
>>>>> Warmington, Scott (POL)
>>>>> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
>>>>> .us>>; Peek, Brian T. (EOTSS)
>>>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>>>> Timothy (EPS)
>>>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
>>>>> Michalski, Maria (EPS)
>>>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
>>>>> Christopher (POL)
>>>>> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
>>>>> Hughes, Sean M. (EOTSS)
>>>>> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
>>>>> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
>>>>> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
>>>>> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
>>>>> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
>>>>> Atchison, Charles (POL)
>>>>> <catchison@massport.com<mailto:catchison@massport.com>>
>>>>> Subject: RE: MassPort LPR Cameras
>>>>> Good Morning,
>>>>> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>>>>> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>>>>> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>>>>> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>>>>> I have received several calls from Massport looking to see where we are as far as being able to accept data

from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>>>>> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>>>>> I can't overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security's technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>>>>> Respectfully,
>>>>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
>>>>> of Homeland Security & Preparedness Massachusetts State Police
>>>>> <image006.png>
>>>>> From: Egnitz, Brian (POL)
>>>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
>>>>> Sent: Friday, January 17, 2020 1:10 PM
>>>>> To: Slater, James (CHS)
>>>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
>>>>> Cc: Quinn, Dermot (POL)
>>>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
>>>>> Guerriero, Robert (EOTSS)
>>>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
>>>>> Brian T. (EOTSS)
>>>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>>>> Timothy (EPS)
>>>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
>>>>> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
>>>>> Maria (EPS)
>>>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
>>>>> Subject: RE: MassPort LPR Cameras
>>>>> Hi Jim,
>>>>> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>>>>> -Brian
>>>>> From: Egnitz, Brian (POL)
>>>>> Sent: Monday, January 6, 2020 1:33 PM
>>>>> To: Slater, James (CHS)
>>>>> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
>>>>> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
>>>>> Crary
>>>>> Subject: RE: MassPort LPR Cameras
>>>>> Hi Jim,
>>>>> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>>>>> Thanks Brian
>>>>> From: John Tedona [mailto:jtedona@neology.net]
>>>>> Sent: Monday, December 9, 2019 4:55 PM
>>>>> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
>>>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,

>>>>> Timothy (EPS); Slater, James (CHS)
>>>>> Subject: RE: MassPort LPR Cameras
>>>>> Alex,
>>>>> I can be available most anytime tomorrow for a call.
>>>>> Regards,
>>>>> John Tedona
>>>>> PIPS TECHNOLOGY - A Neology Business
>>>>> Sales Manager
>>>>> 12760 Danielson Ct. Suite A
>>>>> Poway, CA 92064
>>>>> Phone: 201-841-6237
>>>>> Email: jtedona@neology.net<mailto:jtedona@neology.net>
>>>>> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
>>>>> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
>>>>> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
>>>>> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
>>>>> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ
>>>>> U2sB_fmM6g&e=>
>>>>> From: Chute, Alexander
>>>>> <AChute@massport.com<mailto:AChute@massport.com>>
>>>>> Sent: Monday, December 9, 2019 4:38 PM
>>>>> To: Egnitz, Brian (POL)
>>>>> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
>>>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
>>>>> <pcrary@neology.net<mailto:pcrary@neology.net>>
>>>>> Cc: Guerriero, Robert (MASSIT)
>>>>> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
>>>>> Peek, Brian T. (EOTSS)
>>>>> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
>>>>> Timothy (EPS)
>>>>> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
>>>>> Slater III, James F (CHS)
>>>>> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
>>>>> Subject: RE: MassPort LPR Cameras
>>>>> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>>>>> Hello All,
>>>>> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>>>>> Respectfully,
>>>>> ~Alex
>>>>> <image007.png>
>>>>> Alexander B. Chute
>>>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>>>> Cell: [redacted]
>>>>> Office: 617.568.5942
>>>>> achute@massport.com<mailto:achute@massport.com>
>>>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>>>> Sent: Monday, November 18, 2019 3:26 PM

>>>>> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
>>>>> pcrary@neology.net<mailto:pcrary@neology.net>
>>>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>>>> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
>>>>> Subject: RE: MassPort LPR Cameras
>>>>> Hi John, Peter
>>>>> Any issues with moving Massports cameras to the Chelsea DB?
>>>>> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>>>>> The current app server
>>>>> <image008.png>
>>>>> Current DB server
>>>>> <image009.png>
>>>>> <image010.png>
>>>>> Our current reads by month for about [redacted]
>>>>> Year
>>>>> Month
>>>>> Day
>>>>> Month Name
>>>>> Reads Count
>>>>> 2019
>>>>> 11
>>>>> 1
>>>>> November
>>>>> 495,113
>>>>> 2019
>>>>> 11
>>>>> 2
>>>>> November
>>>>> 472,907
>>>>> 2019
>>>>> 11
>>>>> 3
>>>>> November
>>>>> 384,409
>>>>> 2019
>>>>> 11
>>>>> 4
>>>>> November
>>>>> 411,440
>>>>> 2019
>>>>> 11
>>>>> 5
>>>>> November
>>>>> 434,085
>>>>> 2019
>>>>> 11
>>>>> 6
>>>>> November
>>>>> 495,537
>>>>> 2019
>>>>> 11
>>>>> 7
>>>>> November
>>>>> 444,123
>>>>> 2019
>>>>> 11
>>>>> 8

>>>>> November
>>>>> 542,492
>>>>> 2019
>>>>> 11
>>>>> 9
>>>>> November
>>>>> 443,463
>>>>> 2019
>>>>> 11
>>>>> 10
>>>>> November
>>>>> 389,514
>>>>> 2019
>>>>> 11
>>>>> 11
>>>>> November
>>>>> 362,548
>>>>> 2019
>>>>> 11
>>>>> 12
>>>>> November
>>>>> 236,539
>>>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>>>> Sent: Wednesday, November 13, 2019 2:49 PM
>>>>> To: Egnitz, Brian (POL)
>>>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>>>> Timothy (EPS)
>>>>> Subject: RE: MassPort LPR Cameras
>>>>> These stats are from the [redacted] we have in the system for this month:
>>>>> <image011.png>
>>>>> ~Alex
>>>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>>>> Sent: Tuesday, November 12, 2019 5:28 PM
>>>>> To: Chute, Alexander
>>>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>>>> Timothy (EPS)
>>>>> Subject: RE: MassPort LPR Cameras
>>>>> Hi Alex,
>>>>> Can you please provide the updated reads per day? Previously you were interested in sharing [redacted] at approximately 75,000 reads per day.
>>>>> Here is the [redacted] confi I mentioned.
>>>>> Set h[redacted]
>>>>> Set i
>>>>> Set n
>>>>> Set P
>>>>> Set u
>>>>> Set p
>>>>> Set s
>>>>> I've [redacted] r team from TSS on the thread. Maybe we can schedule a call in the next week.
>>>>> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>>>>> -Brian
>>>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>>>> Sent: Tuesday, November 12, 2019 2:08 PM
>>>>> To: Egnitz, Brian (POL)
>>>>> Subject: MassPort LPR Cameras

>>>>> Brian,
>>>>> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to approximately [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.
>>>>> Respectfully,
>>>>> ~Alex
>>>>> <image007.png>
>>>>> Alexander B. Chute
>>>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>>>> Cell: [redacted]
>>>>> Office: 617.568.5942
>>>>> achute@massport.com<mailto:achute@massport.com>
>>>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>> <SierraQuoteForMassPort.pdf>

The information contained in this communication, including any attachments, is confidential and is intended only for the use of the recipient(s) named above. If the reader of this message is not an intended recipient, you are notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you receive this communication in error, please notify the sender immediately, and delete the communication, any attachments, and all copies.

From: Mason, Christopher (POL)
To: Egnitz, Brian (POL)
Cc: Warmington, Scott (POL); Quinn, Dermot (POL); Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL); Crouse, David (POL)
Subject: Re: MassPort LPR Cameras
Date: Tuesday, August 18, 2020 7:20:50 PM

Outstanding work by the team!

I know this data will aid In future investigations and all should be proud of the work done to get this project across the finish line.

Colonel Christopher Mason
Superintendent
Massachusetts State Police

> On Aug 18, 2020, at 7:08 PM, Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us> wrote:
>
> The Technical Service Unit and I have completed cutting over all of the Massport LPR cameras and they are reporting back to boss and Chelsea.
>
> Brian
>
>> On May 6, 2020, at 6:57 PM, Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us> wrote:
>>
>> Hi Sirs,
>>
>> We have begun cutting over the MassPort LPR Cameras into the EOPSS BOSS LPR Server. Today, [redacted] at Airport Road arrivals were migrated and are now writing data to Chelsea. I will continue to cut the remaining cameras over in the next few days and weeks. I will advise when the project is complete.
>>
>> - Brian
>>
>> -----Original Message-----
>> From: Warmington, Scott (POL)
>> Sent: Tuesday, March 10, 2020 11:36 AM
>> To: Quinn, Dermot (POL)
>> Cc: Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Mason, Christopher (POL); Egnitz, Brian (POL); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL)
>> Subject: Re: MassPort LPR Cameras
>>
>> What is the cost?
>>
>> Sent from my iPhone
>>
>>>>>> On Mar 10, 2020, at 11:28 AM, Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us> wrote:
>>> Michelle and Kyra,
>>> This purchase request is for equipment to allow Mass Port Sierra Wireless modems to communicate directly with the existing ALPR Boss server in Chelsea. This is the fastest way to bring the Massport LPR cameras on line. EOTSS and EOPSS are OK with this solution as is Major Deb Ryan, the CO at Troop F.
>>> As you can see from the thread, this has been going on for some time. I think we can close it out with this small

purchase.
>>> This does not resolve the replacement of the existing ALPR equipment that we discussed at Command Staff yesterday. That is a different issue.
>>> Thanks
>>> Lieutenant Colonel Dermot J. Quinn #1765
>>> Division Commander
>>> Division of Homeland Security & Preparedness
>>> Massachusetts State Police
>>> -----Original Message-----
>>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>>> Sent: Tuesday, March 10, 2020 10:52 AM
>>> To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>>> Subject: FW: MassPort LPR Cameras
>>> Hi LTC.,
>>> Can we order this equipment for the MassPort project?
>>> Thanks, Brian
>>> -----Original Message-----
>>> From: Slater, James (CHS)
>>> Sent: Tuesday, March 10, 2020 10:26 AM
>>> To: Egnitz, Brian (POL)
>>> Subject: RE: MassPort LPR Cameras
>>> Hi, Brian!
>>> This needs to go through MSP fiscal. They need to enter the purchase in OPAS.
>>> Jim
>>> -----Original Message-----
>>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>>> Sent: Tuesday, March 10, 2020 08:06
>>> To: Slater, James (CHS) <james.slater@mass.gov>
>>> Subject: RE: MassPort LPR Cameras
>>> Is this something you can order or does it need to go through MSP?
>>> -----Original Message-----
>>> From: Slater, James (CHS)
>>> Sent: Monday, March 9, 2020 10:36 AM
>>> To: Egnitz, Brian (POL)
>>> Subject: RE: MassPort LPR Cameras
>>> Thanks, Brian...I will check with TSS.
>>> Jim
>>> -----Original Message-----
>>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>>> Sent: Monday, March 9, 2020 10:29
>>> To: Slater, James (CHS) <james.slater@mass.gov>
>>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>>> Subject: RE: MassPort LPR Cameras
>>> Thanks Jim,
>>> I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need [G.L. c. 4,sec. 7,c [redacted] wireless AC adapters and [G.L. c. 4,sec. 7,cl.26 (n)(sec [redacted] I have reached out to BCM for a quote.
>>> I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.
>>> I plan to cut one sector ([G.L. c. 4,sec. 7,cl.26 (n);26 (n)(security) [redacted] over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?
>>> -Brian
>>> -----Original Message-----
>>> From: Slater, James (CHS)
>>> Sent: Friday, March 6, 2020 1:43 PM
>>> To: Egnitz, Brian (POL)

>>> Cc: Quinn, Dermot (POL)
>>> Subject: RE: MassPort LPR Cameras
>>> Hi, Brian!
>>> I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.
>>> So, assuming you move forward with this, who would actually make this happen?
>>> Thanks.
>>> Jim
>>> -----Original Message-----
>>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>>> Sent: Wednesday, March 4, 2020 17:53
>>> To: Slater, James (CHS) <james.slater@mass.gov>
>>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>>> Subject: Re: MassPort LPR Cameras
>>> Hi Jim,
>>> Regarding the Massport cameras; in the early days of AVL we installed [redacted] modem's in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don't we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn't have to do any firewall work either because they have a 166. and communicate like all of the MDT's . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.
>>> We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.
>>> Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.
>>>>> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>>>> Thank you sir
>>>> Major Charles W. Atchison III
>>>> Troop F Commander
>>>> Massachusetts State Police
>>>> Director of Aviation Security
>>>> 2 Service Road
>>>> East Boston, Ma 02128
>>>> Office: 617-568-7555
>>>> Cell: [redacted] 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>>>> All,
>>>> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>>>> Thanks
>>>> CW
>>>> From: Quinn, Dermot (POL)
>>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
>>>> Sent: Monday, February 10, 2020 10:31 AM
>>>> To: Egnitz, Brian (POL)
>>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
>>>> Slater, James (CHS)
>>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
>>>> Robert (EOTSS)
>>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
>>>> Warmington, Scott (POL)
>>>> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
>>>> .us>>; Peek, Brian T. (EOTSS)
>>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,

>>>> Timothy (EPS)
>>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
>>>> Michalski, Maria (EPS)
>>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
>>>> Christopher (POL)
>>>> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
>>>> Hughes, Sean M. (EOTSS)
>>>> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
>>>> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
>>>> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
>>>> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
>>>> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
>>>> Atchison, Charles (POL)
>>>> <catchison@massport.com<mailto:catchison@massport.com>>
>>>> Subject: RE: MassPort LPR Cameras
>>>> Good Morning,
>>>> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>>>> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>>>> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>>>> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>>>> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>>>> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>>>> I can’t overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security’s technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>>>> Respectfully,
>>>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
>>>> of Homeland Security & Preparedness Massachusetts State Police
>>>> <image006.png>
>>>> From: Egnitz, Brian (POL)
>>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
>>>> Sent: Friday, January 17, 2020 1:10 PM

>>>> To: Slater, James (CHS)
>>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
>>>> Cc: Quinn, Dermot (POL)
>>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
>>>> Guerriero, Robert (EOTSS)
>>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
>>>> Brian T. (EOTSS)
>>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>>> Timothy (EPS)
>>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
>>>> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
>>>> Maria (EPS)
>>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
>>>> Subject: RE: MassPort LPR Cameras
>>>> Hi Jim,
>>>> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>>>> -Brian
>>>> From: Egnitz, Brian (POL)
>>>> Sent: Monday, January 6, 2020 1:33 PM
>>>> To: Slater, James (CHS)
>>>> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
>>>> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
>>>> Crary
>>>> Subject: RE: MassPort LPR Cameras
>>>> Hi Jim,
>>>> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>>>> Thanks Brian
>>>> From: John Tedona [mailto:jtedona@neology.net]
>>>> Sent: Monday, December 9, 2019 4:55 PM
>>>> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
>>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>>> Timothy (EPS); Slater, James (CHS)
>>>> Subject: RE: MassPort LPR Cameras
>>>> Alex,
>>>> I can be available most anytime tomorrow for a call.
>>>> Regards,
>>>> John Tedona
>>>> PIPS TECHNOLOGY - A Neology Business
>>>> Sales Manager
>>>> 12760 Danielson Ct. Suite A
>>>> Poway, CA 92064
>>>> Phone: 201-841-6237
>>>> Email: jtedona@neology.net<mailto:jtedona@neology.net>
>>>> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
>>>> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
>>>> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
>>>> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
>>>> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ
>>>> U2sB_fmM6g&e=>

>>>> From: Chute, Alexander
>>>> <AChute@massport.com<mailto:AChute@massport.com>>
>>>> Sent: Monday, December 9, 2019 4:38 PM
>>>> To: Egnitz, Brian (POL)
>>>> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
>>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
>>>> <pcrary@neology.net<mailto:pcrary@neology.net>>
>>>> Cc: Guerriero, Robert (MASSIT)
>>>> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
>>>> Peek, Brian T. (EOTSS)
>>>> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
>>>> Timothy (EPS)
>>>> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
>>>> Slater III, James F (CHS)
>>>> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
>>>> Subject: RE: MassPort LPR Cameras
>>>> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>>>> Hello All,
>>>> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>>>> Respectfully,
>>>> ~Alex
>>>> <image007.png>
>>>> Alexander B. Chute
>>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>>> Cell: [redacted]
>>>> Office: 617.568.5942
>>>> achute@massport.com<mailto:achute@massport.com>
>>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>>> Sent: Monday, November 18, 2019 3:26 PM
>>>> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
>>>> pcrary@neology.net<mailto:pcrary@neology.net>
>>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>>> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
>>>> Subject: RE: MassPort LPR Cameras
>>>> Hi John, Peter
>>>> Any issues with moving Massports cameras to the Chelsea DB?
>>>> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>>>> The current app server
>>>> <image008.png>
>>>> Current DB server
>>>> <image009.png>
>>>> <image010.png>
>>>> Our current reads by month for about [redacted]
>>>> Year
>>>> Month
>>>> Day
>>>> Month Name
>>>> Reads Count

>>>> 2019
>>>> 11
>>>> 1
>>>> November
>>>> 495,113
>>>> 2019
>>>> 11
>>>> 2
>>>> November
>>>> 472,907
>>>> 2019
>>>> 11
>>>> 3
>>>> November
>>>> 384,409
>>>> 2019
>>>> 11
>>>> 4
>>>> November
>>>> 411,440
>>>> 2019
>>>> 11
>>>> 5
>>>> November
>>>> 434,085
>>>> 2019
>>>> 11
>>>> 6
>>>> November
>>>> 495,537
>>>> 2019
>>>> 11
>>>> 7
>>>> November
>>>> 444,123
>>>> 2019
>>>> 11
>>>> 8
>>>> November
>>>> 542,492
>>>> 2019
>>>> 11
>>>> 9
>>>> November
>>>> 443,463
>>>> 2019
>>>> 11
>>>> 10
>>>> November
>>>> 389,514
>>>> 2019
>>>> 11
>>>> 11
>>>> November
>>>> 362,548
>>>> 2019
>>>> 11

>>>> 12
>>>> November
>>>> 236,539
>>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>>> Sent: Wednesday, November 13, 2019 2:49 PM
>>>> To: Egnitz, Brian (POL)
>>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>>> Timothy (EPS)
>>>> Subject: RE: MassPort LPR Cameras
>>>> These stats are from the [redacted] we have in the system for this month:
>>>> <image011.png>
>>>> ~Alex
>>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>>> Sent: Tuesday, November 12, 2019 5:28 PM
>>>> To: Chute, Alexander
>>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>>> Timothy (EPS)
>>>> Subject: RE: MassPort LPR Cameras
>>>> Hi Alex,
>>>> Can you please provide the updated reads per day? Previously you were interested in sharing [redacted] at approximately 75,000 reads per day.
>>>> Here is the [redacted] confi I mentioned.
>>>> Set h[redacted]
>>>> Set i
>>>> Set n
>>>> Set P
>>>> Set u
>>>> Set p
>>>> Set s
>>>> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
>>>> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>>>> -Brian
>>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>>> Sent: Tuesday, November 12, 2019 2:08 PM
>>>> To: Egnitz, Brian (POL)
>>>> Subject: MassPort LPR Cameras
>>>> Brian,
>>>> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to approximately [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.
>>>> Respectfully,
>>>> ~Alex
>>>> <image007.png>
>>>> Alexander B. Chute
>>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>>> Cell: [redacted]
>>>> Office: 617.568.5942
>>>> achute@massport.com<mailto:achute@massport.com>
>>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15

and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>> <SierraQuoteForMassPort.pdf>

From: Egnitz, Brian (POL)
To: Warmington, Scott (POL); Quinn, Dermot (POL)
Cc: Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Mason, Christopher (POL); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL); Crouse, David (POL)
Subject: Re: MassPort LPR Cameras
Date: Tuesday, August 18, 2020 7:08:51 PM

The Technical Service Unit and I have completed cutting over all of the Massport LPR cameras and they are reporting back to boss and Chelsea.

Brian

> On May 6, 2020, at 6:57 PM, Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us> wrote:
>
> Hi Sirs,
>
> We have begun cutting over the MassPort LPR Cameras into the EOPSS BOSS LPR Server. Today, [redacted] at Airport Road arrivals were migrated and are now writing data to Chelsea. I will continue to cut the remaining cameras over in the next few days and weeks. I will advise when the project is complete.
>
> - Brian
>
> -----Original Message-----
> From: Warmington, Scott (POL)
> Sent: Tuesday, March 10, 2020 11:36 AM
> To: Quinn, Dermot (POL)
> Cc: Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Mason, Christopher (POL); Egnitz, Brian (POL); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL)
> Subject: Re: MassPort LPR Cameras
>
> What is the cost?
>
> Sent from my iPhone
>
>>> On Mar 10, 2020, at 11:28 AM, Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us> wrote:
>> Michelle and Kyra,
>> This purchase request is for equipment to allow Mass Port Sierra Wireless modems to communicate directly with the existing ALPR Boss server in Chelsea. This is the fastest way to bring the Massport LPR cameras on line. EOTSS and EOPSS are OK with this solution as is Major Deb Ryan, the CO at Troop F.
>> As you can see from the thread, this has been going on for some time. I think we can close it out with this small purchase.
>> This does not resolve the replacement of the existing ALPR equipment that we discussed at Command Staff yesterday. That is a different issue.
>> Thanks
>> Lieutenant Colonel Dermot J. Quinn #1765
>> Division Commander
>> Division of Homeland Security & Preparedness
>> Massachusetts State Police
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 10:52 AM
>> To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: FW: MassPort LPR Cameras
>> Hi LTC.,
>> Can we order this equipment for the MassPort project?
>> Thanks, Brian

>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Tuesday, March 10, 2020 10:26 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>> Hi, Brian!
>> This needs to go through MSP fiscal. They need to enter the purchase in OPAS.
>> Jim
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 08:06
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Subject: RE: MassPort LPR Cameras
>> Is this something you can order or does it need to go through MSP?
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Monday, March 9, 2020 10:36 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>> Thanks, Brian...I will check with TSS.
>> Jim
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Monday, March 9, 2020 10:29
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: RE: MassPort LPR Cameras
>> Thanks Jim,
>> I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need [redacted] wireless AC adapters and [redacted] I have reached out to BCM for a quote.
>> I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.
>> I plan to cut one sector ([redacted]) over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?
>> -Brian
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Friday, March 6, 2020 1:43 PM
>> To: Egnitz, Brian (POL)
>> Cc: Quinn, Dermot (POL)
>> Subject: RE: MassPort LPR Cameras
>> Hi, Brian!
>> I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.
>> So, assuming you move forward with this, who would actually make this happen?
>> Thanks.
>> Jim
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Wednesday, March 4, 2020 17:53
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: Re: MassPort LPR Cameras
>> Hi Jim,
>> Regarding the Massport cameras; in the early days of AVL we installed [redacted] modem's in cruisers

that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don't we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn't have to do any firewall work either because they have a 166. and communicate like all of the MDT's . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.
>> We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.
>> Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.
>>>> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>>> Thank you sir
>>> Major Charles W. Atchison III
>>> Troop F Commander
>>> Massachusetts State Police
>>> Director of Aviation Security
>>> 2 Service Road
>>> East Boston, Ma 02128
>>> Office: 617-568-7555
>>> Cell: 508-[redacted]
>>>> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>>> All,
>>> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>>> Thanks
>>> CW
>>> From: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
>>> Sent: Monday, February 10, 2020 10:31 AM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
>>> Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
>>> Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
>>> Warmington, Scott (POL)
>>> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
>>> .us>>; Peek, Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
>>> Michalski, Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
>>> Christopher (POL)
>>> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
>>> Hughes, Sean M. (EOTSS)
>>> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
>>> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
>>> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
>>> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
>>> Atchison, Charles (POL)
>>> <catchison@massport.com<mailto:catchison@massport.com>>
>>> Subject: RE: MassPort LPR Cameras

>>> Good Morning,
>>> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>>> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>>> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as "BOSS" and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport's cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>>> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>>> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>>> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>>> I can't overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security's technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>>> Respectfully,
>>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
>>> of Homeland Security & Preparedness Massachusetts State Police
>>> <image006.png>
>>> From: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
>>> Sent: Friday, January 17, 2020 1:10 PM
>>> To: Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
>>> Cc: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
>>> Guerriero, Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
>>> Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
>>> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
>>> Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
>>> Subject: RE: MassPort LPR Cameras
>>> Hi Jim,

>>> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>>> -Brian
>>> From: Egnitz, Brian (POL)
>>> Sent: Monday, January 6, 2020 1:33 PM
>>> To: Slater, James (CHS)
>>> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
>>> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
>>> Crary
>>> Subject: RE: MassPort LPR Cameras
>>> Hi Jim,
>>> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>>> Thanks Brian
>>> From: John Tedona [mailto:jtedona@neology.net]
>>> Sent: Monday, December 9, 2019 4:55 PM
>>> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Slater, James (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>> Alex,
>>> I can be available most anytime tomorrow for a call.
>>> Regards,
>>> John Tedona
>>> PIPS TECHNOLOGY - A Neology Business
>>> Sales Manager
>>> 12760 Danielson Ct. Suite A
>>> Poway, CA 92064
>>> Phone: 201-841-6237
>>> Email: jtedona@neology.net<mailto:jtedona@neology.net>
>>> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
>>> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
>>> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
>>> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
>>> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ
>>> U2sB_fmM6g&e=>
>>> From: Chute, Alexander
>>> <AChute@massport.com<mailto:AChute@massport.com>>
>>> Sent: Monday, December 9, 2019 4:38 PM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>
>>> Cc: Guerriero, Robert (MASSIT)
>>> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
>>> Peek, Brian T. (EOTSS)
>>> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
>>> Slater III, James F (CHS)
>>> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
>>> Subject: RE: MassPort LPR Cameras
>>> CAUTION: This email originated from outside of the organization. Do not click links or open attachments

unless you recognize the sender and know the content is safe.
>>> Hello All,
>>> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>>> Respectfully,
>>> ~Alex
>>> <image007.png>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Monday, November 18, 2019 3:26 PM
>>> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
>>> pcrary@neology.net<mailto:pcrary@neology.net>
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>> Hi John, Peter
>>> Any issues with moving Massports cameras to the Chelsea DB?
>>> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>>> The current app server
>>> <image008.png>
>>> Current DB server
>>> <image009.png>
>>> <image010.png>
>>> Our current reads by month for about [redacted]
>>> Year
>>> Month
>>> Day
>>> Month Name
>>> Reads Count
>>> 2019
>>> 11
>>> 1
>>> November
>>> 495,113
>>> 2019
>>> 11
>>> 2
>>> November
>>> 472,907
>>> 2019
>>> 11
>>> 3
>>> November
>>> 384,409
>>> 2019
>>> 11

>>> 4
>>> November
>>> 411,440
>>> 2019
>>> 11
>>> 5
>>> November
>>> 434,085
>>> 2019
>>> 11
>>> 6
>>> November
>>> 495,537
>>> 2019
>>> 11
>>> 7
>>> November
>>> 444,123
>>> 2019
>>> 11
>>> 8
>>> November
>>> 542,492
>>> 2019
>>> 11
>>> 9
>>> November
>>> 443,463
>>> 2019
>>> 11
>>> 10
>>> November
>>> 389,514
>>> 2019
>>> 11
>>> 11
>>> November
>>> 362,548
>>> 2019
>>> 11
>>> 12
>>> November
>>> 236,539
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Wednesday, November 13, 2019 2:49 PM
>>> To: Egnitz, Brian (POL)
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>> These stats are from the [redacted] we have in the system for this month:
>>> <image011.png>
>>> ~Alex
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Tuesday, November 12, 2019 5:28 PM
>>> To: Chute, Alexander
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)

>>> Subject: RE: MassPort LPR Cameras
>>> Hi Alex,
>>> Can you please provide the updated reads per day? Previously you were interested in sharing [redacted] at approximately 75,000 reads per day.
>>> Here is the [redacted] confi I mentioned.
>>> Set host to boss [redacted]
>>> Set image [redacted]
>>> Set number of [redacted]
>>> Set Ping [redacted]
>>> Set udp ping [redacted]
>>> Set ping [redacted]
>>> Set security [redacted]
>>> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
>>> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>>> -Brian
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Tuesday, November 12, 2019 2:08 PM
>>> To: Egnitz, Brian (POL)
>>> Subject: MassPort LPR Cameras
>>> Brian,
>>> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to approximately [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.
>>> Respectfully,
>>> ~Alex
>>> <image007.png>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>> <SierraQuoteForMassPort.pdf>

From: brian.egnitz@pol.state.ma.us
To: Warmington, Scott (POL); Quinn, Dermot (POL)
Cc: Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Mason, Christopher (POL); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL); Crouse, David (POL)
Subject: Re: MassPort LPR Cameras
Date: Tuesday, August 18, 2020 7:08:49 PM

The Technical Service Unit and I have completed cutting over all of the Massport LPR cameras and they are reporting back to boss and Chelsea.

Brian

> On May 6, 2020, at 6:57 PM, Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us> wrote:
>
> Hi Sirs,
>
> We have begun cutting over the MassPort LPR Cameras into the EOPSS BOSS LPR Server. Today, [redacted] at Airport Road arrivals were migrated and are now writing data to Chelsea. I will continue to cut the remaining cameras over in the next few days and weeks. I will advise when the project is complete.
>
> - Brian
>
> -----Original Message-----
> From: Warmington, Scott (POL)
> Sent: Tuesday, March 10, 2020 11:36 AM
> To: Quinn, Dermot (POL)
> Cc: Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Mason, Christopher (POL); Egnitz, Brian (POL); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL)
> Subject: Re: MassPort LPR Cameras
>
> What is the cost?
>
> Sent from my iPhone
>
>>> On Mar 10, 2020, at 11:28 AM, Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us> wrote:
>> Michelle and Kyra,
>> This purchase request is for equipment to allow Mass Port Sierra Wireless modems to communicate directly with the existing ALPR Boss server in Chelsea. This is the fastest way to bring the Massport LPR cameras on line. EOTSS and EOPSS are OK with this solution as is Major Deb Ryan, the CO at Troop F.
>> As you can see from the thread, this has been going on for some time. I think we can close it out with this small purchase.
>> This does not resolve the replacement of the existing ALPR equipment that we discussed at Command Staff yesterday. That is a different issue.
>> Thanks
>> Lieutenant Colonel Dermot J. Quinn #1765
>> Division Commander
>> Division of Homeland Security & Preparedness
>> Massachusetts State Police
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 10:52 AM
>> To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: FW: MassPort LPR Cameras
>> Hi LTC.,
>> Can we order this equipment for the MassPort project?
>> Thanks, Brian

>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Tuesday, March 10, 2020 10:26 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>> Hi, Brian!
>> This needs to go through MSP fiscal. They need to enter the purchase in OPAS.
>> Jim
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 08:06
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Subject: RE: MassPort LPR Cameras
>> Is this something you can order or does it need to go through MSP?
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Monday, March 9, 2020 10:36 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>> Thanks, Brian...I will check with TSS.
>> Jim
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Monday, March 9, 2020 10:29
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: RE: MassPort LPR Cameras
>> Thanks Jim,
>> I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need [G.L. c. 4.sec. 7c] wireless AC adapters and [G.L. c. 4.sec. 7.cl.26 (n)(sec] I have reached out to BCM for a quote.
>> I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.
>> I plan to cut one sector ([G.L. c. 4.sec. 7.cl.26 (n)]26 (n)(security) over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?
>> -Brian
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Friday, March 6, 2020 1:43 PM
>> To: Egnitz, Brian (POL)
>> Cc: Quinn, Dermot (POL)
>> Subject: RE: MassPort LPR Cameras
>> Hi, Brian!
>> I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.
>> So, assuming you move forward with this, who would actually make this happen?
>> Thanks.
>> Jim
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Wednesday, March 4, 2020 17:53
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: Re: MassPort LPR Cameras
>> Hi Jim,
>> Regarding the Massport cameras; in the early days of AVL we installed [G.L. c. 4.sec. 7.cl.26 (n)(security)] modem's in cruisers

that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don't we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn't have to do any firewall work either because they have a 166. and communicate like all of the MDT's . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.
>> We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.
>> Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.
>>>> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>>> Thank you sir
>>> Major Charles W. Atchison III
>>> Troop F Commander
>>> Massachusetts State Police
>>> Director of Aviation Security
>>> 2 Service Road
>>> East Boston, Ma 02128
>>> Office: 617-568-7555
>>> Cell: 50[redacted]
>>>> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>>> All,
>>> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>>> Thanks
>>> CW
>>> From: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
>>> Sent: Monday, February 10, 2020 10:31 AM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
>>> Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
>>> Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
>>> Warmington, Scott (POL)
>>> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
>>> .us>>; Peek, Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
>>> Michalski, Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
>>> Christopher (POL)
>>> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
>>> Hughes, Sean M. (EOTSS)
>>> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
>>> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
>>> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
>>> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
>>> Atchison, Charles (POL)
>>> <catchison@massport.com<mailto:catchison@massport.com>>
>>> Subject: RE: MassPort LPR Cameras

>>> Good Morning,
>>> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>>> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>>> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as "BOSS" and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport's cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>>> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>>> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>>> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>>> I can't overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security's technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>>> Respectfully,
>>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
>>> of Homeland Security & Preparedness Massachusetts State Police
>>> <image006.png>
>>> From: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
>>> Sent: Friday, January 17, 2020 1:10 PM
>>> To: Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
>>> Cc: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
>>> Guerriero, Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
>>> Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
>>> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
>>> Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
>>> Subject: RE: MassPort LPR Cameras
>>> Hi Jim,

>>> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>>> -Brian
>>> From: Egnitz, Brian (POL)
>>> Sent: Monday, January 6, 2020 1:33 PM
>>> To: Slater, James (CHS)
>>> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
>>> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
>>> Crary
>>> Subject: RE: MassPort LPR Cameras
>>> Hi Jim,
>>> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>>> Thanks Brian
>>> From: John Tedona [mailto:jtedona@neology.net]
>>> Sent: Monday, December 9, 2019 4:55 PM
>>> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Slater, James (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>> Alex,
>>> I can be available most anytime tomorrow for a call.
>>> Regards,
>>> John Tedona
>>> PIPS TECHNOLOGY - A Neology Business
>>> Sales Manager
>>> 12760 Danielson Ct. Suite A
>>> Poway, CA 92064
>>> Phone: 201-841-6237
>>> Email: jtedona@neology.net<mailto:jtedona@neology.net>
>>> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
>>> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
>>> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
>>> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
>>> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ
>>> U2sB_fmM6g&e=>
>>> From: Chute, Alexander
>>> <AChute@massport.com<mailto:AChute@massport.com>>
>>> Sent: Monday, December 9, 2019 4:38 PM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>
>>> Cc: Guerriero, Robert (MASSIT)
>>> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
>>> Peek, Brian T. (EOTSS)
>>> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
>>> Slater III, James F (CHS)
>>> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
>>> Subject: RE: MassPort LPR Cameras
>>> CAUTION: This email originated from outside of the organization. Do not click links or open attachments

unless you recognize the sender and know the content is safe.
>>> Hello All,
>>> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>>> Respectfully,
>>> ~Alex
>>> <image007.png>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Monday, November 18, 2019 3:26 PM
>>> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
>>> pcrary@neology.net<mailto:pcrary@neology.net>
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>> Hi John, Peter
>>> Any issues with moving Massports cameras to the Chelsea DB?
>>> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>>> The current app server
>>> <image008.png>
>>> Current DB server
>>> <image009.png>
>>> <image010.png>
>>> Our current reads by month for about [redacted]
>>> Year
>>> Month
>>> Day
>>> Month Name
>>> Reads Count
>>> 2019
>>> 11
>>> 1
>>> November
>>> 495,113
>>> 2019
>>> 11
>>> 2
>>> November
>>> 472,907
>>> 2019
>>> 11
>>> 3
>>> November
>>> 384,409
>>> 2019
>>> 11

>>> 4
>>> November
>>> 411,440
>>> 2019
>>> 11
>>> 5
>>> November
>>> 434,085
>>> 2019
>>> 11
>>> 6
>>> November
>>> 495,537
>>> 2019
>>> 11
>>> 7
>>> November
>>> 444,123
>>> 2019
>>> 11
>>> 8
>>> November
>>> 542,492
>>> 2019
>>> 11
>>> 9
>>> November
>>> 443,463
>>> 2019
>>> 11
>>> 10
>>> November
>>> 389,514
>>> 2019
>>> 11
>>> 11
>>> November
>>> 362,548
>>> 2019
>>> 11
>>> 12
>>> November
>>> 236,539
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Wednesday, November 13, 2019 2:49 PM
>>> To: Egnitz, Brian (POL)
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>> These stats are from the [redacted] we have in the system for this month:
>>> <image011.png>
>>> ~Alex
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Tuesday, November 12, 2019 5:28 PM
>>> To: Chute, Alexander
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)

>>> Subject: RE: MassPort LPR Cameras
>>> Hi Alex,
>>> Can you please provide the updated reads per day? Previously you were interested in sharing [redacted] at approximately 75,000 reads per day.
>>> Here is the [redacted] confi I mentioned
>>> Set ho
>>> Set im
>>> Set nu
>>> Set Pi
>>> Set ud
>>> Set pi
>>> Set se
>>> I've lo [redacted] team from TSS on the thread. Maybe we can schedule a call in the next week.
>>> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>>> -Brian
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Tuesday, November 12, 2019 2:08 PM
>>> To: Egnitz, Brian (POL)
>>> Subject: MassPort LPR Cameras
>>> Brian,
>>> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to approximately [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.
>>> Respectfully,
>>> ~Alex
>>> <image007.png>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>> <SierraQuoteForMassPort.pdf>

From: brian.egnitz@pol.state.ma.us
To: Warmington, Scott (POL); Quinn, Dermot (POL)
Cc: Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Mason, Christopher (POL); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL); Crouse, David (POL)
Subject: Re: MassPort LPR Cameras
Date: Tuesday, August 18, 2020 7:07:59 PM

The Technical Service Unit and I have completed cutting over all of the Massport LPR cameras and they are reporting back to boss and Chelsea.

> On May 6, 2020, at 6:57 PM, Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us> wrote:
>
> Hi Sirs,
>
> We have begun cutting over the MassPort LPR Cameras into the EOPSS BOSS LPR Server. Today, [redacted] at Airport Road arrivals were migrated and are now writing data to Chelsea. I will continue to cut the remaining cameras over in the next few days and weeks. I will advise when the project is complete.
>
> - Brian
>
> -----Original Message-----
> From: Warmington, Scott (POL)
> Sent: Tuesday, March 10, 2020 11:36 AM
> To: Quinn, Dermot (POL)
> Cc: Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Mason, Christopher (POL); Egnitz, Brian (POL); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL)
> Subject: Re: MassPort LPR Cameras
>
> What is the cost?
>
> Sent from my iPhone
>
>> On Mar 10, 2020, at 11:28 AM, Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us> wrote:
>>
>> Michelle and Kyra,
>>
>> This purchase request is for equipment to allow Mass Port Sierra Wireless modems to communicate directly with the existing ALPR Boss server in Chelsea. This is the fastest way to bring the Massport LPR cameras on line. EOTSS and EOPSS are OK with this solution as is Major Deb Ryan, the CO at Troop F.
>>
>> As you can see from the thread, this has been going on for some time. I think we can close it out with this small purchase.
>>
>> This does not resolve the replacement of the existing ALPR equipment that we discussed at Command Staff yesterday. That is a different issue.
>>
>> Thanks
>>
>>
>> Lieutenant Colonel Dermot J. Quinn #1765
>> Division Commander
>> Division of Homeland Security & Preparedness
>> Massachusetts State Police
>>
>>
>>

>>
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 10:52 AM
>> To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: FW: MassPort LPR Cameras
>>
>> Hi LTC.,
>>
>> Can we order this equipment for the MassPort project?
>>
>> Thanks, Brian
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Tuesday, March 10, 2020 10:26 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> This needs to go through MSP fiscal. They need to enter the purchase in OPAS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 08:06
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Subject: RE: MassPort LPR Cameras
>>
>> Is this something you can order or does it need to go through MSP?
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Monday, March 9, 2020 10:36 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks, Brian...I will check with TSS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Monday, March 9, 2020 10:29
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks Jim,
>>
>> I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need [redacted] wireless AC adapters and [redacted] I have reached out to BCM for a quote.
>>

>> I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.
>>
>> I plan to cut one sector ([redacted]) over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?
>>
>> -Brian
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Friday, March 6, 2020 1:43 PM
>> To: Egnitz, Brian (POL)
>> Cc: Quinn, Dermot (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.
>>
>> So, assuming you move forward with this, who would actually make this happen?
>>
>> Thanks.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Wednesday, March 4, 2020 17:53
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: Re: MassPort LPR Cameras
>>
>> Hi Jim,
>>
>> Regarding the Massport cameras; in the early days of AVL we installed [redacted] modem's in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don't we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn't have to do any firewall work either because they have a 166. and communicate like all of the MDT's . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.
>>
>> We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.
>>
>> Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.
>>
>>>> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>>>
>>> Thank you sir
>>>
>>> Major Charles W. Atchison III
>>> Troop F Commander
>>> Massachusetts State Police

>>> Director of Aviation Security
>>> 2 Service Road
>>> East Boston, Ma 02128
>>> Office: 617-568-7555
>>> Cell: 508-[redacted]
>>>
>>>
>>>> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>>>
>>> All,
>>> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>>>
>>> Thanks
>>>
>>> CW
>>>
>>> From: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
>>> Sent: Monday, February 10, 2020 10:31 AM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
>>> Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
>>> Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
>>> Warmington, Scott (POL)
>>> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
>>> .us>>; Peek, Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
>>> Michalski, Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
>>> Christopher (POL)
>>> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
>>> Hughes, Sean M. (EOTSS)
>>> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
>>> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
>>> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
>>> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
>>> Atchison, Charles (POL)
>>> <catchison@massport.com<mailto:catchison@massport.com>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Good Morning,
>>>
>>> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.

>>>
>>> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>>>
>>> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>>>
>>> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>>>
>>> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>>>
>>> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>>>
>>> I can’t overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security’s technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>>>
>>> Respectfully,
>>>
>>>
>>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
>>> of Homeland Security & Preparedness Massachusetts State Police
>>> <image006.png>
>>>
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
>>> Sent: Friday, January 17, 2020 1:10 PM
>>> To: Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
>>> Cc: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
>>> Guerriero, Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
>>> Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,

>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
>>> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
>>> Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>
>>> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>>>
>>> -Brian
>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> Sent: Monday, January 6, 2020 1:33 PM
>>> To: Slater, James (CHS)
>>> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
>>> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
>>> Crary
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>
>>> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>>>
>>> Thanks Brian
>>>
>>>
>>> From: John Tedona [mailto:jtedona@neology.net]
>>> Sent: Monday, December 9, 2019 4:55 PM
>>> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Slater, James (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Alex,
>>>
>>> I can be available most anytime tomorrow for a call.
>>>
>>>
>>> Regards,
>>>
>>> John Tedona
>>> PIPS TECHNOLOGY - A Neology Business
>>> Sales Manager
>>> 12760 Danielson Ct. Suite A
>>> Poway, CA 92064
>>> Phone: 201-841-6237
>>> Email: jtedona@neology.net<mailto:jtedona@neology.net>
>>> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
>>> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http

>>> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
>>> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
>>> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ
>>> U2sB_fmM6g&e=>
>>>
>>>
>>> From: Chute, Alexander
>>> <AChute@massport.com<mailto:AChute@massport.com>>
>>> Sent: Monday, December 9, 2019 4:38 PM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>
>>> Cc: Guerriero, Robert (MASSIT)
>>> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
>>> Peek, Brian T. (EOTSS)
>>> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
>>> Slater III, James F (CHS)
>>> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>>>
>>> Hello All,
>>>
>>> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>>>
>>> Respectfully,
>>>
>>> ~Alex
>>>
>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Monday, November 18, 2019 3:26 PM
>>> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);

>>> pcrary@neology.net<mailto:pcrary@neology.net>
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi John, Peter
>>>
>>> Any issues with moving Massports cameras to the Chelsea DB?
>>>
>>> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>>>
>>> The current app server
>>> <image008.png>
>>>
>>> Current DB server
>>>
>>> <image009.png>
>>> <image010.png>
>>>
>>> Our current reads by month for about [redacted]
>>>
>>> Year
>>>
>>> Month
>>>
>>> Day
>>>
>>> Month Name
>>>
>>> Reads Count
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 1
>>>
>>> November
>>>
>>>   495,113
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 2
>>>
>>> November
>>>
>>>   472,907
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 3
>>>

>>> November
>>>
>>> 384,409
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 4
>>>
>>> November
>>>
>>> 411,440
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 5
>>>
>>> November
>>>
>>> 434,085
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 6
>>>
>>> November
>>>
>>> 495,537
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 7
>>>
>>> November
>>>
>>> 444,123
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 8
>>>
>>> November
>>>
>>> 542,492
>>>
>>> 2019
>>>
>>> 11

>>>
>>> 9
>>>
>>> November
>>>
>>> 443,463
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 10
>>>
>>> November
>>>
>>> 389,514
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 11
>>>
>>> November
>>>
>>> 362,548
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 12
>>>
>>> November
>>>
>>> 236,539
>>>
>>>
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Wednesday, November 13, 2019 2:49 PM
>>> To: Egnitz, Brian (POL)
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> These stats are from the [redacted] we have in the system for this month:
>>>
>>> <image011.png>
>>>
>>> ~Alex
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Tuesday, November 12, 2019 5:28 PM

>>> To: Chute, Alexander
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Alex,
>>>
>>> Can you please provide the updated reads per day? Previously you were interested in sharing [redacted] at approximately 75,000 reads per day.
>>>
>>> Here is the [redacted] confi I mentioned.
>>>
>>> Set host to [redacted]
>>> Set image [redacted]
>>> Set number [redacted]
>>> Set Ping [redacted]
>>> Set udp pin [redacted]
>>> Set ping [redacted]
>>> Set security [redacted]
>>>
>>> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
>>> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>>>
>>> -Brian
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Tuesday, November 12, 2019 2:08 PM
>>> To: Egnitz, Brian (POL)
>>> Subject: MassPort LPR Cameras
>>>
>>> Brian,
>>>
>>> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to approximately [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.
>>>
>>> Respectfully,
>>>
>>> ~Alex
>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>

>>>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>> <SierraQuoteForMassPort.pdf>

From: Alves, Joe
To: Egnitz, Brian (POL); Haverty, Robert
Cc: Chavis, Michael J.; O'Leary, John F
Subject: Re: MassPort LPR Cameras
Date: Wednesday, July 22, 2020 7:54:57 PM

Looping in Bob.

Sent from my iPhone

On Jul 22, 2020, at 7:54 PM, Egnitz, Brian (POL) <brian.egnitz@state.ma.us> wrote:

Hi all,

Any luck on scheduling?

-Brian

From: Chavis, Michael J. [mailto:MChavis@massport.com]
Sent: Thursday, July 16, 2020 12:48 PM
To: Alves, Joe
Cc: O'Leary, John F; Egnitz, Brian (POL)
Subject: FW: MassPort LPR Cameras

Joe,

Thank you for getting back to me about the LPR work mentioned in the email thread below. I've been told that the remaining 2 locations are in areas that require Detail Support due to the length of time required to perform the work and the fact that partial lane closures are necessary.

Any information you could provide would be helpful so that we could figure out logistics (exact locations, how the detail areas will be set up and billing. As you can see, they would like to complete this work sometime in the next month.

I look forward to hearing from you.

Sgt Michael J. Chavis #0751
Paid Detail Office Supervisor
Mass. State Police – Logan International Airport
2 Service Road
East Boston, MA 02128
(617)568-7324

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Wednesday, July 15, 2020 11:28 AM
To: Chavis, Michael J.
Cc: Ryan, Deborah (POL); Alves, Joe; Gilmore, Joey; Crouse, David (POL); Doherty, Gregory (POL)
Subject: RE: MassPort LPR Cameras

Hi Sgt.,

Thanks for taking my call, as follow up:

· There are 2 sites remaining for cutover.

· I've included the MassPort IT contacts who can tell you specifically where the sites are located.

· I estimate the job to take between 2-6 hours per site.

· I'd like to do one site per day

· Afterhours would be preferred when traffic is lower and there are less eyeballs.

· Tuesday or Thursday eves are open for me now for the next 4 weeks

· A member of the Technical Services Unit will be onsite with me during the cutover in case we have a problem with one of the cameras (you do not need to include them in the detail, they will use TSU OT budget)

-Brian

From: Ryan, Deborah (POL)
Sent: Wednesday, July 15, 2020 11:01 AM
To: Egnitz, Brian (POL)
Subject: Re: MassPort LPR Cameras

Ok, you can work with Sgt. Mike Chavis directly to coordinate details. mchavis@massport.com 617-568-7518

Best,

Major Ryan

THIS EMAIL MAY CONTAIN INFORMATION FOR OFFICIAL USE ONLY AND LAW ENFORCEMENT SENSITIVE INFORMATION. This E-mail (including attachments) is covered by the Electronic Communications Privacy Act, 18 USC 2510-2521, is confidential and may be legally privileged. If you are not the intended recipient, you are hereby notified that any retention, dissemination, distribution, or copying of this communication is strictly prohibited and may be unlawful. Please reply to the sender that you have received the message in error and then delete the message and any attachments.

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Tuesday, July 14, 2020 8:59 AM
To: Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>
Subject: Re: MassPort LPR Cameras

Yes, it hasn't been scheduled

On Jul 14, 2020, at 7:52 AM, Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us> wrote:

Hi Brian,

Where was it left off? Utilizing details for the road closure?

THIS EMAIL MAY CONTAIN INFORMATION FOR OFFICIAL USE ONLY AND LAW ENFORCEMENT SENSITIVE INFORMATION. This E-mail (including attachments) is covered by the Electronic Communications Privacy Act, 18 USC 2510-2521, is confidential and may be legally privileged. If you are not the intended recipient, you are hereby notified that any retention, dissemination, distribution, or copying of this communication is strictly prohibited and may be unlawful. Please reply to the sender that you have received the message in error and then delete the message and any attachments.

_____

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Tuesday, July 14, 2020 7:29 AM
To: Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>
Subject: Re: MassPort LPR Cameras

Hi Maj.,

Are you aware of any movement on this? I'd like to finish the cutover of the remaining cameras.

Thanks, Brian

On May 21, 2020, at 10:57 AM, Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us> wrote:

Hi Brian,

Could you give me a call at your convenience regarding the rest of the LPR cutovers.

Thank you,

Major Ryan
781-281-5177

THIS EMAIL MAY CONTAIN INFORMATION FOR OFFICIAL USE ONLY AND LAW ENFORCEMENT SENSITIVE INFORMATION. This E-mail (including attachments) is covered by the Electronic Communications Privacy Act, 18 USC 2510-2521, is confidential and may be legally privileged. If you are not the intended recipient, you are hereby notified that any retention, dissemination, distribution, or copying of this communication is strictly prohibited and may be unlawful. Please reply to the sender that you have received the message in error and then delete the message and any attachments.

_____

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Monday, May 18, 2020 4:58 PM
To: Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>
Cc: Crouse, David (POL) <david.crouse@pol.state.ma.us>
Subject: RE: MassPort LPR Cameras

Hi Major,

I have finished cutting over the LPR cameras that were accessible off the road. G.L. c. 4.sec. 7.cl.26 (n)(security) cameras (G.L. c. 4.sec. 7.cl.26 (n)(security) and needs inspection). G.L. c. 4.sec. 7.cl.26 (n)(security) need lane closures. G.L. c. 4.sec. 7.cl.26 (n)(s

G.L. c. 4.sec. 7.cl.26 (n)(security) G.L. c. 4.sec. 7.cl.26 (n)(security) I estimate needing 2-5 hours per site. Lt. Crouse has offered to assist in lane closures using unmarked vehicles, how would you like to proceeded in completing the cut over of the remaining sites.

Thanks, Brian

From: Ryan, Deborah (POL)
Sent: Wednesday, May 6, 2020 9:46 PM
To: Mason, Christopher (POL); Egnitz, Brian (POL)
Cc: Warmington, Scott (POL); Quinn, Dermot (POL); Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Warren, Rosemary (POL); Shaw, Harold; Ball, Richard (POL)
Subject: Re: MassPort LPR Cameras

Thank you Brian.

Major Deborah A. Ryan
Massachusetts State Police
Troop F Commander
485 Maple St

From: Mason, Christopher (POL) <Chris.Mason@pol.state.ma.us>
Sent: Wednesday, May 6, 2020 7:00 PM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Cc: Warmington, Scott (POL) <Scott.Warmington@pol.state.ma.us>; Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Small, Michelle (POL) <Michelle.E.Small@pol.state.ma.us>; Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>; Slater, James (CHS) <james.slater@mass.gov>; Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>; Shaw, Harold <HShaw@massport.com>; Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>; Ball, Richard (POL) <Richard.Ball@pol.state.ma.us>
Subject: Re: MassPort LPR Cameras

Thank you Brian. Great work grabbing this data.

Colonel Christopher Mason
Superintendent
Massachusetts State Police

> On May 6, 2020, at 6:57 PM, Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us> wrote:
>
> Hi Sirs,
>
> We have begun cutting over the MassPort LPR Cameras into the EOPSS BOSS LPR Server. Today, [redacted] G.L. c. 4.sec. 7.cl.26 (n)(security) [redacted]. I will continue to cut the remaining cameras over in the next few days and weeks. I will advise when the project is complete.
>
> - Brian
>
> -----Original Message-----
> From: Warmington, Scott (POL)
> Sent: Tuesday, March 10, 2020 11:36 AM
> To: Quinn, Dermot (POL)
> Cc: Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Mason, Christopher (POL); Egnitz, Brian (POL); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL)
> Subject: Re: MassPort LPR Cameras
>
> What is the cost?
>
> Sent from my iPhone
>
>> On Mar 10, 2020, at 11:28 AM, Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us> wrote:
>>
>> Michelle and Kyra,
>>
>> This purchase request is for equipment to allow Mass Port Sierra Wireless modems to communicate directly with the existing ALPR Boss server in Chelsea. This is the fastest way to bring the Massport LPR cameras on line. EOTSS and EOPSS are OK with this solution as is Major Deb Ryan, the CO at Troop F.
>>
>> As you can see from the thread, this has been going on for some time. I think we can close it out with this small purchase.
>>
>> This does not resolve the replacement of the existing ALPR equipment that we discussed at Command Staff yesterday. That is a different issue.
>>
>> Thanks
>>
>>
>> Lieutenant Colonel Dermot J. Quinn #1765
>> Division Commander
>> Division of Homeland Security & Preparedness
>> Massachusetts State Police
>>
>>
>>
>>
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 10:52 AM
>> To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: FW: MassPort LPR Cameras
>>
>> Hi LTC.,

>>
>> Can we order this equipment for the MassPort project?
>>
>> Thanks, Brian
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Tuesday, March 10, 2020 10:26 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> This needs to go through MSP fiscal. They need to enter the purchase in OPAS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 08:06
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Subject: RE: MassPort LPR Cameras
>>
>> Is this something you can order or does it need to go through MSP?
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Monday, March 9, 2020 10:36 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks, Brian...I will check with TSS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Monday, March 9, 2020 10:29
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks Jim,
>>
>> I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need [redacted] wireless AC adapters and [redacted] I have reached out to BCM for a quote.
>>
>> I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.
>>
>> I plan to cut one sector ([redacted]) over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?
>>
>> -Brian
>>

>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Friday, March 6, 2020 1:43 PM
>> To: Egnitz, Brian (POL)
>> Cc: Quinn, Dermot (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.
>>
>> So, assuming you move forward with this, who would actually make this happen?
>>
>> Thanks.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Wednesday, March 4, 2020 17:53
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: Re: MassPort LPR Cameras
>>
>> Hi Jim,
>>
>> Regarding the Massport cameras; in the early days of AVL we installed [G.L. c. 4.sec. 7.cl.26 (n)(security)] modem's in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don't we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn't have to do any firewall work either because they have a 166. and communicate like all of the MDT's . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.
>>
>> We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.
>>
>> Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.
>>
>>>> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>>>
>>> Thank you sir
>>>
>>> Major Charles W. Atchison III
>>> Troop F Commander
>>> Massachusetts State Police
>>> Director of Aviation Security
>>> 2 Service Road
>>> East Boston, Ma 02128
>>> Office: 617-568-7555
>>> Cell: 508[G.L. c. 4.sec. 7.cl.26 (n)]
>>>
>>>
>>>> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:

>>>
>>> All,
>>> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>>>
>>> Thanks
>>>
>>> CW
>>>
>>> From: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
>>> Sent: Monday, February 10, 2020 10:31 AM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
>>> Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
>>> Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
>>> Warmington, Scott (POL)
>>> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
>>> .us>>; Peek, Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
>>> Michalski, Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
>>> Christopher (POL)
>>> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
>>> Hughes, Sean M. (EOTSS)
>>> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
>>> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
>>> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
>>> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
>>> Atchison, Charles (POL)
>>> <catchison@massport.com<mailto:catchison@massport.com>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Good Morning,
>>>
>>> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>>>
>>> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>>>
>>> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the

potential for Massport's cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>>>
>>> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>>>
>>> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>>>
>>> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>>>
>>> I can't overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security's technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>>>
>>> Respectfully,
>>>
>>>
>>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
>>> of Homeland Security & Preparedness Massachusetts State Police
>>> <image006.png>
>>>
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
>>> Sent: Friday, January 17, 2020 1:10 PM
>>> To: Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
>>> Cc: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
>>> Guerriero, Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
>>> Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
>>> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
>>> Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>
>>> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also

submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>>>
>>> -Brian
>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> Sent: Monday, January 6, 2020 1:33 PM
>>> To: Slater, James (CHS)
>>> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
>>> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
>>> Crary
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>
>>> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>>>
>>> Thanks Brian
>>>
>>>
>>> From: John Tedona [mailto:jtedona@neology.net]
>>> Sent: Monday, December 9, 2019 4:55 PM
>>> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Slater, James (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Alex,
>>>
>>> I can be available most anytime tomorrow for a call.
>>>
>>>
>>> Regards,
>>>
>>> John Tedona
>>> PIPS TECHNOLOGY - A Neology Business
>>> Sales Manager
>>> 12760 Danielson Ct. Suite A
>>> Poway, CA 92064
>>> Phone: 201-841-6237
>>> Email: jtedona@neology.net<mailto:jtedona@neology.net>
>>> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
>>> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http<https://urldefense.proofpoint.com/v2/url?u=http-3A__www.pipstechnology.com-253chttps-3A_urldefense.proofpoint.com_v2_url-3Fu-3Dhttp&d=DwMGaQ&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FNEWIHnzbfZimE&r=jetJ-_o8TxNcyW0Pxse8hZLfJPoOY2-vOv20KWc05ik&m=bDQ7iSuWHluIoFRZDVD0elN0wOufXHelVZqtJZwj42k&s=pervenL-GCfuIqjoBN9oZTaON87brs1rDhRqNAKlmLg&e=>
>>> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
>>> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
>>> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ

>>> U2sB_fmM6g&e=>
>>>
>>>
>>> From: Chute, Alexander
>>> <AChute@massport.com<mailto:AChute@massport.com>>
>>> Sent: Monday, December 9, 2019 4:38 PM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>
>>> Cc: Guerriero, Robert (MASSIT)
>>> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
>>> Peek, Brian T. (EOTSS)
>>> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
>>> Slater III, James F (CHS)
>>> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>>>
>>> Hello All,
>>>
>>> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>>>
>>> Respectfully,
>>>
>>> ~Alex
>>>
>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Monday, November 18, 2019 3:26 PM
>>> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
>>> pcrary@neology.net<mailto:pcrary@neology.net>
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)

>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi John, Peter
>>>
>>> Any issues with moving Massports cameras to the Chelsea DB?
>>>
>>> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>>>
>>> The current app server
>>> <image008.png>
>>>
>>> Current DB server
>>>
>>> <image009.png>
>>> <image010.png>
>>>
>>> Our current reads by month for about [redacted]
>>>
>>> Year
>>>
>>> Month
>>>
>>> Day
>>>
>>> Month Name
>>>
>>> Reads Count
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 1
>>>
>>> November
>>>
>>> 495,113
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 2
>>>
>>> November
>>>
>>> 472,907
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 3
>>>
>>> November
>>>
>>> 384,409

>>>
>>> 2019
>>>
>>> 11
>>>
>>> 4
>>>
>>> November
>>>
>>> 411,440
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 5
>>>
>>> November
>>>
>>> 434,085
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 6
>>>
>>> November
>>>
>>> 495,537
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 7
>>>
>>> November
>>>
>>> 444,123
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 8
>>>
>>> November
>>>
>>> 542,492
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 9
>>>

>>> November
>>>
>>> 443,463
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 10
>>>
>>> November
>>>
>>> 389,514
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 11
>>>
>>> November
>>>
>>> 362,548
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 12
>>>
>>> November
>>>
>>> 236,539
>>>
>>>
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Wednesday, November 13, 2019 2:49 PM
>>> To: Egnitz, Brian (POL)
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> These stats are from the [redacted] we have in the system for this month:
>>>
>>> <image011.png>
>>>
>>> ~Alex
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Tuesday, November 12, 2019 5:28 PM
>>> To: Chute, Alexander
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)

>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Alex,
>>>
>>> Can you please provide the updated reads per day? Previously you were interested in sharing [redacted] at approximately 75,000 reads per day.
>>>
>>> Here is the [redacted] confi I mentioned.
>>>
>>> Set host [redacted]
>>> Set imag
>>> Set num
>>> Set Ping
>>> Set udp
>>> Set ping
>>> Set secur
>>>
>>> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
>>> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>>>
>>> -Brian
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Tuesday, November 12, 2019 2:08 PM
>>> To: Egnitz, Brian (POL)
>>> Subject: MassPort LPR Cameras
>>>
>>> Brian,
>>>
>>> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to approximately [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.
>>>
>>> Respectfully,
>>>
>>> ~Alex
>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts

15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>> <SierraQuoteForMassPort.pdf>

The information contained in this communication, including any attachments, is confidential and is intended only for the use of the recipient(s) named above. If the reader of this message is not an intended recipient, you are notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you receive this communication in error, please notify the sender immediately, and delete the communication, any attachments, and all copies.

From: Ryan, Deborah (POL)
To: Egnitz, Brian (POL)
Subject: Re: MassPort LPR Cameras
Date: Wednesday, July 15, 2020 11:00:47 AM

Ok, you can work with Sgt. Mike Chavis directly to coordinate details. mchavis@massport.com 617-568-7518

Best,

Major Ryan

THIS EMAIL MAY CONTAIN INFORMATION FOR OFFICIAL USE ONLY AND LAW ENFORCEMENT SENSITIVE INFORMATION. This E-mail (including attachments) is covered by the Electronic Communications Privacy Act, 18 USC 2510-2521, is confidential and may be legally privileged. If you are not the intended recipient, you are hereby notified that any retention, dissemination, distribution, or copying of this communication is strictly prohibited and may be unlawful. Please reply to the sender that you have received the message in error and then delete the message and any attachments.

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Tuesday, July 14, 2020 8:59 AM
To: Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>
Subject: Re: MassPort LPR Cameras

Yes, it hasn't been scheduled

> On Jul 14, 2020, at 7:52 AM, Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us> wrote:
>
> Hi Brian,
>
> Where was it left off? Utilizing details for the road closure?
>
> THIS EMAIL MAY CONTAIN INFORMATION FOR OFFICIAL USE ONLY AND LAW ENFORCEMENT SENSITIVE INFORMATION. This E-mail (including attachments) is covered by the Electronic Communications Privacy Act, 18 USC 2510-2521, is confidential and may be legally privileged. If you are not the intended recipient, you are hereby notified that any retention, dissemination, distribution, or copying of this communication is strictly prohibited and may be unlawful. Please reply to the sender that you have received the message in error and then delete the message and any attachments.
>
> ---
>
> **From:** Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>

Sent: Tuesday, July 14, 2020 7:29 AM
To: Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>
Subject: Re: MassPort LPR Cameras

Hi Maj.,

Are you aware of any movement on this? I'd like to finish the cutover of the remaining cameras.

Thanks, Brian

> On May 21, 2020, at 10:57 AM, Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us> wrote:
>
> Hi Brian,
>
> Could you give me a call at your convenience regarding the rest of the LPR cutovers.
>
> Thank you,
>
> Major Ryan
> 781-281-5177
>
> THIS EMAIL MAY CONTAIN INFORMATION FOR OFFICIAL USE ONLY AND LAW ENFORCEMENT SENSITIVE INFORMATION. This E-mail (including attachments) is covered by the Electronic Communications Privacy Act, 18 USC 2510-2521, is confidential and may be legally privileged. If you are not the intended recipient, you are hereby notified that any retention, dissemination, distribution, or copying of this communication is strictly prohibited and may be unlawful. Please reply to the sender that you have received the message in error and then delete the message and any attachments.

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Monday, May 18, 2020 4:58 PM
To: Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>
Cc: Crouse, David (POL) <david.crouse@pol.state.ma.us>
Subject: RE: MassPort LPR Cameras

Hi Major,

I have finished cutting over the LPR cameras that were accessible off the road. [redacted] cameras (G.L. c. 4.sec. 7.cl.26 (n)(security) and needs inspection). G.L. c. 4.sec. 7.cl.26 (n)(security) need lane closures. G.L. c. 4.sec. 7.cl.26 (n)(security) [redacted] and G.L. c. 4.sec. 7.cl.26 (n)(security) I estimate needing 2-5 hours per site. Lt. Crouse has offered to assist in lane closures using unmarked vehicles, how would you like to proceeded in completing the cut over of the remaining sites.

Thanks, Brian

From: Ryan, Deborah (POL)
Sent: Wednesday, May 6, 2020 9:46 PM
To: Mason, Christopher (POL); Egnitz, Brian (POL)
Cc: Warmington, Scott (POL); Quinn, Dermot (POL); Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Warren, Rosemary (POL); Shaw, Harold; Ball, Richard (POL)
Subject: Re: MassPort LPR Cameras

Thank you Brian.

Major Deborah A. Ryan
Massachusetts State Police
Troop F Commander
485 Maple St

From: Mason, Christopher (POL) <Chris.Mason@pol.state.ma.us>
Sent: Wednesday, May 6, 2020 7:00 PM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Cc: Warmington, Scott (POL) <Scott.Warmington@pol.state.ma.us>; Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Small, Michelle (POL) <Michelle.E.Small@pol.state.ma.us>; Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>; Slater, James (CHS) <james.slater@mass.gov>; Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>; Shaw, Harold <HShaw@massport.com>; Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>; Ball, Richard (POL) <Richard.Ball@pol.state.ma.us>
Subject: Re: MassPort LPR Cameras

Thank you Brian. Great work grabbing this data.

Colonel Christopher Mason
Superintendent
Massachusetts State Police

> On May 6, 2020, at 6:57 PM, Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us> wrote:
>
> Hi Sirs,
>
> We have begun cutting over the MassPort LPR Cameras into the EOPSS BOSS LPR Server. Today, G.L. c. 4.sec. 7.cl.26 (n)(security) at Airport Road arrivals were migrated and are now writing data to Chelsea. I will continue to cut the remaining cameras over in the next few days and weeks. I will advise when the

project is complete.
>
> - Brian
>
> -----Original Message-----
> From: Warmington, Scott (POL)
> Sent: Tuesday, March 10, 2020 11:36 AM
> To: Quinn, Dermot (POL)
> Cc: Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Mason, Christopher (POL); Egnitz, Brian (POL); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL)
> Subject: Re: MassPort LPR Cameras
>
> What is the cost?
>
> Sent from my iPhone
>
>> On Mar 10, 2020, at 11:28 AM, Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us> wrote:
>>
>> Michelle and Kyra,
>>
>> This purchase request is for equipment to allow Mass Port Sierra Wireless modems to communicate directly with the existing ALPR Boss server in Chelsea. This is the fastest way to bring the Massport LPR cameras on line. EOTSS and EOPSS are OK with this solution as is Major Deb Ryan, the CO at Troop F.
>>
>> As you can see from the thread, this has been going on for some time. I think we can close it out with this small purchase.
>>
>> This does not resolve the replacement of the existing ALPR equipment that we discussed at Command Staff yesterday. That is a different issue.
>>
>> Thanks
>>
>>
>> Lieutenant Colonel Dermot J. Quinn #1765
>> Division Commander
>> Division of Homeland Security & Preparedness
>> Massachusetts State Police
>>
>>
>>
>>
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 10:52 AM
>> To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: FW: MassPort LPR Cameras
>>
>> Hi LTC.,
>>
>> Can we order this equipment for the MassPort project?
>>
>> Thanks, Brian

>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Tuesday, March 10, 2020 10:26 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> This needs to go through MSP fiscal. They need to enter the purchase in OPAS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 08:06
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Subject: RE: MassPort LPR Cameras
>>
>> Is this something you can order or does it need to go through MSP?
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Monday, March 9, 2020 10:36 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks, Brian...I will check with TSS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Monday, March 9, 2020 10:29
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks Jim,
>>
>> I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need [redacted] wireless AC adapters and [redacted] I have reached out to BCM for a quote.
>>
>> I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.
>>
>> I plan to cut one sector ([redacted]) over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?
>>
>> -Brian
>>

>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Friday, March 6, 2020 1:43 PM
>> To: Egnitz, Brian (POL)
>> Cc: Quinn, Dermot (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.
>>
>> So, assuming you move forward with this, who would actually make this happen?
>>
>> Thanks.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Wednesday, March 4, 2020 17:53
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: Re: MassPort LPR Cameras
>>
>> Hi Jim,
>>
>> Regarding the Massport cameras; in the early days of AVL we installed [redacted] modem's in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don't we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn't have to do any firewall work either because they have a 166. and communicate like all of the MDT's . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.
>>
>> We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.
>>
>> Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.
>>
>>>> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>>>
>>> Thank you sir
>>>
>>> Major Charles W. Atchison III
>>> Troop F Commander
>>> Massachusetts State Police

>>> Director of Aviation Security
>>> 2 Service Road
>>> East Boston, Ma 02128
>>> Office: 617-568-7555
>>> Cell: 508[redacted]
>>>
>>>
>>>> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>>>
>>> All,
>>> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>>>
>>> Thanks
>>>
>>> CW
>>>
>>> From: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
>>> Sent: Monday, February 10, 2020 10:31 AM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
>>> Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
>>> Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
>>> Warmington, Scott (POL)
>>>
<Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
>>> .us>>; Peek, Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
>>> Michalski, Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>;
Mason,
>>> Christopher (POL)
>>> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
>>> Hughes, Sean M. (EOTSS)
>>> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis
(EOTSS)
>>> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
>>> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard
(POL)
>>> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
>>> Atchison, Charles (POL)
>>> <catchison@massport.com<mailto:catchison@massport.com>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Good Morning,
>>>
>>> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time

ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>>>
>>> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>>>
>>> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>>>
>>> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>>>
>>> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>>>
>>> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>>>
>>> I can’t overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security’s technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>>>
>>> Respectfully,
>>>
>>>
>>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
>>> of Homeland Security & Preparedness Massachusetts State Police
>>> <image006.png>
>>>
>>>

>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
>>> Sent: Friday, January 17, 2020 1:10 PM
>>> To: Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
>>> Cc: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
>>> Guerriero, Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
Peek,
>>> Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
Peter
>>> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
>>> Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>
>>> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>>>
>>> -Brian
>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> Sent: Monday, January 6, 2020 1:33 PM
>>> To: Slater, James (CHS)
>>> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
>>> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
>>> Crary
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>
>>> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>>>
>>> Thanks Brian
>>>
>>>
>>> From: John Tedona [mailto:jtedona@neology.net]
>>> Sent: Monday, December 9, 2019 4:55 PM
>>> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary

>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Slater, James (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Alex,
>>>
>>> I can be available most anytime tomorrow for a call.
>>>
>>>
>>> Regards,
>>>
>>> John Tedona
>>> PIPS TECHNOLOGY - A Neology Business
>>> Sales Manager
>>> 12760 Danielson Ct. Suite A
>>> Poway, CA 92064
>>> Phone: 201-841-6237
>>> Email: jtedona@neology.net<mailto:jtedona@neology.net>
>>> PIPS Support:
support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-
7577, Option 1 for sales, Option 2 for Support
>>> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
>>>
-3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
>>>
EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
>>>
baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-
lyPhyJ
>>> U2sB_fmM6g&e=>
>>>
>>>
>>> From: Chute, Alexander
>>> <AChute@massport.com<mailto:AChute@massport.com>>
>>> Sent: Monday, December 9, 2019 4:38 PM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>
>>> Cc: Guerriero, Robert (MASSIT)
>>> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
>>> Peek, Brian T. (EOTSS)
>>> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
>>> Slater III, James F (CHS)
>>> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> CAUTION: This email originated from outside of the organization. Do not
click links or open attachments unless you recognize the sender and know the
content is safe.
>>>
>>> Hello All,
>>>
>>> I just wanted to follow up with this request to see what the next steps for
this project are. I believe that we can make the connections to the EOPSS

network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>>>
>>> Respectfully,
>>>
>>> ~Alex
>>>
>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Monday, November 18, 2019 3:26 PM
>>> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
>>> pcrary@neology.net<mailto:pcrary@neology.net>
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi John, Peter
>>>
>>> Any issues with moving Massports cameras to the Chelsea DB?
>>>
>>> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>>>
>>> The current app server
>>> <image008.png>
>>>
>>> Current DB server
>>>
>>> <image009.png>
>>> <image010.png>
>>>
>>> Our current reads by month for about [redacted]
>>>
>>> Year
>>>
>>> Month
>>>

>>> Day
>>>
>>> Month Name
>>>
>>> Reads Count
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 1
>>>
>>> November
>>>
>>> 495,113
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 2
>>>
>>> November
>>>
>>> 472,907
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 3
>>>
>>> November
>>>
>>> 384,409
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 4
>>>
>>> November
>>>
>>> 411,440
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 5
>>>
>>> November
>>>
>>> 434,085
>>>
>>> 2019

>>>
>>> 11
>>>
>>> 6
>>>
>>> November
>>>
>>> 495,537
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 7
>>>
>>> November
>>>
>>> 444,123
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 8
>>>
>>> November
>>>
>>> 542,492
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 9
>>>
>>> November
>>>
>>> 443,463
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 10
>>>
>>> November
>>>
>>> 389,514
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 11
>>>
>>> November
>>>

>>> 362,548
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 12
>>>
>>> November
>>>
>>> 236,539
>>>
>>>
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Wednesday, November 13, 2019 2:49 PM
>>> To: Egnitz, Brian (POL)
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> These stats are from the [redacted] we have in the system for this month:
>>>
>>> <image011.png>
>>>
>>> ~Alex
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Tuesday, November 12, 2019 5:28 PM
>>> To: Chute, Alexander
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Alex,
>>>
>>> Can you please provide the updated reads per day? Previously you were interested in sharing [redacted] at approximately 75,000 reads per day.
>>>
>>> Here is the [redacted] confi I mentioned.
>>>
>>> Set hos
>>> Set im
>>> Set nu
>>> Set Pin
>>> Set ud
>>> Set pin
>>> Set sec
>>>
>>> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
>>> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.

>>>
>>> -Brian
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Tuesday, November 12, 2019 2:08 PM
>>> To: Egnitz, Brian (POL)
>>> Subject: MassPort LPR Cameras
>>>
>>> Brian,
>>>
>>> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to approximately [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.
>>>
>>> Respectfully,
>>>
>>> ~Alex
>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>> <SierraQuoteForMassPort.pdf>

From: Egnitz, Brian (POL)
To: Ryan, Deborah (POL)
Subject: Re: MassPort LPR Cameras
Date: Tuesday, July 14, 2020 8:59:39 AM

Yes, it hasn't been scheduled

> On Jul 14, 2020, at 7:52 AM, Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us> wrote:
>
> Hi Brian,
>
> Where was it left off? Utilizing details for the road closure?

THIS EMAIL MAY CONTAIN INFORMATION FOR OFFICIAL USE ONLY AND LAW ENFORCEMENT SENSITIVE INFORMATION. This E-mail (including attachments) is covered by the Electronic Communications Privacy Act, 18 USC 2510-2521, is confidential and may be legally privileged. If you are not the intended recipient, you are hereby notified that any retention, dissemination, distribution, or copying of this communication is strictly prohibited and may be unlawful. Please reply to the sender that you have received the message in error and then delete the message and any attachments.

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Tuesday, July 14, 2020 7:29 AM
To: Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>
Subject: Re: MassPort LPR Cameras

Hi Maj.,

Are you aware of any movement on this? I'd like to finish the cutover of the remaining cameras.

Thanks, Brian

> On May 21, 2020, at 10:57 AM, Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us> wrote:
>
> Hi Brian,
>
> Could you give me a call at your convenience regarding the rest of the LPR cutovers.
>
> Thank you,

Major Ryan
781-281-5177

THIS EMAIL MAY CONTAIN INFORMATION FOR OFFICIAL USE ONLY AND LAW ENFORCEMENT SENSITIVE INFORMATION. This E-mail (including attachments) is covered by the Electronic Communications Privacy Act, 18 USC 2510-2521, is confidential and may be legally privileged. If you are not the intended recipient, you are hereby notified that any retention, dissemination, distribution, or copying of this communication is strictly prohibited and may be unlawful. Please reply to the sender that you have received the message in error and then delete the message and any attachments.

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Monday, May 18, 2020 4:58 PM
To: Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>
Cc: Crouse, David (POL) <david.crouse@pol.state.ma.us>
Subject: RE: MassPort LPR Cameras

Hi Major,

I have finished cutting over the LPR cameras that were accessible off the road. [redacted] cameras ([redacted] G.L. c. 4.sec. 7.cl.26 (n)(security) and needs inspection). G.L. c. 4.sec. 7.cl.26 (n)(security) need lane closures. G.L. c. 4.sec. 7.cl.26 (n)(security) [redacted] and G.L. c. 4.sec. 7.cl.26 (n)(security) I estimate needing 2-5 hours per site. Lt. Crouse has offered to assist in lane closures using unmarked vehicles, how would you like to proceeded in completing the cut over of the remaining sites.

Thanks, Brian

From: Ryan, Deborah (POL)
Sent: Wednesday, May 6, 2020 9:46 PM
To: Mason, Christopher (POL); Egnitz, Brian (POL)
Cc: Warmington, Scott (POL); Quinn, Dermot (POL); Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Warren, Rosemary (POL); Shaw, Harold; Ball, Richard (POL)
Subject: Re: MassPort LPR Cameras

Thank you Brian.

Major Deborah A. Ryan
Massachusetts State Police
Troop F Commander
485 Maple St

From: Mason, Christopher (POL) <Chris.Mason@pol.state.ma.us>
Sent: Wednesday, May 6, 2020 7:00 PM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Cc: Warmington, Scott (POL) <Scott.Warmington@pol.state.ma.us>; Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Small, Michelle (POL) <Michelle.E.Small@pol.state.ma.us>; Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>; Slater, James (CHS) <james.slater@mass.gov>; Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>; Shaw, Harold <HShaw@massport.com>; Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>; Ball, Richard (POL) <Richard.Ball@pol.state.ma.us>
Subject: Re: MassPort LPR Cameras

Thank you Brian. Great work grabbing this data.

Colonel Christopher Mason
Superintendent
Massachusetts State Police

> On May 6, 2020, at 6:57 PM, Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us> wrote:
>
> Hi Sirs,
>
> We have begun cutting over the MassPort LPR Cameras into the EOPSS BOSS LPR Server. Today, [redacted] G.L. c. 4.sec. 7.cl.26 (n)(security) at Airport Road arrivals were migrated and are now writing data to Chelsea. I will continue to cut the remaining cameras over in the next few days and weeks. I will advise when the project is complete.
>
> - Brian
>
> -----Original Message-----
> From: Warmington, Scott (POL)
> Sent: Tuesday, March 10, 2020 11:36 AM
> To: Quinn, Dermot (POL)
> Cc: Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Mason, Christopher (POL); Egnitz, Brian (POL); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL)
> Subject: Re: MassPort LPR Cameras
>
> What is the cost?
>
> Sent from my iPhone
>
>> On Mar 10, 2020, at 11:28 AM, Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us> wrote:
>>
>> Michelle and Kyra,

>>
>> This purchase request is for equipment to allow Mass Port Sierra Wireless modems to communicate directly with the existing ALPR Boss server in Chelsea. This is the fastest way to bring the Massport LPR cameras on line. EOTSS and EOPSS are OK with this solution as is Major Deb Ryan, the CO at Troop F.
>>
>> As you can see from the thread, this has been going on for some time. I think we can close it out with this small purchase.
>>
>> This does not resolve the replacement of the existing ALPR equipment that we discussed at Command Staff yesterday. That is a different issue.
>>
>> Thanks
>>
>>
>> Lieutenant Colonel Dermot J. Quinn #1765
>> Division Commander
>> Division of Homeland Security & Preparedness
>> Massachusetts State Police
>>
>>
>>
>>
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 10:52 AM
>> To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: FW: MassPort LPR Cameras
>>
>> Hi LTC.,
>>
>> Can we order this equipment for the MassPort project?
>>
>> Thanks, Brian
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Tuesday, March 10, 2020 10:26 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> This needs to go through MSP fiscal. They need to enter the purchase in OPAS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 08:06
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Subject: RE: MassPort LPR Cameras
>>
>> Is this something you can order or does it need to go through MSP?

>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Monday, March 9, 2020 10:36 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks, Brian...I will check with TSS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Monday, March 9, 2020 10:29
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks Jim,
>>
>> I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need [redacted] wireless AC adapters and [redacted] I have reached out to BCM for a quote.
>>
>> I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.
>>
>> I plan to cut one sector ([redacted]) over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?
>>
>> -Brian
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Friday, March 6, 2020 1:43 PM
>> To: Egnitz, Brian (POL)
>> Cc: Quinn, Dermot (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.
>>
>> So, assuming you move forward with this, who would actually make this happen?
>>
>> Thanks.
>>
>> Jim
>>
>> -----Original Message-----

>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Wednesday, March 4, 2020 17:53
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: Re: MassPort LPR Cameras
>>
>> Hi Jim,
>>
>> Regarding the Massport cameras; in the early days of AVL we installed [redacted] modem's in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don't we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn't have to do any firewall work either because they have a 166. and communicate like all of the MDT's . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.
>>
>> We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.
>>
>> Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.
>>
>>>> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>>>
>>> Thank you sir
>>>
>>> Major Charles W. Atchison III
>>> Troop F Commander
>>> Massachusetts State Police
>>> Director of Aviation Security
>>> 2 Service Road
>>> East Boston, Ma 02128
>>> Office: 617-568-7555
>>> Cell: 508-[redacted]
>>>
>>>
>>>> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT) <curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>>>
>>> All,
>>> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>>>
>>> Thanks
>>>
>>> CW
>>>
>>> From: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
>>> Sent: Monday, February 10, 2020 10:31 AM

>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
>>> Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
>>> Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
>>> Warmington, Scott (POL)
>>>
<Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
>>> .us>>; Peek, Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
>>> Michalski, Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>;
Mason,
>>> Christopher (POL)
>>> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
>>> Hughes, Sean M. (EOTSS)
>>> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis
(EOTSS)
>>> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
>>> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard
(POL)
>>> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
>>> Atchison, Charles (POL)
>>> <catchison@massport.com<mailto:catchison@massport.com>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Good Morning,
>>>
>>> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>>>
>>> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>>>
>>> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS

server located at DCJIS is a much better plan.
>>>
>>> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>>>
>>> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>>>
>>> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>>>
>>> I can't overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security's technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>>>
>>> Respectfully,
>>>
>>>
>>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
>>> of Homeland Security & Preparedness Massachusetts State Police
>>> <image006.png>
>>>
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
>>> Sent: Friday, January 17, 2020 1:10 PM
>>> To: Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
>>> Cc: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
>>> Guerriero, Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
Peek,
>>> Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
Peter
>>> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
>>> Maria (EPS)

>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>
>>> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>>>
>>> -Brian
>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> Sent: Monday, January 6, 2020 1:33 PM
>>> To: Slater, James (CHS)
>>> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
>>> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
>>> Crary
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>
>>> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>>>
>>> Thanks Brian
>>>
>>>
>>> From: John Tedona [mailto:jtedona@neology.net]
>>> Sent: Monday, December 9, 2019 4:55 PM
>>> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Slater, James (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Alex,
>>>
>>> I can be available most anytime tomorrow for a call.
>>>
>>>
>>> Regards,
>>>
>>> John Tedona
>>> PIPS TECHNOLOGY - A Neology Business
>>> Sales Manager
>>> 12760 Danielson Ct. Suite A
>>> Poway, CA 92064
>>> Phone: 201-841-6237
>>> Email: jtedona@neology.net<mailto:jtedona@neology.net>
>>> PIPS Support:
support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support

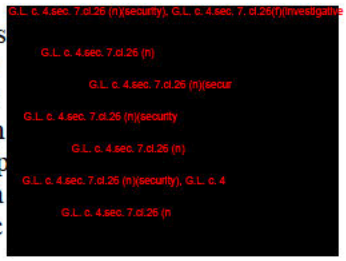
>>> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
>>>
-3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
>>>
EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
>>>
baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-
lyPhyJ
>>> U2sB_fmM6g&e=>
>>>
>>>
>>> From: Chute, Alexander
>>> <AChute@massport.com<mailto:AChute@massport.com>>
>>> Sent: Monday, December 9, 2019 4:38 PM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>
>>> Cc: Guerriero, Robert (MASSIT)
>>> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
>>> Peek, Brian T. (EOTSS)
>>> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
>>> Slater III, James F (CHS)
>>> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> CAUTION: This email originated from outside of the organization. Do not
click links or open attachments unless you recognize the sender and know the
content is safe.
>>>
>>> Hello All,
>>>
>>> I just wanted to follow up with this request to see what the next steps for
this project are. I believe that we can make the connections to the EOPSS
network, but will want to work within your desired IP scheme and ensure that
there aren't any concerns around the network routing, security, etc. Let me
know if we can have a quick call to discuss the details.
>>>
>>> Respectfully,
>>>
>>> ~Alex
>>>
>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>>
>>> WARNING: This record may contain Sensitive Security Information that is
controlled under 49 CFR parts 15 and 1520. No part of this record may be
disclosed to persons without a "need to know", as defined in 49 CFR parts 15
and 1520, except with the written permission of the Administrator of the

Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Monday, November 18, 2019 3:26 PM
>>> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
>>> pcrary@neology.net<mailto:pcrary@neology.net>
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi John, Peter
>>>
>>> Any issues with moving Massports cameras to the Chelsea DB?
>>>
>>> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>>>
>>> The current app server
>>> <image008.png>
>>>
>>> Current DB server
>>>
>>> <image009.png>
>>> <image010.png>
>>>
>>> Our current reads by month for about [redacted]
>>>
>>> Year
>>>
>>> Month
>>>
>>> Day
>>>
>>> Month Name
>>>
>>> Reads Count
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 1
>>>
>>> November
>>>
>>>   495,113
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 2

>>>
>>> November
>>>
>>> 472,907
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 3
>>>
>>> November
>>>
>>> 384,409
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 4
>>>
>>> November
>>>
>>> 411,440
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 5
>>>
>>> November
>>>
>>> 434,085
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 6
>>>
>>> November
>>>
>>> 495,537
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 7
>>>
>>> November
>>>
>>> 444,123
>>>
>>> 2019
>>>

>>> 11
>>>
>>> 8
>>>
>>> November
>>>
>>> 542,492
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 9
>>>
>>> November
>>>
>>> 443,463
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 10
>>>
>>> November
>>>
>>> 389,514
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 11
>>>
>>> November
>>>
>>> 362,548
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 12
>>>
>>> November
>>>
>>> 236,539
>>>
>>>
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Wednesday, November 13, 2019 2:49 PM
>>> To: Egnitz, Brian (POL)
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)

>>> Subject: RE: MassPort LPR Cameras
>>>
>>> These stats are from the [redacted] we have in the system for this month:
>>>
>>> <image011.png>
>>>
>>> ~Alex
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Tuesday, November 12, 2019 5:28 PM
>>> To: Chute, Alexander
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Alex,
>>>
>>> Can you please provide the updated reads per day? Previously you were interested in sharing [redacted] at approximately 75,000 reads per day.
>>>
>>> Here is the [redacted] confi I mentioned.
>>>
>>> Set hos
>>> Set im
>>> Set nu
>>> Set Pin
>>> Set udp
>>> Set pin
>>> Set sec
>>>



>>> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
>>> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>>>
>>> -Brian
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Tuesday, November 12, 2019 2:08 PM
>>> To: Egnitz, Brian (POL)
>>> Subject: MassPort LPR Cameras
>>>
>>> Brian,
>>>
>>> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we

have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to approximately [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.
>>>
>>> Respectfully,
>>>
>>> ~Alex
>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>> <SierraQuoteForMassPort.pdf>

From: brian.egnitz@pol.state.ma.us
To: Ryan, Deborah (POL)
Subject: Re: MassPort LPR Cameras
Date: Tuesday, July 14, 2020 8:59:39 AM

Yes, it hasn't been scheduled

> On Jul 14, 2020, at 7:52 AM, Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us> wrote:
>
> Hi Brian,
>
> Where was it left off? Utilizing details for the road closure?

THIS EMAIL MAY CONTAIN INFORMATION FOR OFFICIAL USE ONLY AND LAW ENFORCEMENT SENSITIVE INFORMATION. This E-mail (including attachments) is covered by the Electronic Communications Privacy Act, 18 USC 2510-2521, is confidential and may be legally privileged. If you are not the intended recipient, you are hereby notified that any retention, dissemination, distribution, or copying of this communication is strictly prohibited and may be unlawful. Please reply to the sender that you have received the message in error and then delete the message and any attachments.

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Tuesday, July 14, 2020 7:29 AM
To: Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>
Subject: Re: MassPort LPR Cameras

Hi Maj.,

Are you aware of any movement on this? I'd like to finish the cutover of the remaining cameras.

Thanks, Brian

> On May 21, 2020, at 10:57 AM, Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us> wrote:
>
> Hi Brian,
>
> Could you give me a call at your convenience regarding the rest of the LPR cutovers.
>
> Thank you,

Major Ryan
781-281-5177

THIS EMAIL MAY CONTAIN INFORMATION FOR OFFICIAL USE ONLY AND LAW ENFORCEMENT SENSITIVE INFORMATION. This E-mail (including attachments) is covered by the Electronic Communications Privacy Act, 18 USC 2510-2521, is confidential and may be legally privileged. If you are not the intended recipient, you are hereby notified that any retention, dissemination, distribution, or copying of this communication is strictly prohibited and may be unlawful. Please reply to the sender that you have received the message in error and then delete the message and any attachments.

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Monday, May 18, 2020 4:58 PM
To: Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>
Cc: Crouse, David (POL) <david.crouse@pol.state.ma.us>
Subject: RE: MassPort LPR Cameras

Hi Major,

I have finished cutting over the LPR cameras that were accessible off the road. [redacted] cameras ([redacted] and needs inspection). [redacted] need lane closures. [redacted] and [redacted] I estimate needing 2-5 hours per site. Lt. Crouse has offered to assist in lane closures using unmarked vehicles, how would you like to proceeded in completing the cut over of the remaining sites.

Thanks, Brian

From: Ryan, Deborah (POL)
Sent: Wednesday, May 6, 2020 9:46 PM
To: Mason, Christopher (POL); Egnitz, Brian (POL)
Cc: Warmington, Scott (POL); Quinn, Dermot (POL); Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Warren, Rosemary (POL); Shaw, Harold; Ball, Richard (POL)
Subject: Re: MassPort LPR Cameras

Thank you Brian.

Major Deborah A. Ryan
Massachusetts State Police
Troop F Commander
485 Maple St

From: Mason, Christopher (POL) <Chris.Mason@pol.state.ma.us>
Sent: Wednesday, May 6, 2020 7:00 PM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Cc: Warmington, Scott (POL) <Scott.Warmington@pol.state.ma.us>; Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Small, Michelle (POL) <Michelle.E.Small@pol.state.ma.us>; Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>; Slater, James (CHS) <james.slater@mass.gov>; Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>; Shaw, Harold <HShaw@massport.com>; Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>; Ball, Richard (POL) <Richard.Ball@pol.state.ma.us>
Subject: Re: MassPort LPR Cameras

Thank you Brian. Great work grabbing this data.

Colonel Christopher Mason
Superintendent
Massachusetts State Police

> On May 6, 2020, at 6:57 PM, Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us> wrote:
>
> Hi Sirs,
>
> We have begun cutting over the MassPort LPR Cameras into the EOPSS BOSS LPR Server. Today, [redacted] G.L. c. 4.sec. 7.cl.26 (n)(security) at Airport Road arrivals were migrated and are now writing data to Chelsea. I will continue to cut the remaining cameras over in the next few days and weeks. I will advise when the project is complete.
>
> - Brian
>
> -----Original Message-----
> From: Warmington, Scott (POL)
> Sent: Tuesday, March 10, 2020 11:36 AM
> To: Quinn, Dermot (POL)
> Cc: Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Mason, Christopher (POL); Egnitz, Brian (POL); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL)
> Subject: Re: MassPort LPR Cameras
>
> What is the cost?
>
> Sent from my iPhone
>
>> On Mar 10, 2020, at 11:28 AM, Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us> wrote:
>>
>> Michelle and Kyra,

>>
>> This purchase request is for equipment to allow Mass Port Sierra Wireless modems to communicate directly with the existing ALPR Boss server in Chelsea. This is the fastest way to bring the Massport LPR cameras on line. EOTSS and EOPSS are OK with this solution as is Major Deb Ryan, the CO at Troop F.
>>
>> As you can see from the thread, this has been going on for some time. I think we can close it out with this small purchase.
>>
>> This does not resolve the replacement of the existing ALPR equipment that we discussed at Command Staff yesterday. That is a different issue.
>>
>> Thanks
>>
>>
>> Lieutenant Colonel Dermot J. Quinn #1765
>> Division Commander
>> Division of Homeland Security & Preparedness
>> Massachusetts State Police
>>
>>
>>
>>
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 10:52 AM
>> To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: FW: MassPort LPR Cameras
>>
>> Hi LTC.,
>>
>> Can we order this equipment for the MassPort project?
>>
>> Thanks, Brian
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Tuesday, March 10, 2020 10:26 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> This needs to go through MSP fiscal. They need to enter the purchase in OPAS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 08:06
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Subject: RE: MassPort LPR Cameras
>>
>> Is this something you can order or does it need to go through MSP?

>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Monday, March 9, 2020 10:36 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks, Brian...I will check with TSS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Monday, March 9, 2020 10:29
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks Jim,
>>
>> I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need [redacted] wireless AC adapters and [redacted] I have reached out to BCM for a quote.
>>
>> I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.
>>
>> I plan to cut one sector ([redacted]) over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?
>>
>> -Brian
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Friday, March 6, 2020 1:43 PM
>> To: Egnitz, Brian (POL)
>> Cc: Quinn, Dermot (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.
>>
>> So, assuming you move forward with this, who would actually make this happen?
>>
>> Thanks.
>>
>> Jim
>>
>> -----Original Message-----

>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Wednesday, March 4, 2020 17:53
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: Re: MassPort LPR Cameras
>>
>> Hi Jim,
>>
>> Regarding the Massport cameras; in the early days of AVL we installed [redacted] modem's in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don't we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn't have to do any firewall work either because they have a 166. and communicate like all of the MDT's . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.
>>
>> We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.
>>
>> Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.
>>
>>>> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>>>
>>> Thank you sir
>>>
>>> Major Charles W. Atchison III
>>> Troop F Commander
>>> Massachusetts State Police
>>> Director of Aviation Security
>>> 2 Service Road
>>> East Boston, Ma 02128
>>> Office: 617-568-7555
>>> Cell: 508-[redacted]
>>>
>>>
>>>> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT) <curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>>>
>>> All,
>>> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>>>
>>> Thanks
>>>
>>> CW
>>>
>>> From: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
>>> Sent: Monday, February 10, 2020 10:31 AM

>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
>>> Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
>>> Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
>>> Warmington, Scott (POL)
>>>
<Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
>>> .us>>; Peek, Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
>>> Michalski, Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>;
Mason,
>>> Christopher (POL)
>>> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
>>> Hughes, Sean M. (EOTSS)
>>> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis
(EOTSS)
>>> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
>>> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard
(POL)
>>> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
>>> Atchison, Charles (POL)
>>> <catchison@massport.com<mailto:catchison@massport.com>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Good Morning,
>>>
>>> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>>>
>>> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>>>
>>> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS

server located at DCJIS is a much better plan.
>>>
>>> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>>>
>>> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>>>
>>> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>>>
>>> I can't overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security's technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>>>
>>> Respectfully,
>>>
>>>
>>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
>>> of Homeland Security & Preparedness Massachusetts State Police
>>> <image006.png>
>>>
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
>>> Sent: Friday, January 17, 2020 1:10 PM
>>> To: Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
>>> Cc: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
>>> Guerriero, Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
Peek,
>>> Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
Peter
>>> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
>>> Maria (EPS)

>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>
>>> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>>>
>>> -Brian
>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> Sent: Monday, January 6, 2020 1:33 PM
>>> To: Slater, James (CHS)
>>> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
>>> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
>>> Crary
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>
>>> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>>>
>>> Thanks Brian
>>>
>>>
>>> From: John Tedona [mailto:jtedona@neology.net]
>>> Sent: Monday, December 9, 2019 4:55 PM
>>> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Slater, James (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Alex,
>>>
>>> I can be available most anytime tomorrow for a call.
>>>
>>>
>>> Regards,
>>>
>>> John Tedona
>>> PIPS TECHNOLOGY - A Neology Business
>>> Sales Manager
>>> 12760 Danielson Ct. Suite A
>>> Poway, CA 92064
>>> Phone: 201-841-6237
>>> Email: jtedona@neology.net<mailto:jtedona@neology.net>
>>> PIPS Support:
support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support

>>> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
>>>
-3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
>>>
EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
>>>
baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-
lyPhyJ
>>> U2sB_fmM6g&e=>
>>>
>>>
>>> From: Chute, Alexander
>>> <AChute@massport.com<mailto:AChute@massport.com>>
>>> Sent: Monday, December 9, 2019 4:38 PM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>
>>> Cc: Guerriero, Robert (MASSIT)
>>> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
>>> Peek, Brian T. (EOTSS)
>>> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
>>> Slater III, James F (CHS)
>>> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> CAUTION: This email originated from outside of the organization. Do not
click links or open attachments unless you recognize the sender and know the
content is safe.
>>>
>>> Hello All,
>>>
>>> I just wanted to follow up with this request to see what the next steps for
this project are. I believe that we can make the connections to the EOPSS
network, but will want to work within your desired IP scheme and ensure that
there aren't any concerns around the network routing, security, etc. Let me
know if we can have a quick call to discuss the details.
>>>
>>> Respectfully,
>>>
>>> ~Alex
>>>
>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>>
>>> WARNING: This record may contain Sensitive Security Information that is
controlled under 49 CFR parts 15 and 1520. No part of this record may be
disclosed to persons without a "need to know", as defined in 49 CFR parts 15
and 1520, except with the written permission of the Administrator of the

Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Monday, November 18, 2019 3:26 PM
>>> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
>>> pcrary@neology.net<mailto:pcrary@neology.net>
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi John, Peter
>>>
>>> Any issues with moving Massports cameras to the Chelsea DB?
>>>
>>> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>>>
>>> The current app server
>>> <image008.png>
>>>
>>> Current DB server
>>>
>>> <image009.png>
>>> <image010.png>
>>>
>>> Our current reads by month for about [redacted]
>>>
>>> Year
>>>
>>> Month
>>>
>>> Day
>>>
>>> Month Name
>>>
>>> Reads Count
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 1
>>>
>>> November
>>>
>>>   495,113
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 2

>>>
>>> November
>>>
>>> 472,907
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 3
>>>
>>> November
>>>
>>> 384,409
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 4
>>>
>>> November
>>>
>>> 411,440
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 5
>>>
>>> November
>>>
>>> 434,085
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 6
>>>
>>> November
>>>
>>> 495,537
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 7
>>>
>>> November
>>>
>>> 444,123
>>>
>>> 2019
>>>

>>> 11
>>>
>>> 8
>>>
>>> November
>>>
>>> 542,492
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 9
>>>
>>> November
>>>
>>> 443,463
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 10
>>>
>>> November
>>>
>>> 389,514
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 11
>>>
>>> November
>>>
>>> 362,548
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 12
>>>
>>> November
>>>
>>> 236,539
>>>
>>>
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Wednesday, November 13, 2019 2:49 PM
>>> To: Egnitz, Brian (POL)
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)

>>> Subject: RE: MassPort LPR Cameras
>>>
>>> These stats are from the [redacted] we have in the system for this month:
>>>
>>> <image011.png>
>>>
>>> ~Alex
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Tuesday, November 12, 2019 5:28 PM
>>> To: Chute, Alexander
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Alex,
>>>
>>> Can you please provide the updated reads per day? Previously you were interested in sharing [redacted] at approximately 75,000 reads per day.
>>>
>>> Here is the [redacted] confi I mentioned.
>>>
>>> Set host
>>> Set ima
>>> Set num
>>> Set Ping
>>> Set udp
>>> Set ping
>>> Set secu
>>>
>>> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
>>> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>>>
>>> -Brian
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Tuesday, November 12, 2019 2:08 PM
>>> To: Egnitz, Brian (POL)
>>> Subject: MassPort LPR Cameras
>>>
>>> Brian,
>>>
>>> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we

have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to approximately [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.
>>>
>>> Respectfully,
>>>
>>> ~Alex
>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>> <SierraQuoteForMassPort.pdf>

From: Ryan, Deborah (POL)
To: Egnitz, Brian (POL)
Subject: Re: MassPort LPR Cameras
Date: Tuesday, July 14, 2020 7:52:18 AM

Hi Brian,

Where was it left off? Utilizing details for the road closure?

THIS EMAIL MAY CONTAIN INFORMATION FOR OFFICIAL USE ONLY AND LAW ENFORCEMENT SENSITIVE INFORMATION. This E-mail (including attachments) is covered by the Electronic Communications Privacy Act, 18 USC 2510-2521, is confidential and may be legally privileged. If you are not the intended recipient, you are hereby notified that any retention, dissemination, distribution, or copying of this communication is strictly prohibited and may be unlawful. Please reply to the sender that you have received the message in error and then delete the message and any attachments.

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Tuesday, July 14, 2020 7:29 AM
To: Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>
Subject: Re: MassPort LPR Cameras

Hi Maj.,

Are you aware of any movement on this? I'd like to finish the cutover of the remaining cameras.

Thanks, Brian

> On May 21, 2020, at 10:57 AM, Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us> wrote:
>
> Hi Brian,
>
> Could you give me a call at your convenience regarding the rest of the LPR cutovers.
>
> Thank you,
>
> Major Ryan
> 781-281-5177
>
> THIS EMAIL MAY CONTAIN INFORMATION FOR OFFICIAL USE ONLY AND LAW ENFORCEMENT SENSITIVE INFORMATION. This E-mail (including attachments) is covered by the Electronic Communications Privacy Act, 18 USC 2510-2521, is confidential and may be legally privileged. If you are not the intended recipient, you are hereby notified that any retention, dissemination,

distribution, or copying of this communication is strictly prohibited and may be unlawful. Please reply to the sender that you have received the message in error and then delete the message and any attachments.

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Monday, May 18, 2020 4:58 PM
To: Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>
Cc: Crouse, David (POL) <david.crouse@pol.state.ma.us>
Subject: RE: MassPort LPR Cameras

Hi Major,

I have finished cutting over the LPR cameras that were accessible off the road. [redacted] cameras ([redacted] G.L. c. 4.sec. 7.cl.26 (n)(security) and needs inspection). G.L. c. 4.sec. 7.cl.26 (n)(security) need lane closures. G.L. c. 4.sec. 7.cl.26 (n)(security) [redacted] and G.L. c. 4.sec. 7.cl.26 (n)(security) I estimate needing 2-5 hours per site. Lt. Crouse has offered to assist in lane closures using unmarked vehicles, how would you like to proceeded in completing the cut over of the remaining sites.

Thanks, Brian

From: Ryan, Deborah (POL)
Sent: Wednesday, May 6, 2020 9:46 PM
To: Mason, Christopher (POL); Egnitz, Brian (POL)
Cc: Warmington, Scott (POL); Quinn, Dermot (POL); Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Warren, Rosemary (POL); Shaw, Harold; Ball, Richard (POL)
Subject: Re: MassPort LPR Cameras

Thank you Brian.

Major Deborah A. Ryan
Massachusetts State Police
Troop F Commander
485 Maple St

From: Mason, Christopher (POL) <Chris.Mason@pol.state.ma.us>
Sent: Wednesday, May 6, 2020 7:00 PM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Cc: Warmington, Scott (POL) <Scott.Warmington@pol.state.ma.us>; Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Small, Michelle (POL) <Michelle.E.Small@pol.state.ma.us>; Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>;

Slater, James (CHS) <james.slater@mass.gov>; Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>; Shaw, Harold <HShaw@massport.com>; Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>; Ball, Richard (POL) <Richard.Ball@pol.state.ma.us>
Subject: Re: MassPort LPR Cameras

Thank you Brian. Great work grabbing this data.

Colonel Christopher Mason
Superintendent
Massachusetts State Police

> On May 6, 2020, at 6:57 PM, Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us> wrote:
>
> Hi Sirs,
>
> We have begun cutting over the MassPort LPR Cameras into the EOPSS BOSS LPR Server. Today, [redacted] at Airport Road arrivals were migrated and are now writing data to Chelsea. I will continue to cut the remaining cameras over in the next few days and weeks. I will advise when the project is complete.
>
> - Brian
>
> -----Original Message-----
> From: Warmington, Scott (POL)
> Sent: Tuesday, March 10, 2020 11:36 AM
> To: Quinn, Dermot (POL)
> Cc: Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Mason, Christopher (POL); Egnitz, Brian (POL); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL)
> Subject: Re: MassPort LPR Cameras
>
> What is the cost?
>
> Sent from my iPhone
>
>> On Mar 10, 2020, at 11:28 AM, Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us> wrote:
>>
>> Michelle and Kyra,
>>
>> This purchase request is for equipment to allow Mass Port Sierra Wireless modems to communicate directly with the existing ALPR Boss server in Chelsea. This is the fastest way to bring the Massport LPR cameras on line. EOTSS and EOPSS are OK with this solution as is Major Deb Ryan, the CO at Troop F.
>>

>> As you can see from the thread, this has been going on for some time. I think we can close it out with this small purchase.
>>
>> This does not resolve the replacement of the existing ALPR equipment that we discussed at Command Staff yesterday. That is a different issue.
>>
>> Thanks
>>
>>
>> Lieutenant Colonel Dermot J. Quinn #1765
>> Division Commander
>> Division of Homeland Security & Preparedness
>> Massachusetts State Police
>>
>>
>>
>>
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 10:52 AM
>> To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: FW: MassPort LPR Cameras
>>
>> Hi LTC.,
>>
>> Can we order this equipment for the MassPort project?
>>
>> Thanks, Brian
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Tuesday, March 10, 2020 10:26 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> This needs to go through MSP fiscal. They need to enter the purchase in OPAS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 08:06
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Subject: RE: MassPort LPR Cameras
>>
>> Is this something you can order or does it need to go through MSP?
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Monday, March 9, 2020 10:36 AM

>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks, Brian...I will check with TSS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Monday, March 9, 2020 10:29
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks Jim,
>>
>> I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need [redacted] wireless AC adapters and [redacted] I have reached out to BCM for a quote.
>>
>> I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.
>>
>> I plan to cut one sector ([redacted]) over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?
>>
>> -Brian
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Friday, March 6, 2020 1:43 PM
>> To: Egnitz, Brian (POL)
>> Cc: Quinn, Dermot (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.
>>
>> So, assuming you move forward with this, who would actually make this happen?
>>
>> Thanks.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Wednesday, March 4, 2020 17:53
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>

>> Subject: Re: MassPort LPR Cameras
>>
>> Hi Jim,
>>
>> Regarding the Massport cameras; in the early days of AVL we installed [redacted] modem‘s in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don’t we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn’t have to do any firewall work either because they have a 166. and communicate like all of the MDT‘s . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.
>>
>> We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.
>>
>> Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.
>>
>>>> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>>>
>>> Thank you sir
>>>
>>> Major Charles W. Atchison III
>>> Troop F Commander
>>> Massachusetts State Police
>>> Director of Aviation Security
>>> 2 Service Road
>>> East Boston, Ma 02128
>>> Office: 617-568-7555
>>> Cell: 508-[redacted]
>>>
>>>
>>>> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT) <curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>>>
>>> All,
>>> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>>>
>>> Thanks
>>>
>>> CW
>>>
>>> From: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
>>> Sent: Monday, February 10, 2020 10:31 AM
>>> To: Egnitz, Brian (POL)

>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
>>> Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
>>> Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
>>> Warmington, Scott (POL)
>>> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
>>> .us>>; Peek, Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
>>> Michalski, Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
>>> Christopher (POL)
>>> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
>>> Hughes, Sean M. (EOTSS)
>>> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
>>> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
>>> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
>>> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
>>> Atchison, Charles (POL)
>>> <catchison@massport.com<mailto:catchison@massport.com>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Good Morning,
>>>
>>> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>>>
>>> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>>>
>>> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>>>

>>> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>>>
>>> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>>>
>>> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>>>
>>> I can't overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security's technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>>>
>>> Respectfully,
>>>
>>>
>>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
>>> of Homeland Security & Preparedness Massachusetts State Police
>>> <image006.png>
>>>
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
>>> Sent: Friday, January 17, 2020 1:10 PM
>>> To: Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
>>> Cc: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
>>> Guerriero, Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
>>> Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
>>> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
>>> Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>

>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>
>>> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>>>
>>> -Brian
>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> Sent: Monday, January 6, 2020 1:33 PM
>>> To: Slater, James (CHS)
>>> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
>>> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
>>> Crary
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>
>>> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>>>
>>> Thanks Brian
>>>
>>>
>>> From: John Tedona [mailto:jtedona@neology.net]
>>> Sent: Monday, December 9, 2019 4:55 PM
>>> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Slater, James (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Alex,
>>>
>>> I can be available most anytime tomorrow for a call.
>>>
>>>
>>> Regards,
>>>
>>> John Tedona
>>> PIPS TECHNOLOGY - A Neology Business
>>> Sales Manager
>>> 12760 Danielson Ct. Suite A
>>> Poway, CA 92064
>>> Phone: 201-841-6237
>>> Email: jtedona@neology.net<mailto:jtedona@neology.net>
>>> PIPS Support:

support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
>>> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
>>>
-3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
>>>
EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
>>>
baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ
>>> U2sB_fmM6g&e=>
>>>
>>>
>>> From: Chute, Alexander
>>> <AChute@massport.com<mailto:AChute@massport.com>>
>>> Sent: Monday, December 9, 2019 4:38 PM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>
>>> Cc: Guerriero, Robert (MASSIT)
>>> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
>>> Peek, Brian T. (EOTSS)
>>> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
>>> Slater III, James F (CHS)
>>> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>>>
>>> Hello All,
>>>
>>> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>>>
>>> Respectfully,
>>>
>>> ~Alex
>>>
>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>

>>>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Monday, November 18, 2019 3:26 PM
>>> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
>>> pcrary@neology.net<mailto:pcrary@neology.net>
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi John, Peter
>>>
>>> Any issues with moving Massports cameras to the Chelsea DB?
>>>
>>> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>>>
>>> The current app server
>>> <image008.png>
>>>
>>> Current DB server
>>>
>>> <image009.png>
>>> <image010.png>
>>>
>>> Our current reads by month for about [redacted]
>>>
>>> Year
>>>
>>> Month
>>>
>>> Day
>>>
>>> Month Name
>>>
>>> Reads Count
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 1
>>>
>>> November
>>>

>>> 495,113
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 2
>>>
>>> November
>>>
>>> 472,907
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 3
>>>
>>> November
>>>
>>> 384,409
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 4
>>>
>>> November
>>>
>>> 411,440
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 5
>>>
>>> November
>>>
>>> 434,085
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 6
>>>
>>> November
>>>
>>> 495,537
>>>
>>> 2019

>>>
>>> 11
>>>
>>> 7
>>>
>>> November
>>>
>>> 444,123
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 8
>>>
>>> November
>>>
>>> 542,492
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 9
>>>
>>> November
>>>
>>> 443,463
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 10
>>>
>>> November
>>>
>>> 389,514
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 11
>>>
>>> November
>>>
>>> 362,548
>>>
>>> 2019
>>>
>>> 11
>>>

>>> 12
>>>
>>> November
>>>
>>> 236,539
>>>
>>>
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Wednesday, November 13, 2019 2:49 PM
>>> To: Egnitz, Brian (POL)
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> These stats are from the [redacted] we have in the system for this month:
>>>
>>> <image011.png>
>>>
>>> ~Alex
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Tuesday, November 12, 2019 5:28 PM
>>> To: Chute, Alexander
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Alex,
>>>
>>> Can you please provide the updated reads per day? Previously you were interested in sharing [redacted] at approximately 75,000 reads per day.
>>>
>>> Here is the [redacted] confi I mentioned.
>>>
>>> Set host to boss [redacted]
>>> Set image [redacted]
>>> Set number of [redacted]
>>> Set Ping [redacted]
>>> Set udp ping [redacted]
>>> Set ping [redacted]
>>> Set security [redacted]
>>>
>>> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
>>> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>>>
>>> -Brian
>>>

>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Tuesday, November 12, 2019 2:08 PM
>>> To: Egnitz, Brian (POL)
>>> Subject: MassPort LPR Cameras
>>>
>>> Brian,
>>>
>>> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to approximately [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.
>>>
>>> Respectfully,
>>>
>>> ~Alex
>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>> <SierraQuoteForMassPort.pdf>

From: Egnitz, Brian (POL)
To: Ryan, Deborah (POL)
Subject: Re: MassPort LPR Cameras
Date: Tuesday, July 14, 2020 7:29:46 AM

Hi Maj.,

Are you aware of any movement on this? I'd like to finish the cutover of the remaining cameras.

Thanks, Brian

> On May 21, 2020, at 10:57 AM, Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us> wrote:
>
> Hi Brian,
>
> Could you give me a call at your convenience regarding the rest of the LPR cutovers.
>
> Thank you,
>
> Major Ryan
> 781-281-5177
>
> THIS EMAIL MAY CONTAIN INFORMATION FOR OFFICIAL USE ONLY AND LAW ENFORCEMENT SENSITIVE INFORMATION. This E-mail (including attachments) is covered by the Electronic Communications Privacy Act, 18 USC 2510-2521, is confidential and may be legally privileged. If you are not the intended recipient, you are hereby notified that any retention, dissemination, distribution, or copying of this communication is strictly prohibited and may be unlawful. Please reply to the sender that you have received the message in error and then delete the message and any attachments.

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Monday, May 18, 2020 4:58 PM
To: Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>
Cc: Crouse, David (POL) <david.crouse@pol.state.ma.us>
Subject: RE: MassPort LPR Cameras

Hi Major,

I have finished cutting over the LPR cameras that were accessible off the road. G.L. [redacted] cameras (G.L. c. 4.sec. 7.cl.26 (n)(security) and needs inspection). G.L. c. 4.sec. 7.cl.26 (n)(security) need lane closures. Site 1 is on the upper level

departures near terminal A and G.L. c. 4.sec. 7.cl.26 (n)(security) I estimate needing 2-5 hours per site. Lt. Crouse has offered to assist in lane closures using unmarked vehicles, how would you like to proceeded in completing the cut over of the remaining sites.

Thanks, Brian

From: Ryan, Deborah (POL)
Sent: Wednesday, May 6, 2020 9:46 PM
To: Mason, Christopher (POL); Egnitz, Brian (POL)
Cc: Warmington, Scott (POL); Quinn, Dermot (POL); Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Warren, Rosemary (POL); Shaw, Harold; Ball, Richard (POL)
Subject: Re: MassPort LPR Cameras

Thank you Brian.

Major Deborah A. Ryan
Massachusetts State Police
Troop F Commander
485 Maple St

From: Mason, Christopher (POL) <Chris.Mason@pol.state.ma.us>
Sent: Wednesday, May 6, 2020 7:00 PM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Cc: Warmington, Scott (POL) <Scott.Warmington@pol.state.ma.us>; Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Small, Michelle (POL) <Michelle.E.Small@pol.state.ma.us>; Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>; Slater, James (CHS) <james.slater@mass.gov>; Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>; Shaw, Harold <HShaw@massport.com>; Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>; Ball, Richard (POL) <Richard.Ball@pol.state.ma.us>
Subject: Re: MassPort LPR Cameras

Thank you Brian. Great work grabbing this data.

Colonel Christopher Mason
Superintendent
Massachusetts State Police

> On May 6, 2020, at 6:57 PM, Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>

wrote:
>
> Hi Sirs,
>
> We have begun cutting over the MassPort LPR Cameras into the EOPSS BOSS LPR Server. Today, [redacted] at Airport Road arrivals were migrated and are now writing data to Chelsea. I will continue to cut the remaining cameras over in the next few days and weeks. I will advise when the project is complete.
>
> - Brian
>
> -----Original Message-----
> From: Warmington, Scott (POL)
> Sent: Tuesday, March 10, 2020 11:36 AM
> To: Quinn, Dermot (POL)
> Cc: Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Mason, Christopher (POL); Egnitz, Brian (POL); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL)
> Subject: Re: MassPort LPR Cameras
>
> What is the cost?
>
> Sent from my iPhone
>
>> On Mar 10, 2020, at 11:28 AM, Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us> wrote:
>>
>> Michelle and Kyra,
>>
>> This purchase request is for equipment to allow Mass Port Sierra Wireless modems to communicate directly with the existing ALPR Boss server in Chelsea. This is the fastest way to bring the Massport LPR cameras on line. EOTSS and EOPSS are OK with this solution as is Major Deb Ryan, the CO at Troop F.
>>
>> As you can see from the thread, this has been going on for some time. I think we can close it out with this small purchase.
>>
>> This does not resolve the replacement of the existing ALPR equipment that we discussed at Command Staff yesterday. That is a different issue.
>>
>> Thanks
>>
>>
>> Lieutenant Colonel Dermot J. Quinn #1765
>> Division Commander
>> Division of Homeland Security & Preparedness
>> Massachusetts State Police
>>
>>
>>
>>
>>
>> -----Original Message-----

>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 10:52 AM
>> To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: FW: MassPort LPR Cameras
>>
>> Hi LTC.,
>>
>> Can we order this equipment for the MassPort project?
>>
>> Thanks, Brian
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Tuesday, March 10, 2020 10:26 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> This needs to go through MSP fiscal. They need to enter the purchase in OPAS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 08:06
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Subject: RE: MassPort LPR Cameras
>>
>> Is this something you can order or does it need to go through MSP?
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Monday, March 9, 2020 10:36 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks, Brian...I will check with TSS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Monday, March 9, 2020 10:29
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks Jim,
>>
>> I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need [redacted] wireless AC adapters and [redacted] I have reached out to BCM for a quote.

>>
>> I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.
>>
>> I plan to cut one sector ([redacted]) over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?
>>
>> -Brian
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Friday, March 6, 2020 1:43 PM
>> To: Egnitz, Brian (POL)
>> Cc: Quinn, Dermot (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.
>>
>> So, assuming you move forward with this, who would actually make this happen?
>>
>> Thanks.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Wednesday, March 4, 2020 17:53
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: Re: MassPort LPR Cameras
>>
>> Hi Jim,
>>
>> Regarding the Massport cameras; in the early days of AVL we installed [redacted] modem's in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don't we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn't have to do any firewall work either because they have a 166. and communicate like all of the MDT's . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.
>>
>> We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.

>>
>> Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.
>>
>>>> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>>>
>>> Thank you sir
>>>
>>> Major Charles W. Atchison III
>>> Troop F Commander
>>> Massachusetts State Police
>>> Director of Aviation Security
>>> 2 Service Road
>>> East Boston, Ma 02128
>>> Office: 617-568-7555
>>> Cell: 508-[redacted]
>>>
>>>
>>>> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT) <curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>>>
>>> All,
>>> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>>>
>>> Thanks
>>>
>>> CW
>>>
>>> From: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
>>> Sent: Monday, February 10, 2020 10:31 AM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
>>> Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
>>> Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
>>> Warmington, Scott (POL)
>>> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
>>> .us>>; Peek, Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
>>> Michalski, Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
>>> Christopher (POL)
>>> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
>>> Hughes, Sean M. (EOTSS)
>>> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary

>>> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
>>> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
>>> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
>>> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
>>> Atchison, Charles (POL)
>>> <catchison@massport.com<mailto:catchison@massport.com>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Good Morning,
>>>
>>> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>>>
>>> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>>>
>>> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>>>
>>> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>>>
>>> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>>>
>>> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>>>
>>> I can’t overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug

trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security's technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>>>
>>> Respectfully,
>>>
>>>
>>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
>>> of Homeland Security & Preparedness Massachusetts State Police
>>> <image006.png>
>>>
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
>>> Sent: Friday, January 17, 2020 1:10 PM
>>> To: Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
>>> Cc: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
>>> Guerriero, Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
>>> Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
>>> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
>>> Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>
>>> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>>>
>>> -Brian
>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> Sent: Monday, January 6, 2020 1:33 PM
>>> To: Slater, James (CHS)
>>> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
>>> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
>>> Crary
>>> Subject: RE: MassPort LPR Cameras
>>>

>>> Hi Jim,
>>>
>>> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>>>
>>> Thanks Brian
>>>
>>>
>>> From: John Tedona [mailto:jtedona@neology.net]
>>> Sent: Monday, December 9, 2019 4:55 PM
>>> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Slater, James (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Alex,
>>>
>>> I can be available most anytime tomorrow for a call.
>>>
>>>
>>> Regards,
>>>
>>> John Tedona
>>> PIPS TECHNOLOGY - A Neology Business
>>> Sales Manager
>>> 12760 Danielson Ct. Suite A
>>> Poway, CA 92064
>>> Phone: 201-841-6237
>>> Email: jtedona@neology.net<mailto:jtedona@neology.net>
>>> PIPS Support:
support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577,
Option 1 for sales, Option 2 for Support
>>> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
>>>
-3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
>>>
EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
>>>
baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-
lyPhyJ
>>> U2sB_fmM6g&e=>
>>>
>>>
>>> From: Chute, Alexander
>>> <AChute@massport.com<mailto:AChute@massport.com>>
>>> Sent: Monday, December 9, 2019 4:38 PM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary

>>> <pcrary@neology.net<mailto:pcrary@neology.net>>
>>> Cc: Guerriero, Robert (MASSIT)
>>> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
>>> Peek, Brian T. (EOTSS)
>>> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
>>> Slater III, James F (CHS)
>>> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>>>
>>> Hello All,
>>>
>>> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>>>
>>> Respectfully,
>>>
>>> ~Alex
>>>
>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Monday, November 18, 2019 3:26 PM
>>> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
>>> pcrary@neology.net<mailto:pcrary@neology.net>
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>

>>> Hi John, Peter
>>>
>>> Any issues with moving Massports cameras to the Chelsea DB?
>>>
>>> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>>>
>>> The current app server
>>> <image008.png>
>>>
>>> Current DB server
>>>
>>> <image009.png>
>>> <image010.png>
>>>
>>> Our current reads by month for about [redacted] G.L. c. 4,sec. 7,cl.26 (n)(security)
>>>
>>> Year
>>>
>>> Month
>>>
>>> Day
>>>
>>> Month Name
>>>
>>> Reads Count
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 1
>>>
>>> November
>>>
>>> 495,113
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 2
>>>
>>> November
>>>
>>> 472,907
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 3
>>>
>>> November

>>>
>>> 384,409
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 4
>>>
>>> November
>>>
>>> 411,440
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 5
>>>
>>> November
>>>
>>> 434,085
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 6
>>>
>>> November
>>>
>>> 495,537
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 7
>>>
>>> November
>>>
>>> 444,123
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 8
>>>
>>> November
>>>
>>> 542,492
>>>

>>> 2019
>>>
>>> 11
>>>
>>> 9
>>>
>>> November
>>>
>>> 443,463
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 10
>>>
>>> November
>>>
>>> 389,514
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 11
>>>
>>> November
>>>
>>> 362,548
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 12
>>>
>>> November
>>>
>>> 236,539
>>>
>>>
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Wednesday, November 13, 2019 2:49 PM
>>> To: Egnitz, Brian (POL)
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> These stats are from the [redacted] we have in the system for this month:
>>>

>>> <image011.png>
>>>
>>> ~Alex
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Tuesday, November 12, 2019 5:28 PM
>>> To: Chute, Alexander
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Alex,
>>>
>>> Can you please provide the updated reads per day? Previously you were interested in sharing [redacted] at approximately 75,000 reads per day.
>>>
>>> Here is the [redacted] confi I mentioned.
>>>
>>> Set host to boss [redacted]
>>> Set image [redacted]
>>> Set number of [redacted]
>>> Set Ping [redacted]
>>> Set udp ping [redacted]
>>> Set ping [redacted]
>>> Set security [redacted]
>>>
>>> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
>>> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>>>
>>> -Brian
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Tuesday, November 12, 2019 2:08 PM
>>> To: Egnitz, Brian (POL)
>>> Subject: MassPort LPR Cameras
>>>
>>> Brian,
>>>
>>> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to

approximately [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.
>>>
>>> Respectfully,
>>>
>>> ~Alex
>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>> <SierraQuoteForMassPort.pdf>

From: brian.egnitz@pol.state.ma.us
To: Ryan, Deborah (POL)
Subject: Re: MassPort LPR Cameras
Date: Tuesday, July 14, 2020 7:29:45 AM

Hi Maj.,

Are you aware of any movement on this? I'd like to finish the cutover of the remaining cameras.

Thanks, Brian

> On May 21, 2020, at 10:57 AM, Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us> wrote:
>
> Hi Brian,
>
> Could you give me a call at your convenience regarding the rest of the LPR cutovers.
>
> Thank you,
>
> Major Ryan
> 781-281-5177
>
> THIS EMAIL MAY CONTAIN INFORMATION FOR OFFICIAL USE ONLY AND LAW ENFORCEMENT SENSITIVE INFORMATION. This E-mail (including attachments) is covered by the Electronic Communications Privacy Act, 18 USC 2510-2521, is confidential and may be legally privileged. If you are not the intended recipient, you are hereby notified that any retention, dissemination, distribution, or copying of this communication is strictly prohibited and may be unlawful. Please reply to the sender that you have received the message in error and then delete the message and any attachments.

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Monday, May 18, 2020 4:58 PM
To: Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>
Cc: Crouse, David (POL) <david.crouse@pol.state.ma.us>
Subject: RE: MassPort LPR Cameras

Hi Major,

I have finished cutting over the LPR cameras that were accessible off the road. [redacted] cameras (G.L. c. 4.sec. 7.cl.26 (n)(security) and needs inspection). G.L. c. 4.sec. 7.cl.26 (n)(security) need lane closures. Site 1 is on the upper level

departures near terminal A and G.L. c. 4.sec. 7.cl.26 (n)(security) I estimate needing 2-5 hours per site. Lt. Crouse has offered to assist in lane closures using unmarked vehicles, how would you like to proceeded in completing the cut over of the remaining sites.

Thanks, Brian

From: Ryan, Deborah (POL)
Sent: Wednesday, May 6, 2020 9:46 PM
To: Mason, Christopher (POL); Egnitz, Brian (POL)
Cc: Warmington, Scott (POL); Quinn, Dermot (POL); Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Warren, Rosemary (POL); Shaw, Harold; Ball, Richard (POL)
Subject: Re: MassPort LPR Cameras

Thank you Brian.

Major Deborah A. Ryan
Massachusetts State Police
Troop F Commander
485 Maple St

From: Mason, Christopher (POL) <Chris.Mason@pol.state.ma.us>
Sent: Wednesday, May 6, 2020 7:00 PM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Cc: Warmington, Scott (POL) <Scott.Warmington@pol.state.ma.us>; Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Small, Michelle (POL) <Michelle.E.Small@pol.state.ma.us>; Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>; Slater, James (CHS) <james.slater@mass.gov>; Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>; Shaw, Harold <HShaw@massport.com>; Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>; Ball, Richard (POL) <Richard.Ball@pol.state.ma.us>
Subject: Re: MassPort LPR Cameras

Thank you Brian. Great work grabbing this data.

Colonel Christopher Mason
Superintendent
Massachusetts State Police

> On May 6, 2020, at 6:57 PM, Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>

wrote:
>
> Hi Sirs,
>
> We have begun cutting over the MassPort LPR Cameras into the EOPSS BOSS LPR Server. Today, [redacted] at Airport Road arrivals were migrated and are now writing data to Chelsea. I will continue to cut the remaining cameras over in the next few days and weeks. I will advise when the project is complete.
>
> - Brian
>
> -----Original Message-----
> From: Warmington, Scott (POL)
> Sent: Tuesday, March 10, 2020 11:36 AM
> To: Quinn, Dermot (POL)
> Cc: Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Mason, Christopher (POL); Egnitz, Brian (POL); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL)
> Subject: Re: MassPort LPR Cameras
>
> What is the cost?
>
> Sent from my iPhone
>
>> On Mar 10, 2020, at 11:28 AM, Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us> wrote:
>>
>> Michelle and Kyra,
>>
>> This purchase request is for equipment to allow Mass Port Sierra Wireless modems to communicate directly with the existing ALPR Boss server in Chelsea. This is the fastest way to bring the Massport LPR cameras on line. EOTSS and EOPSS are OK with this solution as is Major Deb Ryan, the CO at Troop F.
>>
>> As you can see from the thread, this has been going on for some time. I think we can close it out with this small purchase.
>>
>> This does not resolve the replacement of the existing ALPR equipment that we discussed at Command Staff yesterday. That is a different issue.
>>
>> Thanks
>>
>>
>> Lieutenant Colonel Dermot J. Quinn #1765
>> Division Commander
>> Division of Homeland Security & Preparedness
>> Massachusetts State Police
>>
>>
>>
>>
>>
>> -----Original Message-----

>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 10:52 AM
>> To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: FW: MassPort LPR Cameras
>>
>> Hi LTC.,
>>
>> Can we order this equipment for the MassPort project?
>>
>> Thanks, Brian
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Tuesday, March 10, 2020 10:26 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> This needs to go through MSP fiscal. They need to enter the purchase in OPAS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 08:06
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Subject: RE: MassPort LPR Cameras
>>
>> Is this something you can order or does it need to go through MSP?
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Monday, March 9, 2020 10:36 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks, Brian...I will check with TSS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Monday, March 9, 2020 10:29
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks Jim,
>>
>> I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need [redacted] wireless AC adapters and [redacted] I have reached out to BCM for a quote.

>>
>> I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.
>>
>> I plan to cut one sector ([redacted]) over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?
>>
>> -Brian
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Friday, March 6, 2020 1:43 PM
>> To: Egnitz, Brian (POL)
>> Cc: Quinn, Dermot (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.
>>
>> So, assuming you move forward with this, who would actually make this happen?
>>
>> Thanks.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Wednesday, March 4, 2020 17:53
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: Re: MassPort LPR Cameras
>>
>> Hi Jim,
>>
>> Regarding the Massport cameras; in the early days of AVL we installed [redacted] modem's in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don't we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn't have to do any firewall work either because they have a 166. and communicate like all of the MDT's . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.
>>
>> We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.

>>
>> Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.
>>
>>>> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>>>
>>> Thank you sir
>>>
>>> Major Charles W. Atchison III
>>> Troop F Commander
>>> Massachusetts State Police
>>> Director of Aviation Security
>>> 2 Service Road
>>> East Boston, Ma 02128
>>> Office: 617-568-7555
>>> Cell: 508-[redacted]
>>>
>>>
>>>> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT) <curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>>>
>>> All,
>>> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>>>
>>> Thanks
>>>
>>> CW
>>>
>>> From: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
>>> Sent: Monday, February 10, 2020 10:31 AM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
>>> Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
>>> Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
>>> Warmington, Scott (POL)
>>> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
>>> .us>>; Peek, Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
>>> Michalski, Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
>>> Christopher (POL)
>>> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
>>> Hughes, Sean M. (EOTSS)
>>> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary

>>> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
>>> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
>>> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
>>> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
>>> Atchison, Charles (POL)
>>> <catchison@massport.com<mailto:catchison@massport.com>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Good Morning,
>>>
>>> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>>>
>>> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>>>
>>> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>>>
>>> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>>>
>>> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>>>
>>> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>>>
>>> I can’t overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug

trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security's technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>>>
>>> Respectfully,
>>>
>>>
>>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
>>> of Homeland Security & Preparedness Massachusetts State Police
>>> <image006.png>
>>>
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
>>> Sent: Friday, January 17, 2020 1:10 PM
>>> To: Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
>>> Cc: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
>>> Guerriero, Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
>>> Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
>>> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
>>> Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>
>>> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>>>
>>> -Brian
>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> Sent: Monday, January 6, 2020 1:33 PM
>>> To: Slater, James (CHS)
>>> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
>>> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
>>> Crary
>>> Subject: RE: MassPort LPR Cameras
>>>

>>> Hi Jim,
>>>
>>> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>>>
>>> Thanks Brian
>>>
>>>
>>> From: John Tedona [mailto:jtedona@neology.net]
>>> Sent: Monday, December 9, 2019 4:55 PM
>>> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Slater, James (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Alex,
>>>
>>> I can be available most anytime tomorrow for a call.
>>>
>>>
>>> Regards,
>>>
>>> John Tedona
>>> PIPS TECHNOLOGY - A Neology Business
>>> Sales Manager
>>> 12760 Danielson Ct. Suite A
>>> Poway, CA 92064
>>> Phone: 201-841-6237
>>> Email: jtedona@neology.net<mailto:jtedona@neology.net>
>>> PIPS Support:
support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577,
Option 1 for sales, Option 2 for Support
>>> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
>>>
-3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
>>>
EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
>>>
baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-
lyPhyJ
>>> U2sB_fmM6g&e=>
>>>
>>>
>>> From: Chute, Alexander
>>> <AChute@massport.com<mailto:AChute@massport.com>>
>>> Sent: Monday, December 9, 2019 4:38 PM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary

>>> <pcrary@neology.net<mailto:pcrary@neology.net>>
>>> Cc: Guerriero, Robert (MASSIT)
>>> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
>>> Peek, Brian T. (EOTSS)
>>> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
>>> Slater III, James F (CHS)
>>> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>>>
>>> Hello All,
>>>
>>> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>>>
>>> Respectfully,
>>>
>>> ~Alex
>>>
>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Monday, November 18, 2019 3:26 PM
>>> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
>>> pcrary@neology.net<mailto:pcrary@neology.net>
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>

>>> Hi John, Peter
>>>
>>> Any issues with moving Massports cameras to the Chelsea DB?
>>>
>>> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>>>
>>> The current app server
>>> <image008.png>
>>>
>>> Current DB server
>>>
>>> <image009.png>
>>> <image010.png>
>>>
>>> Our current reads by month for about [redacted]
>>>
>>> Year
>>>
>>> Month
>>>
>>> Day
>>>
>>> Month Name
>>>
>>> Reads Count
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 1
>>>
>>> November
>>>
>>> 495,113
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 2
>>>
>>> November
>>>
>>> 472,907
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 3
>>>
>>> November

>>>
>>> 384,409
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 4
>>>
>>> November
>>>
>>> 411,440
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 5
>>>
>>> November
>>>
>>> 434,085
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 6
>>>
>>> November
>>>
>>> 495,537
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 7
>>>
>>> November
>>>
>>> 444,123
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 8
>>>
>>> November
>>>
>>> 542,492
>>>

>>> 2019
>>>
>>> 11
>>>
>>> 9
>>>
>>> November
>>>
>>> 443,463
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 10
>>>
>>> November
>>>
>>> 389,514
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 11
>>>
>>> November
>>>
>>> 362,548
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 12
>>>
>>> November
>>>
>>> 236,539
>>>
>>>
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Wednesday, November 13, 2019 2:49 PM
>>> To: Egnitz, Brian (POL)
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> These stats are from the G.L. c. 4.sec. 7.cl.26 (n)(security) we have in the system for this month:
>>>

>>> <image011.png>
>>>
>>> ~Alex
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Tuesday, November 12, 2019 5:28 PM
>>> To: Chute, Alexander
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Alex,
>>>
>>> Can you please provide the updated reads per day? Previously you were interested in sharing [redacted] at approximately 75,000 reads per day.
>>>
>>> Here is the [redacted] confi I mentioned.
>>>
>>> Set host to boss [redacted]
>>> Set image [redacted]
>>> Set number of [redacted]
>>> Set Ping [redacted]
>>> Set udp ping [redacted]
>>> Set ping [redacted]
>>> Set security [redacted]
>>>
>>> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
>>> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>>>
>>> -Brian
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Tuesday, November 12, 2019 2:08 PM
>>> To: Egnitz, Brian (POL)
>>> Subject: MassPort LPR Cameras
>>>
>>> Brian,
>>>
>>> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to

approximately G.L. c. 4.sec. 7.cl.26 (n)(security) within our campus over the next year. Let me know what you think the appropriate next steps would be.
>>>
>>> Respectfully,
>>>
>>> ~Alex
>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: G.L. c. 4.sec. 7.cl.26 (n)(security)
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>> <SierraQuoteForMassPort.pdf>

From: Ryan, Deborah (POL)
To: Egnitz, Brian (POL)
Subject: Re: MassPort LPR Cameras
Date: Thursday, May 21, 2020 10:57:37 AM

Hi Brian,

Could you give me a call at your convenience regarding the rest of the LPR cutovers.

Thank you,

Major Ryan
781-281-5177

THIS EMAIL MAY CONTAIN INFORMATION FOR OFFICIAL USE ONLY AND LAW ENFORCEMENT SENSITIVE INFORMATION. This E-mail (including attachments) is covered by the Electronic Communications Privacy Act, 18 USC 2510-2521, is confidential and may be legally privileged. If you are not the intended recipient, you are hereby notified that any retention, dissemination, distribution, or copying of this communication is strictly prohibited and may be unlawful. Please reply to the sender that you have received the message in error and then delete the message and any attachments.

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Monday, May 18, 2020 4:58 PM
To: Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>
Cc: Crouse, David (POL) <david.crouse@pol.state.ma.us>
Subject: RE: MassPort LPR Cameras

Hi Major,

I have finished cutting over the LPR cameras that were accessible off the road. [redacted] cameras ([redacted] and needs inspection). [redacted] need lane closures. [redacted] and [redacted] I estimate needing 2-5 hours per site. Lt. Crouse has offered to assist in lane closures using unmarked vehicles, how would you like to proceeded in completing the cut over of the remaining sites.

Thanks, Brian

From: Ryan, Deborah (POL)
Sent: Wednesday, May 6, 2020 9:46 PM
To: Mason, Christopher (POL); Egnitz, Brian (POL)
Cc: Warmington, Scott (POL); Quinn, Dermot (POL); Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Warren, Rosemary (POL); Shaw, Harold; Ball, Richard (POL)
Subject: Re: MassPort LPR Cameras

Thank you Brian.

Major Deborah A. Ryan
Massachusetts State Police
Troop F Commander
485 Maple St

From: Mason, Christopher (POL) <Chris.Mason@pol.state.ma.us>
Sent: Wednesday, May 6, 2020 7:00 PM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Cc: Warmington, Scott (POL) <Scott.Warmington@pol.state.ma.us>; Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Small, Michelle (POL) <Michelle.E.Small@pol.state.ma.us>; Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>; Slater, James (CHS) <james.slater@mass.gov>; Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>; Shaw, Harold <HShaw@massport.com>; Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>; Ball, Richard (POL) <Richard.Ball@pol.state.ma.us>
Subject: Re: MassPort LPR Cameras

Thank you Brian. Great work grabbing this data.

Colonel Christopher Mason
Superintendent
Massachusetts State Police

> On May 6, 2020, at 6:57 PM, Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us> wrote:
>
> Hi Sirs,
>
> We have begun cutting over the MassPort LPR Cameras into the EOPSS BOSS LPR Server. Today, G.L. c. 4.sec. 7.cl.26 (n)(security) at Airport Road arrivals were migrated and are now writing data to Chelsea. I will continue to cut the remaining cameras over in the next few days and weeks. I will advise when the project is complete.
>
> - Brian
>
> -----Original Message-----
> From: Warmington, Scott (POL)
> Sent: Tuesday, March 10, 2020 11:36 AM
> To: Quinn, Dermot (POL)
> Cc: Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Mason, Christopher (POL); Egnitz, Brian (POL); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL)
> Subject: Re: MassPort LPR Cameras
>

> What is the cost?
>
> Sent from my iPhone
>
>> On Mar 10, 2020, at 11:28 AM, Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us> wrote:
>>
>> Michelle and Kyra,
>>
>> This purchase request is for equipment to allow Mass Port Sierra Wireless modems to communicate directly with the existing ALPR Boss server in Chelsea. This is the fastest way to bring the Massport LPR cameras on line. EOTSS and EOPSS are OK with this solution as is Major Deb Ryan, the CO at Troop F.
>>
>> As you can see from the thread, this has been going on for some time. I think we can close it out with this small purchase.
>>
>> This does not resolve the replacement of the existing ALPR equipment that we discussed at Command Staff yesterday. That is a different issue.
>>
>> Thanks
>>
>>
>> Lieutenant Colonel Dermot J. Quinn #1765
>> Division Commander
>> Division of Homeland Security & Preparedness
>> Massachusetts State Police
>>
>>
>>
>>
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 10:52 AM
>> To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: FW: MassPort LPR Cameras
>>
>> Hi LTC.,
>>
>> Can we order this equipment for the MassPort project?
>>
>> Thanks, Brian
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Tuesday, March 10, 2020 10:26 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> This needs to go through MSP fiscal. They need to enter the purchase in OPAS.
>>

>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 08:06
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Subject: RE: MassPort LPR Cameras
>>
>> Is this something you can order or does it need to go through MSP?
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Monday, March 9, 2020 10:36 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks, Brian...I will check with TSS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Monday, March 9, 2020 10:29
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks Jim,
>>
>> I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need [redacted] wireless AC adapters and [redacted] I have reached out to BCM for a quote.
>>
>> I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.
>>
>> I plan to cut one sector ([redacted]) over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?
>>
>> -Brian
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Friday, March 6, 2020 1:43 PM
>> To: Egnitz, Brian (POL)
>> Cc: Quinn, Dermot (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.

>>
>> So, assuming you move forward with this, who would actually make this happen?
>>
>> Thanks.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Wednesday, March 4, 2020 17:53
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: Re: MassPort LPR Cameras
>>
>> Hi Jim,
>>
>> Regarding the Massport cameras; in the early days of AVL we installed G.L. c. 4.sec. 7.cl.26 (n)(security) modem's in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don't we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn't have to do any firewall work either because they have a 166. and communicate like all of the MDT's . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.
>>
>> We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.
>>
>> Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.
>>
>>>> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>>>
>>> Thank you sir
>>>
>>> Major Charles W. Atchison III
>>> Troop F Commander
>>> Massachusetts State Police
>>> Director of Aviation Security
>>> 2 Service Road
>>> East Boston, Ma 02128
>>> Office: 617-568-7555
>>> Cell: 508-[redacted]
>>>
>>>
>>>> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT) <curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>>>
>>> All,
>>> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.

>>>
>>> Thanks
>>>
>>> CW
>>>
>>> From: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
>>> Sent: Monday, February 10, 2020 10:31 AM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
>>> Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
>>> Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
>>> Warmington, Scott (POL)
>>> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
>>> .us>>; Peek, Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
>>> Michalski, Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
>>> Christopher (POL)
>>> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
>>> Hughes, Sean M. (EOTSS)
>>> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
>>> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
>>> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
>>> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
>>> Atchison, Charles (POL)
>>> <catchison@massport.com<mailto:catchison@massport.com>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Good Morning,
>>>
>>> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>>>
>>> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>>>
>>> Recently Massport has decided not to maintain its own ALPR BOSS database server. The

database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>>>
>>> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>>>
>>> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>>>
>>> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>>>
>>> I can’t overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security’s technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>>>
>>> Respectfully,
>>>
>>>
>>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
>>> of Homeland Security & Preparedness Massachusetts State Police
>>> <image006.png>
>>>
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
>>> Sent: Friday, January 17, 2020 1:10 PM
>>> To: Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
>>> Cc: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
>>> Guerriero, Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
>>> Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,

>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
>>> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
>>> Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>
>>> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>>>
>>> -Brian
>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> Sent: Monday, January 6, 2020 1:33 PM
>>> To: Slater, James (CHS)
>>> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
>>> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
>>> Crary
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>
>>> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>>>
>>> Thanks Brian
>>>
>>>
>>> From: John Tedona [mailto:jtedona@neology.net]
>>> Sent: Monday, December 9, 2019 4:55 PM
>>> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Slater, James (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Alex,
>>>
>>> I can be available most anytime tomorrow for a call.
>>>
>>>
>>> Regards,
>>>
>>> John Tedona
>>> PIPS TECHNOLOGY - A Neology Business
>>> Sales Manager
>>> 12760 Danielson Ct. Suite A
>>> Poway, CA 92064

>>> Phone: 201-841-6237
>>> Email: jtedona@neology.net<mailto:jtedona@neology.net>
>>> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
>>> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
>>> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
>>> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
>>> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ
>>> U2sB_fmM6g&e=>
>>>
>>>
>>> From: Chute, Alexander
>>> <AChute@massport.com<mailto:AChute@massport.com>>
>>> Sent: Monday, December 9, 2019 4:38 PM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>
>>> Cc: Guerriero, Robert (MASSIT)
>>> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
>>> Peek, Brian T. (EOTSS)
>>> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
>>> Slater III, James F (CHS)
>>> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>>>
>>> Hello All,
>>>
>>> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>>>
>>> Respectfully,
>>>
>>> ~Alex
>>>
>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted] c.L. c. 4,sec. 7 cl.26 (m)(security
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to

know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Monday, November 18, 2019 3:26 PM
>>> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
>>> pcrary@neology.net<mailto:pcrary@neology.net>
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi John, Peter
>>>
>>> Any issues with moving Massports cameras to the Chelsea DB?
>>>
>>> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>>>
>>> The current app server
>>> <image008.png>
>>>
>>> Current DB server
>>>
>>> <image009.png>
>>> <image010.png>
>>>
>>> Our current reads by month for about [redacted]
>>>
>>> Year
>>>
>>> Month
>>>
>>> Day
>>>
>>> Month Name
>>>
>>> Reads Count
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 1
>>>
>>> November
>>>
>>>   495,113
>>>
>>> 2019
>>>

>>> 11
>>>
>>> 2
>>>
>>> November
>>>
>>> 472,907
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 3
>>>
>>> November
>>>
>>> 384,409
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 4
>>>
>>> November
>>>
>>> 411,440
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 5
>>>
>>> November
>>>
>>> 434,085
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 6
>>>
>>> November
>>>
>>> 495,537
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 7

>>>
>>> November
>>>
>>> 444,123
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 8
>>>
>>> November
>>>
>>> 542,492
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 9
>>>
>>> November
>>>
>>> 443,463
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 10
>>>
>>> November
>>>
>>> 389,514
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 11
>>>
>>> November
>>>
>>> 362,548
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 12
>>>
>>> November
>>>

>>> 236,539
>>>
>>>
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Wednesday, November 13, 2019 2:49 PM
>>> To: Egnitz, Brian (POL)
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> These stats are from the [redacted] we have in the system for this month:
>>>
>>> <image011.png>
>>>
>>> ~Alex
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Tuesday, November 12, 2019 5:28 PM
>>> To: Chute, Alexander
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Alex,
>>>
>>> Can you please provide the updated reads per day? Previously you were interested in sharing [redacted] at approximately 75,000 reads per day.
>>>
>>> Here is the [redacted] confi I mentioned.
>>>
>>> Set host to boss [redacted]
>>> Set image [redacted]
>>> Set number of [redacted]
>>> Set Ping [redacted]
>>> Set udp ping [redacted]
>>> Set ping [redacted]
>>> Set security [redacted]
>>>
>>> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
>>> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>>>
>>> -Brian
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Tuesday, November 12, 2019 2:08 PM

>>> To: Egnitz, Brian (POL)
>>> Subject: MassPort LPR Cameras
>>>
>>> Brian,
>>>
>>> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to approximately [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.
>>>
>>> Respectfully,
>>>
>>> ~Alex
>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>> <SierraQuoteForMassPort.pdf>

From: Ryan, Deborah (POL)
To: Egnitz, Brian (POL)
Subject: Re: MassPort LPR Cameras
Date: Tuesday, May 19, 2020 2:14:02 PM

Hi Brian,

Any particular date or time you were thinking?

Major Deborah A. Ryan
Massachusetts State Police
Troop F Commander

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Monday, May 18, 2020 4:58 PM
To: Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>
Cc: Crouse, David (POL) <david.crouse@pol.state.ma.us>
Subject: RE: MassPort LPR Cameras

Hi Major,

I have finished cutting over the LPR cameras that were accessible off the road. G.L. c. 4.sec. 7.cl.26 (n)(security) cameras (G.L. c. 4.sec. 7.cl.26 (n)(security) and needs inspection). G.L. c. 4.sec. 7.cl.26 (n)(security) need lane closures. G.L. c. 4.sec. 7.cl.26 (n)(security) and G.L. c. 4.sec. 7.cl.26 (n)(security) I estimate needing 2-5 hours per site. Lt. Crouse has offered to assist in lane closures using unmarked vehicles, how would you like to proceeded in completing the cut over of the remaining sites.

Thanks, Brian

From: Ryan, Deborah (POL)
Sent: Wednesday, May 6, 2020 9:46 PM
To: Mason, Christopher (POL); Egnitz, Brian (POL)
Cc: Warmington, Scott (POL); Quinn, Dermot (POL); Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Warren, Rosemary (POL); Shaw, Harold; Ball, Richard (POL)
Subject: Re: MassPort LPR Cameras

Thank you Brian.

Major Deborah A. Ryan
Massachusetts State Police
Troop F Commander
485 Maple St

From: Mason, Christopher (POL) <Chris.Mason@pol.state.ma.us>
Sent: Wednesday, May 6, 2020 7:00 PM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Cc: Warmington, Scott (POL) <Scott.Warmington@pol.state.ma.us>; Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Small, Michelle (POL) <Michelle.E.Small@pol.state.ma.us>; Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>; Slater, James (CHS) <james.slater@mass.gov>; Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>; Shaw, Harold <HShaw@massport.com>; Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>; Ball, Richard (POL) <Richard.Ball@pol.state.ma.us>
Subject: Re: MassPort LPR Cameras

Thank you Brian. Great work grabbing this data.

Colonel Christopher Mason
Superintendent
Massachusetts State Police

> On May 6, 2020, at 6:57 PM, Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us> wrote:
>
> Hi Sirs,
>
> We have begun cutting over the MassPort LPR Cameras into the EOPSS BOSS LPR Server. Today, [redacted] at Airport Road arrivals were migrated and are now writing data to Chelsea. I will continue to cut the remaining cameras over in the next few days and weeks. I will advise when the project is complete.
>
> - Brian
>
> -----Original Message-----
> From: Warmington, Scott (POL)
> Sent: Tuesday, March 10, 2020 11:36 AM
> To: Quinn, Dermot (POL)
> Cc: Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Mason, Christopher (POL); Egnitz, Brian (POL); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL)
> Subject: Re: MassPort LPR Cameras
>
> What is the cost?
>
> Sent from my iPhone
>
>> On Mar 10, 2020, at 11:28 AM, Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us> wrote:
>>
>> Michelle and Kyra,
>>

>> This purchase request is for equipment to allow Mass Port Sierra Wireless modems to communicate directly with the existing ALPR Boss server in Chelsea. This is the fastest way to bring the Massport LPR cameras on line. EOTSS and EOPSS are OK with this solution as is Major Deb Ryan, the CO at Troop F.
>>
>> As you can see from the thread, this has been going on for some time. I think we can close it out with this small purchase.
>>
>> This does not resolve the replacement of the existing ALPR equipment that we discussed at Command Staff yesterday. That is a different issue.
>>
>> Thanks
>>
>>
>> Lieutenant Colonel Dermot J. Quinn #1765
>> Division Commander
>> Division of Homeland Security & Preparedness
>> Massachusetts State Police
>>
>>
>>
>>
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 10:52 AM
>> To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: FW: MassPort LPR Cameras
>>
>> Hi LTC.,
>>
>> Can we order this equipment for the MassPort project?
>>
>> Thanks, Brian
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Tuesday, March 10, 2020 10:26 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> This needs to go through MSP fiscal. They need to enter the purchase in OPAS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 08:06
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Subject: RE: MassPort LPR Cameras
>>

>> Is this something you can order or does it need to go through MSP?
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Monday, March 9, 2020 10:36 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks, Brian...I will check with TSS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Monday, March 9, 2020 10:29
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks Jim,
>>
>> I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need [redacted] wireless AC adapters and [redacted] I have reached out to BCM for a quote.
>>
>> I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.
>>
>> I plan to cut one sector ([redacted]) over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?
>>
>> -Brian
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Friday, March 6, 2020 1:43 PM
>> To: Egnitz, Brian (POL)
>> Cc: Quinn, Dermot (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.
>>
>> So, assuming you move forward with this, who would actually make this happen?
>>
>> Thanks.
>>
>> Jim
>>
>> -----Original Message-----

>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Wednesday, March 4, 2020 17:53
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: Re: MassPort LPR Cameras
>>
>> Hi Jim,
>>
>> Regarding the Massport cameras; in the early days of AVL we installed [redacted] modem's in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don't we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn't have to do any firewall work either because they have a 166. and communicate like all of the MDT's . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.
>>
>> We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.
>>
>> Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.
>>
>>>> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>>>
>>> Thank you sir
>>>
>>> Major Charles W. Atchison III
>>> Troop F Commander
>>> Massachusetts State Police
>>> Director of Aviation Security
>>> 2 Service Road
>>> East Boston, Ma 02128
>>> Office: 617-568-7555
>>> Cell: 508-[redacted]
>>>
>>>
>>>> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>>>
>>> All,
>>> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>>>
>>> Thanks
>>>
>>> CW
>>>
>>> From: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
>>> Sent: Monday, February 10, 2020 10:31 AM

>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
>>> Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
>>> Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
>>> Warmington, Scott (POL)
>>> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
>>> .us>>; Peek, Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
>>> Michalski, Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
>>> Christopher (POL)
>>> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
>>> Hughes, Sean M. (EOTSS)
>>> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
>>> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
>>> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
>>> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
>>> Atchison, Charles (POL)
>>> <catchison@massport.com<mailto:catchison@massport.com>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Good Morning,
>>>
>>> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>>>
>>> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>>>
>>> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>>>
>>> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for

hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>>>
>>> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>>>
>>> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>>>
>>> I can't overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security's technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>>>
>>> Respectfully,
>>>
>>>
>>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
>>> of Homeland Security & Preparedness Massachusetts State Police
>>> <image006.png>
>>>
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
>>> Sent: Friday, January 17, 2020 1:10 PM
>>> To: Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
>>> Cc: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
>>> Guerriero, Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
>>> Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
>>> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
>>> Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>

>>> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>>>
>>> -Brian
>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> Sent: Monday, January 6, 2020 1:33 PM
>>> To: Slater, James (CHS)
>>> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
>>> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
>>> Crary
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>
>>> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>>>
>>> Thanks Brian
>>>
>>>
>>> From: John Tedona [mailto:jtedona@neology.net]
>>> Sent: Monday, December 9, 2019 4:55 PM
>>> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Slater, James (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Alex,
>>>
>>> I can be available most anytime tomorrow for a call.
>>>
>>>
>>> Regards,
>>>
>>> John Tedona
>>> PIPS TECHNOLOGY - A Neology Business
>>> Sales Manager
>>> 12760 Danielson Ct. Suite A
>>> Poway, CA 92064
>>> Phone: 201-841-6237
>>> Email: jtedona@neology.net<mailto:jtedona@neology.net>
>>> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
>>> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
>>> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
>>> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
>>> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ

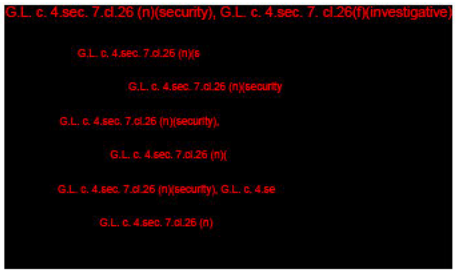
>>> U2sB_fmM6g&e=>
>>>
>>>
>>> From: Chute, Alexander
>>> <AChute@massport.com<mailto:AChute@massport.com>>
>>> Sent: Monday, December 9, 2019 4:38 PM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>
>>> Cc: Guerriero, Robert (MASSIT)
>>> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
>>> Peek, Brian T. (EOTSS)
>>> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
>>> Slater III, James F (CHS)
>>> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>>>
>>> Hello All,
>>>
>>> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>>>
>>> Respectfully,
>>>
>>> ~Alex
>>>
>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]

>>> Sent: Monday, November 18, 2019 3:26 PM
>>> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
>>> pcrary@neology.net<mailto:pcrary@neology.net>
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi John, Peter
>>>
>>> Any issues with moving Massports cameras to the Chelsea DB?
>>>
>>> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>>>
>>> The current app server
>>> <image008.png>
>>>
>>> Current DB server
>>>
>>> <image009.png>
>>> <image010.png>
>>>
>>> Our current reads by month for about [redacted]
>>>
>>> Year
>>>
>>> Month
>>>
>>> Day
>>>
>>> Month Name
>>>
>>> Reads Count
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 1
>>>
>>> November
>>>
>>> 495,113
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 2
>>>
>>> November
>>>
>>> 472,907
>>>

>>> 2019
>>>
>>> 11
>>>
>>> 3
>>>
>>> November
>>>
>>> 384,409
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 4
>>>
>>> November
>>>
>>> 411,440
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 5
>>>
>>> November
>>>
>>> 434,085
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 6
>>>
>>> November
>>>
>>> 495,537
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 7
>>>
>>> November
>>>
>>> 444,123
>>>
>>> 2019
>>>
>>> 11

>>>
>>> 8
>>>
>>> November
>>>
>>> 542,492
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 9
>>>
>>> November
>>>
>>> 443,463
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 10
>>>
>>> November
>>>
>>> 389,514
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 11
>>>
>>> November
>>>
>>> 362,548
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 12
>>>
>>> November
>>>
>>> 236,539
>>>
>>>
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Wednesday, November 13, 2019 2:49 PM

>>> To: Egnitz, Brian (POL)
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> These stats are from the [redacted] we have in the system for this month:
>>>
>>> <image011.png>
>>>
>>> ~Alex
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Tuesday, November 12, 2019 5:28 PM
>>> To: Chute, Alexander
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Alex,
>>>
>>> Can you please provide the updated reads per day? Previously you were interested in sharing [redacted] at approximately 75,000 reads per day.
>>>
>>> Here is the [redacted] confi I mentioned.
>>>
>>> Set
>>> Set
>>> Set
>>> Set
>>> Set
>>> Set
>>> Set
>>> Set
>>>



>>> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
>>> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>>>
>>> -Brian
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Tuesday, November 12, 2019 2:08 PM
>>> To: Egnitz, Brian (POL)
>>> Subject: MassPort LPR Cameras
>>>
>>> Brian,
>>>
>>> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well

as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to approximately [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.
>>>
>>> Respectfully,
>>>
>>> ~Alex
>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>> <SierraQuoteForMassPort.pdf>

From: Ryan, Deborah (POL)
To: Ryan, Deborah (POL)
Subject: Re: MassPort LPR Cameras
Date: Thursday, May 7, 2020 8:16:53 AM

From: Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>
Sent: Wednesday, May 6, 2020 9:46 PM
To: Mason, Christopher (POL) <Chris.Mason@pol.state.ma.us>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Cc: Warmington, Scott (POL) <Scott.Warmington@pol.state.ma.us>; Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Small, Michelle (POL) <Michelle.E.Small@pol.state.ma.us>; Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>; Slater, James (CHS) <james.slater@mass.gov>; Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>; Shaw, Harold <HShaw@massport.com>; Ball, Richard (POL) <Richard.Ball@pol.state.ma.us>
Subject: Re: MassPort LPR Cameras

Thank you Brian.

Major Deborah A. Ryan
Massachusetts State Police
Troop F Commander
485 Maple St

From: Mason, Christopher (POL) <Chris.Mason@pol.state.ma.us>
Sent: Wednesday, May 6, 2020 7:00 PM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Cc: Warmington, Scott (POL) <Scott.Warmington@pol.state.ma.us>; Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Small, Michelle (POL) <Michelle.E.Small@pol.state.ma.us>; Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>; Slater, James (CHS) <james.slater@mass.gov>; Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>; Shaw, Harold <HShaw@massport.com>; Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>; Ball, Richard (POL) <Richard.Ball@pol.state.ma.us>
Subject: Re: MassPort LPR Cameras

Thank you Brian. Great work grabbing this data.

Colonel Christopher Mason
Superintendent
Massachusetts State Police

> On May 6, 2020, at 6:57 PM, Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us> wrote:
>
> Hi Sirs,
>
> We have begun cutting over the MassPort LPR Cameras into the EOPSS BOSS LPR Server. Today, G.L. c. 4.sec. 7.cl.26 (n)(security) at Airport Road arrivals were migrated and are now writing data to Chelsea. I will continue to cut the remaining cameras over in the next few days and weeks. I will advise when the project is complete.
>
> - Brian
>
> -----Original Message-----
> From: Warmington, Scott (POL)
> Sent: Tuesday, March 10, 2020 11:36 AM
> To: Quinn, Dermot (POL)
> Cc: Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Mason, Christopher (POL); Egnitz, Brian (POL); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL)
> Subject: Re: MassPort LPR Cameras
>
> What is the cost?
>
> Sent from my iPhone
>
>> On Mar 10, 2020, at 11:28 AM, Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us> wrote:
>>
>> Michelle and Kyra,
>>
>> This purchase request is for equipment to allow Mass Port Sierra Wireless modems to communicate directly with the existing ALPR Boss server in Chelsea. This is the fastest way to bring the Massport LPR cameras on line. EOTSS and EOPSS are OK with this solution as is Major Deb Ryan, the CO at Troop F.
>>
>> As you can see from the thread, this has been going on for some time. I think we can close it out with this small purchase.
>>
>> This does not resolve the replacement of the existing ALPR equipment that we discussed at Command Staff yesterday. That is a different issue.
>>
>> Thanks
>>
>>
>> Lieutenant Colonel Dermot J. Quinn #1765
>> Division Commander
>> Division of Homeland Security & Preparedness
>> Massachusetts State Police
>>
>>
>>
>>
>>

>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 10:52 AM
>> To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: FW: MassPort LPR Cameras
>>
>> Hi LTC.,
>>
>> Can we order this equipment for the MassPort project?
>>
>> Thanks, Brian
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Tuesday, March 10, 2020 10:26 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> This needs to go through MSP fiscal. They need to enter the purchase in OPAS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 08:06
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Subject: RE: MassPort LPR Cameras
>>
>> Is this something you can order or does it need to go through MSP?
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Monday, March 9, 2020 10:36 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks, Brian...I will check with TSS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Monday, March 9, 2020 10:29
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks Jim,
>>
>> I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need [redacted] wireless AC adapters and [redacted]

I have reached out to BCM for a quote.
>>
>> I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.
>>
>> I plan to cut one sector ([redacted]) over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?
>>
>> -Brian
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Friday, March 6, 2020 1:43 PM
>> To: Egnitz, Brian (POL)
>> Cc: Quinn, Dermot (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.
>>
>> So, assuming you move forward with this, who would actually make this happen?
>>
>> Thanks.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Wednesday, March 4, 2020 17:53
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: Re: MassPort LPR Cameras
>>
>> Hi Jim,
>>
>> Regarding the Massport cameras; in the early days of AVL we installed [redacted] modem's in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don't we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn't have to do any firewall work either because they have a 166. and communicate like all of the MDT's . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.
>>
>> We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.
>>
>> Let me know what you think, Lieutenant Colonel Quinn and I could make the request to

Massport if needed.
>>
>>>> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>>>
>>> Thank you sir
>>>
>>> Major Charles W. Atchison III
>>> Troop F Commander
>>> Massachusetts State Police
>>> Director of Aviation Security
>>> 2 Service Road
>>> East Boston, Ma 02128
>>> Office: 617-568-7555
>>> Cell: 508-[redacted] G.L. c. 4,sec. 7,cl.26 (f)
>>>
>>>
>>>> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>>>
>>> All,
>>> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>>>
>>> Thanks
>>>
>>> CW
>>>
>>> From: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
>>> Sent: Monday, February 10, 2020 10:31 AM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
>>> Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
>>> Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
>>> Warmington, Scott (POL)
>>> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
>>> .us>>; Peek, Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
>>> Michalski, Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
>>> Christopher (POL)
>>> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
>>> Hughes, Sean M. (EOTSS)
>>> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
>>> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
>>> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)

>>> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
>>> Atchison, Charles (POL)
>>> <catchison@massport.com<mailto:catchison@massport.com>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Good Morning,
>>>
>>> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>>>
>>> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>>>
>>> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>>>
>>> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>>>
>>> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>>>
>>> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>>>
>>> I can’t overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security’s technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>>>
>>> Respectfully,
>>>

>>>
>>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
>>> of Homeland Security & Preparedness Massachusetts State Police
>>> <image006.png>
>>>
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
>>> Sent: Friday, January 17, 2020 1:10 PM
>>> To: Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
>>> Cc: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
>>> Guerriero, Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
>>> Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
>>> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
>>> Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>
>>> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>>>
>>> -Brian
>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> Sent: Monday, January 6, 2020 1:33 PM
>>> To: Slater, James (CHS)
>>> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
>>> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
>>> Crary
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>
>>> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>>>

>>> Thanks Brian
>>>
>>>
>>> From: John Tedona [mailto:jtedona@neology.net]
>>> Sent: Monday, December 9, 2019 4:55 PM
>>> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Slater, James (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Alex,
>>>
>>> I can be available most anytime tomorrow for a call.
>>>
>>>
>>> Regards,
>>>
>>> John Tedona
>>> PIPS TECHNOLOGY - A Neology Business
>>> Sales Manager
>>> 12760 Danielson Ct. Suite A
>>> Poway, CA 92064
>>> Phone: 201-841-6237
>>> Email: jtedona@neology.net<mailto:jtedona@neology.net>
>>> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-
7577, Option 1 for sales, Option 2 for Support
>>> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
>>> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
>>> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
>>> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ
>>> U2sB_fmM6g&e=>
>>>
>>>
>>> From: Chute, Alexander
>>> <AChute@massport.com<mailto:AChute@massport.com>>
>>> Sent: Monday, December 9, 2019 4:38 PM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>
>>> Cc: Guerriero, Robert (MASSIT)
>>> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
>>> Peek, Brian T. (EOTSS)
>>> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
>>> Slater III, James F (CHS)
>>> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> CAUTION: This email originated from outside of the organization. Do not click links or open
attachments unless you recognize the sender and know the content is safe.
>>>

>>> Hello All,
>>>
>>> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>>>
>>> Respectfully,
>>>
>>> ~Alex
>>>
>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: G.L. c. 4.sec. 7.cl.26 (n)(security)
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Monday, November 18, 2019 3:26 PM
>>> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
>>> pcrary@neology.net<mailto:pcrary@neology.net>
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi John, Peter
>>>
>>> Any issues with moving Massports cameras to the Chelsea DB?
>>>
>>> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>>>
>>> The current app server
>>> <image008.png>
>>>
>>> Current DB server
>>>
>>> <image009.png>
>>> <image010.png>
>>>
>>> Our current reads by month for about G.L. c. 4.sec. 7.cl.26 (n)(security)
>>>

>>> Year
>>>
>>> Month
>>>
>>> Day
>>>
>>> Month Name
>>>
>>> Reads Count
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 1
>>>
>>> November
>>>
>>> 495,113
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 2
>>>
>>> November
>>>
>>> 472,907
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 3
>>>
>>> November
>>>
>>> 384,409
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 4
>>>
>>> November
>>>
>>> 411,440
>>>
>>> 2019
>>>
>>> 11

>>>
>>> 5
>>>
>>> November
>>>
>>> 434,085
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 6
>>>
>>> November
>>>
>>> 495,537
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 7
>>>
>>> November
>>>
>>> 444,123
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 8
>>>
>>> November
>>>
>>> 542,492
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 9
>>>
>>> November
>>>
>>> 443,463
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 10
>>>

>>> November
>>>
>>> 389,514
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 11
>>>
>>> November
>>>
>>> 362,548
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 12
>>>
>>> November
>>>
>>> 236,539
>>>
>>>
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Wednesday, November 13, 2019 2:49 PM
>>> To: Egnitz, Brian (POL)
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> These stats are from the [redacted] we have in the system for this month:
>>>
>>> <image011.png>
>>>
>>> ~Alex
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Tuesday, November 12, 2019 5:28 PM
>>> To: Chute, Alexander
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Alex,
>>>
>>> Can you please provide the updated reads per day? Previously you were interested in sharing [redacted] at approximately 75,000 reads per day.

>>>
>>> Here is the [redacted] confi I mentioned.
>>>
>>> Set [redacted]
>>> Set
>>> Set
>>> Set
>>> Set
>>> Set
>>> Set
>>>
>>> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
>>> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>>>
>>> -Brian
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Tuesday, November 12, 2019 2:08 PM
>>> To: Egnitz, Brian (POL)
>>> Subject: MassPort LPR Cameras
>>>
>>> Brian,
>>>
>>> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to approximately [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.
>>>
>>> Respectfully,
>>>
>>> ~Alex
>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the

Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>> <SierraQuoteForMassPort.pdf>

From: Shaw, Harold
To: Egnitz, Brian (POL)
Cc: Ryan, Deborah A
Subject: Re: MassPort LPR Cameras
Date: Thursday, May 7, 2020 8:05:41 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Thanks Brian. Please let us know if you need anything from the MASSPORT side.

Hank

Harold H. Shaw
Chief Security Officer
Massachusetts Port Authority
617-568-3173 (w)
347-582-9976 (c)

> On May 6, 2020, at 6:57 PM, Egnitz, Brian (POL) <brian.egnitz@state.ma.us> wrote:
>
> Hi Sirs,
>
> We have begun cutting over the MassPort LPR Cameras into the EOPSS BOSS LPR Server. Today, [redacted] at Airport Road arrivals were migrated and are now writing data to Chelsea. I will continue to cut the remaining cameras over in the next few days and weeks. I will advise when the project is complete.
>
> - Brian
>
> -----Original Message-----
> From: Warmington, Scott (POL)
> Sent: Tuesday, March 10, 2020 11:36 AM
> To: Quinn, Dermot (POL)
> Cc: Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Mason, Christopher (POL); Egnitz, Brian (POL); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL)
> Subject: Re: MassPort LPR Cameras
>
> What is the cost?
>
> Sent from my iPhone
>
>> On Mar 10, 2020, at 11:28 AM, Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us> wrote:
>>
>> Michelle and Kyra,
>>
>> This purchase request is for equipment to allow Mass Port Sierra Wireless modems to communicate directly with the existing ALPR Boss server in Chelsea. This is the fastest way to bring the Massport LPR cameras on line. EOTSS and EOPSS are OK with this solution as is Major Deb Ryan, the CO at Troop F.
>>
>> As you can see from the thread, this has been going on for some time. I think we can close it out with this small purchase.
>>

>> This does not resolve the replacement of the existing ALPR equipment that we discussed at Command Staff yesterday. That is a different issue.
>>
>> Thanks
>>
>>
>> Lieutenant Colonel Dermot J. Quinn #1765
>> Division Commander
>> Division of Homeland Security & Preparedness
>> Massachusetts State Police
>>
>>
>>
>>
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 10:52 AM
>> To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: FW: MassPort LPR Cameras
>>
>> Hi LTC.,
>>
>> Can we order this equipment for the MassPort project?
>>
>> Thanks, Brian
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Tuesday, March 10, 2020 10:26 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> This needs to go through MSP fiscal. They need to enter the purchase in OPAS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 08:06
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Subject: RE: MassPort LPR Cameras
>>
>> Is this something you can order or does it need to go through MSP?
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Monday, March 9, 2020 10:36 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks, Brian...I will check with TSS.
>>
>> Jim
>>

>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Monday, March 9, 2020 10:29
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks Jim,
>>
>> I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need [G.L. c. 4.sec. 7.c] wireless AC adapters and [G.L. c. 4.sec. 7.cl.26 (n)(sec] I have reached out to BCM for a quote.
>>
>> I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.
>>
>> I plan to cut one sector ([G.L. c. 4.sec. 7.cl.26 (n)26 (n)(security)] over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?
>>
>> -Brian
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Friday, March 6, 2020 1:43 PM
>> To: Egnitz, Brian (POL)
>> Cc: Quinn, Dermot (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.
>>
>> So, assuming you move forward with this, who would actually make this happen?
>>
>> Thanks.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Wednesday, March 4, 2020 17:53
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: Re: MassPort LPR Cameras
>>
>> Hi Jim,
>>
>> Regarding the Massport cameras; in the early days of AVL we installed [G.L. c. 4.sec. 7.cl.26 (n)(security)] modem's in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don't we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn't have to do any firewall work either because they have a 166. and communicate like all of the MDT's . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them

back their data plans and modems.
>>
>> We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.
>>
>> Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.
>>
>>>> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>>>
>>> Thank you sir
>>>
>>> Major Charles W. Atchison III
>>> Troop F Commander
>>> Massachusetts State Police
>>> Director of Aviation Security
>>> 2 Service Road
>>> East Boston, Ma 02128
>>> Office: 617-568-7555
>>> Cell: 508-[redacted]
>>>
>>>
>>>> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>>>
>>> All,
>>> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>>>
>>> Thanks
>>>
>>> CW
>>>
>>> From: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
>>> Sent: Monday, February 10, 2020 10:31 AM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
>>> Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
>>> Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
>>> Warmington, Scott (POL)
>>> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
>>> .us>>; Peek, Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
>>> Michalski, Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
>>> Christopher (POL)
>>> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
>>> Hughes, Sean M. (EOTSS)
>>> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
>>> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
>>> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)

>>> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
>>> Atchison, Charles (POL)
>>> <catchison@massport.com<mailto:catchison@massport.com>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Good Morning,
>>>
>>> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>>>
>>> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>>>
>>> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>>>
>>> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>>>
>>> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>>>
>>> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>>>
>>> I can’t overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security’s technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>>>
>>> Respectfully,
>>>
>>>
>>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
>>> of Homeland Security & Preparedness Massachusetts State Police
>>> <image006.png>
>>>
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL)

>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
>>> Sent: Friday, January 17, 2020 1:10 PM
>>> To: Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
>>> Cc: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
>>> Guerriero, Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
>>> Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
>>> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
>>> Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>
>>> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>>>
>>> -Brian
>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> Sent: Monday, January 6, 2020 1:33 PM
>>> To: Slater, James (CHS)
>>> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
>>> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
>>> Crary
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>
>>> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>>>
>>> Thanks Brian
>>>
>>>
>>> From: John Tedona [mailto:jtedona@neology.net]
>>> Sent: Monday, December 9, 2019 4:55 PM
>>> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Slater, James (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Alex,
>>>
>>> I can be available most anytime tomorrow for a call.
>>>

>>>
>>> Regards,
>>>
>>> John Tedona
>>> PIPS TECHNOLOGY - A Neology Business
>>> Sales Manager
>>> 12760 Danielson Ct. Suite A
>>> Poway, CA 92064
>>> Phone: 201-841-6237
>>> Email: jtedona@neology.net<mailto:jtedona@neology.net>
>>> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
>>> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
>>> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
>>> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
>>> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ
>>> U2sB_fmM6g&e=>
>>>
>>>
>>> From: Chute, Alexander
>>> <AChute@massport.com<mailto:AChute@massport.com>>
>>> Sent: Monday, December 9, 2019 4:38 PM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>
>>> Cc: Guerriero, Robert (MASSIT)
>>> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
>>> Peek, Brian T. (EOTSS)
>>> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
>>> Slater III, James F (CHS)
>>> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>>>
>>> Hello All,
>>>
>>> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>>>
>>> Respectfully,
>>>
>>> ~Alex
>>>
>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942

>>> achute@massport.com<mailto:achute@massport.com>
>>>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Monday, November 18, 2019 3:26 PM
>>> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
>>> pcrary@neology.net<mailto:pcrary@neology.net>
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi John, Peter
>>>
>>> Any issues with moving Massports cameras to the Chelsea DB?
>>>
>>> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>>>
>>> The current app server
>>> <image008.png>
>>>
>>> Current DB server
>>>
>>> <image009.png>
>>> <image010.png>
>>>
>>> Our current reads by month for about [redacted]
>>>
>>> Year
>>>
>>> Month
>>>
>>> Day
>>>
>>> Month Name
>>>
>>> Reads Count
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 1
>>>
>>> November
>>>
>>>   495,113
>>>
>>> 2019
>>>
>>> 11

>>>
>>> 2
>>>
>>> November
>>>
>>> 472,907
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 3
>>>
>>> November
>>>
>>> 384,409
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 4
>>>
>>> November
>>>
>>> 411,440
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 5
>>>
>>> November
>>>
>>> 434,085
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 6
>>>
>>> November
>>>
>>> 495,537
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 7
>>>
>>> November
>>>
>>> 444,123
>>>

>>> 2019
>>>
>>> 11
>>>
>>> 8
>>>
>>> November
>>>
>>> 542,492
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 9
>>>
>>> November
>>>
>>> 443,463
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 10
>>>
>>> November
>>>
>>> 389,514
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 11
>>>
>>> November
>>>
>>> 362,548
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 12
>>>
>>> November
>>>
>>> 236,539
>>>
>>>
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Wednesday, November 13, 2019 2:49 PM
>>> To: Egnitz, Brian (POL)

>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> These stats are from the [redacted] we have in the system for this month:
>>>
>>> <image011.png>
>>>
>>> ~Alex
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Tuesday, November 12, 2019 5:28 PM
>>> To: Chute, Alexander
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Alex,
>>>
>>> Can you please provide the updated reads per day? Previously you were interested in sharing [redacted] at approximately 75,000 reads per day.
>>>
>>> Here is the [redacted] confi I mentioned.
>>>
>>> Set host to boss [redacted]
>>> Set image [redacted]
>>> Set number of [redacted]
>>> Set Ping [redacted]
>>> Set udp ping [redacted]
>>> Set ping [redacted]
>>> Set security [redacted]
>>>
>>> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
>>> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>>>
>>> -Brian
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Tuesday, November 12, 2019 2:08 PM
>>> To: Egnitz, Brian (POL)
>>> Subject: MassPort LPR Cameras
>>>
>>> Brian,
>>>
>>> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to approximately [redacted] within our campus over the

next year. Let me know what you think the appropriate next steps would be.
>>>
>>> Respectfully,
>>>
>>> ~Alex
>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>> <SierraQuoteForMassPort.pdf>

From:	Ryan, Deborah (POL)
To:	Mason, Christopher (POL); Egnitz, Brian (POL)
Cc:	Warmington, Scott (POL); Quinn, Dermot (POL); Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Warren, Rosemary (POL); Shaw, Harold; Ball, Richard (POL)
Subject:	Re: MassPort LPR Cameras
Date:	Wednesday, May 6, 2020 9:46:14 PM

Thank you Brian.

Major Deborah A. Ryan
Massachusetts State Police
Troop F Commander
485 Maple St

From: Mason, Christopher (POL) <Chris.Mason@pol.state.ma.us>
Sent: Wednesday, May 6, 2020 7:00 PM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Cc: Warmington, Scott (POL) <Scott.Warmington@pol.state.ma.us>; Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Small, Michelle (POL) <Michelle.E.Small@pol.state.ma.us>; Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>; Slater, James (CHS) <james.slater@mass.gov>; Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>; Shaw, Harold <HShaw@massport.com>; Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>; Ball, Richard (POL) <Richard.Ball@pol.state.ma.us>
Subject: Re: MassPort LPR Cameras

Thank you Brian. Great work grabbing this data.

Colonel Christopher Mason
Superintendent
Massachusetts State Police

> On May 6, 2020, at 6:57 PM, Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us> wrote:
>
> Hi Sirs,
>
> We have begun cutting over the MassPort LPR Cameras into the EOPSS BOSS LPR Server. Today, [redacted] at Airport Road arrivals were migrated and are now writing data to Chelsea. I will continue to cut the remaining cameras over in the next few days and weeks. I will advise when the project is complete.
>
> - Brian
>

> -----Original Message-----
> From: Warmington, Scott (POL)
> Sent: Tuesday, March 10, 2020 11:36 AM
> To: Quinn, Dermot (POL)
> Cc: Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Mason, Christopher (POL); Egnitz, Brian (POL); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL)
> Subject: Re: MassPort LPR Cameras
>
> What is the cost?
>
> Sent from my iPhone
>
>> On Mar 10, 2020, at 11:28 AM, Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us> wrote:
>>
>> Michelle and Kyra,
>>
>> This purchase request is for equipment to allow Mass Port Sierra Wireless modems to communicate directly with the existing ALPR Boss server in Chelsea. This is the fastest way to bring the Massport LPR cameras on line. EOTSS and EOPSS are OK with this solution as is Major Deb Ryan, the CO at Troop F.
>>
>> As you can see from the thread, this has been going on for some time. I think we can close it out with this small purchase.
>>
>> This does not resolve the replacement of the existing ALPR equipment that we discussed at Command Staff yesterday. That is a different issue.
>>
>> Thanks
>>
>>
>> Lieutenant Colonel Dermot J. Quinn #1765
>> Division Commander
>> Division of Homeland Security & Preparedness
>> Massachusetts State Police
>>
>>
>>
>>
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 10:52 AM
>> To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: FW: MassPort LPR Cameras
>>
>> Hi LTC.,
>>
>> Can we order this equipment for the MassPort project?
>>
>> Thanks, Brian
>>
>> -----Original Message-----

>> From: Slater, James (CHS)
>> Sent: Tuesday, March 10, 2020 10:26 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> This needs to go through MSP fiscal. They need to enter the purchase in OPAS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 08:06
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Subject: RE: MassPort LPR Cameras
>>
>> Is this something you can order or does it need to go through MSP?
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Monday, March 9, 2020 10:36 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks, Brian...I will check with TSS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Monday, March 9, 2020 10:29
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks Jim,
>>
>> I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need [redacted] wireless AC adapters and [redacted] I have reached out to BCM for a quote.
>>
>> I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.
>>
>> I plan to cut one sector ([redacted]) over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?
>>
>> -Brian
>>
>> -----Original Message-----
>> From: Slater, James (CHS)

>> Sent: Friday, March 6, 2020 1:43 PM
>> To: Egnitz, Brian (POL)
>> Cc: Quinn, Dermot (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.
>>
>> So, assuming you move forward with this, who would actually make this happen?
>>
>> Thanks.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Wednesday, March 4, 2020 17:53
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: Re: MassPort LPR Cameras
>>
>> Hi Jim,
>>
>> Regarding the Massport cameras; in the early days of AVL we installed [redacted] M.G.L. c. 4.sec. 7.cl.26 (n)(security) modem‘s in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don’t we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn’t have to do any firewall work either because they have a 166. and communicate like all of the MDT‘s . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.
>>
>> We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.
>>
>> Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.
>>
>>>> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>>>
>>> Thank you sir
>>>
>>> Major Charles W. Atchison III
>>> Troop F Commander
>>> Massachusetts State Police
>>> Director of Aviation Security
>>> 2 Service Road
>>> East Boston, Ma 02128
>>> Office: 617-568-7555

>>> Cell: 508-[redacted]
>>>
>>>
>>>> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>>>
>>> All,
>>> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>>>
>>> Thanks
>>>
>>> CW
>>>
>>> From: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
>>> Sent: Monday, February 10, 2020 10:31 AM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
>>> Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
>>> Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
>>> Warmington, Scott (POL)
>>> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
>>> .us>>; Peek, Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
>>> Michalski, Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
>>> Christopher (POL)
>>> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
>>> Hughes, Sean M. (EOTSS)
>>> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
>>> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
>>> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
>>> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
>>> Atchison, Charles (POL)
>>> <catchison@massport.com<mailto:catchison@massport.com>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Good Morning,
>>>
>>> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public

well being events.
>>>
>>> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>>>
>>> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>>>
>>> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>>>
>>> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>>>
>>> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>>>
>>> I can’t overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security’s technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>>>
>>> Respectfully,
>>>
>>>
>>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
>>> of Homeland Security & Preparedness Massachusetts State Police
>>> <image006.png>
>>>
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
>>> Sent: Friday, January 17, 2020 1:10 PM
>>> To: Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>

>>> Cc: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
>>> Guerriero, Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
>>> Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
>>> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
>>> Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>
>>> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>>>
>>> -Brian
>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> Sent: Monday, January 6, 2020 1:33 PM
>>> To: Slater, James (CHS)
>>> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
>>> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
>>> Crary
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>
>>> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>>>
>>> Thanks Brian
>>>
>>>
>>> From: John Tedona [mailto:jtedona@neology.net]
>>> Sent: Monday, December 9, 2019 4:55 PM
>>> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Slater, James (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Alex,
>>>
>>> I can be available most anytime tomorrow for a call.

>>>
>>>
>>> Regards,
>>>
>>> John Tedona
>>> PIPS TECHNOLOGY - A Neology Business
>>> Sales Manager
>>> 12760 Danielson Ct. Suite A
>>> Poway, CA 92064
>>> Phone: 201-841-6237
>>> Email: jtedona@neology.net<mailto:jtedona@neology.net>
>>> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
>>> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
>>> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
>>> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
>>> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ
>>> U2sB_fmM6g&e=>
>>>
>>>
>>> From: Chute, Alexander
>>> <AChute@massport.com<mailto:AChute@massport.com>>
>>> Sent: Monday, December 9, 2019 4:38 PM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>
>>> Cc: Guerriero, Robert (MASSIT)
>>> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
>>> Peek, Brian T. (EOTSS)
>>> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
>>> Slater III, James F (CHS)
>>> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>>>
>>> Hello All,
>>>
>>> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>>>
>>> Respectfully,
>>>
>>> ~Alex
>>>
>>>
>>> <image007.png>

>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Monday, November 18, 2019 3:26 PM
>>> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
>>> pcrary@neology.net<mailto:pcrary@neology.net>
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi John, Peter
>>>
>>> Any issues with moving Massports cameras to the Chelsea DB?
>>>
>>> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>>>
>>> The current app server
>>> <image008.png>
>>>
>>> Current DB server
>>>
>>> <image009.png>
>>> <image010.png>
>>>
>>> Our current reads by month for about [redacted]
>>>
>>> Year
>>>
>>> Month
>>>
>>> Day
>>>
>>> Month Name
>>>
>>> Reads Count
>>>
>>> 2019
>>>
>>> 11

>>>
>>> 1
>>>
>>> November
>>>
>>> 495,113
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 2
>>>
>>> November
>>>
>>> 472,907
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 3
>>>
>>> November
>>>
>>> 384,409
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 4
>>>
>>> November
>>>
>>> 411,440
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 5
>>>
>>> November
>>>
>>> 434,085
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 6
>>>

>>> November
>>>
>>> 495,537
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 7
>>>
>>> November
>>>
>>> 444,123
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 8
>>>
>>> November
>>>
>>> 542,492
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 9
>>>
>>> November
>>>
>>> 443,463
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 10
>>>
>>> November
>>>
>>> 389,514
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 11
>>>
>>> November
>>>
>>> 362,548

>>>
>>> 2019
>>>
>>> 11
>>>
>>> 12
>>>
>>> November
>>>
>>> 236,539
>>>
>>>
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Wednesday, November 13, 2019 2:49 PM
>>> To: Egnitz, Brian (POL)
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> These stats are from the [redacted] we have in the system for this month:
>>>
>>> <image011.png>
>>>
>>> ~Alex
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Tuesday, November 12, 2019 5:28 PM
>>> To: Chute, Alexander
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Alex,
>>>
>>> Can you please provide the updated reads per day? Previously you were interested in sharing [redacted] at approximately 75,000 reads per day.
>>>
>>> Here is the [redacted] confi I mentioned.
>>>
>>> Set host to boss [redacted]
>>> Set image [redacted]
>>> Set number of [redacted]
>>> Set Ping [redacted]
>>> Set udp ping [redacted]
>>> Set ping [redacted]
>>> Set security [redacted]
>>>
>>> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.

>>> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>>>
>>> -Brian
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Tuesday, November 12, 2019 2:08 PM
>>> To: Egnitz, Brian (POL)
>>> Subject: MassPort LPR Cameras
>>>
>>> Brian,
>>>
>>> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to approximately [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.
>>>
>>> Respectfully,
>>>
>>> ~Alex
>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>> <SierraQuoteForMassPort.pdf>

From: Mason, Christopher (POL)
To: Egnitz, Brian (POL)
Cc: Warmington, Scott (POL); Quinn, Dermot (POL); Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL)
Subject: Re: MassPort LPR Cameras
Date: Wednesday, May 6, 2020 7:00:08 PM

Thank you Brian. Great work grabbing this data.

Colonel Christopher Mason
Superintendent
Massachusetts State Police

> On May 6, 2020, at 6:57 PM, Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us> wrote:
>
> Hi Sirs,
>
> We have begun cutting over the MassPort LPR Cameras into the EOPSS BOSS LPR Server. Today, [redacted] at Airport Road arrivals were migrated and are now writing data to Chelsea. I will continue to cut the remaining cameras over in the next few days and weeks. I will advise when the project is complete.
>
> - Brian
>
> -----Original Message-----
> From: Warmington, Scott (POL)
> Sent: Tuesday, March 10, 2020 11:36 AM
> To: Quinn, Dermot (POL)
> Cc: Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Mason, Christopher (POL); Egnitz, Brian (POL); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL)
> Subject: Re: MassPort LPR Cameras
>
> What is the cost?
>
> Sent from my iPhone
>
>> On Mar 10, 2020, at 11:28 AM, Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us> wrote:
>>
>> Michelle and Kyra,
>>
>> This purchase request is for equipment to allow Mass Port Sierra Wireless modems to communicate directly with the existing ALPR Boss server in Chelsea. This is the fastest way to bring the Massport LPR cameras on line. EOTSS and EOPSS are OK with this solution as is Major Deb Ryan, the CO at Troop F.
>>
>> As you can see from the thread, this has been going on for some time. I think we can close it out with this small purchase.
>>
>> This does not resolve the replacement of the existing ALPR equipment that we discussed at Command Staff yesterday. That is a different issue.
>>
>> Thanks
>>

>>
>> Lieutenant Colonel Dermot J. Quinn #1765
>> Division Commander
>> Division of Homeland Security & Preparedness
>> Massachusetts State Police
>>
>>
>>
>>
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 10:52 AM
>> To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: FW: MassPort LPR Cameras
>>
>> Hi LTC.,
>>
>> Can we order this equipment for the MassPort project?
>>
>> Thanks, Brian
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Tuesday, March 10, 2020 10:26 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> This needs to go through MSP fiscal. They need to enter the purchase in OPAS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 08:06
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Subject: RE: MassPort LPR Cameras
>>
>> Is this something you can order or does it need to go through MSP?
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Monday, March 9, 2020 10:36 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks, Brian...I will check with TSS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Monday, March 9, 2020 10:29
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>

>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks Jim,
>>
>> I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need [redacted] wireless AC adapters and [redacted] I have reached out to BCM for a quote.
>>
>> I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.
>>
>> I plan to cut one sector [redacted] over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?
>>
>> -Brian
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Friday, March 6, 2020 1:43 PM
>> To: Egnitz, Brian (POL)
>> Cc: Quinn, Dermot (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.
>>
>> So, assuming you move forward with this, who would actually make this happen?
>>
>> Thanks.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Wednesday, March 4, 2020 17:53
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: Re: MassPort LPR Cameras
>>
>> Hi Jim,
>>
>> Regarding the Massport cameras; in the early days of AVL we installed [redacted] modem's in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don't we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn't have to do any firewall work either because they have a 166. and communicate like all of the MDT's . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.
>>
>> We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.
>>
>> Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.

>>
>>>> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>>>
>>> Thank you sir
>>>
>>> Major Charles W. Atchison III
>>> Troop F Commander
>>> Massachusetts State Police
>>> Director of Aviation Security
>>> 2 Service Road
>>> East Boston, Ma 02128
>>> Office: 617-568-7555
>>> Cell: 508-[redacted]
>>>
>>>
>>>> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>>>
>>> All,
>>> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>>>
>>> Thanks
>>>
>>> CW
>>>
>>> From: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
>>> Sent: Monday, February 10, 2020 10:31 AM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
>>> Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
>>> Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
>>> Warmington, Scott (POL)
>>> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
>>> .us>>; Peek, Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
>>> Michalski, Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
>>> Christopher (POL)
>>> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
>>> Hughes, Sean M. (EOTSS)
>>> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
>>> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
>>> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
>>> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
>>> Atchison, Charles (POL)
>>> <catchison@massport.com<mailto:catchison@massport.com>>
>>> Subject: RE: MassPort LPR Cameras
>>>

>>> Good Morning,
>>>
>>> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>>>
>>> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>>>
>>> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>>>
>>> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>>>
>>> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>>>
>>> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>>>
>>> I can’t overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security’s technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>>>
>>> Respectfully,
>>>
>>>
>>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
>>> of Homeland Security & Preparedness Massachusetts State Police
>>> <image006.png>
>>>
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
>>> Sent: Friday, January 17, 2020 1:10 PM
>>> To: Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
>>> Cc: Quinn, Dermot (POL)

>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
>>> Guerriero, Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
>>> Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
>>> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
>>> Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>
>>> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>>>
>>> -Brian
>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> Sent: Monday, January 6, 2020 1:33 PM
>>> To: Slater, James (CHS)
>>> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
>>> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
>>> Crary
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>
>>> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>>>
>>> Thanks Brian
>>>
>>>
>>> From: John Tedona [mailto:jtedona@neology.net]
>>> Sent: Monday, December 9, 2019 4:55 PM
>>> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Slater, James (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Alex,
>>>
>>> I can be available most anytime tomorrow for a call.
>>>
>>>
>>> Regards,
>>>
>>> John Tedona
>>> PIPS TECHNOLOGY - A Neology Business

>>> Sales Manager
>>> 12760 Danielson Ct. Suite A
>>> Poway, CA 92064
>>> Phone: 201-841-6237
>>> Email: jtedona@neology.net<mailto:jtedona@neology.net>
>>> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
>>> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
>>> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
>>> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
>>> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ
>>> U2sB_fmM6g&e=>
>>>
>>>
>>> From: Chute, Alexander
>>> <AChute@massport.com<mailto:AChute@massport.com>>
>>> Sent: Monday, December 9, 2019 4:38 PM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>
>>> Cc: Guerriero, Robert (MASSIT)
>>> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
>>> Peek, Brian T. (EOTSS)
>>> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
>>> Slater III, James F (CHS)
>>> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>>>
>>> Hello All,
>>>
>>> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>>>
>>> Respectfully,
>>>
>>> ~Alex
>>>
>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration

or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Monday, November 18, 2019 3:26 PM
>>> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
>>> pcrary@neology.net<mailto:pcrary@neology.net>
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi John, Peter
>>>
>>> Any issues with moving Massports cameras to the Chelsea DB?
>>>
>>> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>>>
>>> The current app server
>>> <image008.png>
>>>
>>> Current DB server
>>>
>>> <image009.png>
>>> <image010.png>
>>>
>>> Our current reads by month for about [redacted]
>>>
>>> Year
>>>
>>> Month
>>>
>>> Day
>>>
>>> Month Name
>>>
>>> Reads Count
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 1
>>>
>>> November
>>>
>>>   495,113
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 2
>>>
>>> November
>>>

>>> 472,907
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 3
>>>
>>> November
>>>
>>> 384,409
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 4
>>>
>>> November
>>>
>>> 411,440
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 5
>>>
>>> November
>>>
>>> 434,085
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 6
>>>
>>> November
>>>
>>> 495,537
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 7
>>>
>>> November
>>>
>>> 444,123
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 8

>>>
>>> November
>>>
>>> 542,492
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 9
>>>
>>> November
>>>
>>> 443,463
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 10
>>>
>>> November
>>>
>>> 389,514
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 11
>>>
>>> November
>>>
>>> 362,548
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 12
>>>
>>> November
>>>
>>> 236,539
>>>
>>>
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Wednesday, November 13, 2019 2:49 PM
>>> To: Egnitz, Brian (POL)
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> These stats are from the [redacted] we have in the system for this month:

>>>
>>> <image011.png>
>>>
>>> ~Alex
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Tuesday, November 12, 2019 5:28 PM
>>> To: Chute, Alexander
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Alex,
>>>
>>> Can you please provide the updated reads per day? Previously you were interested in sharing [redacted] at approximately 75,000 reads per day.
>>>
>>> Here is the [redacted] confi I mentioned.
>>>
>>> Set host to boss [redacted]
>>> Set image [redacted]
>>> Set number of [redacted]
>>> Set Ping [redacted]
>>> Set udp ping [redacted]
>>> Set ping [redacted]
>>> Set security [redacted]
>>>
>>> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
>>> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>>>
>>> -Brian
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Tuesday, November 12, 2019 2:08 PM
>>> To: Egnitz, Brian (POL)
>>> Subject: MassPort LPR Cameras
>>>
>>> Brian,
>>>
>>> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to approximately [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.
>>>
>>> Respectfully,
>>>
>>> ~Alex

>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>> <SierraQuoteForMassPort.pdf>

From: Chris.Mason@pol.state.ma.us
To: Egnitz, Brian (POL)
Cc: Warmington, Scott (POL); Quinn, Dermot (POL); Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL)
Subject: Re: MassPort LPR Cameras
Date: Wednesday, May 6, 2020 7:00:07 PM

Thank you Brian. Great work grabbing this data.

Colonel Christopher Mason
Superintendent
Massachusetts State Police

> On May 6, 2020, at 6:57 PM, Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us> wrote:
>
> Hi Sirs,
>
> We have begun cutting over the MassPort LPR Cameras into the EOPSS BOSS LPR Server. Today, [redacted] at Airport Road arrivals were migrated and are now writing data to Chelsea. I will continue to cut the remaining cameras over in the next few days and weeks. I will advise when the project is complete.
>
> - Brian
>
> -----Original Message-----
> From: Warmington, Scott (POL)
> Sent: Tuesday, March 10, 2020 11:36 AM
> To: Quinn, Dermot (POL)
> Cc: Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Mason, Christopher (POL); Egnitz, Brian (POL); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL)
> Subject: Re: MassPort LPR Cameras
>
> What is the cost?
>
> Sent from my iPhone
>
>> On Mar 10, 2020, at 11:28 AM, Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us> wrote:
>>
>> Michelle and Kyra,
>>
>> This purchase request is for equipment to allow Mass Port Sierra Wireless modems to communicate directly with the existing ALPR Boss server in Chelsea. This is the fastest way to bring the Massport LPR cameras on line. EOTSS and EOPSS are OK with this solution as is Major Deb Ryan, the CO at Troop F.
>>
>> As you can see from the thread, this has been going on for some time. I think we can close it out with this small purchase.
>>
>> This does not resolve the replacement of the existing ALPR equipment that we discussed at Command Staff yesterday. That is a different issue.
>>
>> Thanks
>>

>>
>> Lieutenant Colonel Dermot J. Quinn #1765
>> Division Commander
>> Division of Homeland Security & Preparedness
>> Massachusetts State Police
>>
>>
>>
>>
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 10:52 AM
>> To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: FW: MassPort LPR Cameras
>>
>> Hi LTC.,
>>
>> Can we order this equipment for the MassPort project?
>>
>> Thanks, Brian
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Tuesday, March 10, 2020 10:26 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> This needs to go through MSP fiscal. They need to enter the purchase in OPAS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 08:06
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Subject: RE: MassPort LPR Cameras
>>
>> Is this something you can order or does it need to go through MSP?
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Monday, March 9, 2020 10:36 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks, Brian...I will check with TSS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Monday, March 9, 2020 10:29
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>

>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks Jim,
>>
>> I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need [redacted] wireless AC adapters and [redacted] I have reached out to BCM for a quote.
>>
>> I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.
>>
>> I plan to cut one sector [redacted] over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?
>>
>> -Brian
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Friday, March 6, 2020 1:43 PM
>> To: Egnitz, Brian (POL)
>> Cc: Quinn, Dermot (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.
>>
>> So, assuming you move forward with this, who would actually make this happen?
>>
>> Thanks.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Wednesday, March 4, 2020 17:53
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: Re: MassPort LPR Cameras
>>
>> Hi Jim,
>>
>> Regarding the Massport cameras; in the early days of AVL we installed [redacted] modem's in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don't we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn't have to do any firewall work either because they have a 166. and communicate like all of the MDT's . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.
>>
>> We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.
>>
>> Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.

>>
>>>> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>>>
>>> Thank you sir
>>>
>>> Major Charles W. Atchison III
>>> Troop F Commander
>>> Massachusetts State Police
>>> Director of Aviation Security
>>> 2 Service Road
>>> East Boston, Ma 02128
>>> Office: 617-568-7555
>>> Cell: 508-[redacted]
>>>
>>>
>>>> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>>>
>>> All,
>>> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>>>
>>> Thanks
>>>
>>> CW
>>>
>>> From: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
>>> Sent: Monday, February 10, 2020 10:31 AM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
>>> Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
>>> Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
>>> Warmington, Scott (POL)
>>> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
>>> .us>>; Peek, Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
>>> Michalski, Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
>>> Christopher (POL)
>>> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
>>> Hughes, Sean M. (EOTSS)
>>> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
>>> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
>>> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
>>> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
>>> Atchison, Charles (POL)
>>> <catchison@massport.com<mailto:catchison@massport.com>>
>>> Subject: RE: MassPort LPR Cameras
>>>

>>> Good Morning,
>>>
>>> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>>>
>>> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>>>
>>> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>>>
>>> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>>>
>>> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>>>
>>> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>>>
>>> I can’t overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security’s technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>>>
>>> Respectfully,
>>>
>>>
>>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
>>> of Homeland Security & Preparedness Massachusetts State Police
>>> <image006.png>
>>>
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
>>> Sent: Friday, January 17, 2020 1:10 PM
>>> To: Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
>>> Cc: Quinn, Dermot (POL)

>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
>>> Guerriero, Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
>>> Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
>>> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
>>> Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>
>>> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>>>
>>> -Brian
>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> Sent: Monday, January 6, 2020 1:33 PM
>>> To: Slater, James (CHS)
>>> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
>>> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
>>> Crary
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>
>>> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>>>
>>> Thanks Brian
>>>
>>>
>>> From: John Tedona [mailto:jtedona@neology.net]
>>> Sent: Monday, December 9, 2019 4:55 PM
>>> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Slater, James (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Alex,
>>>
>>> I can be available most anytime tomorrow for a call.
>>>
>>>
>>> Regards,
>>>
>>> John Tedona
>>> PIPS TECHNOLOGY - A Neology Business

>>> Sales Manager
>>> 12760 Danielson Ct. Suite A
>>> Poway, CA 92064
>>> Phone: 201-841-6237
>>> Email: jtedona@neology.net<mailto:jtedona@neology.net>
>>> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
>>> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
>>> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
>>> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
>>> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ
>>> U2sB_fmM6g&e=>
>>>
>>>
>>> From: Chute, Alexander
>>> <AChute@massport.com<mailto:AChute@massport.com>>
>>> Sent: Monday, December 9, 2019 4:38 PM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>
>>> Cc: Guerriero, Robert (MASSIT)
>>> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
>>> Peek, Brian T. (EOTSS)
>>> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
>>> Slater III, James F (CHS)
>>> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>>>
>>> Hello All,
>>>
>>> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>>>
>>> Respectfully,
>>>
>>> ~Alex
>>>
>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration

or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Monday, November 18, 2019 3:26 PM
>>> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
>>> pcrary@neology.net<mailto:pcrary@neology.net>
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi John, Peter
>>>
>>> Any issues with moving Massports cameras to the Chelsea DB?
>>>
>>> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>>>
>>> The current app server
>>> <image008.png>
>>>
>>> Current DB server
>>>
>>> <image009.png>
>>> <image010.png>
>>>
>>> Our current reads by month for about [redacted]
>>>
>>> Year
>>>
>>> Month
>>>
>>> Day
>>>
>>> Month Name
>>>
>>> Reads Count
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 1
>>>
>>> November
>>>
>>>   495,113
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 2
>>>
>>> November
>>>

>>> 472,907
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 3
>>>
>>> November
>>>
>>> 384,409
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 4
>>>
>>> November
>>>
>>> 411,440
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 5
>>>
>>> November
>>>
>>> 434,085
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 6
>>>
>>> November
>>>
>>> 495,537
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 7
>>>
>>> November
>>>
>>> 444,123
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 8

>>>
>>> November
>>>
>>> 542,492
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 9
>>>
>>> November
>>>
>>> 443,463
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 10
>>>
>>> November
>>>
>>> 389,514
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 11
>>>
>>> November
>>>
>>> 362,548
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 12
>>>
>>> November
>>>
>>> 236,539
>>>
>>>
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Wednesday, November 13, 2019 2:49 PM
>>> To: Egnitz, Brian (POL)
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> These stats are from the [redacted] we have in the system for this month:

>>>
>>> <image011.png>
>>>
>>> ~Alex
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Tuesday, November 12, 2019 5:28 PM
>>> To: Chute, Alexander
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Alex,
>>>
>>> Can you please provide the updated reads per day? Previously you were interested in sharing [redacted] at approximately 75,000 reads per day.
>>>
>>> Here is the [redacted] confi I mentioned.
>>>
>>> Set host to boss [redacted]
>>> Set image [redacted]
>>> Set number of [redacted]
>>> Set Ping [redacted]
>>> Set udp ping [redacted]
>>> Set ping [redacted]
>>> Set security [redacted]
>>>
>>> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
>>> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>>>
>>> -Brian
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Tuesday, November 12, 2019 2:08 PM
>>> To: Egnitz, Brian (POL)
>>> Subject: MassPort LPR Cameras
>>>
>>> Brian,
>>>
>>> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to approximately [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.
>>>
>>> Respectfully,
>>>
>>> ~Alex

>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>> <SierraQuoteForMassPort.pdf>

From: Egnitz, Brian (POL)
To: Silva, Kyra (POL)
Subject: Re: MassPort LPR Cameras
Date: Thursday, April 16, 2020 4:26:26 PM

Thank you

> On Apr 16, 2020, at 3:53 PM, Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us> wrote:
>
> This was submitted into OPAS today and will be processed.
>
> -----Original Message-----
> From: Egnitz, Brian (POL)
> Sent: Thursday, April 16, 2020 3:27 PM
> To: Silva, Kyra (POL)
> Subject: Re: MassPort LPR Cameras
>
> No to from, just a email request from LTC., to Me, then forward. Let me know if you want me to write one.
>
>> On Apr 16, 2020, at 3:18 PM, Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us> wrote:
>>
>> Was there a to/from on this? If so, can you please send me a copy?
>>
>> Thanks
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL)
>> Sent: Thursday, April 16, 2020 3:15 PM
>> To: Silva, Kyra (POL)
>> Subject: Re: MassPort LPR Cameras
>>
>> Not that I'm aware of, its our understanding that we submit them to the LTC. , then it goes over to Michelle and then IT. We've done tickets in the past but then were advised that the proper channel is a to/from through the chain.
>>
>> Thanks, Brian
>>
>>>> On Apr 16, 2020, at 3:02 PM, Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us> wrote:
>>>
>>> Hi,
>>>
>>> Checking on this and will advise. Was the request submitted to IT?
>>>
>>> -----Original Message-----
>>> From: Egnitz, Brian (POL)
>>> Sent: Thursday, April 09, 2020 4:06 PM
>>> To: Silva, Kyra (POL)
>>> Subject: FW: MassPort LPR Cameras
>>>
>>> Hi Kyra,
>>>
>>> Can you please see below and attached. Let me know if you have any questions.
>>>
>>> Thanks, Brian
>>>
>>> -----Original Message-----

>>> From: Quinn, Dermot (POL)
>>> Sent: Thursday, April 9, 2020 2:00 PM
>>> To: Egnitz, Brian (POL)
>>> Cc: Warren, Rosemary (POL)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> This is to allow the Massport ALPR cameras to write to thestate ALPR server in Chelsea. Approved at DHS. Please forward to Kyra Silva in Fiscal for funding.
>>>
>>>
>>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division of Homeland Security & Preparedness Massachusetts State Police
>>>
>>>
>>>
>>>
>>>
>>> -----Original Message-----
>>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>>> Sent: Thursday, April 9, 2020 1:58 PM
>>> To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Do you know if this was moved on? We need it for the MassPort modem project.
>>>
>>> -----Original Message-----
>>> From: Egnitz, Brian (POL)
>>> Sent: Tuesday, March 10, 2020 10:52 AM
>>> To: Quinn, Dermot (POL)
>>> Subject: FW: MassPort LPR Cameras
>>>
>>> Hi LTC.,
>>>
>>> Can we order this equipment for the MassPort project?
>>>
>>> Thanks, Brian
>>>
>>> -----Original Message-----
>>> From: Slater, James (CHS)
>>> Sent: Tuesday, March 10, 2020 10:26 AM
>>> To: Egnitz, Brian (POL)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi, Brian!
>>>
>>> This needs to go through MSP fiscal. They need to enter the purchase in OPAS.
>>>
>>> Jim
>>>
>>> -----Original Message-----
>>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>>> Sent: Tuesday, March 10, 2020 08:06
>>> To: Slater, James (CHS) <james.slater@mass.gov>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Is this something you can order or does it need to go through MSP?
>>>

>>> -----Original Message-----
>>> From: Slater, James (CHS)
>>> Sent: Monday, March 9, 2020 10:36 AM
>>> To: Egnitz, Brian (POL)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Thanks, Brian...I will check with TSS.
>>>
>>> Jim
>>>
>>> -----Original Message-----
>>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>>> Sent: Monday, March 9, 2020 10:29
>>> To: Slater, James (CHS) <james.slater@mass.gov>
>>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Thanks Jim,
>>>
>>> I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need [redacted] wireless AC adapters and [redacted] I have reached out to BCM for a quote.
>>>
>>> I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.
>>>
>>> I plan to cut one sector ([redacted]) over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?
>>>
>>> -Brian
>>>
>>> -----Original Message-----
>>> From: Slater, James (CHS)
>>> Sent: Friday, March 6, 2020 1:43 PM
>>> To: Egnitz, Brian (POL)
>>> Cc: Quinn, Dermot (POL)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi, Brian!
>>>
>>> I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.
>>>
>>> So, assuming you move forward with this, who would actually make this happen?
>>>
>>> Thanks.
>>>
>>> Jim
>>>
>>> -----Original Message-----
>>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>>> Sent: Wednesday, March 4, 2020 17:53
>>> To: Slater, James (CHS) <james.slater@mass.gov>
>>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>>> Subject: Re: MassPort LPR Cameras
>>>

>>> Hi Jim,
>>>
>>> Regarding the Massport cameras; in the early days of AVL we installed [redacted] modem's in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don't we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn't have to do any firewall work either because they have a 166. and communicate like all of the MDT's . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.
>>>
>>> We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.
>>>
>>> Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.
>>>
>>>>> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>>>>
>>>> Thank you sir
>>>>
>>>> Major Charles W. Atchison III
>>>> Troop F Commander
>>>> Massachusetts State Police
>>>> Director of Aviation Security
>>>> 2 Service Road
>>>> East Boston, Ma 02128
>>>> Office: 617-568-7555
>>>> Cell: 508-[redacted]
>>>>
>>>>
>>>>> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>>>>
>>>> All,
>>>> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>>>>
>>>> Thanks
>>>>
>>>> CW
>>>>
>>>> From: Quinn, Dermot (POL)
>>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
>>>> Sent: Monday, February 10, 2020 10:31 AM
>>>> To: Egnitz, Brian (POL)
>>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
>>>> Slater, James (CHS)
>>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
>>>> Robert (EOTSS)
>>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
>>>> Warmington, Scott (POL)
>>>> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
>>>> .us>>; Peek, Brian T. (EOTSS)
>>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>>> Timothy (EPS)
>>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John

>>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
>>>> Michalski, Maria (EPS)
>>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
>>>> Christopher (POL)
>>>> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
>>>> Hughes, Sean M. (EOTSS)
>>>> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
>>>> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
>>>> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
>>>> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
>>>> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
>>>> Atchison, Charles (POL)
>>>> <catchison@massport.com<mailto:catchison@massport.com>>
>>>> Subject: RE: MassPort LPR Cameras
>>>>
>>>> Good Morning,
>>>>
>>>> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>>>>
>>>> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>>>>
>>>> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>>>>
>>>> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>>>>
>>>> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>>>>
>>>> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>>>>
>>>> I can’t overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security’s technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>>>>

>>>> Respectfully,
>>>>
>>>>
>>>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
>>>> of Homeland Security & Preparedness Massachusetts State Police
>>>> <image006.png>
>>>>
>>>>
>>>>
>>>>
>>>> From: Egnitz, Brian (POL)
>>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
>>>> Sent: Friday, January 17, 2020 1:10 PM
>>>> To: Slater, James (CHS)
>>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
>>>> Cc: Quinn, Dermot (POL)
>>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
>>>> Guerriero, Robert (EOTSS)
>>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
>>>> Brian T. (EOTSS)
>>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>>> Timothy (EPS)
>>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
>>>> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
>>>> Maria (EPS)
>>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
>>>> Subject: RE: MassPort LPR Cameras
>>>>
>>>> Hi Jim,
>>>>
>>>> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>>>>
>>>> -Brian
>>>>
>>>>
>>>> From: Egnitz, Brian (POL)
>>>> Sent: Monday, January 6, 2020 1:33 PM
>>>> To: Slater, James (CHS)
>>>> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
>>>> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
>>>> Crary
>>>> Subject: RE: MassPort LPR Cameras
>>>>
>>>> Hi Jim,
>>>>
>>>> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>>>>
>>>> Thanks Brian
>>>>
>>>>

>>>> From: John Tedona [mailto:jtedona@neology.net]
>>>> Sent: Monday, December 9, 2019 4:55 PM
>>>> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
>>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>>> Timothy (EPS); Slater, James (CHS)
>>>> Subject: RE: MassPort LPR Cameras
>>>>
>>>> Alex,
>>>>
>>>> I can be available most anytime tomorrow for a call.
>>>>
>>>>
>>>> Regards,
>>>>
>>>> John Tedona
>>>> PIPS TECHNOLOGY - A Neology Business
>>>> Sales Manager
>>>> 12760 Danielson Ct. Suite A
>>>> Poway, CA 92064
>>>> Phone: 201-841-6237
>>>> Email: jtedona@neology.net<mailto:jtedona@neology.net>
>>>> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
>>>> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
>>>> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
>>>> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
>>>> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ
>>>> U2sB_fmM6g&e=>
>>>>
>>>>
>>>> From: Chute, Alexander
>>>> <AChute@massport.com<mailto:AChute@massport.com>>
>>>> Sent: Monday, December 9, 2019 4:38 PM
>>>> To: Egnitz, Brian (POL)
>>>> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
>>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
>>>> <pcrary@neology.net<mailto:pcrary@neology.net>>
>>>> Cc: Guerriero, Robert (MASSIT)
>>>> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
>>>> Peek, Brian T. (EOTSS)
>>>> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
>>>> Timothy (EPS)
>>>> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
>>>> Slater III, James F (CHS)
>>>> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
>>>> Subject: RE: MassPort LPR Cameras
>>>>
>>>> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>>>>
>>>> Hello All,
>>>>
>>>> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>>>>

>>>> Respectfully,
>>>>
>>>> ~Alex
>>>>
>>>>
>>>> <image007.png>
>>>>
>>>> Alexander B. Chute
>>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>>> Cell: [redacted]
>>>> Office: 617.568.5942
>>>> achute@massport.com<mailto:achute@massport.com>
>>>>
>>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>>
>>>>
>>>>
>>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>>> Sent: Monday, November 18, 2019 3:26 PM
>>>> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
>>>> pcrary@neology.net<mailto:pcrary@neology.net>
>>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>>> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
>>>> Subject: RE: MassPort LPR Cameras
>>>>
>>>> Hi John, Peter
>>>>
>>>> Any issues with moving Massports cameras to the Chelsea DB?
>>>>
>>>> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>>>>
>>>> The current app server
>>>> <image008.png>
>>>>
>>>> Current DB server
>>>>
>>>> <image009.png>
>>>> <image010.png>
>>>>
>>>> Our current reads by month for about [redacted]
>>>>
>>>> Year
>>>>
>>>> Month
>>>>
>>>> Day
>>>>
>>>> Month Name
>>>>
>>>> Reads Count
>>>>
>>>> 2019
>>>>

>>>> 11
>>>>
>>>> 1
>>>>
>>>> November
>>>>
>>>> 495,113
>>>>
>>>> 2019
>>>>
>>>> 11
>>>>
>>>> 2
>>>>
>>>> November
>>>>
>>>> 472,907
>>>>
>>>> 2019
>>>>
>>>> 11
>>>>
>>>> 3
>>>>
>>>> November
>>>>
>>>> 384,409
>>>>
>>>> 2019
>>>>
>>>> 11
>>>>
>>>> 4
>>>>
>>>> November
>>>>
>>>> 411,440
>>>>
>>>> 2019
>>>>
>>>> 11
>>>>
>>>> 5
>>>>
>>>> November
>>>>
>>>> 434,085
>>>>
>>>> 2019
>>>>
>>>> 11
>>>>
>>>> 6
>>>>
>>>> November
>>>>
>>>> 495,537

>>>>
>>>> 2019
>>>>
>>>> 11
>>>>
>>>> 7
>>>>
>>>> November
>>>>
>>>> 444,123
>>>>
>>>> 2019
>>>>
>>>> 11
>>>>
>>>> 8
>>>>
>>>> November
>>>>
>>>> 542,492
>>>>
>>>> 2019
>>>>
>>>> 11
>>>>
>>>> 9
>>>>
>>>> November
>>>>
>>>> 443,463
>>>>
>>>> 2019
>>>>
>>>> 11
>>>>
>>>> 10
>>>>
>>>> November
>>>>
>>>> 389,514
>>>>
>>>> 2019
>>>>
>>>> 11
>>>>
>>>> 11
>>>>
>>>> November
>>>>
>>>> 362,548
>>>>
>>>> 2019
>>>>
>>>> 11
>>>>
>>>> 12
>>>>

>>>> November
>>>>
>>>> 236,539
>>>>
>>>>
>>>>
>>>>
>>>>
>>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>>> Sent: Wednesday, November 13, 2019 2:49 PM
>>>> To: Egnitz, Brian (POL)
>>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>>> Timothy (EPS)
>>>> Subject: RE: MassPort LPR Cameras
>>>>
>>>> These stats are from the [redacted] we have in the system for this month:
>>>>
>>>> <image011.png>
>>>>
>>>> ~Alex
>>>>
>>>>
>>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>>> Sent: Tuesday, November 12, 2019 5:28 PM
>>>> To: Chute, Alexander
>>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>>> Timothy (EPS)
>>>> Subject: RE: MassPort LPR Cameras
>>>>
>>>> Hi Alex,
>>>>
>>>> Can you please provide the updated reads per day? Previously you were interested in sharing [redacted] at approximately 75,000 reads per day.
>>>>
>>>> Here is the [redacted] confi I mentioned.
>>>>
>>>> Set host to boss [redacted]
>>>> Set image [redacted]
>>>> Set number of [redacted]
>>>> Set Ping [redacted]
>>>> Set udp ping [redacted]
>>>> Set ping [redacted]
>>>> Set security [redacted]
>>>>
>>>> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
>>>> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>>>>
>>>> -Brian
>>>>
>>>>
>>>>
>>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>>> Sent: Tuesday, November 12, 2019 2:08 PM
>>>> To: Egnitz, Brian (POL)
>>>> Subject: MassPort LPR Cameras

>>>>
>>>> Brian,
>>>>
>>>> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to approximately [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.
>>>>
>>>> Respectfully,
>>>>
>>>> ~Alex
>>>>
>>>> <image007.png>
>>>>
>>>> Alexander B. Chute
>>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>>> Cell: [redacted]
>>>> Office: 617.568.5942
>>>> achute@massport.com<mailto:achute@massport.com>
>>>>
>>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>>

From: brian.egnitz@pol.state.ma.us
To: Silva, Kyra (POL)
Subject: Re: MassPort LPR Cameras
Date: Thursday, April 16, 2020 4:26:25 PM

Thank you

> On Apr 16, 2020, at 3:53 PM, Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us> wrote:
>
> This was submitted into OPAS today and will be processed.
>
> -----Original Message-----
> From: Egnitz, Brian (POL)
> Sent: Thursday, April 16, 2020 3:27 PM
> To: Silva, Kyra (POL)
> Subject: Re: MassPort LPR Cameras
>
> No to from, just a email request from LTC., to Me, then forward. Let me know if you want me to write one.
>
>> On Apr 16, 2020, at 3:18 PM, Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us> wrote:
>>
>> Was there a to/from on this? If so, can you please send me a copy?
>>
>> Thanks
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL)
>> Sent: Thursday, April 16, 2020 3:15 PM
>> To: Silva, Kyra (POL)
>> Subject: Re: MassPort LPR Cameras
>>
>> Not that I'm aware of, its our understanding that we submit them to the LTC. , then it goes over to Michelle and then IT. We've done tickets in the past but then were advised that the proper channel is a to/from through the chain.
>>
>> Thanks, Brian
>>
>>>> On Apr 16, 2020, at 3:02 PM, Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us> wrote:
>>>
>>> Hi,
>>>
>>> Checking on this and will advise. Was the request submitted to IT?
>>>
>>> -----Original Message-----
>>> From: Egnitz, Brian (POL)
>>> Sent: Thursday, April 09, 2020 4:06 PM
>>> To: Silva, Kyra (POL)
>>> Subject: FW: MassPort LPR Cameras
>>>
>>> Hi Kyra,
>>>
>>> Can you please see below and attached. Let me know if you have any questions.
>>>
>>> Thanks, Brian
>>>
>>> -----Original Message-----

>>> From: Quinn, Dermot (POL)
>>> Sent: Thursday, April 9, 2020 2:00 PM
>>> To: Egnitz, Brian (POL)
>>> Cc: Warren, Rosemary (POL)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> This is to allow the Massport ALPR cameras to write to thestate ALPR server in Chelsea. Approved at DHS. Please forward to Kyra Silva in Fiscal for funding.
>>>
>>>
>>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division of Homeland Security & Preparedness Massachusetts State Police
>>>
>>>
>>>
>>>
>>>
>>> -----Original Message-----
>>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>>> Sent: Thursday, April 9, 2020 1:58 PM
>>> To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Do you know if this was moved on? We need it for the MassPort modem project.
>>>
>>> -----Original Message-----
>>> From: Egnitz, Brian (POL)
>>> Sent: Tuesday, March 10, 2020 10:52 AM
>>> To: Quinn, Dermot (POL)
>>> Subject: FW: MassPort LPR Cameras
>>>
>>> Hi LTC.,
>>>
>>> Can we order this equipment for the MassPort project?
>>>
>>> Thanks, Brian
>>>
>>> -----Original Message-----
>>> From: Slater, James (CHS)
>>> Sent: Tuesday, March 10, 2020 10:26 AM
>>> To: Egnitz, Brian (POL)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi, Brian!
>>>
>>> This needs to go through MSP fiscal. They need to enter the purchase in OPAS.
>>>
>>> Jim
>>>
>>> -----Original Message-----
>>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>>> Sent: Tuesday, March 10, 2020 08:06
>>> To: Slater, James (CHS) <james.slater@mass.gov>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Is this something you can order or does it need to go through MSP?
>>>

>>> -----Original Message-----
>>> From: Slater, James (CHS)
>>> Sent: Monday, March 9, 2020 10:36 AM
>>> To: Egnitz, Brian (POL)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Thanks, Brian...I will check with TSS.
>>>
>>> Jim
>>>
>>> -----Original Message-----
>>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>>> Sent: Monday, March 9, 2020 10:29
>>> To: Slater, James (CHS) <james.slater@mass.gov>
>>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Thanks Jim,
>>>
>>> I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need [redacted] wireless AC adapters and [redacted] I have reached out to BCM for a quote.
>>>
>>> I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.
>>>
>>> I plan to cut one sector ([redacted]) over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?
>>>
>>> -Brian
>>>
>>> -----Original Message-----
>>> From: Slater, James (CHS)
>>> Sent: Friday, March 6, 2020 1:43 PM
>>> To: Egnitz, Brian (POL)
>>> Cc: Quinn, Dermot (POL)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi, Brian!
>>>
>>> I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.
>>>
>>> So, assuming you move forward with this, who would actually make this happen?
>>>
>>> Thanks.
>>>
>>> Jim
>>>
>>> -----Original Message-----
>>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>>> Sent: Wednesday, March 4, 2020 17:53
>>> To: Slater, James (CHS) <james.slater@mass.gov>
>>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>>> Subject: Re: MassPort LPR Cameras
>>>

>>> Hi Jim,
>>>
>>> Regarding the Massport cameras; in the early days of AVL we installed [redacted] modem's in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don't we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn't have to do any firewall work either because they have a 166. and communicate like all of the MDT's . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.
>>>
>>> We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.
>>>
>>> Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.
>>>
>>>>> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>>>>
>>>> Thank you sir
>>>>
>>>> Major Charles W. Atchison III
>>>> Troop F Commander
>>>> Massachusetts State Police
>>>> Director of Aviation Security
>>>> 2 Service Road
>>>> East Boston, Ma 02128
>>>> Office: 617-568-7555
>>>> Cell: 508-[redacted]
>>>>
>>>>
>>>>> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>>>>
>>>> All,
>>>> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>>>>
>>>> Thanks
>>>>
>>>> CW
>>>>
>>>> From: Quinn, Dermot (POL)
>>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
>>>> Sent: Monday, February 10, 2020 10:31 AM
>>>> To: Egnitz, Brian (POL)
>>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
>>>> Slater, James (CHS)
>>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
>>>> Robert (EOTSS)
>>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
>>>> Warmington, Scott (POL)
>>>> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
>>>> .us>>; Peek, Brian T. (EOTSS)
>>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>>> Timothy (EPS)
>>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John

>>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
>>>> Michalski, Maria (EPS)
>>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
>>>> Christopher (POL)
>>>> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
>>>> Hughes, Sean M. (EOTSS)
>>>> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
>>>> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
>>>> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
>>>> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
>>>> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
>>>> Atchison, Charles (POL)
>>>> <catchison@massport.com<mailto:catchison@massport.com>>
>>>> Subject: RE: MassPort LPR Cameras
>>>>
>>>> Good Morning,
>>>>
>>>> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>>>>
>>>> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>>>>
>>>> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>>>>
>>>> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>>>>
>>>> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>>>>
>>>> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>>>>
>>>> I can’t overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security’s technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>>>>

>>>> Respectfully,
>>>>
>>>>
>>>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
>>>> of Homeland Security & Preparedness Massachusetts State Police
>>>> <image006.png>
>>>>
>>>>
>>>>
>>>>
>>>> From: Egnitz, Brian (POL)
>>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
>>>> Sent: Friday, January 17, 2020 1:10 PM
>>>> To: Slater, James (CHS)
>>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
>>>> Cc: Quinn, Dermot (POL)
>>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
>>>> Guerriero, Robert (EOTSS)
>>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
>>>> Brian T. (EOTSS)
>>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>>> Timothy (EPS)
>>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
>>>> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
>>>> Maria (EPS)
>>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
>>>> Subject: RE: MassPort LPR Cameras
>>>>
>>>> Hi Jim,
>>>>
>>>> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>>>>
>>>> -Brian
>>>>
>>>>
>>>> From: Egnitz, Brian (POL)
>>>> Sent: Monday, January 6, 2020 1:33 PM
>>>> To: Slater, James (CHS)
>>>> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
>>>> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
>>>> Crary
>>>> Subject: RE: MassPort LPR Cameras
>>>>
>>>> Hi Jim,
>>>>
>>>> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>>>>
>>>> Thanks Brian
>>>>
>>>>

>>>> From: John Tedona [mailto:jtedona@neology.net]
>>>> Sent: Monday, December 9, 2019 4:55 PM
>>>> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
>>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>>> Timothy (EPS); Slater, James (CHS)
>>>> Subject: RE: MassPort LPR Cameras
>>>>
>>>> Alex,
>>>>
>>>> I can be available most anytime tomorrow for a call.
>>>>
>>>>
>>>> Regards,
>>>>
>>>> John Tedona
>>>> PIPS TECHNOLOGY - A Neology Business
>>>> Sales Manager
>>>> 12760 Danielson Ct. Suite A
>>>> Poway, CA 92064
>>>> Phone: 201-841-6237
>>>> Email: jtedona@neology.net<mailto:jtedona@neology.net>
>>>> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
>>>> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
>>>> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
>>>> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
>>>> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ
>>>> U2sB_fmM6g&e=>
>>>>
>>>>
>>>> From: Chute, Alexander
>>>> <AChute@massport.com<mailto:AChute@massport.com>>
>>>> Sent: Monday, December 9, 2019 4:38 PM
>>>> To: Egnitz, Brian (POL)
>>>> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
>>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
>>>> <pcrary@neology.net<mailto:pcrary@neology.net>>
>>>> Cc: Guerriero, Robert (MASSIT)
>>>> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
>>>> Peek, Brian T. (EOTSS)
>>>> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
>>>> Timothy (EPS)
>>>> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
>>>> Slater III, James F (CHS)
>>>> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
>>>> Subject: RE: MassPort LPR Cameras
>>>>
>>>> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>>>>
>>>> Hello All,
>>>>
>>>> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>>>>

>>>> Respectfully,
>>>>
>>>> ~Alex
>>>>
>>>>
>>>> <image007.png>
>>>>
>>>> Alexander B. Chute
>>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>>> Cell: [redacted]
>>>> Office: 617.568.5942
>>>> achute@massport.com<mailto:achute@massport.com>
>>>>
>>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>>
>>>>
>>>>
>>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>>> Sent: Monday, November 18, 2019 3:26 PM
>>>> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
>>>> pcrary@neology.net<mailto:pcrary@neology.net>
>>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>>> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
>>>> Subject: RE: MassPort LPR Cameras
>>>>
>>>> Hi John, Peter
>>>>
>>>> Any issues with moving Massports cameras to the Chelsea DB?
>>>>
>>>> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>>>>
>>>> The current app server
>>>> <image008.png>
>>>>
>>>> Current DB server
>>>>
>>>> <image009.png>
>>>> <image010.png>
>>>>
>>>> Our current reads by month for about [redacted]
>>>>
>>>> Year
>>>>
>>>> Month
>>>>
>>>> Day
>>>>
>>>> Month Name
>>>>
>>>> Reads Count
>>>>
>>>> 2019
>>>>

>>>> 11
>>>>
>>>> 1
>>>>
>>>> November
>>>>
>>>> 495,113
>>>>
>>>> 2019
>>>>
>>>> 11
>>>>
>>>> 2
>>>>
>>>> November
>>>>
>>>> 472,907
>>>>
>>>> 2019
>>>>
>>>> 11
>>>>
>>>> 3
>>>>
>>>> November
>>>>
>>>> 384,409
>>>>
>>>> 2019
>>>>
>>>> 11
>>>>
>>>> 4
>>>>
>>>> November
>>>>
>>>> 411,440
>>>>
>>>> 2019
>>>>
>>>> 11
>>>>
>>>> 5
>>>>
>>>> November
>>>>
>>>> 434,085
>>>>
>>>> 2019
>>>>
>>>> 11
>>>>
>>>> 6
>>>>
>>>> November
>>>>
>>>> 495,537

>>>>
>>>> 2019
>>>>
>>>> 11
>>>>
>>>> 7
>>>>
>>>> November
>>>>
>>>> 444,123
>>>>
>>>> 2019
>>>>
>>>> 11
>>>>
>>>> 8
>>>>
>>>> November
>>>>
>>>> 542,492
>>>>
>>>> 2019
>>>>
>>>> 11
>>>>
>>>> 9
>>>>
>>>> November
>>>>
>>>> 443,463
>>>>
>>>> 2019
>>>>
>>>> 11
>>>>
>>>> 10
>>>>
>>>> November
>>>>
>>>> 389,514
>>>>
>>>> 2019
>>>>
>>>> 11
>>>>
>>>> 11
>>>>
>>>> November
>>>>
>>>> 362,548
>>>>
>>>> 2019
>>>>
>>>> 11
>>>>
>>>> 12
>>>>

>>>> November
>>>>
>>>> 236,539
>>>>
>>>>
>>>>
>>>>
>>>>
>>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>>> Sent: Wednesday, November 13, 2019 2:49 PM
>>>> To: Egnitz, Brian (POL)
>>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>>> Timothy (EPS)
>>>> Subject: RE: MassPort LPR Cameras
>>>>
>>>> These stats are from the [redacted] we have in the system for this month:
>>>>
>>>> <image011.png>
>>>>
>>>> ~Alex
>>>>
>>>>
>>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>>> Sent: Tuesday, November 12, 2019 5:28 PM
>>>> To: Chute, Alexander
>>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>>> Timothy (EPS)
>>>> Subject: RE: MassPort LPR Cameras
>>>>
>>>> Hi Alex,
>>>>
>>>> Can you please provide the updated reads per day? Previously you were interested in sharing [redacted] at approximately 75,000 reads per day.
>>>>
>>>> Here is the [redacted] confi I mentioned.
>>>>
>>>> Set host to boss [redacted]
>>>> Set image [redacted]
>>>> Set number of [redacted]
>>>> Set Ping [redacted]
>>>> Set udp ping [redacted]
>>>> Set ping [redacted]
>>>> Set security [redacted]
>>>>
>>>> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
>>>> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>>>>
>>>> -Brian
>>>>
>>>>
>>>>
>>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>>> Sent: Tuesday, November 12, 2019 2:08 PM
>>>> To: Egnitz, Brian (POL)
>>>> Subject: MassPort LPR Cameras

>>>>
>>>> Brian,
>>>>
>>>> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to approximately [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.
>>>>
>>>> Respectfully,
>>>>
>>>> ~Alex
>>>>
>>>> <image007.png>
>>>>
>>>> Alexander B. Chute
>>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>>> Cell: [redacted]
>>>> Office: 617.568.5942
>>>> achute@massport.com<mailto:achute@massport.com>
>>>>
>>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>>

From: Egnitz, Brian (POL)
To: Silva, Kyra (POL)
Subject: Re: MassPort LPR Cameras
Date: Thursday, April 16, 2020 3:27:10 PM

No to from, just a email request from LTC., to Me, then forward. Let me know if you want me to write one.

> On Apr 16, 2020, at 3:18 PM, Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us> wrote:
>
> Was there a to/from on this? If so, can you please send me a copy?
>
> Thanks
>
> -----Original Message-----
> From: Egnitz, Brian (POL)
> Sent: Thursday, April 16, 2020 3:15 PM
> To: Silva, Kyra (POL)
> Subject: Re: MassPort LPR Cameras
>
> Not that I'm aware of, its our understanding that we submit them to the LTC. , then it goes over to Michelle and then IT. We've done tickets in the past but then were advised that the proper channel is a to/from through the chain.
>
> Thanks, Brian
>
>> On Apr 16, 2020, at 3:02 PM, Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us> wrote:
>>
>> Hi,
>>
>> Checking on this and will advise. Was the request submitted to IT?
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL)
>> Sent: Thursday, April 09, 2020 4:06 PM
>> To: Silva, Kyra (POL)
>> Subject: FW: MassPort LPR Cameras
>>
>> Hi Kyra,
>>
>> Can you please see below and attached. Let me know if you have any questions.
>>
>> Thanks, Brian
>>
>> -----Original Message-----
>> From: Quinn, Dermot (POL)
>> Sent: Thursday, April 9, 2020 2:00 PM
>> To: Egnitz, Brian (POL)
>> Cc: Warren, Rosemary (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> This is to allow the Massport ALPR cameras to write to thestate ALPR server in Chelsea. Approved at DHS. Please forward to Kyra Silva in Fiscal for funding.
>>
>>
>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division of Homeland Security & Preparedness Massachusetts State Police

>>
>>
>>
>>
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Thursday, April 9, 2020 1:58 PM
>> To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: RE: MassPort LPR Cameras
>>
>> Do you know if this was moved on? We need it for the MassPort modem project.
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL)
>> Sent: Tuesday, March 10, 2020 10:52 AM
>> To: Quinn, Dermot (POL)
>> Subject: FW: MassPort LPR Cameras
>>
>> Hi LTC.,
>>
>> Can we order this equipment for the MassPort project?
>>
>> Thanks, Brian
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Tuesday, March 10, 2020 10:26 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> This needs to go through MSP fiscal. They need to enter the purchase in OPAS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 08:06
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Subject: RE: MassPort LPR Cameras
>>
>> Is this something you can order or does it need to go through MSP?
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Monday, March 9, 2020 10:36 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks, Brian...I will check with TSS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>

>> Sent: Monday, March 9, 2020 10:29
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks Jim,
>>
>> I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need [redacted] wireless AC adapters and [redacted] I have reached out to BCM for a quote.
>>
>> I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.
>>
>> I plan to cut one sector [redacted] over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?
>>
>> -Brian
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Friday, March 6, 2020 1:43 PM
>> To: Egnitz, Brian (POL)
>> Cc: Quinn, Dermot (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.
>>
>> So, assuming you move forward with this, who would actually make this happen?
>>
>> Thanks.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Wednesday, March 4, 2020 17:53
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: Re: MassPort LPR Cameras
>>
>> Hi Jim,
>>
>> Regarding the Massport cameras; in the early days of AVL we installed [redacted] modem's in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don't we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn't have to do any firewall work either because they have a 166. and communicate like all of the MDT's . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.
>>

>> We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.
>>
>> Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.
>>
>>>> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>>>
>>> Thank you sir
>>>
>>> Major Charles W. Atchison III
>>> Troop F Commander
>>> Massachusetts State Police
>>> Director of Aviation Security
>>> 2 Service Road
>>> East Boston, Ma 02128
>>> Office: 617-568-7555
>>> Cell: 508-[redacted]
>>>
>>>
>>>> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>>>
>>> All,
>>> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>>>
>>> Thanks
>>>
>>> CW
>>>
>>> From: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
>>> Sent: Monday, February 10, 2020 10:31 AM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
>>> Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
>>> Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
>>> Warmington, Scott (POL)
>>> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
>>> .us>>; Peek, Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
>>> Michalski, Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
>>> Christopher (POL)
>>> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
>>> Hughes, Sean M. (EOTSS)
>>> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
>>> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
>>> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
>>> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
>>> Atchison, Charles (POL)

>>> <catchison@massport.com<mailto:catchison@massport.com>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Good Morning,
>>>
>>> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>>>
>>> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>>>
>>> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>>>
>>> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>>>
>>> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>>>
>>> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>>>
>>> I can’t overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security’s technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>>>
>>> Respectfully,
>>>
>>>
>>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
>>> of Homeland Security & Preparedness Massachusetts State Police
>>> <image006.png>
>>>
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
>>> Sent: Friday, January 17, 2020 1:10 PM

>>> To: Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
>>> Cc: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
>>> Guerriero, Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
>>> Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
>>> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
>>> Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>
>>> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>>>
>>> -Brian
>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> Sent: Monday, January 6, 2020 1:33 PM
>>> To: Slater, James (CHS)
>>> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
>>> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
>>> Crary
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>
>>> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>>>
>>> Thanks Brian
>>>
>>>
>>> From: John Tedona [mailto:jtedona@neology.net]
>>> Sent: Monday, December 9, 2019 4:55 PM
>>> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Slater, James (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Alex,
>>>
>>> I can be available most anytime tomorrow for a call.
>>>
>>>
>>> Regards,

>>>
>>> John Tedona
>>> PIPS TECHNOLOGY - A Neology Business
>>> Sales Manager
>>> 12760 Danielson Ct. Suite A
>>> Poway, CA 92064
>>> Phone: 201-841-6237
>>> Email: jtedona@neology.net<mailto:jtedona@neology.net>
>>> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
>>> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
>>> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
>>> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
>>> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ
>>> U2sB_fmM6g&e=>
>>>
>>>
>>> From: Chute, Alexander
>>> <AChute@massport.com<mailto:AChute@massport.com>>
>>> Sent: Monday, December 9, 2019 4:38 PM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>
>>> Cc: Guerriero, Robert (MASSIT)
>>> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
>>> Peek, Brian T. (EOTSS)
>>> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
>>> Slater III, James F (CHS)
>>> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>>>
>>> Hello All,
>>>
>>> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>>>
>>> Respectfully,
>>>
>>> ~Alex
>>>
>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>>

>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Monday, November 18, 2019 3:26 PM
>>> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
>>> pcrary@neology.net<mailto:pcrary@neology.net>
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi John, Peter
>>>
>>> Any issues with moving Massports cameras to the Chelsea DB?
>>>
>>> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>>>
>>> The current app server
>>> <image008.png>
>>>
>>> Current DB server
>>>
>>> <image009.png>
>>> <image010.png>
>>>
>>> Our current reads by month for about [redacted]
>>>
>>> Year
>>>
>>> Month
>>>
>>> Day
>>>
>>> Month Name
>>>
>>> Reads Count
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 1
>>>
>>> November
>>>
>>>   495,113
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 2

>>>
>>> November
>>>
>>> 472,907
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 3
>>>
>>> November
>>>
>>> 384,409
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 4
>>>
>>> November
>>>
>>> 411,440
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 5
>>>
>>> November
>>>
>>> 434,085
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 6
>>>
>>> November
>>>
>>> 495,537
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 7
>>>
>>> November
>>>
>>> 444,123
>>>
>>> 2019
>>>

>>> 11
>>>
>>> 8
>>>
>>> November
>>>
>>> 542,492
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 9
>>>
>>> November
>>>
>>> 443,463
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 10
>>>
>>> November
>>>
>>> 389,514
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 11
>>>
>>> November
>>>
>>> 362,548
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 12
>>>
>>> November
>>>
>>> 236,539
>>>
>>>
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Wednesday, November 13, 2019 2:49 PM
>>> To: Egnitz, Brian (POL)
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)

>>> Subject: RE: MassPort LPR Cameras
>>>
>>> These stats are from the [redacted] we have in the system for this month:
>>>
>>> <image011.png>
>>>
>>> ~Alex
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Tuesday, November 12, 2019 5:28 PM
>>> To: Chute, Alexander
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Alex,
>>>
>>> Can you please provide the updated reads per day? Previously you were interested in sharing [redacted] at approximately 75,000 reads per day.
>>>
>>> Here is the [redacted] confi I mentioned.
>>>
>>> Set host to boss [redacted]
>>> Set image [redacted]
>>> Set number of [redacted]
>>> Set Ping [redacted]
>>> Set udp ping [redacted]
>>> Set ping [redacted]
>>> Set security [redacted]
>>>
>>> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
>>> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>>>
>>> -Brian
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Tuesday, November 12, 2019 2:08 PM
>>> To: Egnitz, Brian (POL)
>>> Subject: MassPort LPR Cameras
>>>
>>> Brian,
>>>
>>> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to approximately [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.
>>>

>>> Respectfully,
>>>
>>> ~Alex
>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>

From: brian.egnitz@pol.state.ma.us
To: Silva, Kyra (POL)
Subject: Re: MassPort LPR Cameras
Date: Thursday, April 16, 2020 3:27:09 PM

No to from, just a email request from LTC., to Me, then forward. Let me know if you want me to write one.

> On Apr 16, 2020, at 3:18 PM, Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us> wrote:
>
> Was there a to/from on this? If so, can you please send me a copy?
>
> Thanks
>
> -----Original Message-----
> From: Egnitz, Brian (POL)
> Sent: Thursday, April 16, 2020 3:15 PM
> To: Silva, Kyra (POL)
> Subject: Re: MassPort LPR Cameras
>
> Not that I'm aware of, its our understanding that we submit them to the LTC. , then it goes over to Michelle and then IT. We've done tickets in the past but then were advised that the proper channel is a to/from through the chain.
>
> Thanks, Brian
>
>> On Apr 16, 2020, at 3:02 PM, Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us> wrote:
>>
>> Hi,
>>
>> Checking on this and will advise. Was the request submitted to IT?
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL)
>> Sent: Thursday, April 09, 2020 4:06 PM
>> To: Silva, Kyra (POL)
>> Subject: FW: MassPort LPR Cameras
>>
>> Hi Kyra,
>>
>> Can you please see below and attached. Let me know if you have any questions.
>>
>> Thanks, Brian
>>
>> -----Original Message-----
>> From: Quinn, Dermot (POL)
>> Sent: Thursday, April 9, 2020 2:00 PM
>> To: Egnitz, Brian (POL)
>> Cc: Warren, Rosemary (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> This is to allow the Massport ALPR cameras to write to thestate ALPR server in Chelsea. Approved at DHS. Please forward to Kyra Silva in Fiscal for funding.
>>
>>
>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division of Homeland Security & Preparedness Massachusetts State Police

>>
>>
>>
>>
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Thursday, April 9, 2020 1:58 PM
>> To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: RE: MassPort LPR Cameras
>>
>> Do you know if this was moved on? We need it for the MassPort modem project.
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL)
>> Sent: Tuesday, March 10, 2020 10:52 AM
>> To: Quinn, Dermot (POL)
>> Subject: FW: MassPort LPR Cameras
>>
>> Hi LTC.,
>>
>> Can we order this equipment for the MassPort project?
>>
>> Thanks, Brian
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Tuesday, March 10, 2020 10:26 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> This needs to go through MSP fiscal. They need to enter the purchase in OPAS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 08:06
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Subject: RE: MassPort LPR Cameras
>>
>> Is this something you can order or does it need to go through MSP?
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Monday, March 9, 2020 10:36 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks, Brian...I will check with TSS.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>

>> Sent: Monday, March 9, 2020 10:29
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: RE: MassPort LPR Cameras
>>
>> Thanks Jim,
>>
>> I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need [redacted] wireless AC adapters and [redacted] I have reached out to BCM for a quote.
>>
>> I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.
>>
>> I plan to cut one sector [redacted] over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?
>>
>> -Brian
>>
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Friday, March 6, 2020 1:43 PM
>> To: Egnitz, Brian (POL)
>> Cc: Quinn, Dermot (POL)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi, Brian!
>>
>> I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.
>>
>> So, assuming you move forward with this, who would actually make this happen?
>>
>> Thanks.
>>
>> Jim
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Wednesday, March 4, 2020 17:53
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: Re: MassPort LPR Cameras
>>
>> Hi Jim,
>>
>> Regarding the Massport cameras; in the early days of AVL we installed [redacted] modem's in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don't we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn't have to do any firewall work either because they have a 166. and communicate like all of the MDT's . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.
>>

>> We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.
>>
>> Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.
>>
>>>> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>>>
>>> Thank you sir
>>>
>>> Major Charles W. Atchison III
>>> Troop F Commander
>>> Massachusetts State Police
>>> Director of Aviation Security
>>> 2 Service Road
>>> East Boston, Ma 02128
>>> Office: 617-568-7555
>>> Cell: 508-[redacted]
>>>
>>>
>>>> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>>>
>>> All,
>>> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>>>
>>> Thanks
>>>
>>> CW
>>>
>>> From: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
>>> Sent: Monday, February 10, 2020 10:31 AM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
>>> Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
>>> Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
>>> Warmington, Scott (POL)
>>> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
>>> .us>>; Peek, Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
>>> Michalski, Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
>>> Christopher (POL)
>>> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
>>> Hughes, Sean M. (EOTSS)
>>> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
>>> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
>>> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
>>> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
>>> Atchison, Charles (POL)

>>> <catchison@massport.com<mailto:catchison@massport.com>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Good Morning,
>>>
>>> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>>>
>>> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>>>
>>> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>>>
>>> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>>>
>>> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>>>
>>> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>>>
>>> I can’t overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security’s technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>>>
>>> Respectfully,
>>>
>>>
>>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
>>> of Homeland Security & Preparedness Massachusetts State Police
>>> <image006.png>
>>>
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
>>> Sent: Friday, January 17, 2020 1:10 PM

>>> To: Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
>>> Cc: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
>>> Guerriero, Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
>>> Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
>>> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
>>> Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>
>>> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>>>
>>> -Brian
>>>
>>>
>>> From: Egnitz, Brian (POL)
>>> Sent: Monday, January 6, 2020 1:33 PM
>>> To: Slater, James (CHS)
>>> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
>>> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
>>> Crary
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Jim,
>>>
>>> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>>>
>>> Thanks Brian
>>>
>>>
>>> From: John Tedona [mailto:jtedona@neology.net]
>>> Sent: Monday, December 9, 2019 4:55 PM
>>> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Slater, James (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Alex,
>>>
>>> I can be available most anytime tomorrow for a call.
>>>
>>>
>>> Regards,

>>>
>>> John Tedona
>>> PIPS TECHNOLOGY - A Neology Business
>>> Sales Manager
>>> 12760 Danielson Ct. Suite A
>>> Poway, CA 92064
>>> Phone: 201-841-6237
>>> Email: jtedona@neology.net<mailto:jtedona@neology.net>
>>> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
>>> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
>>> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
>>> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
>>> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ
>>> U2sB_fmM6g&e=>
>>>
>>>
>>> From: Chute, Alexander
>>> <AChute@massport.com<mailto:AChute@massport.com>>
>>> Sent: Monday, December 9, 2019 4:38 PM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>
>>> Cc: Guerriero, Robert (MASSIT)
>>> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
>>> Peek, Brian T. (EOTSS)
>>> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
>>> Slater III, James F (CHS)
>>> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>>>
>>> Hello All,
>>>
>>> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>>>
>>> Respectfully,
>>>
>>> ~Alex
>>>
>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>>

>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Monday, November 18, 2019 3:26 PM
>>> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
>>> pcrary@neology.net<mailto:pcrary@neology.net>
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi John, Peter
>>>
>>> Any issues with moving Massports cameras to the Chelsea DB?
>>>
>>> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>>>
>>> The current app server
>>> <image008.png>
>>>
>>> Current DB server
>>>
>>> <image009.png>
>>> <image010.png>
>>>
>>> Our current reads by month for about [redacted]
>>>
>>> Year
>>>
>>> Month
>>>
>>> Day
>>>
>>> Month Name
>>>
>>> Reads Count
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 1
>>>
>>> November
>>>
>>>   495,113
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 2

>>>
>>> November
>>>
>>> 472,907
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 3
>>>
>>> November
>>>
>>> 384,409
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 4
>>>
>>> November
>>>
>>> 411,440
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 5
>>>
>>> November
>>>
>>> 434,085
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 6
>>>
>>> November
>>>
>>> 495,537
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 7
>>>
>>> November
>>>
>>> 444,123
>>>
>>> 2019
>>>

>>> 11
>>>
>>> 8
>>>
>>> November
>>>
>>> 542,492
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 9
>>>
>>> November
>>>
>>> 443,463
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 10
>>>
>>> November
>>>
>>> 389,514
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 11
>>>
>>> November
>>>
>>> 362,548
>>>
>>> 2019
>>>
>>> 11
>>>
>>> 12
>>>
>>> November
>>>
>>> 236,539
>>>
>>>
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Wednesday, November 13, 2019 2:49 PM
>>> To: Egnitz, Brian (POL)
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)

>>> Subject: RE: MassPort LPR Cameras
>>>
>>> These stats are from the [redacted] we have in the system for this month:
>>>
>>> <image011.png>
>>>
>>> ~Alex
>>>
>>>
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Tuesday, November 12, 2019 5:28 PM
>>> To: Chute, Alexander
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>>
>>> Hi Alex,
>>>
>>> Can you please provide the updated reads per day? Previously you were interested in sharing [redacted] at approximately 75,000 reads per day.
>>>
>>> Here is the [redacted] confi I mentioned.
>>>
>>> Set host to boss [redacted]
>>> Set image [redacted]
>>> Set number of [redacted]
>>> Set Ping [redacted]
>>> Set udp ping [redacted]
>>> Set ping [redacted]
>>> Set security [redacted]
>>>
>>> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
>>> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>>>
>>> -Brian
>>>
>>>
>>>
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Tuesday, November 12, 2019 2:08 PM
>>> To: Egnitz, Brian (POL)
>>> Subject: MassPort LPR Cameras
>>>
>>> Brian,
>>>
>>> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to approximately [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.
>>>

>>> Respectfully,
>>>
>>> ~Alex
>>>
>>> <image007.png>
>>>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>>

From: Egnitz, Brian (POL)
To: Silva, Kyra (POL)
Subject: Re: MassPort LPR Cameras
Date: Thursday, April 16, 2020 3:15:03 PM

Not that I'm aware of, its our understanding that we submit them to the LTC. , then it goes over to Michelle and then IT. We've done tickets in the past but then were advised that the proper channel is a to/from through the chain.

Thanks, Brian

> On Apr 16, 2020, at 3:02 PM, Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us> wrote:
>
> Hi,
>
> Checking on this and will advise. Was the request submitted to IT?
>
> -----Original Message-----
> From: Egnitz, Brian (POL)
> Sent: Thursday, April 09, 2020 4:06 PM
> To: Silva, Kyra (POL)
> Subject: FW: MassPort LPR Cameras
>
> Hi Kyra,
>
> Can you please see below and attached. Let me know if you have any questions.
>
> Thanks, Brian
>
> -----Original Message-----
> From: Quinn, Dermot (POL)
> Sent: Thursday, April 9, 2020 2:00 PM
> To: Egnitz, Brian (POL)
> Cc: Warren, Rosemary (POL)
> Subject: RE: MassPort LPR Cameras
>
> This is to allow the Massport ALPR cameras to write to thestate ALPR server in Chelsea. Approved at DHS. Please forward to Kyra Silva in Fiscal for funding.
>
>
> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division of Homeland Security & Preparedness Massachusetts State Police
>
>
>
>
>
> -----Original Message-----
> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> Sent: Thursday, April 9, 2020 1:58 PM
> To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
> Subject: RE: MassPort LPR Cameras
>
> Do you know if this was moved on? We need it for the MassPort modem project.
>
> -----Original Message-----

> From: Egnitz, Brian (POL)
> Sent: Tuesday, March 10, 2020 10:52 AM
> To: Quinn, Dermot (POL)
> Subject: FW: MassPort LPR Cameras
>
> Hi LTC.,
>
> Can we order this equipment for the MassPort project?
>
> Thanks, Brian
>
> -----Original Message-----
> From: Slater, James (CHS)
> Sent: Tuesday, March 10, 2020 10:26 AM
> To: Egnitz, Brian (POL)
> Subject: RE: MassPort LPR Cameras
>
> Hi, Brian!
>
> This needs to go through MSP fiscal. They need to enter the purchase in OPAS.
>
> Jim
>
> -----Original Message-----
> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> Sent: Tuesday, March 10, 2020 08:06
> To: Slater, James (CHS) <james.slater@mass.gov>
> Subject: RE: MassPort LPR Cameras
>
> Is this something you can order or does it need to go through MSP?
>
> -----Original Message-----
> From: Slater, James (CHS)
> Sent: Monday, March 9, 2020 10:36 AM
> To: Egnitz, Brian (POL)
> Subject: RE: MassPort LPR Cameras
>
> Thanks, Brian...I will check with TSS.
>
> Jim
>
> -----Original Message-----
> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> Sent: Monday, March 9, 2020 10:29
> To: Slater, James (CHS) <james.slater@mass.gov>
> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
> Subject: RE: MassPort LPR Cameras
>
> Thanks Jim,
>
> I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need [redacted] wireless AC adapters and [redacted] I have reached out to BCM for a quote.
>
> I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.
>

> I plan to cut one sector ([redacted] over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?
>
> -Brian
>
> -----Original Message-----
> From: Slater, James (CHS)
> Sent: Friday, March 6, 2020 1:43 PM
> To: Egnitz, Brian (POL)
> Cc: Quinn, Dermot (POL)
> Subject: RE: MassPort LPR Cameras
>
> Hi, Brian!
>
> I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.
>
> So, assuming you move forward with this, who would actually make this happen?
>
> Thanks.
>
> Jim
>
> -----Original Message-----
> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> Sent: Wednesday, March 4, 2020 17:53
> To: Slater, James (CHS) <james.slater@mass.gov>
> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
> Subject: Re: MassPort LPR Cameras
>
> Hi Jim,
>
> Regarding the Massport cameras; in the early days of AVL we installed [redacted] modem's in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don't we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn't have to do any firewall work either because they have a 166. and communicate like all of the MDT's . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.
>
> We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.
>
> Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.
>
>> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>>
>> Thank you sir
>>
>> Major Charles W. Atchison III
>> Troop F Commander
>> Massachusetts State Police
>> Director of Aviation Security
>> 2 Service Road
>> East Boston, Ma 02128

>> Office: 617-568-7555
>> Cell: 508-[redacted]
>>
>>
>> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>>
>> All,
>> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>>
>> Thanks
>>
>> CW
>>
>> From: Quinn, Dermot (POL)
>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
>> Sent: Monday, February 10, 2020 10:31 AM
>> To: Egnitz, Brian (POL)
>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
>> Slater, James (CHS)
>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
>> Robert (EOTSS)
>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
>> Warmington, Scott (POL)
>> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
>> .us>>; Peek, Brian T. (EOTSS)
>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>> Timothy (EPS)
>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
>> Michalski, Maria (EPS)
>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
>> Christopher (POL)
>> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
>> Hughes, Sean M. (EOTSS)
>> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
>> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
>> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
>> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
>> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
>> Atchison, Charles (POL)
>> <catchison@massport.com<mailto:catchison@massport.com>>
>> Subject: RE: MassPort LPR Cameras
>>
>> Good Morning,
>>
>> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>>
>> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so

that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>>
>> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>>
>> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>>
>> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>>
>> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>>
>> I can’t overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security’s technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>>
>> Respectfully,
>>
>>
>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
>> of Homeland Security & Preparedness Massachusetts State Police
>> <image006.png>
>>
>>
>>
>>
>> From: Egnitz, Brian (POL)
>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
>> Sent: Friday, January 17, 2020 1:10 PM
>> To: Slater, James (CHS)
>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
>> Cc: Quinn, Dermot (POL)
>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
>> Guerriero, Robert (EOTSS)
>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
>> Brian T. (EOTSS)
>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>> Timothy (EPS)
>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
>> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
>> Maria (EPS)

>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi Jim,
>>
>> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>>
>> -Brian
>>
>>
>> From: Egnitz, Brian (POL)
>> Sent: Monday, January 6, 2020 1:33 PM
>> To: Slater, James (CHS)
>> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
>> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
>> Crary
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi Jim,
>>
>> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>>
>> Thanks Brian
>>
>>
>> From: John Tedona [mailto:jtedona@neology.net]
>> Sent: Monday, December 9, 2019 4:55 PM
>> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>> Timothy (EPS); Slater, James (CHS)
>> Subject: RE: MassPort LPR Cameras
>>
>> Alex,
>>
>> I can be available most anytime tomorrow for a call.
>>
>>
>> Regards,
>>
>> John Tedona
>> PIPS TECHNOLOGY - A Neology Business
>> Sales Manager
>> 12760 Danielson Ct. Suite A
>> Poway, CA 92064
>> Phone: 201-841-6237
>> Email: jtedona@neology.net<mailto:jtedona@neology.net>
>> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
>> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
>> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
>> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
>> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ

>> U2sB_fmM6g&e=>
>>
>>
>> From: Chute, Alexander
>> <AChute@massport.com<mailto:AChute@massport.com>>
>> Sent: Monday, December 9, 2019 4:38 PM
>> To: Egnitz, Brian (POL)
>> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
>> <pcrary@neology.net<mailto:pcrary@neology.net>>
>> Cc: Guerriero, Robert (MASSIT)
>> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
>> Peek, Brian T. (EOTSS)
>> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
>> Timothy (EPS)
>> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
>> Slater III, James F (CHS)
>> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
>> Subject: RE: MassPort LPR Cameras
>>
>> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>>
>> Hello All,
>>
>> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>>
>> Respectfully,
>>
>> ~Alex
>>
>>
>> <image007.png>
>>
>> Alexander B. Chute
>> Program Manager, Public Safety Systems Massachusetts Port Authority
>> Cell: [redacted]
>> Office: 617.568.5942
>> achute@massport.com<mailto:achute@massport.com>
>>
>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>
>>
>>
>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>> Sent: Monday, November 18, 2019 3:26 PM
>> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
>> pcrary@neology.net<mailto:pcrary@neology.net>
>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)

>> Subject: RE: MassPort LPR Cameras
>>
>> Hi John, Peter
>>
>> Any issues with moving Massports cameras to the Chelsea DB?
>>
>> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>>
>> The current app server
>> <image008.png>
>>
>> Current DB server
>>
>> <image009.png>
>> <image010.png>
>>
>> Our current reads by month for about [redacted]
>>
>> Year
>>
>> Month
>>
>> Day
>>
>> Month Name
>>
>> Reads Count
>>
>> 2019
>>
>> 11
>>
>> 1
>>
>> November
>>
>> 495,113
>>
>> 2019
>>
>> 11
>>
>> 2
>>
>> November
>>
>> 472,907
>>
>> 2019
>>
>> 11
>>
>> 3
>>
>> November
>>
>> 384,409

>>
>> 2019
>>
>> 11
>>
>> 4
>>
>> November
>>
>> 411,440
>>
>> 2019
>>
>> 11
>>
>> 5
>>
>> November
>>
>> 434,085
>>
>> 2019
>>
>> 11
>>
>> 6
>>
>> November
>>
>> 495,537
>>
>> 2019
>>
>> 11
>>
>> 7
>>
>> November
>>
>> 444,123
>>
>> 2019
>>
>> 11
>>
>> 8
>>
>> November
>>
>> 542,492
>>
>> 2019
>>
>> 11
>>
>> 9
>>

>> November
>>
>> 443,463
>>
>> 2019
>>
>> 11
>>
>> 10
>>
>> November
>>
>> 389,514
>>
>> 2019
>>
>> 11
>>
>> 11
>>
>> November
>>
>> 362,548
>>
>> 2019
>>
>> 11
>>
>> 12
>>
>> November
>>
>> 236,539
>>
>>
>>
>>
>>
>> From: Chute, Alexander [mailto:AChute@massport.com]
>> Sent: Wednesday, November 13, 2019 2:49 PM
>> To: Egnitz, Brian (POL)
>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>> Timothy (EPS)
>> Subject: RE: MassPort LPR Cameras
>>
>> These stats are from the [redacted] we have in the system for this month:
>>
>> <image011.png>
>>
>> ~Alex
>>
>>
>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>> Sent: Tuesday, November 12, 2019 5:28 PM
>> To: Chute, Alexander
>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>> Timothy (EPS)

>> Subject: RE: MassPort LPR Cameras
>>
>> Hi Alex,
>>
>> Can you please provide the updated reads per day? Previously you were interested in sharing [redacted] at approximately 75,000 reads per day.
>>
>> Here is the [redacted] confi I mentioned.
>>
>> Set host to boss [redacted]
>> Set image [redacted]
>> Set number of [redacted]
>> Set Ping [redacted]
>> Set udp ping [redacted]
>> Set ping [redacted]
>> Set security [redacted]
>>
>> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
>> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>>
>> -Brian
>>
>>
>>
>> From: Chute, Alexander [mailto:AChute@massport.com]
>> Sent: Tuesday, November 12, 2019 2:08 PM
>> To: Egnitz, Brian (POL)
>> Subject: MassPort LPR Cameras
>>
>> Brian,
>>
>> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to approximately [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.
>>
>> Respectfully,
>>
>> ~Alex
>>
>> <image007.png>
>>
>> Alexander B. Chute
>> Program Manager, Public Safety Systems Massachusetts Port Authority
>> Cell: [redacted]
>> Office: 617.568.5942
>> achute@massport.com<mailto:achute@massport.com>
>>
>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts

15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>

From: brian.egnitz@pol.state.ma.us
To: Silva, Kyra (POL)
Subject: Re: MassPort LPR Cameras
Date: Thursday, April 16, 2020 3:15:01 PM

Not that I'm aware of, its our understanding that we submit them to the LTC. , then it goes over to Michelle and then IT. We've done tickets in the past but then were advised that the proper channel is a to/from through the chain.

Thanks, Brian

> On Apr 16, 2020, at 3:02 PM, Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us> wrote:
>
> Hi,
>
> Checking on this and will advise. Was the request submitted to IT?
>
> -----Original Message-----
> From: Egnitz, Brian (POL)
> Sent: Thursday, April 09, 2020 4:06 PM
> To: Silva, Kyra (POL)
> Subject: FW: MassPort LPR Cameras
>
> Hi Kyra,
>
> Can you please see below and attached. Let me know if you have any questions.
>
> Thanks, Brian
>
> -----Original Message-----
> From: Quinn, Dermot (POL)
> Sent: Thursday, April 9, 2020 2:00 PM
> To: Egnitz, Brian (POL)
> Cc: Warren, Rosemary (POL)
> Subject: RE: MassPort LPR Cameras
>
> This is to allow the Massport ALPR cameras to write to thestate ALPR server in Chelsea. Approved at DHS. Please forward to Kyra Silva in Fiscal for funding.
>
>
> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division of Homeland Security & Preparedness Massachusetts State Police
>
>
>
>
>
> -----Original Message-----
> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> Sent: Thursday, April 9, 2020 1:58 PM
> To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
> Subject: RE: MassPort LPR Cameras
>
> Do you know if this was moved on? We need it for the MassPort modem project.
>
> -----Original Message-----

> From: Egnitz, Brian (POL)
> Sent: Tuesday, March 10, 2020 10:52 AM
> To: Quinn, Dermot (POL)
> Subject: FW: MassPort LPR Cameras
>
> Hi LTC.,
>
> Can we order this equipment for the MassPort project?
>
> Thanks, Brian
>
> -----Original Message-----
> From: Slater, James (CHS)
> Sent: Tuesday, March 10, 2020 10:26 AM
> To: Egnitz, Brian (POL)
> Subject: RE: MassPort LPR Cameras
>
> Hi, Brian!
>
> This needs to go through MSP fiscal. They need to enter the purchase in OPAS.
>
> Jim
>
> -----Original Message-----
> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> Sent: Tuesday, March 10, 2020 08:06
> To: Slater, James (CHS) <james.slater@mass.gov>
> Subject: RE: MassPort LPR Cameras
>
> Is this something you can order or does it need to go through MSP?
>
> -----Original Message-----
> From: Slater, James (CHS)
> Sent: Monday, March 9, 2020 10:36 AM
> To: Egnitz, Brian (POL)
> Subject: RE: MassPort LPR Cameras
>
> Thanks, Brian...I will check with TSS.
>
> Jim
>
> -----Original Message-----
> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> Sent: Monday, March 9, 2020 10:29
> To: Slater, James (CHS) <james.slater@mass.gov>
> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
> Subject: RE: MassPort LPR Cameras
>
> Thanks Jim,
>
> I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need [redacted] wireless AC adapters and [redacted] I have reached out to BCM for a quote.
>
> I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.
>

> I plan to cut one sector ([redacted] over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?
>
> -Brian
>
> -----Original Message-----
> From: Slater, James (CHS)
> Sent: Friday, March 6, 2020 1:43 PM
> To: Egnitz, Brian (POL)
> Cc: Quinn, Dermot (POL)
> Subject: RE: MassPort LPR Cameras
>
> Hi, Brian!
>
> I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.
>
> So, assuming you move forward with this, who would actually make this happen?
>
> Thanks.
>
> Jim
>
> -----Original Message-----
> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> Sent: Wednesday, March 4, 2020 17:53
> To: Slater, James (CHS) <james.slater@mass.gov>
> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
> Subject: Re: MassPort LPR Cameras
>
> Hi Jim,
>
> Regarding the Massport cameras; in the early days of AVL we installed [redacted] modem's in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don't we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn't have to do any firewall work either because they have a 166. and communicate like all of the MDT's . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.
>
> We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.
>
> Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.
>
>> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>>
>> Thank you sir
>>
>> Major Charles W. Atchison III
>> Troop F Commander
>> Massachusetts State Police
>> Director of Aviation Security
>> 2 Service Road
>> East Boston, Ma 02128

>> Office: 617-568-7555
>> Cell: 508-[redacted]
>>
>>
>> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>>
>> All,
>> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>>
>> Thanks
>>
>> CW
>>
>> From: Quinn, Dermot (POL)
>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
>> Sent: Monday, February 10, 2020 10:31 AM
>> To: Egnitz, Brian (POL)
>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
>> Slater, James (CHS)
>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
>> Robert (EOTSS)
>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
>> Warmington, Scott (POL)
>> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
>> .us>>; Peek, Brian T. (EOTSS)
>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>> Timothy (EPS)
>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
>> Michalski, Maria (EPS)
>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
>> Christopher (POL)
>> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
>> Hughes, Sean M. (EOTSS)
>> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
>> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
>> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
>> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
>> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
>> Atchison, Charles (POL)
>> <catchison@massport.com<mailto:catchison@massport.com>>
>> Subject: RE: MassPort LPR Cameras
>>
>> Good Morning,
>>
>> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>>
>> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so

that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>>
>> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>>
>> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>>
>> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>>
>> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>>
>> I can’t overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security’s technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>>
>> Respectfully,
>>
>>
>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
>> of Homeland Security & Preparedness Massachusetts State Police
>> <image006.png>
>>
>>
>>
>>
>> From: Egnitz, Brian (POL)
>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
>> Sent: Friday, January 17, 2020 1:10 PM
>> To: Slater, James (CHS)
>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
>> Cc: Quinn, Dermot (POL)
>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
>> Guerriero, Robert (EOTSS)
>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
>> Brian T. (EOTSS)
>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>> Timothy (EPS)
>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
>> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
>> Maria (EPS)

>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi Jim,
>>
>> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>>
>> -Brian
>>
>>
>> From: Egnitz, Brian (POL)
>> Sent: Monday, January 6, 2020 1:33 PM
>> To: Slater, James (CHS)
>> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
>> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
>> Crary
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi Jim,
>>
>> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>>
>> Thanks Brian
>>
>>
>> From: John Tedona [mailto:jtedona@neology.net]
>> Sent: Monday, December 9, 2019 4:55 PM
>> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>> Timothy (EPS); Slater, James (CHS)
>> Subject: RE: MassPort LPR Cameras
>>
>> Alex,
>>
>> I can be available most anytime tomorrow for a call.
>>
>>
>> Regards,
>>
>> John Tedona
>> PIPS TECHNOLOGY - A Neology Business
>> Sales Manager
>> 12760 Danielson Ct. Suite A
>> Poway, CA 92064
>> Phone: 201-841-6237
>> Email: jtedona@neology.net<mailto:jtedona@neology.net>
>> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
>> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
>> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
>> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
>> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ

>> U2sB_fmM6g&e=>
>>
>>
>> From: Chute, Alexander
>> <AChute@massport.com<mailto:AChute@massport.com>>
>> Sent: Monday, December 9, 2019 4:38 PM
>> To: Egnitz, Brian (POL)
>> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
>> <pcrary@neology.net<mailto:pcrary@neology.net>>
>> Cc: Guerriero, Robert (MASSIT)
>> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
>> Peek, Brian T. (EOTSS)
>> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
>> Timothy (EPS)
>> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
>> Slater III, James F (CHS)
>> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
>> Subject: RE: MassPort LPR Cameras
>>
>> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>>
>> Hello All,
>>
>> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>>
>> Respectfully,
>>
>> ~Alex
>>
>>
>> <image007.png>
>>
>> Alexander B. Chute
>> Program Manager, Public Safety Systems Massachusetts Port Authority
>> Cell: [redacted]
>> Office: 617.568.5942
>> achute@massport.com<mailto:achute@massport.com>
>>
>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>
>>
>>
>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>> Sent: Monday, November 18, 2019 3:26 PM
>> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
>> pcrary@neology.net<mailto:pcrary@neology.net>
>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)

>> Subject: RE: MassPort LPR Cameras
>>
>> Hi John, Peter
>>
>> Any issues with moving Massports cameras to the Chelsea DB?
>>
>> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>>
>> The current app server
>> <image008.png>
>>
>> Current DB server
>>
>> <image009.png>
>> <image010.png>
>>
>> Our current reads by month for about [redacted]
>>
>> Year
>>
>> Month
>>
>> Day
>>
>> Month Name
>>
>> Reads Count
>>
>> 2019
>>
>> 11
>>
>> 1
>>
>> November
>>
>> 495,113
>>
>> 2019
>>
>> 11
>>
>> 2
>>
>> November
>>
>> 472,907
>>
>> 2019
>>
>> 11
>>
>> 3
>>
>> November
>>
>> 384,409

>>
>> 2019
>>
>> 11
>>
>> 4
>>
>> November
>>
>> 411,440
>>
>> 2019
>>
>> 11
>>
>> 5
>>
>> November
>>
>> 434,085
>>
>> 2019
>>
>> 11
>>
>> 6
>>
>> November
>>
>> 495,537
>>
>> 2019
>>
>> 11
>>
>> 7
>>
>> November
>>
>> 444,123
>>
>> 2019
>>
>> 11
>>
>> 8
>>
>> November
>>
>> 542,492
>>
>> 2019
>>
>> 11
>>
>> 9
>>

>> November
>>
>> 443,463
>>
>> 2019
>>
>> 11
>>
>> 10
>>
>> November
>>
>> 389,514
>>
>> 2019
>>
>> 11
>>
>> 11
>>
>> November
>>
>> 362,548
>>
>> 2019
>>
>> 11
>>
>> 12
>>
>> November
>>
>> 236,539
>>
>>
>>
>>
>>
>> From: Chute, Alexander [mailto:AChute@massport.com]
>> Sent: Wednesday, November 13, 2019 2:49 PM
>> To: Egnitz, Brian (POL)
>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>> Timothy (EPS)
>> Subject: RE: MassPort LPR Cameras
>>
>> These stats are from the [redacted] we have in the system for this month:
>>
>> <image011.png>
>>
>> ~Alex
>>
>>
>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>> Sent: Tuesday, November 12, 2019 5:28 PM
>> To: Chute, Alexander
>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>> Timothy (EPS)

>> Subject: RE: MassPort LPR Cameras
>>
>> Hi Alex,
>>
>> Can you please provide the updated reads per day? Previously you were interested in sharing [redacted] at approximately 75,000 reads per day.
>>
>> Here is the [redacted] confi I mentioned.
>>
>> Set host to boss [redacted]
>> Set image [redacted]
>> Set number of [redacted]
>> Set Ping [redacted]
>> Set udp ping [redacted]
>> Set ping [redacted]
>> Set security [redacted]
>>
>> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
>> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>>
>> -Brian
>>
>>
>>
>> From: Chute, Alexander [mailto:AChute@massport.com]
>> Sent: Tuesday, November 12, 2019 2:08 PM
>> To: Egnitz, Brian (POL)
>> Subject: MassPort LPR Cameras
>>
>> Brian,
>>
>> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to approximately [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.
>>
>> Respectfully,
>>
>> ~Alex
>>
>> <image007.png>
>>
>> Alexander B. Chute
>> Program Manager, Public Safety Systems Massachusetts Port Authority
>> Cell: [redacted]
>> Office: 617.568.5942
>> achute@massport.com<mailto:achute@massport.com>
>>
>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts

15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>

From: Warmington, Scott (POL)
To: Quinn, Dermot (POL)
Cc: Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Mason, Christopher (POL); Egnitz, Brian (POL); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL)
Subject: Re: MassPort LPR Cameras
Date: Tuesday, March 10, 2020 11:36:13 AM

What is the cost?

Sent from my iPhone

> On Mar 10, 2020, at 11:28 AM, Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us> wrote:
>
> Michelle and Kyra,
>
> This purchase request is for equipment to allow Mass Port Sierra Wireless modems to communicate directly with the existing ALPR Boss server in Chelsea. This is the fastest way to bring the Massport LPR cameras on line. EOTSS and EOPSS are OK with this solution as is Major Deb Ryan, the CO at Troop F.
>
> As you can see from the thread, this has been going on for some time. I think we can close it out with this small purchase.
>
> This does not resolve the replacement of the existing ALPR equipment that we discussed at Command Staff yesterday. That is a different issue.
>
> Thanks
>
>
> Lieutenant Colonel Dermot J. Quinn #1765
> Division Commander
> Division of Homeland Security & Preparedness
> Massachusetts State Police
>
>
>
>
>
> -----Original Message-----
> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> Sent: Tuesday, March 10, 2020 10:52 AM
> To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
> Subject: FW: MassPort LPR Cameras
>
> Hi LTC.,
>
> Can we order this equipment for the MassPort project?
>
> Thanks, Brian
>
> -----Original Message-----
> From: Slater, James (CHS)
> Sent: Tuesday, March 10, 2020 10:26 AM
> To: Egnitz, Brian (POL)
> Subject: RE: MassPort LPR Cameras
>
> Hi, Brian!

>
> This needs to go through MSP fiscal. They need to enter the purchase in OPAS.
>
> Jim
>
> -----Original Message-----
> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> Sent: Tuesday, March 10, 2020 08:06
> To: Slater, James (CHS) <james.slater@mass.gov>
> Subject: RE: MassPort LPR Cameras
>
> Is this something you can order or does it need to go through MSP?
>
> -----Original Message-----
> From: Slater, James (CHS)
> Sent: Monday, March 9, 2020 10:36 AM
> To: Egnitz, Brian (POL)
> Subject: RE: MassPort LPR Cameras
>
> Thanks, Brian...I will check with TSS.
>
> Jim
>
> -----Original Message-----
> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> Sent: Monday, March 9, 2020 10:29
> To: Slater, James (CHS) <james.slater@mass.gov>
> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
> Subject: RE: MassPort LPR Cameras
>
> Thanks Jim,
>
> I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need [redacted] wireless AC adapters and [redacted] I have reached out to BCM for a quote.
>
> I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.
>
> I plan to cut one sector ([redacted]) over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?
>
> -Brian
>
> -----Original Message-----
> From: Slater, James (CHS)
> Sent: Friday, March 6, 2020 1:43 PM
> To: Egnitz, Brian (POL)
> Cc: Quinn, Dermot (POL)
> Subject: RE: MassPort LPR Cameras
>
> Hi, Brian!
>
> I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.
>

> So, assuming you move forward with this, who would actually make this happen?
>
> Thanks.
>
> Jim
>
> -----Original Message-----
> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> Sent: Wednesday, March 4, 2020 17:53
> To: Slater, James (CHS) <james.slater@mass.gov>
> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
> Subject: Re: MassPort LPR Cameras
>
> Hi Jim,
>
> Regarding the Massport cameras; in the early days of AVL we installed [redacted] modem's in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don't we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn't have to do any firewall work either because they have a 166. and communicate like all of the MDT's . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.
>
> We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.
>
> Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.
>
>> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>>
>> Thank you sir
>>
>> Major Charles W. Atchison III
>> Troop F Commander
>> Massachusetts State Police
>> Director of Aviation Security
>> 2 Service Road
>> East Boston, Ma 02128
>> Office: 617-568-7555
>> Cell: 508-[redacted]
>>
>>
>> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>>
>> All,
>> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>>
>> Thanks
>>
>> CW
>>
>> From: Quinn, Dermot (POL)
>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
>> Sent: Monday, February 10, 2020 10:31 AM

>> To: Egnitz, Brian (POL)
>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
>> Slater, James (CHS)
>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
>> Robert (EOTSS)
>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
>> Warmington, Scott (POL)
>> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
>> .us>>; Peek, Brian T. (EOTSS)
>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>> Timothy (EPS)
>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
>> Michalski, Maria (EPS)
>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
>> Christopher (POL)
>> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
>> Hughes, Sean M. (EOTSS)
>> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
>> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
>> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
>> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
>> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
>> Atchison, Charles (POL)
>> <catchison@massport.com<mailto:catchison@massport.com>>
>> Subject: RE: MassPort LPR Cameras
>>
>> Good Morning,
>>
>> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>>
>> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>>
>> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>>
>> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>>
>> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.

>>
>> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>>
>> I can't overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security's technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>>
>> Respectfully,
>>
>>
>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
>> of Homeland Security & Preparedness Massachusetts State Police
>> <image006.png>
>>
>>
>>
>>
>> From: Egnitz, Brian (POL)
>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
>> Sent: Friday, January 17, 2020 1:10 PM
>> To: Slater, James (CHS)
>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
>> Cc: Quinn, Dermot (POL)
>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
>> Guerriero, Robert (EOTSS)
>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
>> Brian T. (EOTSS)
>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>> Timothy (EPS)
>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
>> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
>> Maria (EPS)
>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi Jim,
>>
>> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>>
>> -Brian
>>
>>
>> From: Egnitz, Brian (POL)
>> Sent: Monday, January 6, 2020 1:33 PM
>> To: Slater, James (CHS)
>> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
>> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
>> Crary
>> Subject: RE: MassPort LPR Cameras

>>
>> Hi Jim,
>>
>> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>>
>> Thanks Brian
>>
>>
>> From: John Tedona [mailto:jtedona@neology.net]
>> Sent: Monday, December 9, 2019 4:55 PM
>> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>> Timothy (EPS); Slater, James (CHS)
>> Subject: RE: MassPort LPR Cameras
>>
>> Alex,
>>
>> I can be available most anytime tomorrow for a call.
>>
>>
>> Regards,
>>
>> John Tedona
>> PIPS TECHNOLOGY - A Neology Business
>> Sales Manager
>> 12760 Danielson Ct. Suite A
>> Poway, CA 92064
>> Phone: 201-841-6237
>> Email: jtedona@neology.net<mailto:jtedona@neology.net>
>> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
>> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
>> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
>> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
>> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ
>> U2sB_fmM6g&e=>
>>
>>
>> From: Chute, Alexander
>> <AChute@massport.com<mailto:AChute@massport.com>>
>> Sent: Monday, December 9, 2019 4:38 PM
>> To: Egnitz, Brian (POL)
>> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
>> <pcrary@neology.net<mailto:pcrary@neology.net>>
>> Cc: Guerriero, Robert (MASSIT)
>> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
>> Peek, Brian T. (EOTSS)
>> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
>> Timothy (EPS)
>> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
>> Slater III, James F (CHS)
>> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>

>> Subject: RE: MassPort LPR Cameras
>>
>> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>>
>> Hello All,
>>
>> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>>
>> Respectfully,
>>
>> ~Alex
>>
>>
>> <image007.png>
>>
>> Alexander B. Chute
>> Program Manager, Public Safety Systems Massachusetts Port Authority
>> Cell: [redacted]
>> Office: 617.568.5942
>> achute@massport.com<mailto:achute@massport.com>
>>
>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>
>>
>>
>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>> Sent: Monday, November 18, 2019 3:26 PM
>> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
>> pcrary@neology.net<mailto:pcrary@neology.net>
>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi John, Peter
>>
>> Any issues with moving Massports cameras to the Chelsea DB?
>>
>> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>>
>> The current app server
>> <image008.png>
>>
>> Current DB server
>>
>> <image009.png>
>> <image010.png>
>>
>> Our current reads by month for about [redacted]
>>

>> Year
>>
>> Month
>>
>> Day
>>
>> Month Name
>>
>> Reads Count
>>
>> 2019
>>
>> 11
>>
>> 1
>>
>> November
>>
>> 495,113
>>
>> 2019
>>
>> 11
>>
>> 2
>>
>> November
>>
>> 472,907
>>
>> 2019
>>
>> 11
>>
>> 3
>>
>> November
>>
>> 384,409
>>
>> 2019
>>
>> 11
>>
>> 4
>>
>> November
>>
>> 411,440
>>
>> 2019
>>
>> 11
>>
>> 5
>>
>> November

>>
>> 434,085
>>
>> 2019
>>
>> 11
>>
>> 6
>>
>> November
>>
>> 495,537
>>
>> 2019
>>
>> 11
>>
>> 7
>>
>> November
>>
>> 444,123
>>
>> 2019
>>
>> 11
>>
>> 8
>>
>> November
>>
>> 542,492
>>
>> 2019
>>
>> 11
>>
>> 9
>>
>> November
>>
>> 443,463
>>
>> 2019
>>
>> 11
>>
>> 10
>>
>> November
>>
>> 389,514
>>
>> 2019
>>
>> 11
>>

>> 11
>>
>> November
>>
>> 362,548
>>
>> 2019
>>
>> 11
>>
>> 12
>>
>> November
>>
>> 236,539
>>
>>
>>
>>
>>
>> From: Chute, Alexander [mailto:AChute@massport.com]
>> Sent: Wednesday, November 13, 2019 2:49 PM
>> To: Egnitz, Brian (POL)
>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>> Timothy (EPS)
>> Subject: RE: MassPort LPR Cameras
>>
>> These stats are from the [redacted] we have in the system for this month:
>>
>> <image011.png>
>>
>> ~Alex
>>
>>
>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>> Sent: Tuesday, November 12, 2019 5:28 PM
>> To: Chute, Alexander
>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>> Timothy (EPS)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi Alex,
>>
>> Can you please provide the updated reads per day? Previously you were interested in sharing [redacted] at approximately 75,000 reads per day.
>>
>> Here is the [redacted] confi I mentioned.
>>
>> Set host to boss [redacted]
>> Set image [redacted]
>> Set number of [redacted]
>> Set Ping [redacted]
>> Set udp ping [redacted]
>> Set ping [redacted]
>> Set security [redacted]
>>
>> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next

week.
>> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>>
>> -Brian
>>
>>
>>
>> From: Chute, Alexander [mailto:AChute@massport.com]
>> Sent: Tuesday, November 12, 2019 2:08 PM
>> To: Egnitz, Brian (POL)
>> Subject: MassPort LPR Cameras
>>
>> Brian,
>>
>> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to approximately [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.
>>
>> Respectfully,
>>
>> ~Alex
>>
>> <image007.png>
>>
>> Alexander B. Chute
>> Program Manager, Public Safety Systems Massachusetts Port Authority
>> Cell: [redacted]
>> Office: 617.568.5942
>> achute@massport.com<mailto:achute@massport.com>
>>
>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>
> <SierraQuoteForMassPort.pdf>

From: Scott.Warmington@pol.state.ma.us
To: Quinn, Dermot (POL)
Cc: Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Mason, Christopher (POL); Egnitz, Brian (POL); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL)
Subject: Re: MassPort LPR Cameras
Date: Tuesday, March 10, 2020 11:36:12 AM

What is the cost?

Sent from my iPhone

> On Mar 10, 2020, at 11:28 AM, Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us> wrote:
>
> Michelle and Kyra,
>
> This purchase request is for equipment to allow Mass Port Sierra Wireless modems to communicate directly with the existing ALPR Boss server in Chelsea. This is the fastest way to bring the Massport LPR cameras on line. EOTSS and EOPSS are OK with this solution as is Major Deb Ryan, the CO at Troop F.
>
> As you can see from the thread, this has been going on for some time. I think we can close it out with this small purchase.
>
> This does not resolve the replacement of the existing ALPR equipment that we discussed at Command Staff yesterday. That is a different issue.
>
> Thanks
>
>
> Lieutenant Colonel Dermot J. Quinn #1765
> Division Commander
> Division of Homeland Security & Preparedness
> Massachusetts State Police
>
>
>
>
>
> -----Original Message-----
> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> Sent: Tuesday, March 10, 2020 10:52 AM
> To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
> Subject: FW: MassPort LPR Cameras
>
> Hi LTC.,
>
> Can we order this equipment for the MassPort project?
>
> Thanks, Brian
>
> -----Original Message-----
> From: Slater, James (CHS)
> Sent: Tuesday, March 10, 2020 10:26 AM
> To: Egnitz, Brian (POL)
> Subject: RE: MassPort LPR Cameras
>
> Hi, Brian!

>
> This needs to go through MSP fiscal. They need to enter the purchase in OPAS.
>
> Jim
>
> -----Original Message-----
> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> Sent: Tuesday, March 10, 2020 08:06
> To: Slater, James (CHS) <james.slater@mass.gov>
> Subject: RE: MassPort LPR Cameras
>
> Is this something you can order or does it need to go through MSP?
>
> -----Original Message-----
> From: Slater, James (CHS)
> Sent: Monday, March 9, 2020 10:36 AM
> To: Egnitz, Brian (POL)
> Subject: RE: MassPort LPR Cameras
>
> Thanks, Brian...I will check with TSS.
>
> Jim
>
> -----Original Message-----
> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> Sent: Monday, March 9, 2020 10:29
> To: Slater, James (CHS) <james.slater@mass.gov>
> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
> Subject: RE: MassPort LPR Cameras
>
> Thanks Jim,
>
> I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need [redacted] wireless AC adapters and [redacted] I have reached out to BCM for a quote.
>
> I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.
>
> I plan to cut one sector ([redacted] over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?
>
> -Brian
>
> -----Original Message-----
> From: Slater, James (CHS)
> Sent: Friday, March 6, 2020 1:43 PM
> To: Egnitz, Brian (POL)
> Cc: Quinn, Dermot (POL)
> Subject: RE: MassPort LPR Cameras
>
> Hi, Brian!
>
> I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.
>

> So, assuming you move forward with this, who would actually make this happen?
>
> Thanks.
>
> Jim
>
> -----Original Message-----
> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
> Sent: Wednesday, March 4, 2020 17:53
> To: Slater, James (CHS) <james.slater@mass.gov>
> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
> Subject: Re: MassPort LPR Cameras
>
> Hi Jim,
>
> Regarding the Massport cameras; in the early days of AVL we installed [G.L. c. 4.sec. 7.cl.26 (n)(security)] modem's in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don't we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn't have to do any firewall work either because they have a 166. and communicate like all of the MDT's . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.
>
> We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.
>
> Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.
>
>> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>>
>> Thank you sir
>>
>> Major Charles W. Atchison III
>> Troop F Commander
>> Massachusetts State Police
>> Director of Aviation Security
>> 2 Service Road
>> East Boston, Ma 02128
>> Office: 617-568-7555
>> Cell: 508-[G.L. c. 4.sec. 7.cl.26]
>>
>>
>> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>>
>> All,
>> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>>
>> Thanks
>>
>> CW
>>
>> From: Quinn, Dermot (POL)
>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
>> Sent: Monday, February 10, 2020 10:31 AM

>> To: Egnitz, Brian (POL)
>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
>> Slater, James (CHS)
>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
>> Robert (EOTSS)
>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
>> Warmington, Scott (POL)
>> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
>> .us>>; Peek, Brian T. (EOTSS)
>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>> Timothy (EPS)
>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
>> Michalski, Maria (EPS)
>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
>> Christopher (POL)
>> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
>> Hughes, Sean M. (EOTSS)
>> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
>> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
>> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
>> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
>> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
>> Atchison, Charles (POL)
>> <catchison@massport.com<mailto:catchison@massport.com>>
>> Subject: RE: MassPort LPR Cameras
>>
>> Good Morning,
>>
>> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>>
>> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>>
>> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>>
>> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>>
>> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.

>>
>> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>>
>> I can't overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security's technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>>
>> Respectfully,
>>
>>
>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
>> of Homeland Security & Preparedness Massachusetts State Police
>> <image006.png>
>>
>>
>>
>>
>> From: Egnitz, Brian (POL)
>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
>> Sent: Friday, January 17, 2020 1:10 PM
>> To: Slater, James (CHS)
>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
>> Cc: Quinn, Dermot (POL)
>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
>> Guerriero, Robert (EOTSS)
>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
>> Brian T. (EOTSS)
>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>> Timothy (EPS)
>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
>> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
>> Maria (EPS)
>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi Jim,
>>
>> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>>
>> -Brian
>>
>>
>> From: Egnitz, Brian (POL)
>> Sent: Monday, January 6, 2020 1:33 PM
>> To: Slater, James (CHS)
>> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
>> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
>> Crary
>> Subject: RE: MassPort LPR Cameras

>>
>> Hi Jim,
>>
>> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>>
>> Thanks Brian
>>
>>
>> From: John Tedona [mailto:jtedona@neology.net]
>> Sent: Monday, December 9, 2019 4:55 PM
>> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>> Timothy (EPS); Slater, James (CHS)
>> Subject: RE: MassPort LPR Cameras
>>
>> Alex,
>>
>> I can be available most anytime tomorrow for a call.
>>
>>
>> Regards,
>>
>> John Tedona
>> PIPS TECHNOLOGY - A Neology Business
>> Sales Manager
>> 12760 Danielson Ct. Suite A
>> Poway, CA 92064
>> Phone: 201-841-6237
>> Email: jtedona@neology.net<mailto:jtedona@neology.net>
>> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
>> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
>> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
>> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
>> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ
>> U2sB_fmM6g&e=>
>>
>>
>> From: Chute, Alexander
>> <AChute@massport.com<mailto:AChute@massport.com>>
>> Sent: Monday, December 9, 2019 4:38 PM
>> To: Egnitz, Brian (POL)
>> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John
>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
>> <pcrary@neology.net<mailto:pcrary@neology.net>>
>> Cc: Guerriero, Robert (MASSIT)
>> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
>> Peek, Brian T. (EOTSS)
>> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
>> Timothy (EPS)
>> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
>> Slater III, James F (CHS)
>> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>

>> Subject: RE: MassPort LPR Cameras
>>
>> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>>
>> Hello All,
>>
>> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>>
>> Respectfully,
>>
>> ~Alex
>>
>>
>> <image007.png>
>>
>> Alexander B. Chute
>> Program Manager, Public Safety Systems Massachusetts Port Authority
>> Cell: [redacted]
>> Office: 617.568.5942
>> achute@massport.com<mailto:achute@massport.com>
>>
>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>
>>
>>
>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>> Sent: Monday, November 18, 2019 3:26 PM
>> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
>> pcrary@neology.net<mailto:pcrary@neology.net>
>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi John, Peter
>>
>> Any issues with moving Massports cameras to the Chelsea DB?
>>
>> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>>
>> The current app server
>> <image008.png>
>>
>> Current DB server
>>
>> <image009.png>
>> <image010.png>
>>
>> Our current reads by month for about [redacted]
>>

>> Year
>>
>> Month
>>
>> Day
>>
>> Month Name
>>
>> Reads Count
>>
>> 2019
>>
>> 11
>>
>> 1
>>
>> November
>>
>> 495,113
>>
>> 2019
>>
>> 11
>>
>> 2
>>
>> November
>>
>> 472,907
>>
>> 2019
>>
>> 11
>>
>> 3
>>
>> November
>>
>> 384,409
>>
>> 2019
>>
>> 11
>>
>> 4
>>
>> November
>>
>> 411,440
>>
>> 2019
>>
>> 11
>>
>> 5
>>
>> November

>>
>> 434,085
>>
>> 2019
>>
>> 11
>>
>> 6
>>
>> November
>>
>> 495,537
>>
>> 2019
>>
>> 11
>>
>> 7
>>
>> November
>>
>> 444,123
>>
>> 2019
>>
>> 11
>>
>> 8
>>
>> November
>>
>> 542,492
>>
>> 2019
>>
>> 11
>>
>> 9
>>
>> November
>>
>> 443,463
>>
>> 2019
>>
>> 11
>>
>> 10
>>
>> November
>>
>> 389,514
>>
>> 2019
>>
>> 11
>>

>> 11
>>
>> November
>>
>> 362,548
>>
>> 2019
>>
>> 11
>>
>> 12
>>
>> November
>>
>> 236,539
>>
>>
>>
>>
>>
>> From: Chute, Alexander [mailto:AChute@massport.com]
>> Sent: Wednesday, November 13, 2019 2:49 PM
>> To: Egnitz, Brian (POL)
>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>> Timothy (EPS)
>> Subject: RE: MassPort LPR Cameras
>>
>> These stats are from the [redacted] we have in the system for this month:
>>
>> <image011.png>
>>
>> ~Alex
>>
>>
>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>> Sent: Tuesday, November 12, 2019 5:28 PM
>> To: Chute, Alexander
>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>> Timothy (EPS)
>> Subject: RE: MassPort LPR Cameras
>>
>> Hi Alex,
>>
>> Can you please provide the updated reads per day? Previously you were interested in sharing [redacted] at approximately 75,000 reads per day.
>>
>> Here is the [redacted] confi I mentioned.
>>
>> Set host to boss [redacted]
>> Set image [redacted]
>> Set number of [redacted]
>> Set Ping [redacted]
>> Set udp ping [redacted]
>> Set ping [redacted]
>> Set security [redacted]
>>
>> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next

week.
>> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>>
>> -Brian
>>
>>
>>
>> From: Chute, Alexander [mailto:AChute@massport.com]
>> Sent: Tuesday, November 12, 2019 2:08 PM
>> To: Egnitz, Brian (POL)
>> Subject: MassPort LPR Cameras
>>
>> Brian,
>>
>> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to approximately [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.
>>
>> Respectfully,
>>
>> ~Alex
>>
>> <image007.png>
>>
>> Alexander B. Chute
>> Program Manager, Public Safety Systems Massachusetts Port Authority
>> Cell: [redacted]
>> Office: 617.568.5942
>> achute@massport.com<mailto:achute@massport.com>
>>
>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>
> <SierraQuoteForMassPort.pdf>

From: Egnitz, Brian (POL)
To: Slater, James (CHS)
Cc: Quinn, Dermot (POL)
Subject: Re: MassPort LPR Cameras
Date: Wednesday, March 4, 2020 5:53:08 PM

Hi Jim,

Regarding the Massport cameras; in the early days of AVL we installed [redacted] modem's in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don't we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn't have to do any firewall work either because they have a 166. and communicate like all of the MDT's . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.

We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.

Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.

> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>
> Thank you sir
>
> Major Charles W. Atchison III
> Troop F Commander
> Massachusetts State Police
> Director of Aviation Security
> 2 Service Road
> East Boston, Ma 02128
> Office: 617-568-7555
> Cell: 508[redacted]s
>
>
> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT) <curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>
> All,
> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>
> Thanks
>
> CW
>
> From: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
> Sent: Monday, February 10, 2020 10:31 AM
> To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>; Slater, James (CHS) <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Warmington, Scott (POL) <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma.us>>; Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute, Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Michalski, Maria (EPS) <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason, Christopher (POL) <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>; Hughes, Sean M. (EOTSS) <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS) <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL) <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>; Atchison, Charles (POL) <catchison@massport.com<mailto:catchison@massport.com>>
> Subject: RE: MassPort LPR Cameras
>
> Good Morning,
>
> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>
> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>
> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as "BOSS" and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport's cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>
> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>
> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>
> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>
> I can't overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security's technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>
> Respectfully,
>
>
> Lieutenant Colonel Dermot J. Quinn #1765
> Division Commander
> Division of Homeland Security & Preparedness
> Massachusetts State Police
> <image006.png>
>
>
>
>
> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
> Sent: Friday, January 17, 2020 1:10 PM
> To: Slater, James (CHS) <james.slater@mass.gov<mailto:james.slater@mass.gov>>
> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>; Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute, Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski, Maria (EPS) <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
> Subject: RE: MassPort LPR Cameras
>
> Hi Jim,
>
> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>
> -Brian
>
>
> From: Egnitz, Brian (POL)
> Sent: Monday, January 6, 2020 1:33 PM
> To: Slater, James (CHS)
> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter Crary
> Subject: RE: MassPort LPR Cameras
>
> Hi Jim,
>
> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>
> Thanks Brian
>
>
> From: John Tedona [mailto:jtedona@neology.net]
> Sent: Monday, December 9, 2019 4:55 PM
> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); Slater, James (CHS)
> Subject: RE: MassPort LPR Cameras
>
> Alex,
>
> I can be available most anytime tomorrow for a call.
>
>
> Regards,
>
> John Tedona
> PIPS TECHNOLOGY - A Neology Business

> Sales Manager
> 12760 Danielson Ct. Suite A
> Poway, CA 92064
> Phone: 201-841-6237
> Email: jtedona@neology.net<mailto:jtedona@neology.net>
> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http-3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FNEWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJbaP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJU2sB_fmM6g&e=>
>
>
> From: Chute, Alexander <AChute@massport.com<mailto:AChute@massport.com>>
> Sent: Monday, December 9, 2019 4:38 PM
> To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary <pcrary@neology.net<mailto:pcrary@neology.net>>
> Cc: Guerriero, Robert (MASSIT) <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>; Peek, Brian T. (EOTSS) <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>; Slater III, James F (CHS) <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
> Subject: RE: MassPort LPR Cameras
>
> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>
> Hello All,
>
> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>
> Respectfully,
>
> ~Alex
>
>
> <image007.png>
>
> Alexander B. Chute
> Program Manager, Public Safety Systems
> Massachusetts Port Authority
> Cell: [redacted]
> Office: 617.568.5942
> achute@massport.com<mailto:achute@massport.com>
>
> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>
>
>
> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
> Sent: Monday, November 18, 2019 3:26 PM
> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>); pcrary@neology.net<mailto:pcrary@neology.net>
> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
> Subject: RE: MassPort LPR Cameras
>
> Hi John, Peter
>
> Any issues with moving Massports cameras to the Chelsea DB?
>
> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>
> The current app server
> <image008.png>
>
> Current DB server
>
> <image009.png>
> <image010.png>
>
> Our current reads by month for about [redacted]
>
> Year
>
> Month
>
> Day
>
> Month Name
>
> Reads Count
>
> 2019
>
> 11
>
> 1
>
> November
>
> 495,113
>
> 2019
>
> 11
>
> 2
>
> November
>
> 472,907
>
> 2019
>
> 11
>
> 3
>
> November
>
> 384,409
>
> 2019
>
> 11
>
> 4
>
> November
>
> 411,440
>
> 2019
>
> 11
>
> 5
>
> November
>
> 434,085
>
> 2019
>
> 11
>
> 6

>
> November
>
> 495,537
>
> 2019
>
> 11
>
> 7
>
> November
>
> 444,123
>
> 2019
>
> 11
>
> 8
>
> November
>
> 542,492
>
> 2019
>
> 11
>
> 9
>
> November
>
> 443,463
>
> 2019
>
> 11
>
> 10
>
> November
>
> 389,514
>
> 2019
>
> 11
>
> 11
>
> November
>
> 362,548
>
> 2019
>
> 11
>
> 12
>
> November
>
> 236,539
>
>
>
>
>
> From: Chute, Alexander [mailto:AChute@massport.com]
> Sent: Wednesday, November 13, 2019 2:49 PM
> To: Egnitz, Brian (POL)
> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
> Subject: RE: MassPort LPR Cameras
>
> These stats are from the G.L. c. 4.sec. 7.6 we have in the system for this month:
>
> <image011.png>
>
> ~Alex
>
>
> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
> Sent: Tuesday, November 12, 2019 5:28 PM
> To: Chute, Alexander
> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
> Subject: RE: MassPort LPR Cameras
>
> Hi Alex,
>
> Can you please provide the updated reads per day? Previously you were interested in sharing G.L. c. 4.s at approximately 75,000 reads per day.
>
> Here is the G.L. c confi I mentioned.
>
> Set host to boss G.L. c. 4.sec. 7
> Set image G.L. c. 4.s
> Set number of G.L. c. 4.sec
> Set Ping G.L. c. 4.sec
> Set udp ping G.L. c. 4.s
> Set ping G.L. c. 4.sec. 7.6
> Set security G.L. c. 4.
>
> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>
> -Brian
>
>
>
> From: Chute, Alexander [mailto:AChute@massport.com]
> Sent: Tuesday, November 12, 2019 2:08 PM
> To: Egnitz, Brian (POL)
> Subject: MassPort LPR Cameras
>
> Brian,
>
> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the G.L. c. 4.sec. 7.6. I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the G.L. c. 4.sec. 7.6 are fed to G.L. c. 4.s network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have G.L. c. 4.se in production, with another G.L. c. 4.sec to come online within the next two months. I anticipate this number growing to approximately G.L. c. 4.sec. 7.6 within our campus over the next year. Let me know what you think the appropriate next steps would be.
>
> Respectfully,
>
> ~Alex
>
> <image007.png>
>
> Alexander B. Chute
> Program Manager, Public Safety Systems
> Massachusetts Port Authority
> Cell: G.L. c. 4.sec
> Office: 617.568.3942

> achute@massport.com<mailto:achute@massport.com>
>
> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>

From: Chris.Mason@pol.state.ma.us
To: Wood, Curtis (EOTSS)
Subject: Re: MassPort LPR Cameras
Date: Tuesday, February 11, 2020 11:59:23 AM

Thank you.

Colonel Christopher Mason
Superintendent
Massachusetts State Police

On Feb 11, 2020, at 11:28 AM, Wood, Curtis (EOTSS) <curtis.wood@mass.gov> wrote:

All,
Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.

Thanks

CW

From: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Sent: Monday, February 10, 2020 10:31 AM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Slater, James (CHS) <james.slater@mass.gov>; Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>; Warmington, Scott (POL) <Scott.Warmington@pol.state.ma.us>; Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; John Tedona <jtedona@neology.net>; Chute, Alexander <AChute@massport.com>; Michalski, Maria (EPS) <maria.michalski@mass.gov>; Mason, Christopher (POL) <Chris.Mason@pol.state.ma.us>; Hughes, Sean M. (EOTSS) <sean.hughes@mass.gov>; Peter Crary <pcrary@neology.net>; Wood, Curtis (EOTSS) <curtis.wood@mass.gov>; Shaw, Harold <HShaw@massport.com>; Ball, Richard (POL) <Richard.Ball@pol.state.ma.us>; Atchison, Charles (POL) <catchison@massport.com>
Subject: RE: MassPort LPR Cameras

Good Morning,

I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged

with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.

Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.

Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as "BOSS" and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport's cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.

MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.

I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.

To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.

I can't overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security's technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.

Respectfully,

Lieutenant Colonel Dermot J. Quinn #1765
Division Commander
Division of Homeland Security & Preparedness
Massachusetts State Police
<image006.png>

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Friday, January 17, 2020 1:10 PM
To: Slater, James (CHS) <james.slater@mass.gov>
Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>; Guerriero, Robert (EOTSS) <Robert.Guerriero@mass.gov>; Peek, Brian T. (EOTSS) <Brian.T.Peek@mass.gov>; Mitchell, Timothy (EPS) <timothy.mitchell@mass.gov>; John Tedona <jtedona@neology.net>; Chute, Alexander <AChute@massport.com>; Peter Crary <pcrary@neology.net>; Michalski, Maria (EPS) <maria.michalski@mass.gov>
Subject: RE: MassPort LPR Cameras

Hi Jim,

BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.

-Brian

From: Egnitz, Brian (POL)
Sent: Monday, January 6, 2020 1:33 PM
To: Slater, James (CHS)
Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter Crary
Subject: RE: MassPort LPR Cameras

Hi Jim,

We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor

network and server impact. Are you available to discuss?

Thanks Brian

From: John Tedona [mailto:jtedona@neology.net]
Sent: Monday, December 9, 2019 4:55 PM
To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); Slater, James (CHS)
Subject: RE: MassPort LPR Cameras

Alex,

I can be available most anytime tomorrow for a call.

Regards,

John Tedona
PIPS TECHNOLOGY - A Neology Business
Sales Manager
12760 Danielson Ct. Suite A
Poway, CA 92064
Phone: 201-841-6237
Email: jtedona@neology.net
PIPS Support: support@pipstechnology.com 833-747-7577, Option 1 for sales, Option 2 for Support
www.pipstechnology.com

From: Chute, Alexander <AChute@massport.com>
Sent: Monday, December 9, 2019 4:38 PM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; John Tedona <jtedona@neology.net>; Peter Crary <pcrary@neology.net>
Cc: Guerriero, Robert (MASSIT) <robert.guerriero@state.ma.us>; Peek, Brian T. (EOTSS) <brian.t.peek@state.ma.us>; Mitchell, Timothy (EPS) <timothy.mitchell@state.ma.us>; Slater III, James F (CHS) <james.slater@state.ma.us>
Subject: RE: MassPort LPR Cameras

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Hello All,

I just wanted to follow up with this request to see what the next steps for this project

are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.

Respectfully,

~Alex

<image007.png>

Alexander B. Chute
Program Manager, Public Safety Systems
Massachusetts Port Authority
Cell: [redacted]
Office: 617.568.5942
achute@massport.com

WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Monday, November 18, 2019 3:26 PM
To: John Tedona (jtedona@neology.net); pcrary@neology.net
Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
Subject: RE: MassPort LPR Cameras

Hi John, Peter

Any issues with moving Massports cameras to the Chelsea DB?

Using the Boss calculator, I estimate that we would need 9-10 TB of storage.

The current app server
<image008.png>

Current DB server

<image009.png>

<image010.png>

Our current reads by month for about G.L. c. 4.sec. 7.cl.26 (n)(security)

Year	Month	Day	Month Name	Reads Count
2019	11	1	November	495,113
2019	11	2	November	472,907
2019	11	3	November	384,409
2019	11	4	November	411,440
2019	11	5	November	434,085
2019	11	6	November	495,537
2019	11	7	November	444,123
2019	11	8	November	542,492
2019	11	9	November	443,463
2019	11	10	November	389,514
2019	11	11	November	362,548
2019	11	12	November	236,539

From: Chute, Alexander [mailto:AChute@massport.com]
Sent: Wednesday, November 13, 2019 2:49 PM
To: Egnitz, Brian (POL)
Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
Subject: RE: MassPort LPR Cameras

These stats are from the G.L. c. 4.sec. 7.cl.26 (n)(security) we have in the system for this month:

<image011.png>

~Alex

From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
Sent: Tuesday, November 12, 2019 5:28 PM
To: Chute, Alexander
Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell, Timothy (EPS)
Subject: RE: MassPort LPR Cameras

Hi Alex,

Can you please provide the updated reads per day? Previously you were interested in sharing [redacted] at approximately 75,000 reads per day.

Here is the [redacted] confi I mentioned.

Set host to boss [redacted]
Set image [redacted]
Set number of [redacted]
Set Ping [redacted]
Set udp ping [redacted]
Set ping [redacted]
Set security [redacted]

I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.

-Brian

From: Chute, Alexander [mailto:AChute@massport.com]
Sent: Tuesday, November 12, 2019 2:08 PM
To: Egnitz, Brian (POL)
Subject: MassPort LPR Cameras

Brian,

Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations.

Currently we have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to approximately [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.

Respectfully,

~Alex

<image007.png>

Alexander B. Chute
Program Manager, Public Safety Systems
Massachusetts Port Authority
Cell: [redacted]
Office: 617.568.5942
achute@massport.com

WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

From: Ryan, Deborah (POL)
To: Egnitz, Brian (POL); Warmington, Scott (POL); Quinn, Dermot (POL)
Cc: Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Mason, Christopher (POL); Warren, Rosemary (POL); Shaw, Harold; Ball, Richard (POL); Crouse, David (POL)
Subject: Re: MassPort LPR Cameras
Date: Wednesday, August 19, 2020 10:42:17 AM

Nice work! Thank you!

Major Deborah A. Ryan, #1460
Troop F Commander
Massachusetts State Police
Director of Aviation Security
2 Service Road
East Boston, MA 02128

THIS EMAIL MAY CONTAIN INFORMATION FOR OFFICIAL USE ONLY AND LAW ENFORCEMENT SENSITIVE INFORMATION. This E-mail (including attachments) is covered by the Electronic Communications Privacy Act, 18 USC 2510-2521, is confidential and may be legally privileged. If you are not the intended recipient, you are hereby notified that any retention, dissemination, distribution, or copying of this communication is strictly prohibited and may be unlawful. Please reply to the sender that you have received the message in error and then delete the message and any attachments.

From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Sent: Tuesday, August 18, 2020 7:08 PM
To: Warmington, Scott (POL) <Scott.Warmington@pol.state.ma.us>; Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
Cc: Small, Michelle (POL) <Michelle.E.Small@pol.state.ma.us>; Silva, Kyra (POL) <Kyra.Silva@pol.state.ma.us>; Slater, James (CHS) <james.slater@mass.gov>; Mason, Christopher (POL) <Chris.Mason@pol.state.ma.us>; Warren, Rosemary (POL) <Rosemary.Warren@pol.state.ma.us>; Shaw, Harold <HShaw@massport.com>; Ryan, Deborah (POL) <Deborah.Ryan@pol.state.ma.us>; Ball, Richard (POL) <Richard.Ball@pol.state.ma.us>; Crouse, David (POL) <david.crouse@pol.state.ma.us>
Subject: Re: MassPort LPR Cameras

The Technical Service Unit and I have completed cutting over all of the Massport LPR cameras and they are reporting back to boss and Chelsea.

Brian

> On May 6, 2020, at 6:57 PM, Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us> wrote:
>
> Hi Sirs,
>
> We have begun cutting over the MassPort LPR Cameras into the EOPSS BOSS LPR Server. Today, G.L. c. 4.sec. 7.cl.26 (n)(security) at Airport Road arrivals were migrated and are now writing data to Chelsea. I will continue to cut the remaining cameras over in the next few days and weeks. I will

advise when the project is complete.
>
> - Brian
>
> -----Original Message-----
> From: Warmington, Scott (POL)
> Sent: Tuesday, March 10, 2020 11:36 AM
> To: Quinn, Dermot (POL)
> Cc: Small, Michelle (POL); Silva, Kyra (POL); Slater, James (CHS); Mason, Christopher (POL); Egnitz, Brian (POL); Warren, Rosemary (POL); Shaw, Harold; Ryan, Deborah (POL); Ball, Richard (POL)
> Subject: Re: MassPort LPR Cameras
>
> What is the cost?
>
> Sent from my iPhone
>
>>> On Mar 10, 2020, at 11:28 AM, Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us> wrote:
>> Michelle and Kyra,
>> This purchase request is for equipment to allow Mass Port Sierra Wireless modems to communicate directly with the existing ALPR Boss server in Chelsea. This is the fastest way to bring the Massport LPR cameras on line. EOTSS and EOPSS are OK with this solution as is Major Deb Ryan, the CO at Troop F.
>> As you can see from the thread, this has been going on for some time. I think we can close it out with this small purchase.
>> This does not resolve the replacement of the existing ALPR equipment that we discussed at Command Staff yesterday. That is a different issue.
>> Thanks
>> Lieutenant Colonel Dermot J. Quinn #1765
>> Division Commander
>> Division of Homeland Security & Preparedness
>> Massachusetts State Police
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 10:52 AM
>> To: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: FW: MassPort LPR Cameras
>> Hi LTC.,
>> Can we order this equipment for the MassPort project?
>> Thanks, Brian
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Tuesday, March 10, 2020 10:26 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>> Hi, Brian!
>> This needs to go through MSP fiscal. They need to enter the purchase in OPAS.
>> Jim
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Tuesday, March 10, 2020 08:06
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Subject: RE: MassPort LPR Cameras

>> Is this something you can order or does it need to go through MSP?
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Monday, March 9, 2020 10:36 AM
>> To: Egnitz, Brian (POL)
>> Subject: RE: MassPort LPR Cameras
>> Thanks, Brian...I will check with TSS.
>> Jim
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Monday, March 9, 2020 10:29
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: RE: MassPort LPR Cameras
>> Thanks Jim,
>> I've reached out to Alex regarding the below and he is fine with the approach. I will coordinate with him and begin cutting over the cameras. I need [redacted] wireless AC adapters and [redacted] I have reached out to BCM for a quote.
>> I have also requested permission from MSP at MassPort to remove the devices and assist with scheduling. Our Technical Services Unit will remove the devices once approved.
>> I plan to cut one sector ([redacted]) over at a time and monitor the server, we may need to shrink our retention if we run up against storage constraints. Can you please see if the SAN can support additional storage and if it can be added?
>> -Brian
>> -----Original Message-----
>> From: Slater, James (CHS)
>> Sent: Friday, March 6, 2020 1:43 PM
>> To: Egnitz, Brian (POL)
>> Cc: Quinn, Dermot (POL)
>> Subject: RE: MassPort LPR Cameras
>> Hi, Brian!
>> I reached out to Rob Guerriero at TSS re this to get his perspective and he sees no problem connecting the cameras to the Boss server in the described manner.
>> So, assuming you move forward with this, who would actually make this happen?
>> Thanks.
>> Jim
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
>> Sent: Wednesday, March 4, 2020 17:53
>> To: Slater, James (CHS) <james.slater@mass.gov>
>> Cc: Quinn, Dermot (POL) <dermot.quinn@pol.state.ma.us>
>> Subject: Re: MassPort LPR Cameras
>> Hi Jim,
>> Regarding the Massport cameras; in the early days of AVL we installed [redacted] modem's in cruisers that did not have laptops. These cruisers now have Geo tab and no longer need the modem or data plan. Massport is currently paying for the data plan and bought the modems. Because Massport wants to move quickly to give us their data and knowing BOSS4.0 Is delayed; Why don't we ask Massport to let us use six of those modems and put one at each LPR Camera sector at Massport. We would next push the data back like we do everything else over Verizon. We wouldn't have to do any firewall work either because they have a 166. and communicate like all of the MDT's . Once the back get squared away with the new boss we can revisit the networking. After we migrate everything to the new environment we would them cut the Massport cameras over to the LAN and then give them back their data plans and modems.

>> We would however need to anticipate expanding the existing sand and run the risk of overburdening the server.
>> Let me know what you think, Lieutenant Colonel Quinn and I could make the request to Massport if needed.
>>>> On Feb 11, 2020, at 11:35 AM, Atchison, Charles W <CAtchison@massport.com> wrote:
>>> Thank you sir
>>> Major Charles W. Atchison III
>>> Troop F Commander
>>> Massachusetts State Police
>>> Director of Aviation Security
>>> 2 Service Road
>>> East Boston, Ma 02128
>>> Office: 617-568-7555
>>> Cell: 508-[redacted]
>>>> On Feb 11, 2020, at 11:28 AM, Wood, Curtis (MASSIT)
<curtis.wood@state.ma.us<mailto:curtis.wood@state.ma.us>> wrote:
>>> All,
>>> Thank you. I have our team looking at this. Once I hear back from them, we will reach out to discuss and plan further.
>>> Thanks
>>> CW
>>> From: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>
>>> Sent: Monday, February 10, 2020 10:31 AM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>;
>>> Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>; Guerriero,
>>> Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>;
>>> Warmington, Scott (POL)
>>> <Scott.Warmington@pol.state.ma.us<mailto:Scott.Warmington@pol.state.ma
>>> .us>>; Peek, Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John
>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>;
>>> Michalski, Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>; Mason,
>>> Christopher (POL)
>>> <Chris.Mason@pol.state.ma.us<mailto:Chris.Mason@pol.state.ma.us>>;
>>> Hughes, Sean M. (EOTSS)
>>> <sean.hughes@mass.gov<mailto:sean.hughes@mass.gov>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>; Wood, Curtis (EOTSS)
>>> <curtis.wood@mass.gov<mailto:curtis.wood@mass.gov>>; Shaw, Harold
>>> <HShaw@massport.com<mailto:HShaw@massport.com>>; Ball, Richard (POL)
>>> <Richard.Ball@pol.state.ma.us<mailto:Richard.Ball@pol.state.ma.us>>;
>>> Atchison, Charles (POL)
>>> <catchison@massport.com<mailto:catchison@massport.com>>
>>> Subject: RE: MassPort LPR Cameras
>>> Good Morning,
>>> I was hoping to get us all on the same page regarding a proposal to push Massport LPR data to

the existing DCJIS BOSS server in Chelsea. Some time ago we (MSP) engaged with Massport regarding Automated License Plate Reader technology (LPR). As most of you know, MSP and DCJIS have been rolling out a very robust LPR network across the Commonwealth. This has been on going for the past several years. The LPR system has paid dividends in numerous criminal cases including crimes of violence, Amber and Silver alerts, and also in many missing/endangered/public well being events.
>>> Our communications with Massport started when we were made aware that they would be purchasing an LPR system. We worked with our counterparts at Massport to make sure that the two systems would be compatible so that information could be shared across all law enforcement agencies through the MSP Fusion Center. Towards that end Massport partnered with Neology for their solution. This is the same vendor used by MSP and DCJIS.
>>> Recently Massport has decided not to maintain its own ALPR BOSS database server. The database and application for LPR in Massachusetts is known as “BOSS” and is a Neology product. Massport would like to feed data from its cameras to the DCJIS BOSS server in Chelsea. Originally we had been discussing with Neology the potential for Massport’s cameras to write two records after scanning a plate, one to Massport BOSS and a duplicate to DCJIS BOSS. We think the current proposal to write all LPR records to the BOSS server located at DCJIS is a much better plan.
>>> MSP has a grant to upgrade the current the current BOSS v3.6 application which is at end of life and no longer supported to version v4.0. We have also submitted a Service Now ticket asking for hardware upgrade costs to the existing BOSS server which MSP will try to acquire funding to upgrade.
>>> I have received several calls from Massport looking to see where we are as far as being able to accept data from their cameras so that they can decommission their BOSS server. I believe their intent is to shut the Massport system down if the MSP and DCJIS are unable to accept the data. I have copied Hank Shaw from Massport into this thread in case I have misstated their intent.
>>> To access the Massport data we will need to be able to pass data from the Massport network to the state network much like we do with case management data. An alternative would be to use 4G modems (like we do with many of our mobile units and cruiser mounted units) on the state network, but this may be an unnecessary cost. Obviously this decision would be driven by the EOTSS and Massport network teams.
>>> I can’t overstate the value that LPR data from Massport would have for MSP and law enforcement in general. Cases involving terrorism, money laundering, and drug trafficking all have significant ties to the port. Being able to hotlist and search on LPR data from Massport facilities would be a significant addition to the MSP Division of Homeland Security’s technology tool set and would have immediate impact. Towards that end, we made be able to leverage Homeland Security grant funds for some of this project.
>>> Respectfully,
>>> Lieutenant Colonel Dermot J. Quinn #1765 Division Commander Division
>>> of Homeland Security & Preparedness Massachusetts State Police
>>> <image006.png>
>>> From: Egnitz, Brian (POL)
>>> <brian.egnitz@pol.state.ma.us<mailto:brian.egnitz@pol.state.ma.us>>
>>> Sent: Friday, January 17, 2020 1:10 PM
>>> To: Slater, James (CHS)
>>> <james.slater@mass.gov<mailto:james.slater@mass.gov>>
>>> Cc: Quinn, Dermot (POL)
>>> <dermot.quinn@pol.state.ma.us<mailto:dermot.quinn@pol.state.ma.us>>;
>>> Guerriero, Robert (EOTSS)
>>> <Robert.Guerriero@mass.gov<mailto:Robert.Guerriero@mass.gov>>; Peek,
>>> Brian T. (EOTSS)
>>> <Brian.T.Peek@mass.gov<mailto:Brian.T.Peek@mass.gov>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@mass.gov<mailto:timothy.mitchell@mass.gov>>; John

>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Chute,
>>> Alexander <AChute@massport.com<mailto:AChute@massport.com>>; Peter
>>> Crary <pcrary@neology.net<mailto:pcrary@neology.net>>; Michalski,
>>> Maria (EPS)
>>> <maria.michalski@mass.gov<mailto:maria.michalski@mass.gov>>
>>> Subject: RE: MassPort LPR Cameras
>>> Hi Jim,
>>> BOSS 3.6 is going end-of-life. We have grant funds to upgrade the EOPSS system's software. I have also submitted a ticket for requesting cost estimations for infrastructure. The below is still outstanding.
>>> -Brian
>>> From: Egnitz, Brian (POL)
>>> Sent: Monday, January 6, 2020 1:33 PM
>>> To: Slater, James (CHS)
>>> Cc: Quinn, Dermot (POL); Guerriero, Robert (EOTSS); Peek, Brian T.
>>> (EOTSS); Mitchell, Timothy (EPS); John Tedona; Chute, Alexander; Peter
>>> Crary
>>> Subject: RE: MassPort LPR Cameras
>>> Hi Jim,
>>> We are looking to consolidate the MassPort ALPR cameras into the main EOPSS ALPR server. After evaluating a number of options purposed by Neology, this appears to be the simplest approach. There is already a network presence at the barracks and it should be easy to point the cameras towards the centralized server. I've spoken to Alex at MassPort and he can volunteer a camera for testing. We could monitor network and server impact. Are you available to discuss?
>>> Thanks Brian
>>> From: John Tedona [mailto:jtedona@neology.net]
>>> Sent: Monday, December 9, 2019 4:55 PM
>>> To: Chute, Alexander; Egnitz, Brian (POL); Peter Crary
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Slater, James (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>> Alex,
>>> I can be available most anytime tomorrow for a call.
>>> Regards,
>>> John Tedona
>>> PIPS TECHNOLOGY - A Neology Business
>>> Sales Manager
>>> 12760 Danielson Ct. Suite A
>>> Poway, CA 92064
>>> Phone: 201-841-6237
>>> Email: jtedona@neology.net<mailto:jtedona@neology.net>
>>> PIPS Support: support@pipstechnology.com<mailto:support@pipstechnology.com> 833-747-7577, Option 1 for sales, Option 2 for Support
>>> www.pipstechnology.com<https://urldefense.proofpoint.com/v2/url?u=http
>>> -3A__www.pipstechnology.com&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FN
>>> EWIHnzbfZimE&r=cQxEzXiBNidUzHb9OviLbzhvVRjr7hazQ0kdCYnx9TI&m=RZW4faTTJ
>>> baP6n2jdwVdMxZBJOrESjbl8l9kYblypag&s=Ct4bp9FJFoKMY9Xgz_OAWMzzVM-lyPhyJ
>>> U2sB_fmM6g&e=>
>>> From: Chute, Alexander
>>> <AChute@massport.com<mailto:AChute@massport.com>>
>>> Sent: Monday, December 9, 2019 4:38 PM
>>> To: Egnitz, Brian (POL)
>>> <brian.egnitz@state.ma.us<mailto:brian.egnitz@state.ma.us>>; John

>>> Tedona <jtedona@neology.net<mailto:jtedona@neology.net>>; Peter Crary
>>> <pcrary@neology.net<mailto:pcrary@neology.net>>
>>> Cc: Guerriero, Robert (MASSIT)
>>> <robert.guerriero@state.ma.us<mailto:robert.guerriero@state.ma.us>>;
>>> Peek, Brian T. (EOTSS)
>>> <brian.t.peek@state.ma.us<mailto:brian.t.peek@state.ma.us>>; Mitchell,
>>> Timothy (EPS)
>>> <timothy.mitchell@state.ma.us<mailto:timothy.mitchell@state.ma.us>>;
>>> Slater III, James F (CHS)
>>> <james.slater@state.ma.us<mailto:james.slater@state.ma.us>>
>>> Subject: RE: MassPort LPR Cameras
>>> CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
>>> Hello All,
>>> I just wanted to follow up with this request to see what the next steps for this project are. I believe that we can make the connections to the EOPSS network, but will want to work within your desired IP scheme and ensure that there aren't any concerns around the network routing, security, etc. Let me know if we can have a quick call to discuss the details.
>>> Respectfully,
>>> ~Alex
>>> <image007.png>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Monday, November 18, 2019 3:26 PM
>>> To: John Tedona (jtedona@neology.net<mailto:jtedona@neology.net>);
>>> pcrary@neology.net<mailto:pcrary@neology.net>
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS); Chute, Alexander; Slater III, James F (CHS)
>>> Subject: RE: MassPort LPR Cameras
>>> Hi John, Peter
>>> Any issues with moving Massports cameras to the Chelsea DB?
>>> Using the Boss calculator, I estimate that we would need 9-10 TB of storage.
>>> The current app server
>>> <image008.png>
>>> Current DB server
>>> <image009.png>
>>> <image010.png>
>>> Our current reads by month for about [redacted]
>>> Year
>>> Month
>>> Day
>>> Month Name
>>> Reads Count

>>> 2019
>>> 11
>>> 1
>>> November
>>> 495,113
>>> 2019
>>> 11
>>> 2
>>> November
>>> 472,907
>>> 2019
>>> 11
>>> 3
>>> November
>>> 384,409
>>> 2019
>>> 11
>>> 4
>>> November
>>> 411,440
>>> 2019
>>> 11
>>> 5
>>> November
>>> 434,085
>>> 2019
>>> 11
>>> 6
>>> November
>>> 495,537
>>> 2019
>>> 11
>>> 7
>>> November
>>> 444,123
>>> 2019
>>> 11
>>> 8
>>> November
>>> 542,492
>>> 2019
>>> 11
>>> 9
>>> November
>>> 443,463
>>> 2019
>>> 11
>>> 10
>>> November
>>> 389,514
>>> 2019
>>> 11
>>> 11

>>> November
>>> 362,548
>>> 2019
>>> 11
>>> 12
>>> November
>>> 236,539
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Wednesday, November 13, 2019 2:49 PM
>>> To: Egnitz, Brian (POL)
>>> Cc: Guerriero, Robert (EOTSS); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>> These stats are from the [redacted] we have in the system for this month:
>>> <image011.png>
>>> ~Alex
>>> From: Egnitz, Brian (POL) [mailto:brian.egnitz@state.ma.us]
>>> Sent: Tuesday, November 12, 2019 5:28 PM
>>> To: Chute, Alexander
>>> Cc: Guerriero, Robert (MASSIT); Peek, Brian T. (EOTSS); Mitchell,
>>> Timothy (EPS)
>>> Subject: RE: MassPort LPR Cameras
>>> Hi Alex,
>>> Can you please provide the updated reads per day? Previously you were interested in sharing [redacted] at approximately 75,000 reads per day.
>>> Here is the [redacted] confi I mentioned.
>>> Set host to boss [redacted]
>>> Set image [redacted]
>>> Set number of [redacted]
>>> Set Ping [redacted]
>>> Set udp ping [redacted]
>>> Set ping [redacted]
>>> Set security [redacted]
>>> I've looped in the network and server team from TSS on the thread. Maybe we can schedule a call in the next week.
>>> For an estimate on impact, the Caper cameras do between 80,000 to 120,000 per day. We average 337,944 reads per day.
>>> -Brian
>>> From: Chute, Alexander [mailto:AChute@massport.com]
>>> Sent: Tuesday, November 12, 2019 2:08 PM
>>> To: Egnitz, Brian (POL)
>>> Subject: MassPort LPR Cameras
>>> Brian,
>>> Thank you again for taking my call today. As discussed, I would like to explore the opportunity to swing all LPR cameras at Logan directly to the MSP BOSS server without the need for the InStation solution. My understanding is that the EOPSS network resides in both the ATCT as well as the [redacted] I would propose that we extend this network via Layer 2 to the main locations that the LPR system terminates to and cut the entire LPR network at MassPort over to EOPSS. Most of the [redacted] are fed to [redacted] network locations. MassPort can supply the necessary fiber paths and switch gear required to extend the EOPSS network to these locations. Currently we have [redacted] in production, with another [redacted] to come online within the next two months. I anticipate this number growing to approximately [redacted] within our campus over the next year. Let me know what you think the appropriate next steps would be.

>>> Respectfully,
>>> ~Alex
>>> <image007.png>
>>> Alexander B. Chute
>>> Program Manager, Public Safety Systems Massachusetts Port Authority
>>> Cell: [redacted]
>>> Office: 617.568.5942
>>> achute@massport.com<mailto:achute@massport.com>
>>> WARNING: This record may contain Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.
>> <SierraQuoteForMassPort.pdf>

From: Gilmore, Joey
To: Egnitz, Brian (POL); Alves, Joe; Haverty, Robert
Cc: Harney, Michael
Subject: RE: MSP LPR
Date: Tuesday, June 16, 2020 11:22:21 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Hello Brian,

Can you please let me know how many of the camera sites have been cut over to EOPSS? Also how many total cameras.

Thank you,
Joey Gilmore
Manager - IT Security Systems
Information Technology
Massachusetts Port Authority
One Harborside Drive, Suite 200S
East Boston, MA 02128-2909
Tel: 617-568-5915
Cell: 617-[redacted]

From: Gilmore, Joey
Sent: Monday, May 4, 2020 9:41 AM
To: 'Egnitz, Brian (POL)' <brian.egnitz@state.ma.us>; Alves, Joe <JAlves@massport.com>; Sillsby, Blane <BSillsby@massport.com>; Quinn, Michael <MQuinn@massport.com>
Cc: Haverty, Robert <RHaverty@massport.com>; Harney, Michael <MHarney@massport.com>
Subject: RE: MSP LPR

Joe,
Later today Brian will send over the actual IMEI numbers that they are using for this project. Once received, can you please confirm if they are unlimited data plans?

Brian,
Joe Alves is in onsite Wednesday and Friday. He said the [redacted] is accessible without road closure and would make a good first install. Can you please reach out to him to arrange a time for Wednesday? Joe's cell number is [redacted]

Thank you,
Joey Gilmore
Manager - IT Security Systems
Information Technology

Massachusetts Port Authority
One Harborside Drive, Suite 200S
East Boston, MA 02128-2909
Tel: 617-568-5915
Cell: 617-[redacted]

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Thursday, April 23, 2020 10:30 AM
To: Gilmore, Joey <JGilmore@massport.com>; Alves, Joe <JAlves@massport.com>; Sillsby, Blane <BSillsby@massport.com>; Quinn, Michael <MQuinn@massport.com>
Cc: Haverty, Robert <RHaverty@massport.com>; Harney, Michael <MHarney@massport.com>
Subject: RE: MSP LPR

-----Original Appointment-----
From: Gilmore, Joey [mailto:JGilmore@massport.com]
Sent: Wednesday, April 22, 2020 11:35 AM
To: Gilmore, Joey; Alves, Joe; Sillsby, Blane; Quinn, Michael; Egnitz, Brian (POL)
Cc: Haverty, Robert; Harney, Michael
Subject: MSP LPR
When: Thursday, April 23, 2020 10:00 AM-11:00 AM (UTC-05:00) Eastern Time (US & Canada).
Where: https://global.gotomeeting.com/join/500426357

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Hi Guys,

This meeting is to discuss the method of bringing Logan LPR cameras to the EOPSS network.

This is the last status update from Chute before he left:

"Currently MassPort has [redacted] After several iterations of the system architecture, it has been decided that the path of least resistance is to employ commercial carrier service on the MSP MPLS to the CJIS Datacenter in Chelsea. MSP is working to procure the necessary power adapter and antenna equipment while also identifying accounts and equipment that can be re-

purposed for this project. If/when it is feasible for this system to be networked through terrestrial means, MassPort has the switch infrastructure in place to make a direct connection to the EOPSS network at [redacted] ([redacted] I hope this gives a brief overview of where we are at, and please do not hesitate to reach out to me via my personal contact information if any questions come up."

MPA - MSP
Thu, Apr 23, 2020 10:00 AM - 11:30 AM (EDT)

Please join my meeting from your computer, tablet or smartphone.
https://global.gotomeeting.com/join/500426357

This meeting is locked with a password : [redacted]

You can also dial in using your phone.
United States: +1 (571) 317-3122

Access Code: 500-426-357

New to GoToMeeting? Get the app now and be ready when your first meeting starts:
https://global.gotomeeting.com/install/500426357

Thank you,

Joey Gilmore

Manager - IT Security Systems
Information Technology
Massachusetts Port Authority
One Harborside Drive, Suite 200S
East Boston, MA 02128-2909
Tel: 617-568-5915
Cell: 617-[redacted]

The information contained in this communication, including any attachments, is confidential and is intended only for the use of the recipient(s) named above. If the reader of this message is not an intended recipient, you are notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you receive this communication in error, please

notify the sender immediately, and delete the communication, any attachments, and all copies.

From: Haverty, Robert
To: Alves, Joe; Egnitz, Brian (POL)
Subject: RE: MSP LPR
Date: Wednesday, June 10, 2020 8:25:24 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

We need a detail. Someone needs to call the detail officer at the SP here at Troop F. The detail should be billed to Massport IT Operations.

Thanks,
Bob

-----Original Message-----
From: Alves, Joe <JAlves@massport.com>
Sent: Wednesday, June 10, 2020 8:23 AM
To: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>; Haverty, Robert <RHaverty@massport.com>
Subject: Re: MSP LPR

Adding Bob. I'm not sure where this is right now.

Sent from my iPhone

> On Jun 10, 2020, at 7:59 AM, Egnitz, Brian (POL) <brian.egnitz@state ma.us> wrote:
>
> Any luck?
>
> -----Original Message-----
> From: Egnitz, Brian (POL)
> Sent: Tuesday, May 26, 2020 9:54 AM
> To: Alves, Joe
> Subject: RE: MSP LPR
>
> Hi Joe,
>
> I'm not sure if this was too short notice. The 3rd & 4th also work.
>
> -Brian
>
> -----Original Message-----
> From: Egnitz, Brian (POL)
> Sent: Thursday, May 21, 2020 2:34 PM
> To: 'Alves, Joe'
> Subject: RE: MSP LPR
>
> Can we schedule last two cut overs for 5/28 & 5/29. In speaking with Maj. Ryan, a coordinated road closure via the detail office is warranted.
>
> Thanks, Brian
>
> -----Original Message-----
> From: Alves, Joe [mailto:JAlves@massport.com]
> Sent: Wednesday, May 13, 2020 6:44 AM
> To: Egnitz, Brian (POL)
> Subject: Re: MSP LPR
>
>
> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>
>
> Ok.
>
> Sent from my iPhone
>
>> On May 13, 2020, at 6:22 AM, Egnitz, Brian (POL) <brian.egnitz@state ma.us> wrote:
>>
>> I have a meeting today at 12:00 that I need to go to, but will try and come in after. -Brian
>>
>>>> On May 8, 2020, at 8:26 AM, Alves, Joe <JAlves@massport.com> wrote:
>>>
>>>
>>> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>>>
>>>
>>> Ok.
>>>
>>> -----Original Message-----
>>> From: Egnitz, Brian (POL) <brian.egnitz@state ma.us>
>>> Sent: Friday, May 08, 2020 8:26 AM
>>> To: Alves, Joe <JAlves@massport.com>
>>> Subject: RE: MSP LPR
>>>
>>> Thanks should be in for 10 ish. I'll give you a call when I'm a few out.
>>>
>>> Tks, Brian
>>>
>>> -----Original Message-----
>>> From: Alves, Joe [mailto:JAlves@massport.com]
>>> Sent: Thursday, May 7, 2020 9:01 PM
>>> To: Egnitz, Brian (POL)
>>> Subject: Re: MSP LPR
>>>
>>>
>>> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>>>
>>>
>>> Yes. I'll be around. I can get you in just let me know the time.
>>>
>>>
>>>
>>> Sent from my iPhone
>>>
>>>
>>>
>>>>> On May 7, 2020, at 7:49 PM, Egnitz, Brian (POL) <brian.egnitz@state ma.us> wrote:
>>>
>>>
>>>
>>>
>>>
>>> Are you available tomorrow?
>>>
>>>

>>>
>>>> On May 4, 2020, at 9:41 AM, Gilmore, Joey <JGilmore@massport.com> wrote:
>>>
>>>
>>>
>>>
>>>
>>> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>>>
>>>
>>>
>>>
>>>
>>> Joe,
>>>
>>> Later today Brian will send over the actual IMEI numbers that they are using for this project. Once received, can you please confirm if they are unlimited data plans?
>>>
>>>
>>>
>>> Brian,
>>>
>>> Joe Alves is in onsite Wednesday and Friday. He said the [redacted] is accessible without road closure and would make a good first install. Can you please reach out to him to arrange a time for Wednesday? Joe's cell number is 781[redacted]
>>>
>>>
>>>
>>>
>>>
>>> Thank you,
>>>
>>> Joey Gilmore
>>>
>>> Manager - IT Security Systems
>>>
>>> Information Technology
>>>
>>> Massachusetts Port Authority
>>>
>>> One Harborside Drive, Suite 200S
>>>
>>> East Boston, MA 02128-2909
>>>
>>> Tel: 617-568-5915
>>>
>>> Cell: 617[redacted]
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL) <brian.egnitz@state ma.us>
>>>
>>> Sent: Thursday, April 23, 2020 10:30 AM
>>>
>>> To: Gilmore, Joey <JGilmore@massport.com>; Alves, Joe <JAlves@massport.com>; Sillsby, Blane <BSillsby@massport.com>; Quinn, Michael <MQuinn@massport.com>
>>>
>>> Cc: Haverty, Robert <RHaverty@massport.com>; Harney, Michael <MHarney@massport.com>
>>>
>>> Subject: RE: MSP LPR
>>>
>>>
>>>
>>>
>>>
>>> -----Original Appointment-----
>>>
>>> From: Gilmore, Joey [mailto:JGilmore@massport.com]
>>>
>>> Sent: Wednesday, April 22, 2020 11:35 AM
>>>
>>> To: Gilmore, Joey; Alves, Joe; Sillsby, Blane; Quinn, Michael; Egnitz, Brian (POL)
>>>
>>> Cc: Haverty, Robert; Harney, Michael
>>>
>>> Subject: MSP LPR
>>>
>>> When: Thursday, April 23, 2020 10:00 AM-11:00 AM (UTC-05:00) Eastern Time (US & Canada).
>>>
>>> Where: https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_join_500426357&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=3ivMD3mXVSpxMv-g-ajiMkf38VVpxAIvxzFU7zoD-C0&s=ZHyfYIPsksOBeyci6ra3KwL4O4SCPoA_7WEhraXS96Y&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_join_500426357&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FNEWIHnzbfZimE&r=v1eRT_PuOlmt3sh7Lyk24rX9MBSQCKldPuclQWjOSPk&m=PXOFyIolm_rZpuk6yADM63jFy9ok8VUjYC-nn_w6rMY&s=1D-DGoR18hVhptpvf47Fn_SFGKSpwE2u7SIK57_YdrA&e=>
>>>
>>>
>>>
>>>
>>>
>>> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>> Hi Guys,
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>> This meeting is to discuss the method of bringing Logan LPR cameras to the EOPSS network.
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>>

>>> This is the last status update from Chute before he left:
>>>
>>>
>>>
>>> “Currently MassPort has [redacted] After several iterations of the system architecture, it has been decided that the path of least resistance is to employ commercial carrier service on the MSP MPLS to the CJIS Datacenter in Chelsea. MSP is working to procure the necessary power adapter and antenna equipment while also identifying accounts and equipment that can be re-purposed for this project. If/when it is feasible for this system to be networked through terrestrial means, MassPort has the switch infrastructure in place to make a direct connection to the EOPSS network at [redacted] I hope this gives a brief overview of where we are at, and please do not hesitate to reach out to me via my personal contact information if any questions come up.”
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>> MPA - MSP
>>>
>>> Thu, Apr 23, 2020 10:00 AM - 11:30 AM (EDT)
>>>
>>>
>>>
>>> Please join my meeting from your computer, tablet or smartphone.
>>>
>>> https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_join_500426357&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=3ivMD3mXVSpxMv-g-ajiMkf38VVpxAIvxzFU7zoD-C0&s=ZHyfYIPsksOBeyci6ra3KwL4O4SCPoA_7WEhraXS96Y&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_join_500426357&d=DwMF-g&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=YrOyBDqzLm4zddutRwcvrC8An9e-bx9zIO8EMq0-X7Q&s=bt8qRm7QQabR-s9uIfBIIjV-_W5RvGI9slrF4D65fw4&e=>
>>>
>>>
>>>
>>> This meeting is locked with a password : [redacted]
>>>
>>>
>>>
>>> You can also dial in using your phone.
>>>
>>> United States: +1 (571) 317-3122<tel:+15713173122,,500426357>
>>>
>>>
>>>
>>> Access Code: 500-426-357
>>>
>>>
>>>
>>> New to GoToMeeting? Get the app now and be ready when your first meeting starts:
>>>
>>> https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_install_500426357&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=3ivMD3mXVSpxMv-g-ajiMkf38VVpxAIvxzFU7zoD-C0&s=sPSeiG_aGKwV8Di-BEroqcIxtAzk0va1AAxVy6gZ3Tg&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_install_500426357&d=DwMF-g&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=YrOyBDqzLm4zddutRwcvrC8An9e-bx9zIO8EMq0-X7Q&s=73yCNI9YJUXzkHRvG6ehrB7JBvLK4l12EYJ4ThBmY-M&e=>
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>> Thank you,
>>>
>>>
>>>
>>> Joey Gilmore
>>>
>>>
>>>
>>> Manager - IT Security Systems
>>>
>>> Information Technology
>>>
>>> Massachusetts Port Authority
>>>
>>> One Harborside Drive, Suite 200S
>>>
>>> East Boston, MA 02128-2909
>>>
>>> Tel: 617-568-5915
>>>
>>> Cell: 617[redacted]
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>>

The information contained in this communication, including any attachments, is confidential and is intended only for the use of the recipient(s) named above. If the reader of this message is not an intended recipient, you are notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you receive this communication in error, please notify the sender immediately, and delete the communication, any attachments, and all copies.

From: Egnitz, Brian (POL)
To: Alves, Joe
Subject: RE: MSP LPR
Date: Wednesday, June 10, 2020 7:59:00 AM

Any luck?

-----Original Message-----
From: Egnitz, Brian (POL)
Sent: Tuesday, May 26, 2020 9:54 AM
To: Alves, Joe
Subject: RE: MSP LPR

Hi Joe,

I'm not sure if this was too short notice. The 3rd & 4th also work.

-Brian

-----Original Message-----
From: Egnitz, Brian (POL)
Sent: Thursday, May 21, 2020 2:34 PM
To: 'Alves, Joe'
Subject: RE: MSP LPR

Can we schedule last two cut overs for 5/28 & 5/29. In speaking with Maj. Ryan, a coordinated road closure via the detail office is warranted.

Thanks, Brian

-----Original Message-----
From: Alves, Joe [mailto:JAlves@massport.com]
Sent: Wednesday, May 13, 2020 6:44 AM
To: Egnitz, Brian (POL)
Subject: Re: MSP LPR

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Ok.

Sent from my iPhone

> On May 13, 2020, at 6:22 AM, Egnitz, Brian (POL) <brian.egnitz@state.ma.us> wrote:
>
> I have a meeting today at 12:00 that I need to go to, but will try and come in after. -Brian
>
>> On May 8, 2020, at 8:26 AM, Alves, Joe <JAlves@massport.com> wrote:
>>
>>
>> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>>
>>
>> Ok.
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@state ma.us>
>> Sent: Friday, May 08, 2020 8:26 AM
>> To: Alves, Joe <JAlves@massport.com>
>> Subject: RE: MSP LPR
>>
>> Thanks should be in for 10 ish. I'll give you a call when I'm a few out.
>>
>> Tks, Brian
>>
>> -----Original Message-----
>> From: Alves, Joe [mailto:JAlves@massport.com]
>> Sent: Thursday, May 7, 2020 9:01 PM
>> To: Egnitz, Brian (POL)
>> Subject: Re: MSP LPR
>>
>>
>> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>>
>>
>> Yes. I'll be around. I can get you in just let me know the time.
>>
>>
>>
>> Sent from my iPhone
>>
>>
>>
>> On May 7, 2020, at 7:49 PM, Egnitz, Brian (POL) <brian.egnitz@state.ma.us> wrote:
>>
>>
>>
>>
>>
>> Are you available tomorrow?
>>
>>
>>
>> On May 4, 2020, at 9:41 AM, Gilmore, Joey <JGilmore@massport.com> wrote:
>>
>>
>>
>>
>>
>> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>>
>>
>>
>>
>>
>> Joe,
>>
>> Later today Brian will send over the actual IMEI numbers that they are using for this project. Once received, can you please confirm if they are unlimited data plans?
>>
>>
>>
>> Brian,
>>
>> Joe Alves is in onsite Wednesday and Friday. He said the G.L. c. 4,sec. 7,cl.26 (n)(sec) is accessible without road closure and would make a good first install. Can you please reach out to him to arrange a time for Wednesday? Joe's cell

number[redacted]
>>
>>
>>
>>
>>
>> Thank you,
>>
>> Joey Gilmore
>>
>> Manager - IT Security Systems
>>
>> Information Technology
>>
>> Massachusetts Port Authority
>>
>> One Harborside Drive, Suite 200S
>>
>> East Boston, MA 02128-2909
>>
>> Tel: 617-568-5915
>>
>> Cell: 617[redacted]
>>
>>
>>
>>
>>
>>
>>
>>
>>
>> From: Egnitz, Brian (POL) <brian.egnitz@state ma.us>
>>
>> Sent: Thursday, April 23, 2020 10:30 AM
>>
>> To: Gilmore, Joey <JGilmore@massport.com>; Alves, Joe <JAlves@massport.com>; Sillsby, Blane <BSillsby@massport.com>; Quinn, Michael <MQuinn@massport.com>
>>
>> Cc: Haverty, Robert <RHaverty@massport.com>; Harney, Michael <MHarney@massport.com>
>>
>> Subject: RE: MSP LPR
>>
>>
>>
>>
>>
>> -----Original Appointment-----
>>
>> From: Gilmore, Joey [mailto:JGilmore@massport.com]
>>
>> Sent: Wednesday, April 22, 2020 11:35 AM
>>
>> To: Gilmore, Joey; Alves, Joe; Sillsby, Blane; Quinn, Michael; Egnitz, Brian (POL)
>>
>> Cc: Haverty, Robert; Harney, Michael
>>
>> Subject: MSP LPR
>>
>> When: Thursday, April 23, 2020 10:00 AM-11:00 AM (UTC-05:00) Eastern Time (US & Canada).
>>
>> Where: https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_join_500426357&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=3ivMD3mXVSpxMv-g-ajiMkf38VVpxAIvxzFU7zoD-C0&s=ZHyfYIPsksOBeyci6ra3KwL4O4SCPoA_7WEhraXS96Y&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_join_500426357&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FNEWIHnzbfZimE&r=v1eRT_PuOlmt3sh7Lyk24rX9MBSQCKldPuclQWjOSPk&m=PXOFyIolm_rZpuk6yADM63jFy9ok8VUjYC-nn_w6rMY&s=1D-DGoR18hVhptpvf47Fn_SFGKSpwE2u7SIK57_YdrA&e=>
>>
>>
>>
>>
>>
>> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>>
>>
>>
>>
>>
>>
>>
>>
>> Hi Guys,
>>
>>
>>
>>
>>
>>
>>
>>
>> This meeting is to discuss the method of bringing Logan LPR cameras to the EOPSS network.
>>
>>
>>
>>
>>
>>
>>
>>
>> This is the last status update from Chute before he left:
>>
>>
>>
>> "Currently MassPort has[redacted] After several iterations of the system architecture, it has been decided that the path of least resistance is to employ commercial carrier service on the MSP MPLS to the CJIS Datacenter in Chelsea. MSP is working to procure the necessary power adapter and antenna equipment while also identifying accounts and equipment that can be re-purposed for this project. If/when it is feasible for this system to be networked through terrestrial means, MassPort has the switch infrastructure in place to make a direct connection to the EOPSS network at[redacted] I hope this gives a brief overview of where we are at, and please do not hesitate to reach out to me via my personal contact information if any questions come up."
>>
>>
>>
>>
>>
>>
>>
>>
>> MPA - MSP
>>
>> Thu, Apr 23, 2020 10:00 AM - 11:30 AM (EDT)
>>
>>
>>
>> Please join my meeting from your computer, tablet or smartphone.

>>
>> https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_join_500426357&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=3ivMD3mXVSpxMv-g-ajiMkf38VVpxAIvxzFU7zoD-C0&s=ZHyfYIPsksOBeyci6ra3KwL4O4SCPoA_7WEhraXS96Y&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_join_500426357&d=DwMF-g&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=YrOyBDqzLm4zddutRwcvrC8An9e-bx9zIO8EMq0-X7Q&s=bt8qRm7QQabR-s9uIfBIIjV-_W5RvGI9slrF4D65fw4&e=>
>>
>>
>>
>> This meeting is locked with a password[illegible]
>>
>>
>>
>> You can also dial in using your phone.
>>
>> United States: +1 (571) 317-3122<tel:+15713173122,,500426357>
>>
>>
>>
>> Access Code: 500-426-357
>>
>>
>>
>> New to GoToMeeting? Get the app now and be ready when your first meeting starts:
>>
>> https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_install_500426357&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=3ivMD3mXVSpxMv-g-ajiMkf38VVpxAIvxzFU7zoD-C0&s=sPSeiG_aGKwV8Di-BEroqcIxtAzk0va1AAxVy6gZ3Tg&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_install_500426357&d=DwMF-g&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=YrOyBDqzLm4zddutRwcvrC8An9e-bx9zIO8EMq0-X7Q&s=73yCNI9YJUXzkHRvG6ehrB7JBvLK4l12EYJ4ThBmY-M&e=>
>>
>>
>>
>>
>>
>>
>>
>> Thank you,
>>
>>
>>
>> Joey Gilmore
>>
>>
>>
>> Manager - IT Security Systems
>>
>> Information Technology
>>
>> Massachusetts Port Authority
>>
>> One Harborside Drive, Suite 200S
>>
>> East Boston, MA 02128-2909
>>
>> Tel: 617-568-5915
>>
>> Cell: 617[illegible]
>>
>>
>>
>>
>>
>>
>>
>>
>>
>>
>>
>>
>>
>>
>>

From: Egnitz, Brian (POL)
To: Alves, Joe
Subject: RE: MSP LPR
Date: Tuesday, May 26, 2020 9:54:00 AM

Hi Joe,

I'm not sure if this was too short notice. The 3rd & 4th also work.

-Brian

-----Original Message-----
From: Egnitz, Brian (POL)
Sent: Thursday, May 21, 2020 2:34 PM
To: 'Alves, Joe'
Subject: RE: MSP LPR

Can we schedule last two cut overs for 5/28 & 5/29. In speaking with Maj. Ryan, a coordinated road closure via the detail office is warranted.

Thanks, Brian

-----Original Message-----
From: Alves, Joe [mailto:JAlves@massport.com]
Sent: Wednesday, May 13, 2020 6:44 AM
To: Egnitz, Brian (POL)
Subject: Re: MSP LPR

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Ok.

Sent from my iPhone

> On May 13, 2020, at 6:22 AM, Egnitz, Brian (POL) <brian.egnitz@state.ma.us> wrote:
>
> I have a meeting today at 12:00 that I need to go to, but will try and come in after. -Brian
>
>> On May 8, 2020, at 8:26 AM, Alves, Joe <JAlves@massport.com> wrote:
>>
>>
>> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>>
>>
>> Ok.
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@state ma.us>
>> Sent: Friday, May 08, 2020 8:26 AM
>> To: Alves, Joe <JAlves@massport.com>
>> Subject: RE: MSP LPR
>>
>> Thanks should be in for 10 ish. I'll give you a call when I'm a few out.
>>
>> Tks, Brian
>>
>> -----Original Message-----
>> From: Alves, Joe [mailto:JAlves@massport.com]
>> Sent: Thursday, May 7, 2020 9:01 PM
>> To: Egnitz, Brian (POL)
>> Subject: Re: MSP LPR
>>
>>
>> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>>
>>
>> Yes. I'll be around. I can get you in just let me know the time.
>>
>>
>>
>> Sent from my iPhone
>>
>>
>>
>> On May 7, 2020, at 7:49 PM, Egnitz, Brian (POL) <brian.egnitz@state.ma.us> wrote:
>>
>>
>>
>>
>>
>> Are you available tomorrow?
>>
>>
>>
>> On May 4, 2020, at 9:41 AM, Gilmore, Joey <JGilmore@massport.com> wrote:
>>
>>
>>
>>
>>
>> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>>
>>
>>
>>
>>
>> Joe,
>>
>> Later today Brian will send over the actual IMEI numbers that they are using for this project. Once received, can you please confirm if they are unlimited data plans?
>>
>>
>>
>> Brian,
>>
>> Joe Alves is in onsite Wednesday and Friday. He said the G.L. c. 4.sec. 7.cl.26 (n)(sec) is accessible without road closure and would make a good first install. Can you please reach out to him to arrange a time for Wednesday? Joe's cell number G.L. c. 4.sec. 7.cl.26
>>
>>
>>
>>
>>
>> Thank you,
>>

>> Joey Gilmore
>>
>> Manager - IT Security Systems
>>
>> Information Technology
>>
>> Massachusetts Port Authority
>>
>> One Harborside Drive, Suite 200S
>>
>> East Boston, MA 02128-2909
>>
>> Tel: 617-568-5915
>>
>> Cell: 617[redacted]
>>
>>
>>
>>
>>
>>
>>
>>
>>
>> From: Egnitz, Brian (POL) <brian.egnitz@state ma.us>
>>
>> Sent: Thursday, April 23, 2020 10:30 AM
>>
>> To: Gilmore, Joey <JGilmore@massport.com>; Alves, Joe <JAlves@massport.com>; Sillsby, Blane <BSillsby@massport.com>; Quinn, Michael <MQuinn@massport.com>
>>
>> Cc: Haverty, Robert <RHaverty@massport.com>; Harney, Michael <MHarney@massport.com>
>>
>> Subject: RE: MSP LPR
>>
>>
>>
>>
>>
>> -----Original Appointment-----
>>
>> From: Gilmore, Joey [mailto:JGilmore@massport.com]
>>
>> Sent: Wednesday, April 22, 2020 11:35 AM
>>
>> To: Gilmore, Joey; Alves, Joe; Sillsby, Blane; Quinn, Michael; Egnitz, Brian (POL)
>>
>> Cc: Haverty, Robert; Harney, Michael
>>
>> Subject: MSP LPR
>>
>> When: Thursday, April 23, 2020 10:00 AM-11:00 AM (UTC-05:00) Eastern Time (US & Canada).
>>
>> Where: https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_join_500426357&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=3ivMD3mXVSpxMv-g-ajiMkf38VVpxAIvxzFU7zoD-C0&s=ZHyfYIPsksOBeyci6ra3KwL4O4SCPoA_7WEhraXS96Y&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_join_500426357&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FNEWIHnzbfZimE&r=v1eRT_PuOlmt3sh7Lyk24rX9MBSQCKldPuclQWjOSPk&m=PXOFyIolm_rZpuk6yADM63jFy9ok8VUjYC-nn_w6rMY&s=1D-DGoR18hVhptpvf47Fn_SFGKSpwE2u7SIK57_YdrA&e=>
>>
>>
>>
>>
>>
>> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>>
>>
>>
>>
>>
>>
>>
>>
>> Hi Guys,
>>
>>
>>
>>
>>
>>
>>
>>
>> This meeting is to discuss the method of bringing Logan LPR cameras to the EOPSS network.
>>
>>
>>
>>
>>
>>
>>
>>
>> This is the last status update from Chute before he left:
>>
>>
>>
>> "Currently MassPort has[redacted] After several iterations of the system architecture, it has been decided that the path of least resistance is to employ commercial carrier service on the MSP MPLS to the CJIS Datacenter in Chelsea. MSP is working to procure the necessary power adapter and antenna equipment while also identifying accounts and equipment that can be re-purposed for this project. If/when it is feasible for this system to be networked through terrestrial means, MassPort has the switch infrastructure in place to make a direct connection to the EOPSS network at[redacted] I hope this gives a brief overview of where we are at, and please do not hesitate to reach out to me via my personal contact information if any questions come up."
>>
>>
>>
>>
>>
>>
>>
>>
>> MPA - MSP
>>
>> Thu, Apr 23, 2020 10:00 AM - 11:30 AM (EDT)
>>
>>
>>
>> Please join my meeting from your computer, tablet or smartphone.
>>
>> https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_join_500426357&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=3ivMD3mXVSpxMv-g-ajiMkf38VVpxAIvxzFU7zoD-C0&s=ZHyfYIPsksOBeyci6ra3KwL4O4SCPoA_7WEhraXS96Y&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_join_500426357&d=DwMF-g&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=YrOyBDqzLm4zddutRwcvrC8An9e-bx9zIO8EMq0-X7Q&s=bt8qRm7QQabR-s9ufBIIjV-_W5RvGI9slrF4D65fw4&e=>
>>
>>
>>

>> This meeting is locked with a password : [redacted]
>>
>>
>>
>> You can also dial in using your phone.
>>
>> United States: +1 (571) 317-3122<tel:+15713173122,,500426357>
>>
>>
>>
>> Access Code: 500-426-357
>>
>>
>>
>> New to GoToMeeting? Get the app now and be ready when your first meeting starts:
>>
>> https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_install_500426357&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=3ivMD3mXVSpxMv-g-ajiMkf38VVpxAIvxzFU7zoD-C0&s=sPSeiG_aGKwV8Di-BEroqcIxtAzk0va1AAxVy6gZ3Tg&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_install_500426357&d=DwMF-g&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=YrOyBDqzLm4zddutRwcvrC8An9e-bx9zIO8EMq0-X7Q&s=73yCNI9YJUXzkHRvG6ehrB7JBvLK4l12EYJ4ThBmY-M&e=>
>>
>>
>>
>>
>>
>>
>>
>> Thank you,
>>
>>
>>
>> Joey Gilmore
>>
>>
>>
>> Manager - IT Security Systems
>>
>> Information Technology
>>
>> Massachusetts Port Authority
>>
>> One Harborside Drive, Suite 200S
>>
>> East Boston, MA 02128-2909
>>
>> Tel: 617-568-5915
>>
>> Cell: 617[redacted]
>>
>>
>>
>>
>>
>>
>>
>>
>>
>>
>>
>>
>>
>>
>>

From: Egnitz, Brian (POL)
To: Alves, Joe
Subject: RE: MSP LPR
Date: Thursday, May 21, 2020 2:34:00 PM

Can we schedule last two cut overs for 5/28 & 5/29. In speaking with Maj. Ryan, a coordinated road closure via the detail office is warranted.

Thanks, Brian

-----Original Message-----
From: Alves, Joe [mailto:JAlves@massport.com]
Sent: Wednesday, May 13, 2020 6:44 AM
To: Egnitz, Brian (POL)
Subject: Re: MSP LPR

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Ok.

Sent from my iPhone

> On May 13, 2020, at 6:22 AM, Egnitz, Brian (POL) <brian.egnitz@state.ma.us> wrote:
>
> I have a meeting today at 12:00 that I need to go to, but will try and come in after. -Brian
>
>> On May 8, 2020, at 8:26 AM, Alves, Joe <JAlves@massport.com> wrote:
>>
>>
>> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>>
>>
>> Ok.
>>
>> -----Original Message-----
>> From: Egnitz, Brian (POL) <brian.egnitz@state ma.us>
>> Sent: Friday, May 08, 2020 8:26 AM
>> To: Alves, Joe <JAlves@massport.com>
>> Subject: RE: MSP LPR
>>
>> Thanks should be in for 10 ish. I'll give you a call when I'm a few out.
>>
>> Tks, Brian
>>
>> -----Original Message-----
>> From: Alves, Joe [mailto:JAlves@massport.com]
>> Sent: Thursday, May 7, 2020 9:01 PM
>> To: Egnitz, Brian (POL)
>> Subject: Re: MSP LPR
>>
>>
>> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>>
>>
>> Yes. I'll be around. I can get you in just let me know the time.
>>
>>
>>
>> Sent from my iPhone
>>
>>
>>
>> On May 7, 2020, at 7:49 PM, Egnitz, Brian (POL) <brian.egnitz@state.ma.us> wrote:
>>
>>
>>
>>
>>
>> Are you available tomorrow?
>>
>>
>>
>> On May 4, 2020, at 9:41 AM, Gilmore, Joey <JGilmore@massport.com> wrote:
>>
>>
>>
>>
>>
>> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>>
>>
>>
>>
>>
>> Joe,
>>
>> Later today Brian will send over the actual IMEI numbers that they are using for this project. Once received, can you please confirm if they are unlimited data plans?
>>
>>
>>
>> Brian,
>>
>> Joe Alves is in onsite Wednesday and Friday. He said the G.L. c. 4.sec. 7.cl.26 (n)(secu is accessible without road closure and would make a good first install. Can you please reach out to him to arrange a time for Wednesday? Joe's cell number is 781 G.L. c. 4.sec
>>
>>
>>
>>
>>
>> Thank you,
>>
>> Joey Gilmore
>>
>> Manager - IT Security Systems
>>
>> Information Technology
>>
>> Massachusetts Port Authority
>>
>> One Harborside Drive, Suite 200S
>>
>> East Boston, MA 02128-2909
>>

>> Tel: 617-568-5915
>>
>> Cell: 617[redacted]
>>
>>
>>
>>
>>
>>
>>
>>
>>
>> From: Egnitz, Brian (POL) <brian.egnitz@state ma.us>
>>
>> Sent: Thursday, April 23, 2020 10:30 AM
>>
>> To: Gilmore, Joey <JGilmore@massport.com>; Alves, Joe <JAlves@massport.com>; Sillsby, Blane <BSillsby@massport.com>; Quinn, Michael <MQuinn@massport.com>
>>
>> Cc: Haverty, Robert <RHaverty@massport.com>; Harney, Michael <MHarney@massport.com>
>>
>> Subject: RE: MSP LPR
>>
>>
>>
>>
>>
>> -----Original Appointment-----
>>
>> From: Gilmore, Joey [mailto:JGilmore@massport.com]
>>
>> Sent: Wednesday, April 22, 2020 11:35 AM
>>
>> To: Gilmore, Joey; Alves, Joe; Sillsby, Blane; Quinn, Michael; Egnitz, Brian (POL)
>>
>> Cc: Haverty, Robert; Harney, Michael
>>
>> Subject: MSP LPR
>>
>> When: Thursday, April 23, 2020 10:00 AM-11:00 AM (UTC-05:00) Eastern Time (US & Canada).
>>
>> Where: https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_join_500426357&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=3ivMD3mXVSpxMv-g-ajiMkf38VVpxAIvxzFU7zoD-C0&s=ZHyfYIPsksOBeyci6ra3KwL4O4SCPoA_7WEhraXS96Y&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_join_500426357&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FNEWIHnzbfZimE&r=v1eRT_PuOlmt3sh7Lyk24rX9MBSQCKldPuclQWjOSPk&m=PXOFyIolm_rZpuk6yADM63jFy9ok8VUjYC-nn_w6rMY&s=1D-DGoR18hVhptpvf47Fn_SFGKSpwE2u7SIK57_YdrA&e=>
>>
>>
>>
>>
>>
>> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>>
>>
>>
>>
>>
>>
>>
>> Hi Guys,
>>
>>
>>
>>
>>
>>
>>
>> This meeting is to discuss the method of bringing Logan LPR cameras to the EOPSS network.
>>
>>
>>
>>
>>
>>
>>
>> This is the last status update from Chute before he left:
>>
>>
>>
>> "Currently MassPort has[redacted] After several iterations of the system architecture, it has been decided that the path of least resistance is to employ commercial carrier service on the MSP MPLS to the CJIS Datacenter in Chelsea. MSP is working to procure the necessary power adapter and antenna equipment while also identifying accounts and equipment that can be re-purposed for this project. If/when it is feasible for this system to be networked through terrestrial means, MassPort has the switch infrastructure in place to make a direct connection to the EOPSS network at[redacted] I hope this gives a brief overview of where we are at, and please do not hesitate to reach out to me via my personal contact information if any questions come up."
>>
>>
>>
>>
>>
>>
>>
>> MPA - MSP
>>
>> Thu, Apr 23, 2020 10:00 AM - 11:30 AM (EDT)
>>
>>
>>
>> Please join my meeting from your computer, tablet or smartphone.
>>
>> https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_join_500426357&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=3ivMD3mXVSpxMv-g-ajiMkf38VVpxAIvxzFU7zoD-C0&s=ZHyfYIPsksOBeyci6ra3KwL4O4SCPoA_7WEhraXS96Y&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_join_500426357&d=DwMF-g&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=YrOyBDqzLm4zddutRwcvrC8An9e-bx9zIO8EMq0-X7Q&s=bt8qRm7QQabR-s9uIfBIIjV-_W5RvGI9slrF4D65fw4&e=>
>>
>>
>>
>> This meeting is locked with a password.[redacted]
>>
>>
>>
>> You can also dial in using your phone.
>>
>> United States: +1 (571) 317-3122<tel:+15713173122,,500426357>
>>
>>
>>
>> Access Code: 500-426-357
>>

>>
>>
>> New to GoToMeeting? Get the app now and be ready when your first meeting starts:
>>
>> https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_install_500426357&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=3ivMD3mXVSpxMv-g-ajiMkf38VVpxAIvxzFU7zoD-C0&s=sPSeiG_aGKwV8Di-BEroqcIxtAzk0va1AAxVy6gZ3Tg&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_install_500426357&d=DwMF-g&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=YrOyBDqzLm4zddutRwcvrC8An9e-bx9zIO8EMq0-X7Q&s=73yCNI9YJUXzkHRvG6ehrB7JBvLK4l12EYJ4ThBmY-M&e=>
>>
>>
>>
>>
>>
>>
>>
>> Thank you,
>>
>>
>>
>> Joey Gilmore
>>
>>
>>
>> Manager - IT Security Systems
>>
>> Information Technology
>>
>> Massachusetts Port Authority
>>
>> One Harborside Drive, Suite 200S
>>
>> East Boston, MA 02128-2909
>>
>> Tel: 617-568-5915
>>
>> Cell: 617[redacted]
>>
>>
>>
>>
>>
>>
>>
>>
>>
>>
>>
>>
>>
>>

From: Alves, Joe
To: Egnitz, Brian (POL)
Subject: RE: MSP LPR
Date: Friday, May 8, 2020 8:26:32 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Ok.

-----Original Message-----
From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Friday, May 08, 2020 8:26 AM
To: Alves, Joe <JAlves@massport.com>
Subject: RE: MSP LPR

Thanks should be in for 10 ish. I'll give you a call when I'm a few out.

Tks, Brian

-----Original Message-----
From: Alves, Joe [mailto:JAlves@massport.com]
Sent: Thursday, May 7, 2020 9:01 PM
To: Egnitz, Brian (POL)
Subject: Re: MSP LPR

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Yes. I'll be around. I can get you in just let me know the time.

Sent from my iPhone

On May 7, 2020, at 7:49 PM, Egnitz, Brian (POL) <brian.egnitz@state ma.us> wrote:

Are you available tomorrow?

On May 4, 2020, at 9:41 AM, Gilmore, Joey <JGilmore@massport.com> wrote:

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Joe,

Later today Brian will send over the actual IMEI numbers that they are using for this project. Once received, can you please confirm if they are unlimited data plans?

Brian,

Joe Alves is in onsite Wednesday and Friday. He said the[redacted] is accessible without road closure and would make a good first install. Can you please reach out to him to arrange a time for Wednesday? Joe's cell number is 781[redacted]

Thank you,

Joey Gilmore

Manager - IT Security Systems

Information Technology

Massachusetts Port Authority

One Harborside Drive, Suite 200S

East Boston, MA 02128-2909

Tel: 617-568-5915

Cell: 617[redacted]

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>

Sent: Thursday, April 23, 2020 10:30 AM

To: Gilmore, Joey <JGilmore@massport.com>; Alves, Joe <JAlves@massport.com>; Sillsby, Blane <BSillsby@massport.com>; Quinn, Michael <MQuinn@massport.com>

Cc: Haverty, Robert <RHaverty@massport.com>; Harney, Michael <MHarney@massport.com>

Subject: RE: MSP LPR

-----Original Appointment-----

From: Gilmore, Joey [mailto:JGilmore@massport.com]

Sent: Wednesday, April 22, 2020 11:35 AM

To: Gilmore, Joey; Alves, Joe; Sillsby, Blane; Quinn, Michael; Egnitz, Brian (POL)

Cc: Haverty, Robert; Harney, Michael

Subject: MSP LPR

When: Thursday, April 23, 2020 10:00 AM-11:00 AM (UTC-05:00) Eastern Time (US & Canada).

Where: https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_join_500426357&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=3ivMD3mXVSpxMv-g-ajiMkf38VVpxAIvxzFU7zoD-C0&s=ZHyfYIPsksOBeyci6ra3KwL4O4SCPoA_7WEhraXS96Y&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_join_500426357&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FNEWIHnzbfZimE&r=v1eRT_PuOlmt3sh7Lyk24rX9MBSQCKldPuclQWjOSPk&m=PXOFyIolm_rZpuk6yADM63jFy9ok8VUjYC-nn_w6rMY&s=1D-DGoR18hVhptpvf47Fn_SFGKSpwE2u7SIK57_YdrA&e=>

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Hi Guys,

This meeting is to discuss the method of bringing Logan LPR cameras to the EOPSS network.

This is the last status update from Chute before he left:

“Currently MassPort has [redacted]: After several iterations of the system architecture, it has been decided that the path of least resistance is to employ commercial carrier service on the MSP MPLS to the CJIS Datacenter in Chelsea. MSP is working to procure the necessary power adapter and antenna equipment while also identifying accounts and equipment that can be re-purposed for this project. If/when it is feasible for this system to be networked through terrestrial means, MassPort has the switch infrastructure in place to make a direct connection to the EOPSS network at [redacted]. I hope this gives a brief overview of where we are at, and please do not hesitate to reach out to me via my personal contact information if any questions come up.”

MPA - MSP

Thu, Apr 23, 2020 10:00 AM - 11:30 AM (EDT)

Please join my meeting from your computer, tablet or smartphone.

https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_join_500426357&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=3ivMD3mXVSpxMv-g-ajiMkf38VVpxAIvxzFU7zoD-C0&s=ZHyfYIPsksOBeyci6ra3KwL4O4SCPoA_7WEhraXS96Y&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_join_500426357&d=DwMF-g&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=YrOyBDqzLm4zddutRwcvrC8An9e-bx9zIO8EMq0-X7Q&s=bt8qRm7QQabR-s9uIfBIlyV-_W5RvGI9slrF4D65fw4&e=>

This meeting is locked with a password : [redacted]

You can also dial in using your phone.

United States: +1 (571) 317-3122<tel:+15713173122,,500426357>

Access Code: 500-426-357

New to GoToMeeting? Get the app now and be ready when your first meeting starts:

https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_install_500426357&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=3ivMD3mXVSpxMv-g-ajiMkf38VVpxAIvxzFU7zoD-C0&s=sPSeiG_aGKwV8Di-BEroqcIxtAzk0va1AAxVy6gZ3Tg&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_install_500426357&d=DwMF-g&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=YrOyBDqzLm4zddutRwcvrC8An9e-bx9zIO8EMq0-X7Q&s=73yCNI9YJUXzkHRvG6ehrB7JBvLK4l12EYJ4ThBmY-M&e=>

Thank you,

Joey Gilmore

Manager - IT Security Systems

Information Technology

Massachusetts Port Authority

One Harborside Drive, Suite 200S

East Boston, MA 02128-2909

Tel: 617-568-5915

Cell: 617[redacted]

From: Egnitz, Brian (POL)
To: Alves, Joe
Subject: RE: MSP LPR
Date: Friday, May 8, 2020 8:25:00 AM

Thanks should be in for 10 ish. I'll give you a call when I'm a few out.

Tks, Brian

-----Original Message-----
From: Alves, Joe [mailto:JAlves@massport.com]
Sent: Thursday, May 7, 2020 9:01 PM
To: Egnitz, Brian (POL)
Subject: Re: MSP LPR

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Yes. I'll be around. I can get you in just let me know the time.

Sent from my iPhone

On May 7, 2020, at 7:49 PM, Egnitz, Brian (POL) <brian.egnitz@state ma.us> wrote:

Are you available tomorrow?

On May 4, 2020, at 9:41 AM, Gilmore, Joey <JGilmore@massport.com> wrote:

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Joe,

Later today Brian will send over the actual IMEI numbers that they are using for this project. Once received, can you please confirm if they are unlimited data plans?

Brian,

Joe Alves is in onsite Wednesday and Friday. He said the [redacted] is accessible without road closure and would make a good first install. Can you please reach out to him to arrange a time for Wednesday? Joe's cell number is 781[redacted]

Thank you,

Joey Gilmore

Manager - IT Security Systems

Information Technology

Massachusetts Port Authority

One Harborside Drive, Suite 200S

East Boston, MA 02128-2909

Tel: 617-568-5915

Cell: 617[redacted]

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>

Sent: Thursday, April 23, 2020 10:30 AM

To: Gilmore, Joey <JGilmore@massport.com>; Alves, Joe <JAlves@massport.com>; Sillsby, Blane <BSillsby@massport.com>; Quinn, Michael <MQuinn@massport.com>

Cc: Haverty, Robert <RHaverty@massport.com>; Harney, Michael <MHarney@massport.com>

Subject: RE: MSP LPR

-----Original Appointment-----

From: Gilmore, Joey [mailto:JGilmore@massport.com]

Sent: Wednesday, April 22, 2020 11:35 AM

To: Gilmore, Joey; Alves, Joe; Sillsby, Blane; Quinn, Michael; Egnitz, Brian (POL)

Cc: Haverty, Robert; Harney, Michael

Subject: MSP LPR

When: Thursday, April 23, 2020 10:00 AM-11:00 AM (UTC-05:00) Eastern Time (US & Canada).

Where: https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_join_500426357&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=3ivMD3mXVSpxMv-g-ajiMkf38VVpxAIvxzFU7zoD-C0&s=ZHyfYIPsksOBeyci6ra3KwL4O4SCPoA_7WEhraXS96Y&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_join_500426357&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FNEWIHnzbfZimE&r=v1eRT_PuOlmt3sh7Lyk24rX9MBSQCKldPuclQWjOSPk&m=PXOFyIolm_rZpuk6yADM63jFy9ok8VUjYC-nn_w6rMY&s=1D-DGoR18hVhptpvf47Fn_SFGKSpwE2u7SIK57_YdrA&e=>

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Hi Guys,

This meeting is to discuss the method of bringing Logan LPR cameras to the EOPSS network.

This is the last status update from Chute before he left:

“Currently MassPort has [redacted] After several iterations of the system architecture, it has been decided that the path of least resistance is to employ commercial carrier service on the MSP MPLS to the CJIS Datacenter in Chelsea. MSP is working to procure the necessary power adapter and antenna equipment while also identifying accounts and equipment that can be re-purposed for this project. If/when it is feasible for this system to be networked through terrestrial means, MassPort has the switch infrastructure in place to make a direct connection to the EOPSS network at [redacted] I hope this gives a brief overview of where we are at, and please do not hesitate to reach out to me via my personal contact information if any questions come up.”

MPA - MSP

Thu, Apr 23, 2020 10:00 AM - 11:30 AM (EDT)

Please join my meeting from your computer, tablet or smartphone.

https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_join_500426357&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=3ivMD3mXVSpxMv-g-ajiMkf38VVpxAIvxzFU7zoD-C0&s=ZHyfYIPsksOBeyci6ra3KwL4O4SCPoA_7WEhraXS96Y&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_join_500426357&d=DwMF-g&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=YrOyBDqzLm4zddutRwcvrC8An9e-bx9zIO8EMq0-X7Q&s=bt8qRm7QQabR-s9uIfBIlyV-_W5RvGI9slrF4D65fw4&e=>

This meeting is locked with a password : [redacted]

You can also dial in using your phone.

United States: +1 (571) 317-3122<tel:+15713173122,,500426357>

Access Code: 500-426-357

New to GoToMeeting? Get the app now and be ready when your first meeting starts:

https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_install_500426357&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=3ivMD3mXVSpxMv-g-ajiMkf38VVpxAIvxzFU7zoD-C0&s=sPSeiG_aGKwV8Di-BEroqcIxtAzk0va1AAxVy6gZ3Tg&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_install_500426357&d=DwMF-g&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=YrOyBDqzLm4zddutRwcvrC8An9e-bx9zIO8EMq0-X7Q&s=73yCNI9YJUXzkHRvG6ehrB7JBvLK4l12EYJ4ThBmY-M&e=>

Thank you,

Joey Gilmore

Manager - IT Security Systems

Information Technology

Massachusetts Port Authority

One Harborside Drive, Suite 200S

East Boston, MA 02128-2909

Tel: 617-568-5915

Cell: 617[redacted]

From: Egnitz, Brian (POL)
To: Gilmore, Joey; Alves, Joe; Sillsby, Blane; Quinn, Michael
Cc: Haverty, Robert; Harney, Michael
Subject: RE: MSP LPR
Date: Wednesday, May 6, 2020 6:47:00 PM

Hi All,

Just a quick update. Joe and I were able to move [redacted] from Airport Road inbound into the EOPSS data center. They are working correctly and are writing data in a timely manner to the BOSS Server. I would like to continue work on the remaining camera tomorrow or Friday. Once complete, I'd like to begin cutting over the cameras by the bus terminal near the barracks.

Thanks for the assistance, Brian

From: Gilmore, Joey [mailto:JGilmore@massport.com]
Sent: Monday, May 4, 2020 9:41 AM
To: Egnitz, Brian (POL); Alves, Joe; Sillsby, Blane; Quinn, Michael
Cc: Haverty, Robert; Harney, Michael
Subject: RE: MSP LPR

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Joe,
Later today Brian will send over the actual IMEI numbers that they are using for this project. Once received, can you please confirm if they are unlimited data plans?

Brian,
Joe Alves is in onsite Wednesday and Friday. He said the [redacted] is accessible without road closure and would make a good first install. Can you please reach out to him to arrange a time for Wednesday? Joe's cell number is 781-[redacted]

Thank you,
Joey Gilmore
Manager - IT Security Systems
Information Technology
Massachusetts Port Authority
One Harborside Drive, Suite 200S
East Boston, MA 02128-2909
Tel: 617-568-5915
Cell: 617-[redacted]

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Thursday, April 23, 2020 10:30 AM
To: Gilmore, Joey <JGilmore@massport.com>; Alves, Joe <JAlves@massport.com>; Sillsby, Blane <BSillsby@massport.com>; Quinn, Michael <MQuinn@massport.com>
Cc: Haverty, Robert <RHaverty@massport.com>; Harney, Michael <MHarney@massport.com>
Subject: RE: MSP LPR

-----Original Appointment-----
From: Gilmore, Joey [mailto:JGilmore@massport.com]
Sent: Wednesday, April 22, 2020 11:35 AM
To: Gilmore, Joey; Alves, Joe; Sillsby, Blane; Quinn, Michael; Egnitz, Brian (POL)
Cc: Haverty, Robert; Harney, Michael
Subject: MSP LPR
When: Thursday, April 23, 2020 10:00 AM-11:00 AM (UTC-05:00) Eastern Time (US & Canada).
Where: https://global.gotomeeting.com/join/500426357

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Hi Guys,

This meeting is to discuss the method of bringing Logan LPR cameras to the EOPSS network.

This is the last status update from Chute before he left:

"Currently MassPort has [redacted] After several iterations of the system architecture, it has been decided that the path of least resistance is to employ commercial carrier service on the MSP MPLS to the CJIS Datacenter in Chelsea. MSP is working to procure the necessary power adapter and antenna equipment while also identifying accounts and equipment that can be re-purposed for this project. If/when it is feasible for this system to be networked through terrestrial means, MassPort has the switch infrastructure in place to make a direct connection to the EOPSS network at [redacted] I hope this gives a brief overview of where we are at, and please do not hesitate to reach out to me via my personal contact information if any questions come up."

MPA - MSP
Thu, Apr 23, 2020 10:00 AM - 11:30 AM (EDT)

Please join my meeting from your computer, tablet or smartphone.
https://global.gotomeeting.com/join/500426357

This meeting is locked with a password : [redacted]

You can also dial in using your phone.
United States: +1 (571) 317-3122

Access Code: 500-426-357

New to GoToMeeting? Get the app now and be ready when your first meeting starts:
https://global.gotomeeting.com/install/500426357

Thank you,

Joey Gilmore

Manager - IT Security Systems
Information Technology
Massachusetts Port Authority
One Harborside Drive, Suite 200S
East Boston, MA 02128-2909
Tel: 617-568-5915
Cell: 617-[redacted]

From: Gilmore, Joey
To: Egnitz, Brian (POL); Alves, Joe; Sillsby, Blane; Quinn, Michael
Cc: Haverty, Robert; Harney, Michael
Subject: RE: MSP LPR
Date: Monday, May 4, 2020 9:41:20 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Joe,
Later today Brian will send over the actual IMEI numbers that they are using for this project. Once received, can you please confirm if they are unlimited data plans?

Brian,
Joe Alves is in onsite Wednesday and Friday. He said the [redacted] is accessible without road closure and would make a good first install. Can you please reach out to him to arrange a time for Wednesday? Joe's cell number is 781-[redacted]

Thank you,
Joey Gilmore
Manager - IT Security Systems
Information Technology
Massachusetts Port Authority
One Harborside Drive, Suite 200S
East Boston, MA 02128-2909
Tel: 617-568-5915
Cell: 617-[redacted]

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Thursday, April 23, 2020 10:30 AM
To: Gilmore, Joey <JGilmore@massport.com>; Alves, Joe <JAlves@massport.com>; Sillsby, Blane <BSillsby@massport.com>; Quinn, Michael <MQuinn@massport.com>
Cc: Haverty, Robert <RHaverty@massport.com>; Harney, Michael <MHarney@massport.com>
Subject: RE: MSP LPR

-----Original Appointment-----
From: Gilmore, Joey [mailto:JGilmore@massport.com]
Sent: Wednesday, April 22, 2020 11:35 AM
To: Gilmore, Joey; Alves, Joe; Sillsby, Blane; Quinn, Michael; Egnitz, Brian (POL)
Cc: Haverty, Robert; Harney, Michael
Subject: MSP LPR
When: Thursday, April 23, 2020 10:00 AM-11:00 AM (UTC-05:00) Eastern Time (US & Canada).
Where: https://global.gotomeeting.com/join/500426357

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Hi Guys,

This meeting is to discuss the method of bringing Logan LPR cameras to the EOPSS network.

This is the last status update from Chute before he left:

"Currently MassPort has [redacted] After several iterations of the system architecture, it has been decided that the path of least resistance is to employ commercial carrier service on the MSP MPLS to the CJIS Datacenter in Chelsea. MSP is working to procure the necessary power adapter and antenna equipment while also identifying accounts and equipment that can be re-purposed for this project. If/when it is feasible for this system to be networked through terrestrial means, MassPort has the switch infrastructure in place to make a direct connection to the EOPSS network at [redacted] I hope this gives a brief overview of where we are at, and please do not hesitate to reach out to me via my personal contact information if any questions come up."

MPA - MSP
Thu, Apr 23, 2020 10:00 AM - 11:30 AM (EDT)

Please join my meeting from your computer, tablet or smartphone.
https://global.gotomeeting.com/join/500426357

This meeting is locked with a password : [redacted]

You can also dial in using your phone.
United States: +1 (571) 317-3122

Access Code: 500-426-357

New to GoToMeeting? Get the app now and be ready when your first meeting starts:
https://global.gotomeeting.com/install/500426357

Thank you,

Joey Gilmore

Manager - IT Security Systems
Information Technology
Massachusetts Port Authority
One Harborside Drive, Suite 200S
East Boston, MA 02128-2909
Tel: 617-568-5915
Cell: 617-[redacted]

From: Haverty, Robert
To: Egnitz, Brian (POL); Gilmore, Joey; Alves, Joe; Sillsby, Blane; Quinn, Michael
Cc: Harney, Michael
Subject: RE: MSP LPR
Date: Friday, May 1, 2020 8:04:40 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

OK, please advise on date and location.

Thanks,
Bob

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Thursday, April 30, 2020 8:59 PM
To: Gilmore, Joey <JGilmore@massport.com>; Alves, Joe <JAlves@massport.com>; Sillsby, Blane <BSillsby@massport.com>; Quinn, Michael <MQuinn@massport.com>
Cc: Haverty, Robert <RHaverty@massport.com>; Harney, Michael <MHarney@massport.com>
Subject: RE: MSP LPR

Just a quick update, LT. Crouse and I will be at Logan tomorrow AM removing the Modems. If all goes well, I'd like to schedule a sector migration next week.

-Brian

From: Gilmore, Joey [mailto:JGilmore@massport.com]
Sent: Thursday, April 23, 2020 10:35 AM
To: Alves, Joe; Sillsby, Blane; Quinn, Michael; Egnitz, Brian (POL)
Cc: Haverty, Robert; Harney, Michael
Subject: RE: MSP LPR

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Just to recap:

The plan is to identify and remove [redacted] MP70 modems from Troop F cruisers. (MSP)
Validate these have unlimited data plans. (MPA – Joe A)
Wait for the power adapters. (MSP – Brian)
[redacted] at the LPR locations inside existing communication boxes and 1 as a spare/test unit. (MSP Harney/Brian & MPA Joe A)
MSP will access the BOSS system through State Police network.

Eventually these modems/routers will be hard wired into MPA network and get a policy that allows

VPN connection to MSP@Chelsea. (MSP Brian & MPA Network/Cyber)
After migration to hard wire, cellular data plans can be cancelled or used for something else at Logan if we want to preserve grandfathered unlimited plan.

Please let me know if I missed any important details.

Thank you,
Joey Gilmore
Manager - IT Security Systems
Information Technology
Massachusetts Port Authority
One Harborside Drive, Suite 200S
East Boston, MA 02128-2909
Tel: 617-568-5915
Cell: 617-[redacted]

-----Original Appointment-----
From: Gilmore, Joey
Sent: Wednesday, April 22, 2020 11:34 AM
To: Gilmore, Joey; Alves, Joe; Sillsby, Blane; Quinn, Michael; brian.egnitz@state.ma.us
Cc: Haverty, Robert; Harney, Michael
Subject: MSP LPR
When: Thursday, April 23, 2020 10:00 AM-11:00 AM (UTC-05:00) Eastern Time (US & Canada).
Where: https://global.gotomeeting.com/join/500426357

Hi Guys,

This meeting is to discuss the method of bringing Logan LPR cameras to the EOPSS network.

This is the last status update from Chute before he left:
"Currently MassPort has [redacted] After several iterations of the system architecture, it has been decided that the path of least resistance is to employ commercial carrier service on the MSP MPLS to the CJIS Datacenter in Chelsea. MSP is working to procure the necessary power adapter and antenna equipment while also identifying accounts and equipment that can be re-purposed for this project. If/when it is feasible for this system to be networked through terrestrial means, MassPort has the switch infrastructure in place to make a direct connection to the EOPSS network at [redacted] I hope this gives a brief overview of where we are at, and please do not hesitate to reach out to me via my personal contact information if any questions come up."

MPA - MSP

Thu, Apr 23, 2020 10:00 AM - 11:30 AM (EDT)

Please join my meeting from your computer, tablet or smartphone.
https://global.gotomeeting.com/join/500426357

This meeting is locked with a password : [redacted]

You can also dial in using your phone.
United States: +1 (571) 317-3122

Access Code: 500-426-357

New to GoToMeeting? Get the app now and be ready when your first meeting starts:
https://global.gotomeeting.com/install/500426357

Thank you,
Joey Gilmore
Manager - IT Security Systems
Information Technology
Massachusetts Port Authority
One Harborside Drive, Suite 200S
East Boston, MA 02128-2909
Tel: 617-568-5915
Cell: 617-[redacted]

From: Egnitz, Brian (POL)
To: Gilmore, Joey; Alves, Joe; Sillsby, Blane; Quinn, Michael
Cc: Haverty, Robert; Harney, Michael
Subject: RE: MSP LPR
Date: Thursday, April 30, 2020 8:58:00 PM

Just a quick update, LT. Crouse and I will be at Logan tomorrow AM removing the Modems. If all goes well, I'd like to schedule a sector migration next week.

-Brian

From: Gilmore, Joey [mailto:JGilmore@massport.com]
Sent: Thursday, April 23, 2020 10:35 AM
To: Alves, Joe; Sillsby, Blane; Quinn, Michael; Egnitz, Brian (POL)
Cc: Haverty, Robert; Harney, Michael
Subject: RE: MSP LPR

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Just to recap:

The plan is to identify and remove [redacted] MP70 modems from Troop F cruisers. (MSP)
Validate these have unlimited data plans. (MPA – Joe A)
Wait for the power adapters. (MSP – Brian)
[redacted] at the LPR locations inside existing communication boxes and 1 as a spare/test unit. (MSP Harney/Brian & MPA Joe A)
MSP will access the BOSS system through State Police network.

Eventually these modems/routers will be hard wired into MPA network and get a policy that allows VPN connection to MSP@Chelsea. (MSP Brian & MPA Network/Cyber)
After migration to hard wire, cellular data plans can be cancelled or used for something else at Logan if we want to preserve grandfathered unlimited plan.

Please let me know if I missed any important details.

Thank you,
Joey Gilmore
Manager - IT Security Systems
Information Technology
Massachusetts Port Authority
One Harborside Drive, Suite 200S
East Boston, MA 02128-2909
Tel: 617-568-5915
Cell: 617-[redacted]

-----Original Appointment-----
From: Gilmore, Joey
Sent: Wednesday, April 22, 2020 11:34 AM
To: Gilmore, Joey; Alves, Joe; Sillsby, Blane; Quinn, Michael; brian.egnitz@state.ma.us
Cc: Haverty, Robert; Harney, Michael
Subject: MSP LPR
When: Thursday, April 23, 2020 10:00 AM-11:00 AM (UTC-05:00) Eastern Time (US & Canada).
Where: https://global.gotomeeting.com/join/500426357

Hi Guys,

This meeting is to discuss the method of bringing Logan LPR cameras to the EOPSS network.

This is the last status update from Chute before he left:
"Currently MassPort has [redacted] After several iterations of the system architecture, it has been decided that the path of least resistance is to employ commercial carrier service on the MSP MPLS to the CJIS Datacenter in Chelsea. MSP is working to procure the necessary power adapter and antenna equipment while also identifying accounts and equipment that can be re-purposed for this project. If/when it is feasible for this system to be networked through terrestrial means, MassPort has the switch infrastructure in place to make a direct connection to the EOPSS network at [redacted] I hope this gives a brief overview of where we are at, and please do not hesitate to reach out to me via my personal contact information if any questions come up."

MPA - MSP

Thu, Apr 23, 2020 10:00 AM - 11:30 AM (EDT)

Please join my meeting from your computer, tablet or smartphone.
https://global.gotomeeting.com/join/500426357

This meeting is locked with a password : [redacted]

You can also dial in using your phone.
United States: +1 (571) 317-3122

Access Code: 500-426-357

New to GoToMeeting? Get the app now and be ready when your first meeting starts:
https://global.gotomeeting.com/install/500426357

Thank you,
Joey Gilmore
Manager - IT Security Systems
Information Technology
Massachusetts Port Authority
One Harborside Drive, Suite 200S
East Boston, MA 02128-2909

Tel: 617-568-5915
Cell: 617-[redacted]

From: Gilmore, Joey
To: Alves, Joe; Sillsby, Blane; Quinn, Michael; Egnitz, Brian (POL)
Cc: Haverty, Robert; Harney, Michael
Subject: RE: MSP LPR
Date: Thursday, April 23, 2020 10:35:36 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Just to recap:

The plan is to identify and remove [redacted] MP70 modems from Troop F cruisers. (MSP)
Validate these have unlimited data plans. (MPA – Joe A)
Wait for the power adapters. (MSP – Brian)
[redacted] at the LPR locations inside existing communication boxes and 1 as a spare/test unit. (MSP Harney/Brian & MPA Joe A)
MSP will access the BOSS system through State Police network.

Eventually these modems/routers will be hard wired into MPA network and get a policy that allows VPN connection to MSP@Chelsea. (MSP Brian & MPA Network/Cyber)
After migration to hard wire, cellular data plans can be cancelled or used for something else at Logan if we want to preserve grandfathered unlimited plan.

Please let me know if I missed any important details.

Thank you,
Joey Gilmore
Manager - IT Security Systems
Information Technology
Massachusetts Port Authority
One Harborside Drive, Suite 200S
East Boston, MA 02128-2909
Tel: 617-568-5915
Cell: 617-[redacted]

-----Original Appointment-----
From: Gilmore, Joey
Sent: Wednesday, April 22, 2020 11:34 AM
To: Gilmore, Joey; Alves, Joe; Sillsby, Blane; Quinn, Michael; brian.egnitz@state.ma.us
Cc: Haverty, Robert; Harney, Michael
Subject: MSP LPR
When: Thursday, April 23, 2020 10:00 AM-11:00 AM (UTC-05:00) Eastern Time (US & Canada).
Where: https://global.gotomeeting.com/join/500426357

Hi Guys,

This meeting is to discuss the method of bringing Logan LPR cameras to the EOPSS network.

This is the last status update from Chute before he left:
"Currently MassPort has [redacted] After several iterations of the system architecture, it has been decided that the path of least resistance is to employ commercial carrier service on the MSP MPLS to the CJIS Datacenter in Chelsea. MSP is working to procure the necessary power adapter and antenna equipment while also identifying accounts and equipment that can be re-purposed for this project. If/when it is feasible for this system to be networked through terrestrial means, MassPort has the switch infrastructure in place to make a direct connection to the EOPSS network at [redacted] I hope this gives a brief overview of where we are at, and please do not hesitate to reach out to me via my personal contact information if any questions come up."

MPA - MSP

Thu, Apr 23, 2020 10:00 AM - 11:30 AM (EDT)

Please join my meeting from your computer, tablet or smartphone.
https://global.gotomeeting.com/join/500426357

This meeting is locked with a password : [redacted]

You can also dial in using your phone.
United States: +1 (571) 317-3122

Access Code: 500-426-357

New to GoToMeeting? Get the app now and be ready when your first meeting starts:
https://global.gotomeeting.com/install/500426357

Thank you,
Joey Gilmore
Manager - IT Security Systems
Information Technology
Massachusetts Port Authority
One Harborside Drive, Suite 200S
East Boston, MA 02128-2909
Tel: 617-568-5915
Cell: 617-[redacted]

From: Alves, Joe
To: Egnitz, Brian (POL); Haverty, Robert
Subject: Re: MSP LPR
Date: Wednesday, June 10, 2020 8:23:35 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Adding Bob. I'm not sure where this is right now.

Sent from my iPhone

> On Jun 10, 2020, at 7:59 AM, Egnitz, Brian (POL) <brian.egnitz@state ma.us> wrote:
>
> Any luck?
>
> -----Original Message-----
> From: Egnitz, Brian (POL)
> Sent: Tuesday, May 26, 2020 9:54 AM
> To: Alves, Joe
> Subject: RE: MSP LPR
>
> Hi Joe,
>
> I'm not sure if this was too short notice. The 3rd & 4th also work.
>
> -Brian
>
> -----Original Message-----
> From: Egnitz, Brian (POL)
> Sent: Thursday, May 21, 2020 2:34 PM
> To: 'Alves, Joe'
> Subject: RE: MSP LPR
>
> Can we schedule last two cut overs for 5/28 & 5/29. In speaking with Maj. Ryan, a coordinated road closure via the detail office is warranted.
>
> Thanks, Brian
>
> -----Original Message-----
> From: Alves, Joe [mailto:JAlves@massport.com]
> Sent: Wednesday, May 13, 2020 6:44 AM
> To: Egnitz, Brian (POL)
> Subject: Re: MSP LPR
>
>
> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>
>
> Ok.
>
> Sent from my iPhone
>
>> On May 13, 2020, at 6:22 AM, Egnitz, Brian (POL) <brian.egnitz@state ma.us> wrote:
>>
>> I have a meeting today at 12:00 that I need to go to, but will try and come in after. -Brian
>>
>>>> On May 8, 2020, at 8:26 AM, Alves, Joe <JAlves@massport.com> wrote:
>>>
>>>
>>> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>>>
>>>
>>> Ok.
>>>
>>> -----Original Message-----
>>> From: Egnitz, Brian (POL) <brian.egnitz@state ma.us>
>>> Sent: Friday, May 08, 2020 8:26 AM
>>> To: Alves, Joe <JAlves@massport.com>
>>> Subject: RE: MSP LPR
>>>
>>> Thanks should be in for 10 ish. I'll give you a call when I'm a few out.
>>>
>>> Tks, Brian
>>>
>>> -----Original Message-----
>>> From: Alves, Joe [mailto:JAlves@massport.com]
>>> Sent: Thursday, May 7, 2020 9:01 PM
>>> To: Egnitz, Brian (POL)
>>> Subject: Re: MSP LPR
>>>
>>>
>>> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>>>
>>>
>>> Yes. I'll be around. I can get you in just let me know the time.
>>>
>>>
>>>
>>> Sent from my iPhone
>>>
>>>
>>>
>>>>> On May 7, 2020, at 7:49 PM, Egnitz, Brian (POL) <brian.egnitz@state ma.us> wrote:
>>>
>>>
>>>
>>>
>>>
>>> Are you available tomorrow?
>>>
>>>
>>>
>>>>> On May 4, 2020, at 9:41 AM, Gilmore, Joey <JGilmore@massport.com> wrote:
>>>
>>>
>>>
>>>
>>>
>>> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>>>
>>>
>>>
>>>

>>>
>>> Joe,
>>>
>>> Later today Brian will send over the actual IMEI numbers that they are using for this project. Once received, can you please confirm if they are unlimited data plans?
>>>
>>>
>>>
>>> Brian,
>>>
>>> Joe Alves is in onsite Wednesday and Friday. He said the G.L. c. 4,sec. 7,cl.26 (n)(sec[illegible] is accessible without road closure and would make a good first install. Can you please reach out to him to arrange a time for Wednesday? Joe's cell number is 781 G.L. c. 4,s[illegible]
>>>
>>>
>>>
>>>
>>>
>>> Thank you,
>>>
>>> Joey Gilmore
>>>
>>> Manager - IT Security Systems
>>>
>>> Information Technology
>>>
>>> Massachusetts Port Authority
>>>
>>> One Harborside Drive, Suite 200S
>>>
>>> East Boston, MA 02128-2909
>>>
>>> Tel: 617-568-5915
>>>
>>> Cell: 617 G.L. c. 4,s[illegible]
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>> From: Egnitz, Brian (POL) <brian.egnitz@state ma.us>
>>>
>>> Sent: Thursday, April 23, 2020 10:30 AM
>>>
>>> To: Gilmore, Joey <JGilmore@massport.com>; Alves, Joe <JAlves@massport.com>; Sillsby, Blane <BSillsby@massport.com>; Quinn, Michael <MQuinn@massport.com>
>>>
>>> Cc: Haverty, Robert <RHaverty@massport.com>; Harney, Michael <MHarney@massport.com>
>>>
>>> Subject: RE: MSP LPR
>>>
>>>
>>>
>>>
>>>
>>> -----Original Appointment-----
>>>
>>> From: Gilmore, Joey [mailto:JGilmore@massport.com]
>>>
>>> Sent: Wednesday, April 22, 2020 11:35 AM
>>>
>>> To: Gilmore, Joey; Alves, Joe; Sillsby, Blane; Quinn, Michael; Egnitz, Brian (POL)
>>>
>>> Cc: Haverty, Robert; Harney, Michael
>>>
>>> Subject: MSP LPR
>>>
>>> When: Thursday, April 23, 2020 10:00 AM-11:00 AM (UTC-05:00) Eastern Time (US & Canada).
>>>
>>> Where: https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_join_500426357&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=3ivMD3mXVSpxMv-g-ajiMkf38VVpxAIvxzFU7zoD-C0&s=ZHyfYIPsksOBeyci6ra3KwL4O4SCPoA_7WEhraXS96Y&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_join_500426357&d=DwMFAg&c=1XoZxQJyt2gHLFE_bvTIdHn1XrU03FNEWIHnzbfZimE&r=v1eRT_PuOlmt3sh7Lyk24rX9MBSQCKldPuclQWjOSPk&m=PXOFyIolm_rZpuk6yADM63jFy9ok8VUjYC-nn_w6rMY&s=1D-DGoR18hVhptpvf47Fn_SFGKSpwE2u7SIK57_YdrA&e=>
>>>
>>>
>>>
>>>
>>>
>>> CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>> Hi Guys,
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>> This meeting is to discuss the method of bringing Logan LPR cameras to the EOPSS network.
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>> This is the last status update from Chute before he left:
>>>
>>>
>>>
>>> "Currently MassPort has G.L. c. 4,sec. 7,cl.26 (n)(security), G.L. c. 4,sec. 7,c[illegible] After several iterations of the system architecture, it has been decided that the path of least resistance is to employ commercial carrier service on the MSP MPLS to the CJIS Datacenter in Chelsea. MSP is working to procure the necessary power adapter and antenna equipment while also identifying accounts and equipment that can be re-purposed for this project. If/when it is feasible for this system to be networked through terrestrial means, MassPort has the switch infrastructure in place to make a direct connection to the EOPSS network at G.L. c. 4,sec. G.L. c. 4,sec. 7,cl.26 (n)(s[illegible] I hope this gives a brief overview of where we are at, and please do not hesitate to reach out to me via my personal contact information if any questions come up."
>>>
>>>
>>>
>>>

>>>
>>>
>>>
>>> MPA - MSP
>>>
>>> Thu, Apr 23, 2020 10:00 AM - 11:30 AM (EDT)
>>>
>>>
>>>
>>> Please join my meeting from your computer, tablet or smartphone.
>>>
>>> https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_join_500426357&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=3ivMD3mXVSpxMv-g-ajiMkf38VVpxAIvxzFU7zoD-C0&s=ZHyfYIPsksOBeyci6ra3KwL4O4SCPoA_7WEhraXS96Y&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_join_500426357&d=DwMF-g&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=YrOyBDqzLm4zddutRwcvrC8An9e-bx9zIO8EMq0-X7Q&s=bt8qRm7QQabR-s9uIfBIlJV-_W5RvGI9slrF4D65fw4&e=>
>>>
>>>
>>>
>>> This meeting is locked with a password : [redacted]
>>>
>>>
>>>
>>> You can also dial in using your phone.
>>>
>>> United States: +1 (571) 317-3122<tel:+15713173122,,500426357>
>>>
>>>
>>>
>>> Access Code: 500-426-357
>>>
>>>
>>>
>>> New to GoToMeeting? Get the app now and be ready when your first meeting starts:
>>>
>>> https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_install_500426357&d=DwIGaQ&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=3ivMD3mXVSpxMv-g-ajiMkf38VVpxAIvxzFU7zoD-C0&s=sPSeiG_aGKwV8Di-BEroqcIxtAzk0va1AAxVy6gZ3Tg&e=<https://urldefense.proofpoint.com/v2/url?u=https-3A__global.gotomeeting.com_install_500426357&d=DwMF-g&c=lDF7oMaPKXpkYvev9V-fVahWL0QWnGCCAfCDz1Bns_w&r=hNTkG2z4MCZ_SB-QH0EEKPBh4IX8nm64tlxI8vzFMhI&m=YrOyBDqzLm4zddutRwcvrC8An9e-bx9zIO8EMq0-X7Q&s=73yCNI9YJUXzkHRvG6ehrB7JBvLK4l12EYJ4ThBmY-M&e=>
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>> Thank you,
>>>
>>>
>>>
>>> Joey Gilmore
>>>
>>>
>>>
>>> Manager - IT Security Systems
>>>
>>> Information Technology
>>>
>>> Massachusetts Port Authority
>>>
>>> One Harborside Drive, Suite 200S
>>>
>>> East Boston, MA 02128-2909
>>>
>>> Tel: 617-568-5915
>>>
>>> Cell: 617[redacted]
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>>

The information contained in this communication, including any attachments, is confidential and is intended only for the use of the recipient(s) named above. If the reader of this message is not an intended recipient, you are notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you receive this communication in error, please notify the sender immediately, and delete the communication, any attachments, and all copies.

To: Quinn, Dermot (POL)
Subject: RE: New Solutions and End-Of-Life Announcement
Date: Tuesday, January 28, 2020 9:07:01 AM

I've archived off the reads of the cameras displaying symptoms identified in the technical bulletin.

-Brian

From: Egnitz, Brian (POL)
Sent: Friday, January 17, 2020 7:52 AM
To: Quinn, Dermot (POL)
Subject: Fwd: New Solutions and End-Of-Life Announcement

Please see attached document regarding the 525 camera GMT issue.

Begin forwarded message:

> **From:** John Tedona <jtedona@neology.net>
> **Date:** January 16, 2020 at 5:52:18 PM EST
> **To:** "Egnitz, Brian (POL)" <brian.egnitz@pol.state.ma.us>
> **Cc:** Miranda Fischer <mfischer@neology.net>, Luke Normington <LNormington@uk.neology.net>
> **Subject: New Solutions and End-Of-Life Announcement**
>
> Mr. Egnitz,
>
> As we step into a new year, and decade, we wanted to take a moment to thank you for your continued loyalty and use of the PIPS Technology by Neology solutions. We are incredibly grateful of the customers, resellers and partners who, over the last years have remained loyal and supported us in our vision of "Driving Detection Innovation". Each day we strive to make a difference in supporting you to achieve your goals, solve your challenges and achieve your mission.
>
> 2019 was a major year for us as we finalised significant elements of the overhaul of our products and solutions, culminating with the release of BOSS 4 in the fall, alongside brand new Fixed and Mobile ALPR solutions. Attached you will find the latest reminders in relation to our products and software versions to ensure you are getting the most out of your Neology products and solutions.
>
> The year ahead is primed to be an exciting one! At Neology we firmly believe that the development doesn't stop – we have almost 30% of our workforce working specifically in the product development area of our business in order to constantly evolve our solutions, improve performance and add new features. We have some exciting additions to the portfolio which are imminent that will provide not only performance improvements to the existing solutions but also provide the ability for greater inter-

operability across the Law Enforcement ALPR market in the US more generally. We believe that you retaining the control and ownership of your data is paramount and we continue to respect that as we always have while supporting those customers who choose to share and provide secure, trusted data sharing between neighbours and friends.

We are always keen to hear your feedback – if there are any elements of our services, solutions or products which you would like to feedback on, please don't hesitate to get in touch with me so I can provide personal attention to both positive and negative feedback. Email me here

Thank you for your continued support – we look forward to serving you in 2020 and beyond.

Best Regards,
Luke & the PIPS Technology team

From: Egnitz, Brian (POL)
To: Quinn, Dermot (POL)
Subject: RE: New Solutions and End-Of-Life Announcement
Date: Monday, March 9, 2020 3:40:00 PM

I've archived off the reads of the 525 cameras displaying symptoms identified in the technical bulletin.

-Brian

From: Egnitz, Brian (POL)
Sent: Friday, January 17, 2020 7:52 AM
To: Quinn, Dermot (POL)
Subject: Fwd: New Solutions and End-Of-Life Announcement

Please see attached document regarding the 525 camera GMT issue.

Begin forwarded message:

> **From:** John Tedona <jtedona@neology.net>
> **Date:** January 16, 2020 at 5:52:18 PM EST
> **To:** "Egnitz, Brian (POL)" <brian.egnitz@pol.state.ma.us>
> **Cc:** Miranda Fischer <mfischer@neology.net>, Luke Normington <LNormington@uk.neology.net>
> **Subject: New Solutions and End-Of-Life Announcement**
>
> Mr. Egnitz,
>
> As we step into a new year, and decade, we wanted to take a moment to thank you for your continued loyalty and use of the PIPS Technology by Neology solutions. We are incredibly grateful of the customers, resellers and partners who, over the last years have remained loyal and supported us in our vision of "Driving Detection Innovation". Each day we strive to make a difference in supporting you to achieve your goals, solve your challenges and achieve your mission.
>
> 2019 was a major year for us as we finalised significant elements of the overhaul of our products and solutions, culminating with the release of BOSS 4 in the fall, alongside brand new Fixed and Mobile ALPR solutions. Attached you will find the latest reminders in relation to our products and software versions to ensure you are getting the most out of your Neology products and solutions.
>
> The year ahead is primed to be an exciting one! At Neology we firmly believe that the development doesn't stop – we have almost 30% of our workforce working specifically in the product development area of our business in order to constantly evolve our solutions, improve performance and add new features. We have some exciting

additions to the portfolio which are imminent that will provide not only performance improvements to the existing solutions but also provide the ability for greater inter-operability across the Law Enforcement ALPR market in the US more generally. We believe that you retaining the control and ownership of your data is paramount and we continue to respect that as we always have while supporting those customers who choose to share and provide secure, trusted data sharing between neighbours and friends.

We are always keen to hear your feedback – if there are any elements of our services, solutions or products which you would like to feedback on, please don't hesitate to get in touch with me so I can provide personal attention to both positive and negative feedback. Email me here

Thank you for your continued support – we look forward to serving you in 2020 and beyond.

Best Regards,
Luke & the PIPS Technology team

From: Egnitz, Brian (POL)
To: Schwarz, William J; Jim Charron; Tiffany Tran
Cc: Mitchell, Timothy P. (EOTSS)
Subject: RE: Plate reader access
Date: Friday, October 23, 2020 9:17:00 AM

Did EOTSS give you access to the DB? Neology does not support direct access to the SQL nor do I recommend it, it could have unintended consequences to the systems ability to keep up with reads and alerts. The current supported method for sharing BOSS data is via a PIPS plugin. I am currently working with a cloud vendor and the plug in. If the cloud vendor I'm working with pans out we would have an API for you to use. I'll know more in a few weeks, please hold off if possible.

-Brian

From: Schwarz, William J <WSchwarz@springfieldpolice.net>
Sent: Thursday, October 22, 2020 2:38 PM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>; Jim Charron <jim.charron@motorolasolutions.com>; Tiffany Tran <tiffanytran@motorolasolutions.com>
Subject: Plate reader access

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Brian:

Can we please chat on a conference call about the access credentials and connections to the alpr system? Jim will send out a link if you have a date and time that your available.

Bill

William Schwarz
Director of Crime Analysis / Real Time Analysis Center
130 Pearl St.
Springfield, MA 01105
413-886-5282

From: Commonwealth Fusion Center (POL)
To: Reid, Nathan
Subject: Re: Plate Readers
Date: Tuesday, December 29, 2020 10:22:36 AM

Good Morning,

Our ALPR system is currently down for maintenance and we do not have a time frame for when it will be operational. We are unable to do historical or create hotlists at this time.

Respectfully,

Kimberly Smallenberger
Intelligence Analyst
Massachusetts State Police | Commonwealth Fusion Center
470 Worcester Road | Framingham, MA 01702
Phone: (508) 820-2233

CONFIDENTIALITY NOTICE: The information contained in this email and any attachment is privileged and confidential law enforcement information. If you are not the intended recipient, you are hereby notified that any disclosure, dissemination, or copying of this communication is strictly prohibited. If you have received this email in error, please call (978) 451-3700 immediately.

From: Reid, Nathan <nreid@sandwichmass.org>
Sent: Tuesday, December 29, 2020 10:19 AM
To: Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>
Subject: Plate Readers

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Good Morning,

I am contacting you in regards to the plate readers on the bridges. My office is curious about the status of those readers and if they are still picking up plates. I know we haven't been getting updates for some time now. We recently had an armed robbery in our town and would like to go throw some of that information if it is still available.

Thank you for your time.

Nate Reid

Nathan Reid
Detective
Sandwich Police Department

255 Cotuit Road
Sandwich, MA 02563
Phone: 508-888-3343 ext 1383
Cell: [redacted] G.L. c. 4 sec. 7 cl.26 (n)(security)
Fax: 508-539-6312

Picture1

****LAW ENFORCEMENT USE ONLY****

The document accompanying this email contains information from the Sandwich Police Department that maybe CONFIDENTIAL and / or PRIVILEGED. The information is intended to be for the use of the individual or entity named on this email. If you are not the intended recipient, be aware that any misuse of this information is strictly PROHIBITED

To: Peter Crary; Luke Normington
Cc: John Tedona
Subject: RE: Quick alignment
Date: Thursday, December 17, 2020 9:12:35 AM

Yes, this was my thought to bring online

Short term:

For Fixed
- Disable all cameras in BOSS 3.6 On-Prem (EOPSS)
- Turn on system (allowing access to users)
- Patch each 492 & 525 Camera, configure new watermark and then enable the camera to send to backend system. (need confirmation that new "NTP Flag" metadata will work with 3.6, also if data without NTP lock is being sent)

For Mobiles
- write a new purge script to delete all Mobile data.
- Remove all of these mobiles from hotlists (except NCIC, RMV, Warrants etc.), ensuring no hits are generated.
- Inventory all SX4 &SX4e systems (2017-Present) to identify which systems can be upgraded
- Older systems will need to be decommissioned or configured not to send data to BOSS 3.6 and data would need to be purged.
- The SX4 &SX4e systems (2017-Present) will need to be Patched in order for reads to be sent to the back end. (still reviewing process, might be able to VNC remote)

-----Original Message-----
From: Peter Crary <pcrary@neology.net>
Sent: Wednesday, December 16, 2020 4:04 PM
To: Luke Normington <LNormington@uk.neology.net>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Cc: John Tedona <jtedona@neology.net>
Subject: Re: Quick alignment

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Brian,

With pagis, I spoke to the team and we want to see if we can try a sql change that will prevent reads from going into the system until the patch is ready. The idea is to add a before_insert trigger that would block the reads from loading into boss. This means we can apply the setting to boss3 without having to reach out to every mobile unit for an update. The reason we are looking at this is that while we can block the silent sync, we do not have a method of preventing a user from hitting the end shift button.

Is this acceptable on your end?

Peter Crary
Global R&D Director, ALPR
PIPS Technology
(Sent from my iPhone)

> On Dec 16, 2020, at 14:57, Luke Normington <LNormington@uk.neology.net> wrote:

>

From: Egnitz, Brian (POL)
To: Peter Crary; Luke Normington
Cc: John Tedona
Subject: RE: Quick alignment
Date: Thursday, December 17, 2020 9:12:00 AM

Yes, this was my thought to bring online

Short term:

For Fixed
- Disable all cameras in BOSS 3.6 On-Prem (EOPSS)
- Turn on system (allowing access to users)
- Patch each 492 & 525 Camera, configure new watermark and then enable the camera to send to backend system. (need confirmation that new "NTP Flag" metadata will work with 3.6, also if data without NTP lock is being sent)

For Mobiles
- write a new purge script to delete all Mobile data.
- Remove all of these mobiles from hotlists (except NCIC, RMV, Warrants etc.), ensuring no hits are generated.
- Inventory all SX4 &SX4e systems (2017-Present) to identify which systems can be upgraded
- Older systems will need to be decommissioned or configured not to send data to BOSS 3.6 or data would need to be purged.
- The SX4 &SX4e systems (2017-Present) will need to be Patched in order for reads to be sent to the back end. (still reviewing process, might be able to VNC remote)

-----Original Message-----
From: Peter Crary <pcrary@neology.net>
Sent: Wednesday, December 16, 2020 4:04 PM
To: Luke Normington <LNormington@uk.neology.net>; Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Cc: John Tedona <jtedona@neology.net>
Subject: Re: Quick alignment

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Brian,

With pagis, I spoke to the team and we want to see if we can try a sql change that will prevent reads from going into the system until the patch is ready. The idea is to add a before_insert trigger that would block the reads from loading into boss. This means we can apply the setting to boss3 without having to reach out to every mobile unit for an update. The reason we are looking at this is that while we can block the silent sync, we do not have a method of preventing a user from hitting the end shift button.

Is this acceptable on your end?

Peter Crary
Global R&D Director, ALPR
PIPS Technology
(Sent from my iPhone)

> On Dec 16, 2020, at 14:57, Luke Normington <LNormington@uk.neology.net> wrote:
>

From: Luke Normington
To: Peter Crary; Egnitz, Brian (POL)
Cc: John Tedona
Subject: Re: Standards etc
Date: Monday, December 7, 2020 4:12:37 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Brian - that message hadn't quite finished....

Re: UK Mobile, we don't actually provide systems into UK forces which aren't part of a wider in-vehicle system. Typically this would involve speed measurement devices where we consume location data, and by their type approval nature, have a higher GPS accuracy/sensitivity.

Hope that makes sense,
Luke

Luke Normington
Managing Director
Email: lnormington@uk.neology.net
P. Direct +44 (0)7375 024539P. Tech Support +44 (0)1256 581135
A Business P. Sales +44 (0)1256 581134 P. Service Centre +44 (0)1513 554313
www.pipstechnology.co.uk Neology UK Ltd: Form 1, 18 Bartley Wood Business Park, Hook, Hampshire, RG27 9XA

Registered Office: 6th Floor, Kildare House, Dorset Rise, London, United Kingdom, EC4Y 8EN
Registered in England & Wales, No 10809863.

The information contained in this communication is confidential and intended only for the use of the recipient named and may also be legally privileged. If you are not the intended recipient (named addressee), you are hereby notified that any dissemination, distribution, copying or making use of this communication, or any of its contents, is strictly prohibited. Please notify the sender immediately by email and delete the original message and any copy of it from your computer system. The integrity, security of and absence of viruses in this message cannot be guaranteed on the internet. The sender therefore does not accept liability for any errors or omissions in the contents of this message, nor any damage caused, which arise as a result of e-mail transmission

---

From: Luke Normington <LNormington@uk.neology.net>
Sent: Monday, December 7, 2020 9:09:17 PM
To: Peter Crary <pcrary@neology.net>; Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Cc: John Tedona <jtedona@neology.net>
Subject: Re: Standards etc

Brian

Re: UK Mobile, we don't actually provide systems into

Luke Normington
Managing Director
Email: lnormington@uk.neology.net
P. Direct +44 (0)7375 024539P. Tech Support +44 (0)1256 581135
A Business P. Sales +44 (0)1256 581134 P. Service Centre +44 (0)1513 554313
www.pipstechnology.co.uk Neology UK Ltd: Form 1, 18 Bartley Wood Business Park, Hook, Hampshire, RG27 9XA

Registered Office: 6th Floor, Kildare House, Dorset Rise, London, United Kingdom, EC4Y 8EN
Registered in England & Wales, No 10809863.

The information contained in this communication is confidential and intended only for the use of the recipient named and may also be legally privileged. If you are not the intended recipient (named addressee), you are hereby notified that any dissemination, distribution, copying or making use of this communication, or any of its contents, is strictly prohibited. Please notify the sender immediately by email and delete the original message and any copy of it from your computer system. The integrity, security of and absence of viruses in this message cannot be guaranteed on the internet. The sender therefore does not accept liability for any errors or omissions in the contents of this message, nor any damage caused, which arise as a result of e-mail transmission

---

From: Egnitz, Brian (POL) <brian.egnitz@state.ma.us>
Sent: Monday, December 7, 2020 8:56:44 PM
To: Peter Crary <pcrary@neology.net>
Cc: John Tedona <jtedona@neology.net>; Luke Normington <LNormington@uk.neology.net>
Subject: RE: Standards etc

Thanks Peter,

Can you please send me a link to download.

Also, what GPS antenna options are there for the mobiles beyond https://static.garmin.com/pumac/GPS_16x_tech_specs.pdf ? The Doc Luke sent earlier stated the UK requirement of 10 Meter accuracy for mobile, but the Garmin GPS 16 is GPS <15 meter accuracy without augmentation. Does the UK use a different puck? Also, do you guys calculate the accuracy or is it pulled from the GPS and is it available? I'd interested to know what NMEA sentences are being used.

-Brian

From: Peter Crary <pcrary@neology.net>
Sent: Monday, December 7, 2020 2:38 PM
To: Egnitz, Brian (POL) <brian.egnitz@pol.state.ma.us>
Cc: John Tedona <jtedona@neology.net>; Luke Normington <LNormington@uk.neology.net>
Subject: Re: Standards etc

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Brian,

The fixed camera patch is ready when you're ready.

Peter Crary
Global R&D Director, ALPR
PIPS Technology
(Sent from my iPhone)

> On Dec 7, 2020, at 11:45, Luke Normington <LNormington@uk.neology.net> wrote:
>
> Brian
>
> I was thinking about our discussion from Friday, especially your question about standards in the industry etc and how you thought that the wider community may start to see a change around several topics such as the importance of time / accuracy etc as well as the obligations for Agencies to have methodology around annual inspections etc.
>
> In several countries in Europe and Australia there are national standards for the use of ALPR/ANPR technology, especially around things like fit for purpose / maintainability / audit etc. See if you can get to the link below as this is the UK standards highlighting what the Police Forces must do when they a) procure technology but also b) maintain it for appropriate use.
>
> https://www.gov.uk/government/publications/national-anpr-standards
>
> Much of this is fairly straight forward – start with the 11page document rather than the 50 page one! Typically the Forces either choose to do the annual activities themselves (like the groundtruthing etc) or they have service contracts with vendors who fulfil this

on their behalf. We have numerous contracts with UK Agencies where we have to abide by these standards as part of annual servicing / inspection contracts and provide the evidence that the steps have been carried out.

May stimulate some thoughts on your side – would love to engage with a standards / best practise drive and whilst, unlike in other countries, I don't think we will ever see a Federal level standards / type approval situation in the US, even having something at a state -level would be great.

Thought it was worth sharing as FYI.

Luke

<image002.png>
Luke Normington
Managing Director
Email: lnormington@uk.neology.net

<image003.png>

P. Direct +44 (0)7375 024539 **P. Tech Support** +44 (0)1256 581135

A

<image004.png>

Business **P. Sales** +44 (0)1256 581134 **P. Service Centre** +44 (0)1513 554313

www.pipstechnology.co.uk Neology UK Ltd: Form 1, 18 Bartley Wood Business Park, Hook, Hampshire, RG27 9XA

Registered Office: 6th Floor, Kildare House, Dorset Rise, London, United Kingdom, EC4Y 8EN Registered in England & Wales, No 10809863.

The information contained in this communication is confidential and intended only for the use of the recipient named and may also be legally privileged. If you are not the intended recipient (named addressee), you are hereby notified that any dissemination, distribution, copying or making use of this communication, or any of its contents, is strictly prohibited. Please notify the sender immediately by email and delete the original message and any copy of it from your computer system. The integrity, security of and absence of viruses in this message cannot be guaranteed on the internet. The sender therefore does not accept liability for any errors or omissions in the contents of this message, nor any damage caused, which arise as a result of e-mail transmission.

From: Commonwealth Fusion Center (POL)
To: Ptlm. Luke Dezago
Cc: Brooks, Brian (POL)
Subject: Re: Stow Police BOLO with PC to Arrest
Date: Friday, September 4, 2020 10:15:51 AM

Good Morning, Sir -

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

[redacted]

Respectfully,

Sean Bender
Intelligence Analyst
Massachusetts State Police | Commonwealth Fusion Center
470 Worcester Road | Framingham, MA 01702
Phone: (508) 820-2233

CONFIDENTIALITY NOTICE: The information contained in this email and any attachment is privileged and confidential law enforcement information. If you are not the intended recipient, you are hereby notified that any disclosure, dissemination, or copying of this communication is strictly prohibited. If you have received this email in error, please call (978) 451-3700 immediately.

From: Ptlm. Luke Dezago <ldezago@stow-ma.gov>
Sent: Friday, September 4, 2020 9:18 AM
To: Commonwealth Fusion Center (POL) <fusion@pol.State.MA.US>
Subject: Stow Police BOLO with PC to Arrest

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

[redacted]

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

Year: G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

Make:

Model:

Style:

Color:

Doors:

VIN:

Ins. Co.:

- Officer DeZago

From: Erika Baburins
To: Bender, Sean (POL)
Subject: RE: Toll Pics
Date: Wednesday, September 9, 2020 2:38:25 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Thanks for the info!

Erika Baburins
Crime Analyst
Mansfield Police Department
500a East St
Mansfield, MA 02048
508-261-7301 x61231

Vice President of Membership, Massachusetts Association of Crime Analysts
http://www.macrimeanalysts.org

When responding, please be advised that the Town of Mansfield and the Office of the Secretary of State has determined that email could be considered a public record.

From: Bender, Sean (POL) [mailto:sean.bender@state.ma.us]
Sent: Wednesday, September 9, 2020 2:02 PM
To: Erika Baburins
Subject: Re: Toll Pics

Good Afternoon, Erika -

Unfortunately, we do not have access to the MA Pike (I-90) ALPR data from the electronic tolling system. That data belongs to MassDOT and I believe they require legal process for those records unless there are exigent circumstances.

I believe this is the number for inquires: 857-368-4636.

I did [redacted] through the LPRs that the MSP does have access to and I'm not finding any hits within the past 30 days - but unfortunately the coverage is pretty spotty in certain parts of the state.

Sorry!

Respectfully,

Sean Bender
Intelligence Analyst
Massachusetts State Police | Commonwealth Fusion Center
470 Worcester Road | Framingham | MA 01702
508-820-2233

From: Erika Baburins <ebaburins@mansfieldma.com>
Sent: Wednesday, September 9, 2020 12:59 PM
To: Bender, Sean (POL) <Sean.Bender@pol.state.ma.us>
Subject: Toll Pics

Hello!

Do you have access to toll pictures? We [G.L. c. 4.sec. 7.cl.26 (n)(security); G.L. c. 4.sec. 7. cl.26(f)(investigative)]

Thanks!

Erika Baburins
Crime Analyst
Mansfield Police Department
500a East St
Mansfield, MA 02048
508-261-7301 x61231

Vice President of Membership, Massachusetts Association of Crime Analysts
http://www.macrimeanalysts.org

When responding, please be advised that the Town of Mansfield and the Office of the Secretary of State has determined that email could be considered a public record.

Disclaimer
The information contained in this communication from the Town of Mansfield is confidential. It is intended solely for use by the recipient and others authorized to receive it. If you are not the recipient, you are hereby notified that any disclosure, copying, distribution or taking action in relation of the contents of this information is strictly prohibited and may be unlawful.

This email has been scanned for viruses and malware, and may have been automatically archived by **Mimecast Ltd**, an innovator in Software as a Service (SaaS) for business. Providing a **safer** and **more useful** place for your human generated data. Specializing in; Security, archiving and compliance. To find out more Click Here.

Disclaimer
The information contained in this communication from the Town of Mansfield is confidential. It is intended solely for use by the recipient and others authorized to receive it. If you are not the recipient, you are

hereby notified that any disclosure, copying, distribution or taking action in relation of the contents of this information is strictly prohibited and may be unlawful.

This email has been scanned for viruses and malware, and may have been automatically archived by **Mimecast Ltd**, an innovator in Software as a Service (SaaS) for business. Providing a **safer** and **more useful** place for your human generated data. Specializing in; Security, archiving and compliance. To find out more Click Here.

From: Thibault, Amy (POL)
To: MACrimeNet (POL)
Subject: RE: Workflow
Date: Thursday, September 24, 2020 1:58:07 PM

I think if you could take some of your work for that day from start to finish and walk us through it, that would be very helpful. I also have a list of things you do when we had to write it for the 960's. They want to know about all processes and duties so if there is something you don't do on a regular basis that's important, you may want to note it so that we cover it.

This is what I have below. I think its more the processes vs the what.

Chris Neville

- Intake, review, editing and redistribution of incoming email and outgoing intelligence to aid local investigators in identifying suspects and patterns of criminal activity to upwards of 2,000 individual recipients 365 days a year.
- Annual selective distribution by county, of approximately 4,000 emails to the email network which includes representatives of almost every State, Local and Federal Agency in Eastern and Central MA, neighboring states, Bank Industry Security Professionals and Retail Asset Protection Professionals.
- Participation in area detective's meetings to share intelligence regarding crimes and arrests of regional significance.
- Comprehensive review and re-distribution in excel spreadsheet format of Pawnshop Information provided by more than a dozen local agencies including highlighting of persons of interest.
- Statewide liaison to NABI (National Association of Bunco Investigators).
- Review and redistribution of Intelligence published by NESPIN and NEORCA.
- Complete responsibility for the addition, subtraction and update of email addresses stored in the 'listserv manager".
- Maintenance, upkeep and distribution of a home-grown Area Wide Detectives Contact List with email and telephone contact information from 1,800 sources.
- Routine access to CJIS systems to perform RMV, CJIS and NCIC related inquiries from law enforcement.
- Routine access to Coplink and other data sources (TLO) to assist local detectives in providing photographs, known associates, associated vehicles and prior incidents while assisting in investigations pertaining to email traffic.
- Routine access and review of ALPR's to provide investigative assistance and documentation to local Law Enforcement, specifically in connection with Organized Crime organizations based out of State but operating in MA and the surrounding New England States.

- Daily review of Area Crime Bulletins from municipal agencies including the BRIC, Cambridge, Everett, Lynn, and others as they are distributed. (Many of whom re-post information previously distributed on Macrimenet).

- Guest presenter to new area detectives providing an overview of what services the CFC provides for local law enforcement.

- Participation in area intelligence sharing meetings specifically directed to targeted crimes such as ATM B&E's, Robberies, Regional Check Frauds or outbreaks of commercial or residential B&Es.

- Daily review of national Crimedex Alerts to ascertain links to other incidents occurring across the country. (ie: Panera Bread Thefts, Felony Lane Gang, and Transient Scams).

From: MACrimeNet (POL)
Sent: Thursday, September 24, 2020 1:54 PM
To: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Subject: RE: Workflow

Thank you.

Do you want me to prepare something in advance of the things that most people might not know that I do, or we just want to pick at it as we go?

Chris

-----Original Appointment-----
From: Thibault, Amy (POL) <amy.thibault@pol.state.ma.us>
Sent: Thursday, September 24, 2020 1:24 PM
To: Smith, Eleanor (POL); MACrimeNet (POL)
Subject: Workflow
When: Thursday, October 1, 2020 10:00 AM-12:00 PM (UTC-05:00) Eastern Time (US & Canada).
Where: gotomeeting

MA Crimenet

Thu, Oct 1, 2020 10:00 AM - 12:30 PM (EDT)

Please join my meeting from your computer, tablet or smartphone.
https://global.gotomeeting.com/join/756196341

You can also dial in using your phone.
United States: +1 (408) 650-3123

Access Code: 756-196-341

New to GoToMeeting? Get the app now and be ready when your first meeting starts:

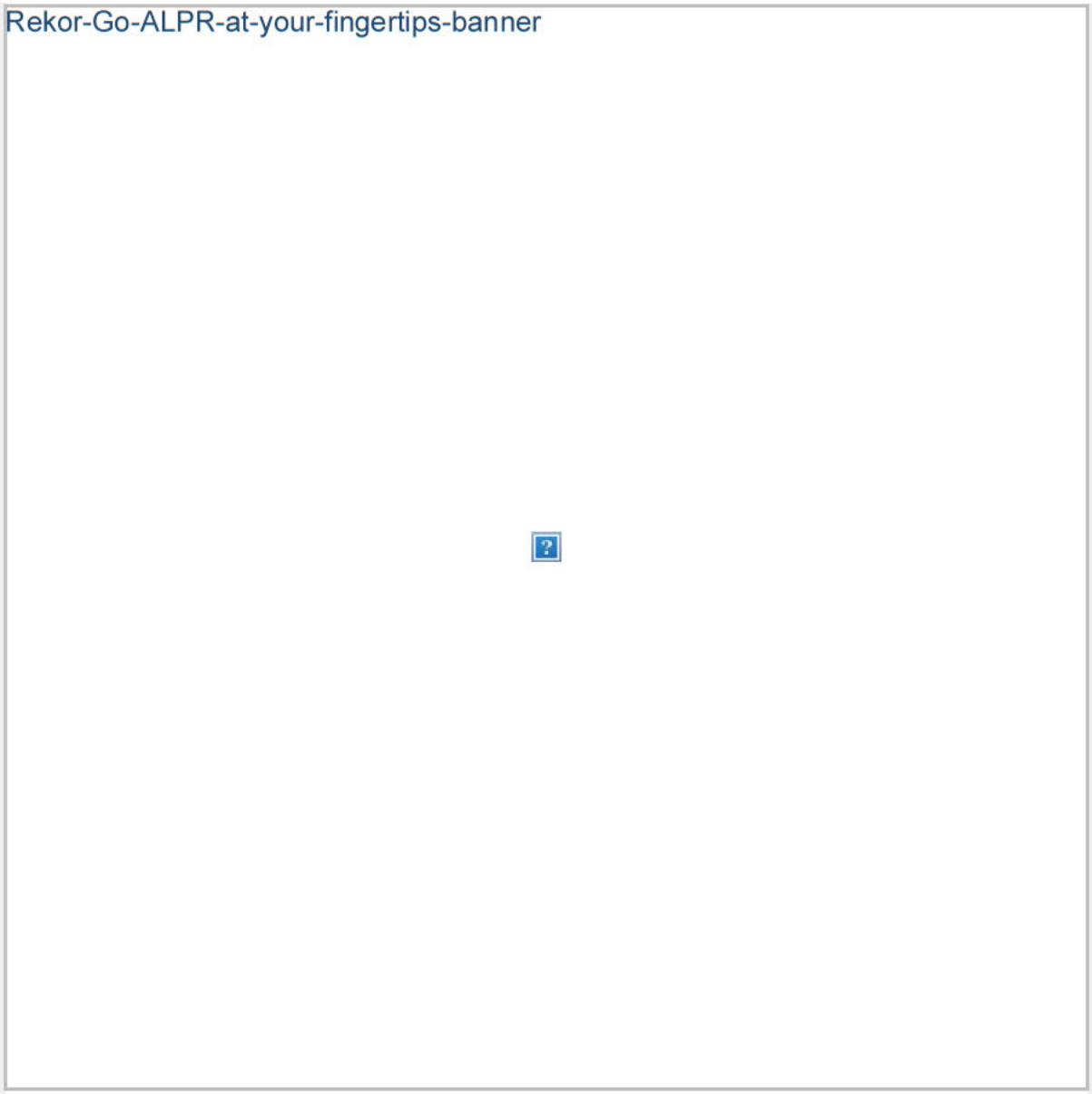
https://global.gotomeeting.com/install/756196341

From: Rekor Systems, Inc.
To: Ferguson, Gary E (POL)
Subject: Rekor Go is now available! Download today!
Date: Tuesday, December 15, 2020 10:02:45 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

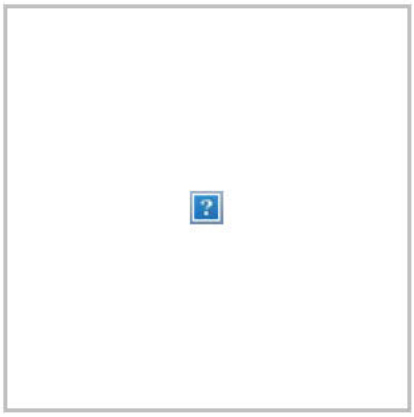
Rekor-Banner-Horizontal-Color-Tag





Rekor Go is now available! Download today!

Introducing Rekor Go, the mobile application that brings the power of accurate Automatic License Plate Recognition (ALPR) to your phone, letting you take ALPR anywhere you need. Instantly read license plates and receive alerts when identified vehicles appear from your custom list.







Extreme portability

With the Rekor Go application on your smartphone you can take the power of advanced ALPR technology to the streets, parking lots and garages, and other hard to access or temporary locations like never before.



Limitless applications

With full ALPR capabilities and customizable alerts, the uses for Rekor Go are endless from parking validation and enforcement, school security, customer validation, investigations, and asset recognition and recovery.



Dependable results

Rekor Go gives you AI-powered, law enforcement-grade license plate recognition with the unmatched quality you need and security you can trust in and easy to use and mange app.

Learn more about Rekor Go

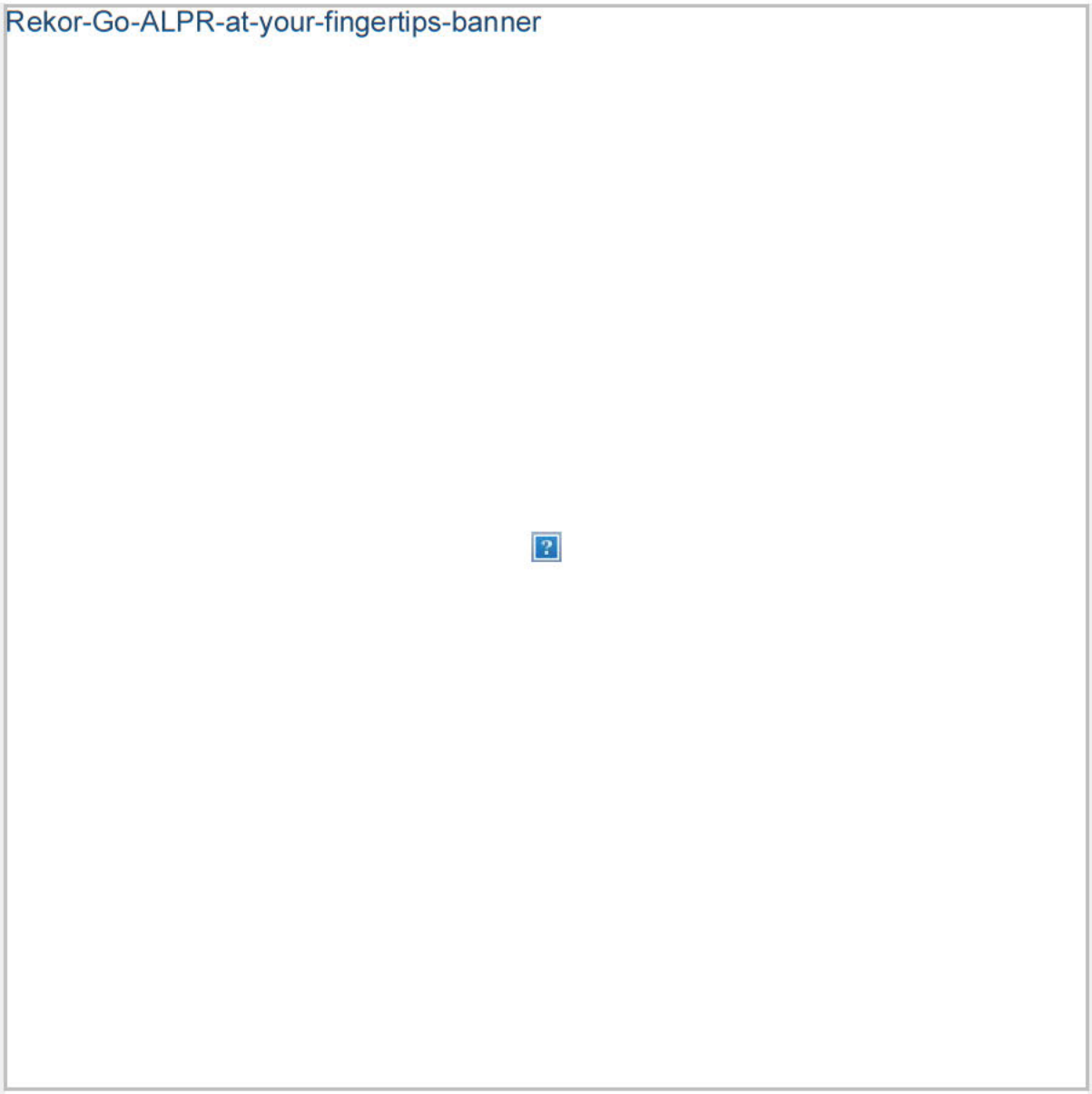


Rekor Systems, Inc., 7172 Columbia Gateway Drive, Suite 400, Columbia, MD 21046, (410) 762-0800
Unsubscribe Manage preferences

From: Rekor Systems, Inc.
To: Egnitz, Brian (POL)
Subject: Rekor Go is now available! Download today!
Date: Tuesday, December 15, 2020 10:03:22 AM

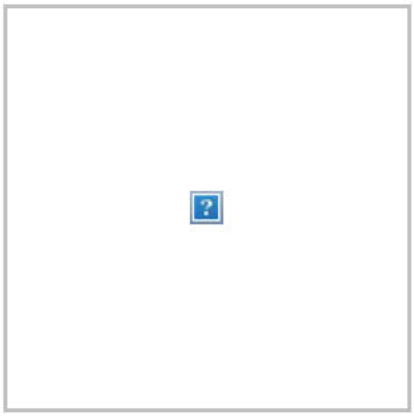
CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Rekor-Banner-Horizontal-Color-Tag



Rekor Go is now available! Download today!

Introducing Rekor Go, the mobile application that brings the power of accurate Automatic License Plate Recognition (ALPR) to your phone, letting you take ALPR anywhere you need. Instantly read license plates and receive alerts when identified vehicles appear from your custom list.







Extreme portability

With the Rekor Go application on your smartphone you can take the power of advanced ALPR technology to the streets, parking lots and garages, and other hard to access or temporary locations like never before.



Limitless applications

With full ALPR capabilities and customizable alerts, the uses for Rekor Go are endless from parking validation and enforcement, school security, customer validation, investigations, and asset recognition and recovery.



Dependable results

Rekor Go gives you AI-powered, law enforcement-grade license plate recognition with the unmatched quality you need and security you can trust in and easy to use and mange app.

Learn more about Rekor Go



Rekor Systems, Inc., 7172 Columbia Gateway Drive, Suite 400, Columbia, MD 21046, (410) 762-0800
Unsubscribe Manage preferences

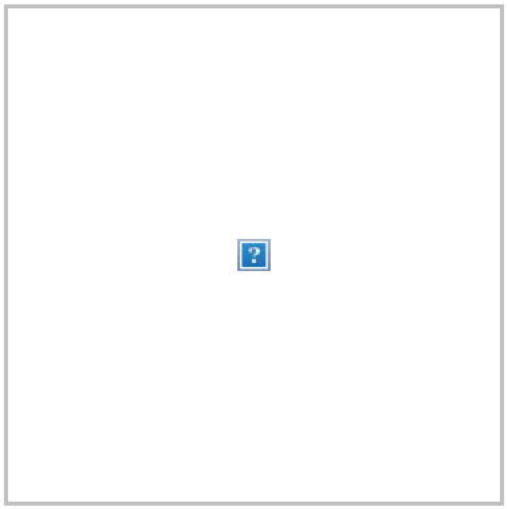
From: Traffic Technology Today
To: Griffin, Daniel (POL)
Subject: Secretary Chao makes historic announcement on USA's freight system
Date: Friday, September 4, 2020 8:25:21 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

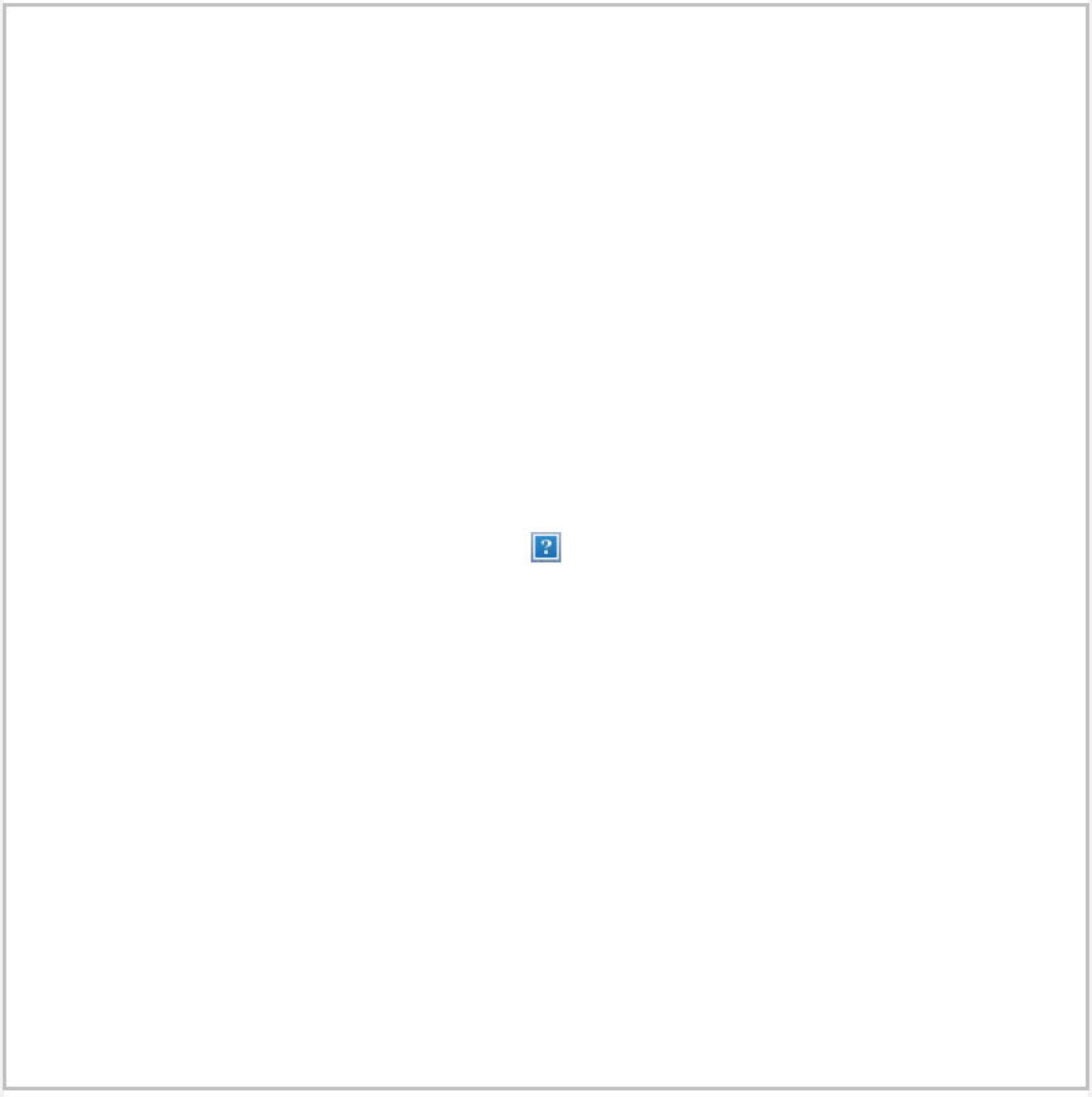
TOP NEWS THIS WEEK

VIDEO: US Transportation Secretary Elaine Chao makes historic announcement on USA's freight system

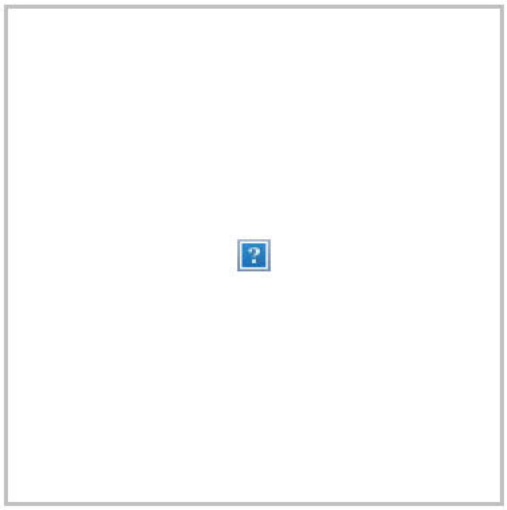
The Transportation Secretary Elaine



Chao has just posted this video announcing the launch of the USA's first ever National Freight Strategic Plan, which will help the nation take full advantage of new technologies such as autonomous vehicles and drones more...

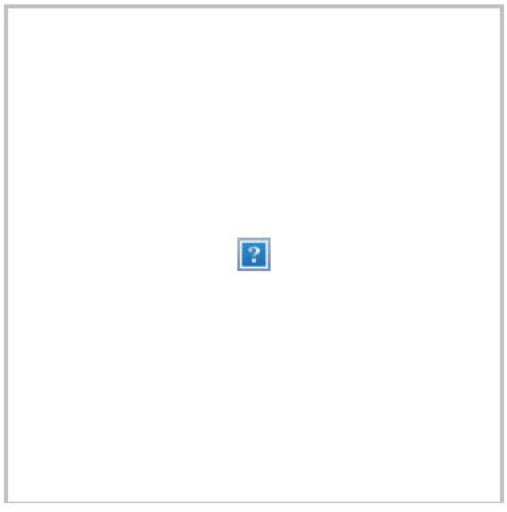


VIDEO: Secretary Chao launches AV test-tracking tool

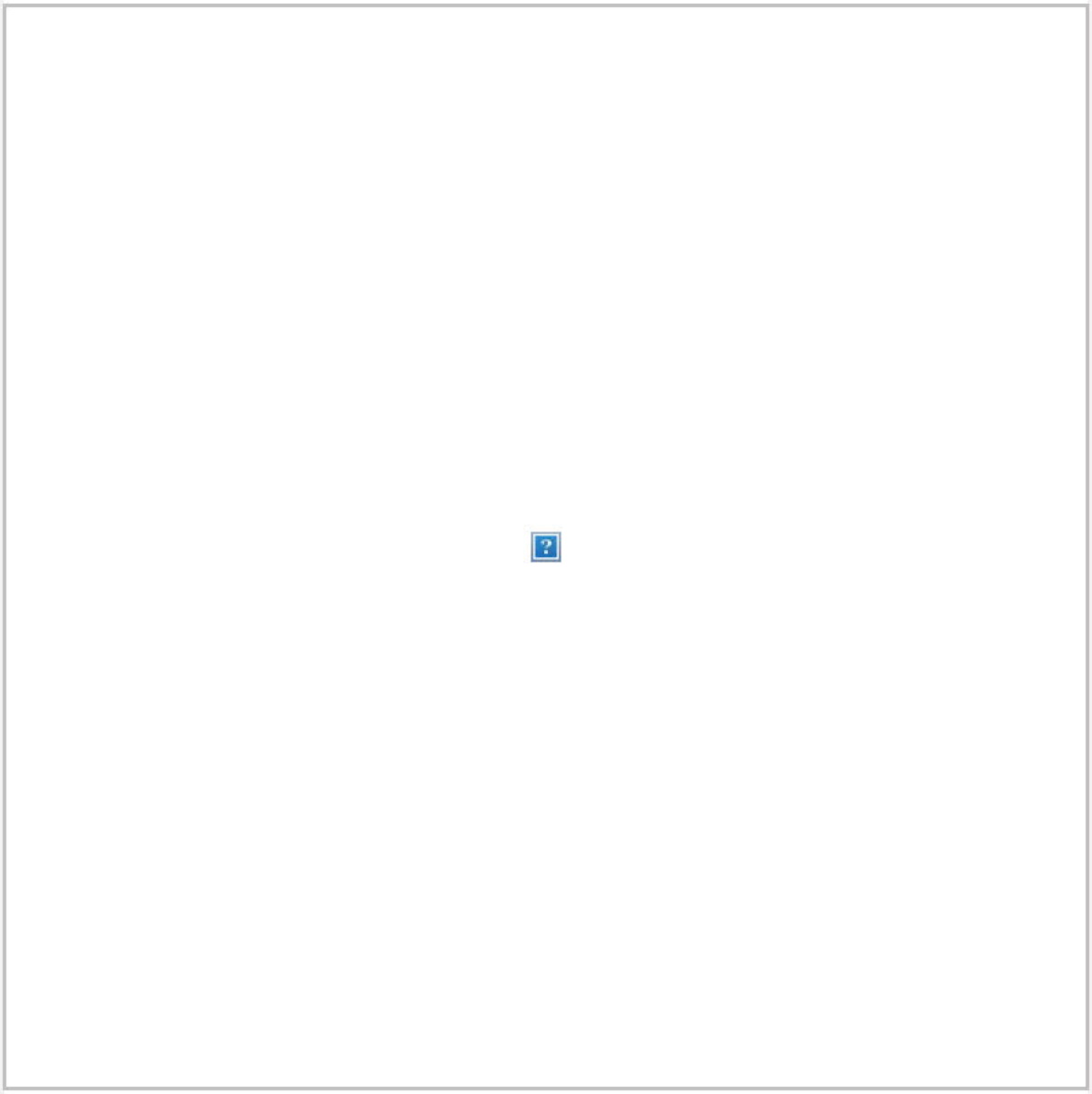


Secretary Chao also this week announced the launch of a new USDOT-backed autonomous vehicle test-tracking tool to enable greater sharing of results and lessons learned about this new technology more...

FEATURE: The impact of Covid-19 on the future of mobility

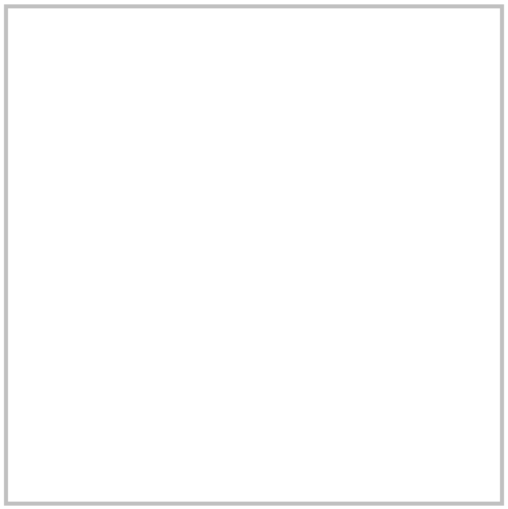


Stephanie Leonard, head of government and regulatory affairs at TomTom, looks at how MaaS, autonomous 'robo-taxis' and electrification could help us to keep moving in the Covid-19 era more...



COVID-19: Smart school-zone beacons help keep students safe from traffic as schedules change

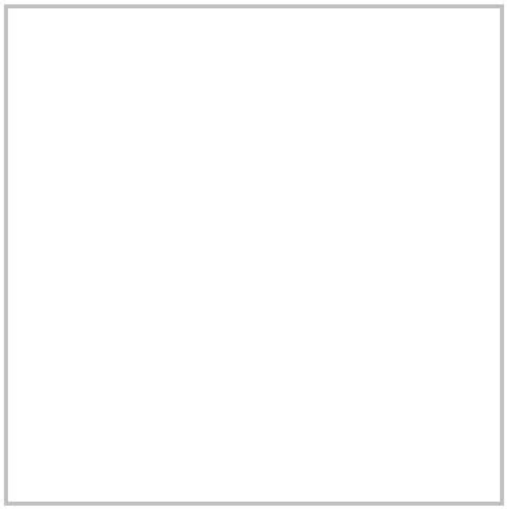
Traffic engineers working with more than 5,000 schools across the US can now use their smartphone or tablet to monitor and control school beacons (the flashing signs intended to slow drivers down as they pass by a school) more...

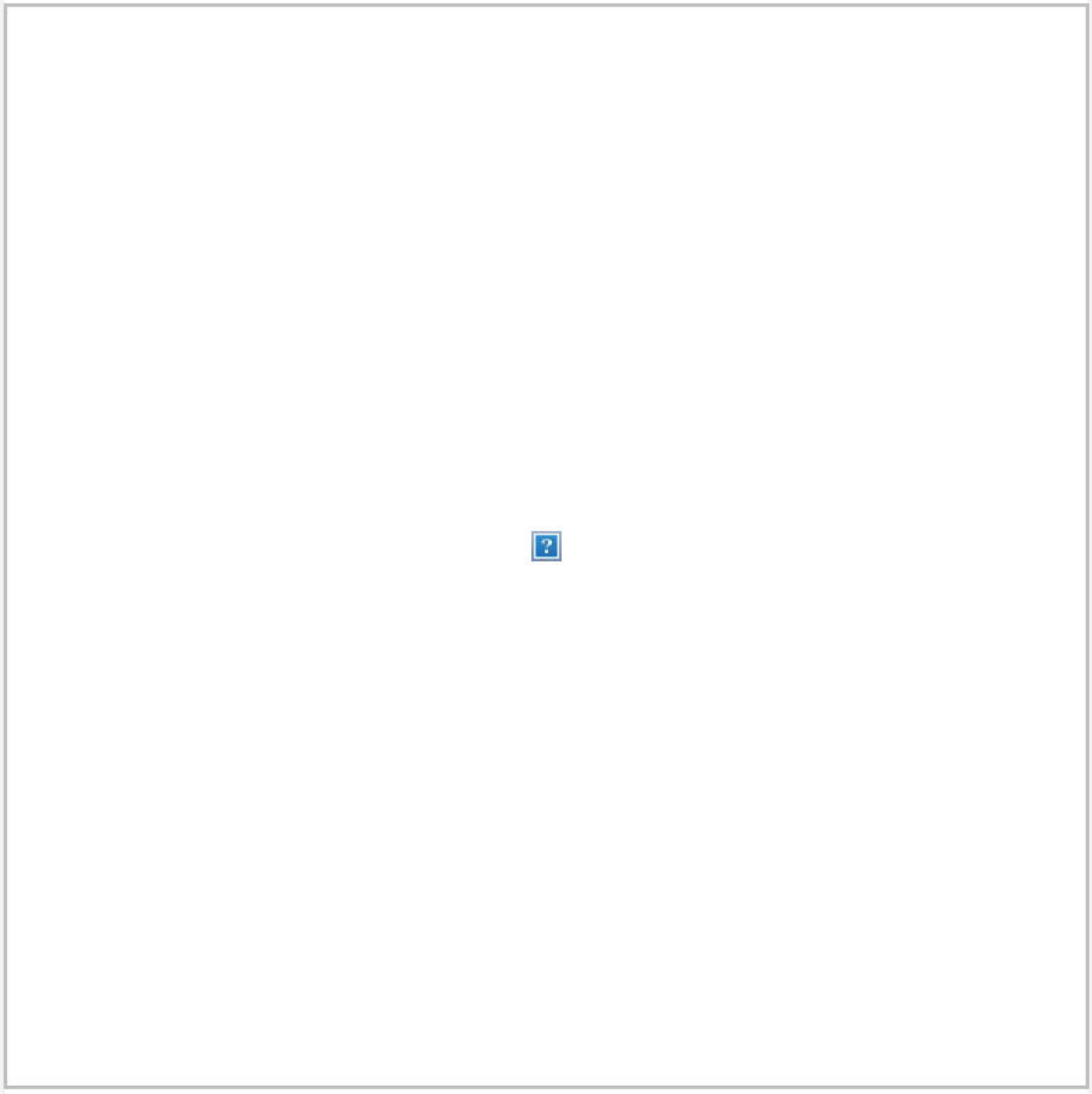


Bookmark our Covid-19 news hub, to stay up-to-date, every day

PTV Group analyses mobility behaviour in Munich to plan potential AV and MaaS deployments

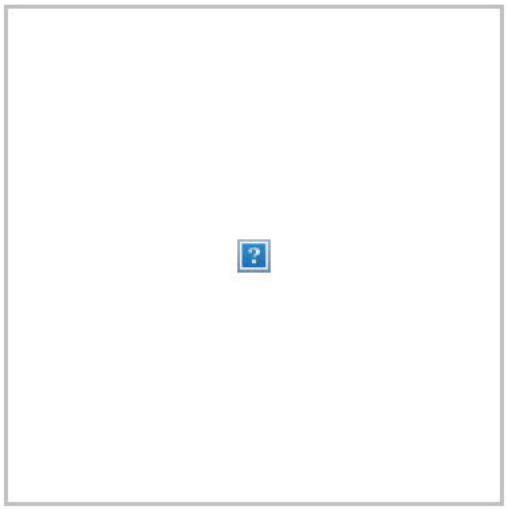
PTV Group, together with a broad-based research team, has been commissioned by the German Federal Ministry of Transport and Digital Infrastructure (BMVI) to analyse mobility behaviour in the city of Munich, with a view to future deployment of autonomous vehicles **more...**



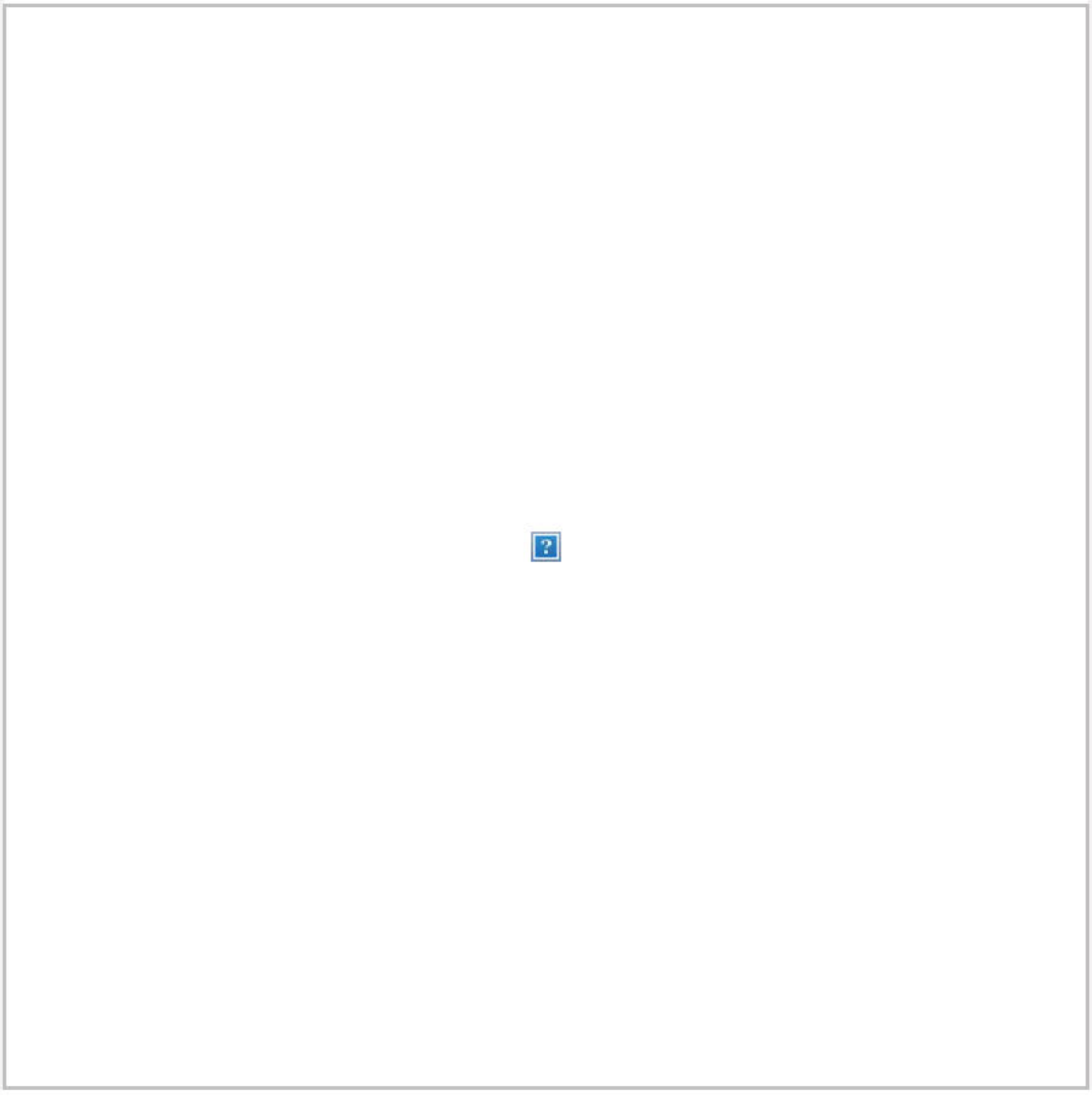


Redflex begins major upgrade of automated enforcement

in Los Angeles

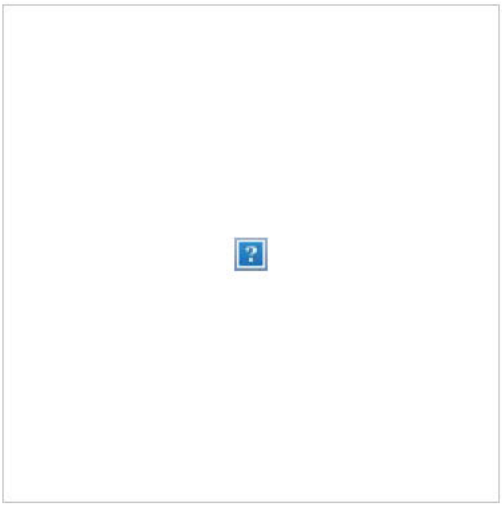


Redflex Traffic Systems is currently in the beginning stages of upgrading 113 automated enforcement camera sites throughout the Los Angeles area that are designed to enhance safety by enforcing traffic laws at bus and rail crossings.
more...



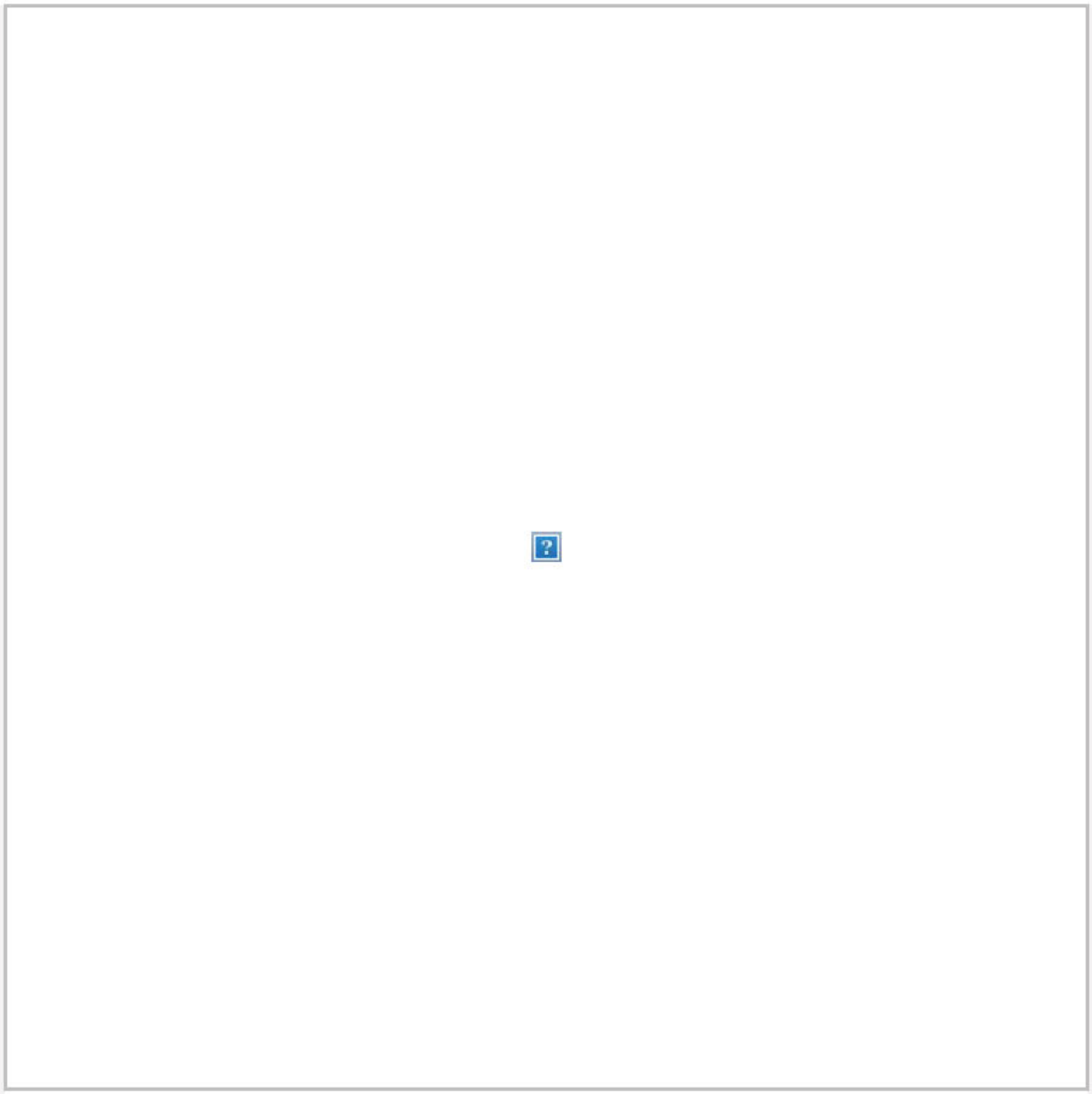
MORE NEWS…

- **Academics at Cal Poly develop system to disable e-scooters if they are ridden on a sidewalk**
- **Millbrook simulator allows real connected vehicles to be tested in virtual world**
- **City of Norwich, England, to launch world's first multi-modal micromobility service**
- **Florida DOT set to deploy near-miss detection system from Iteris and AMAG**
- **Vaisala Digital to deliver real-time weather data to new Hyundai cars**
- **Econolite's Centracs Mobility now able to use crowdsourced traffic data**
- **AMG launches new AMG250 Series Ethernet SFP media converters**

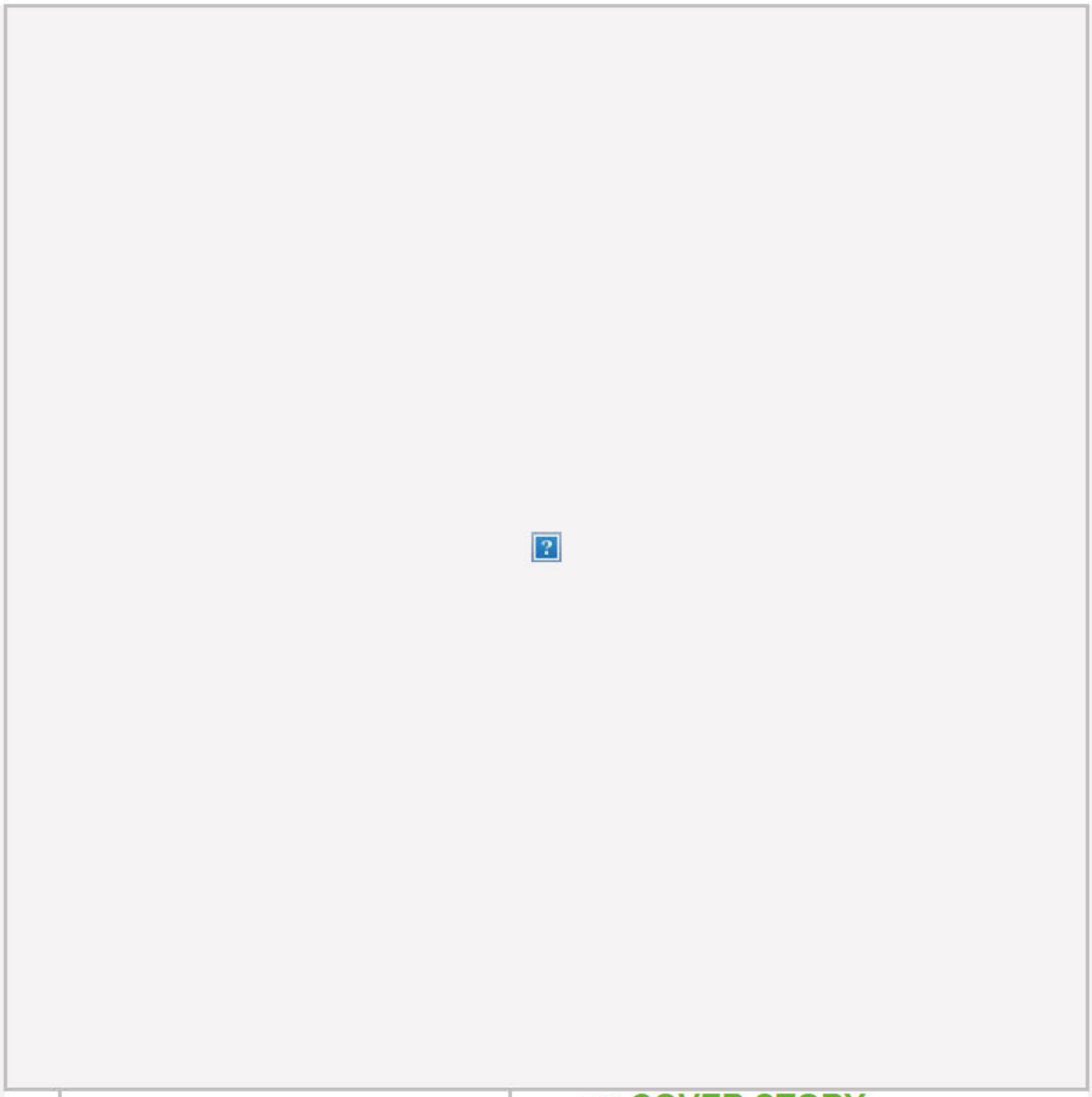


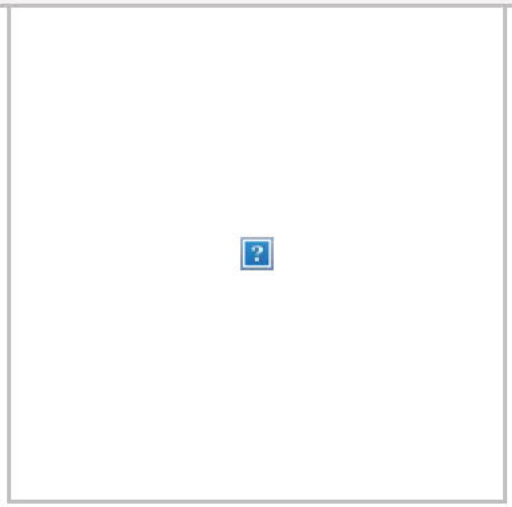
Supplier of the week

CARRIDA Technologies
Your partner for ALPR solutions. CARRIDA Technologies has a simple mission: to detect all cars and licence plates. The root to achieving this goal is the CARRIDA software engine. It is based on modern AI technology and one of world's best recognition software suites. It is designed for all kinds of ALPR/ANPR applications.



BRAND NEW DIGITAL MAGAZINE PLATFORM!





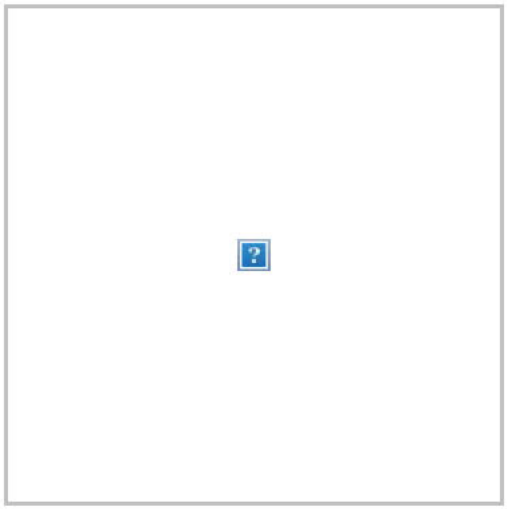
<< COVER STORY

Nineteen ways to start the Covid-19 transport revolution

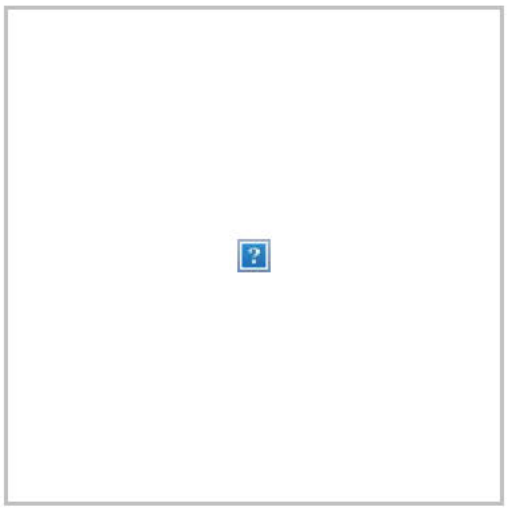
How can we redefine transportation in the 'new normal'? International thought leaders seize the opportunity to create a roadmap to a better future

<< ENFORCEMENT ALPR

Pedal to the metal



Covid-19 lockdowns around the world saw a surge in super-speeders. Saul Wordsworth unpicks the root causes and asks, is the technology up to the task of catching them?



<< WIM INTERVIEW
Chris Koniditsiotis

The president of the International Society for Weigh-in-Motion talks Covid-19, in-vehicle scales and why international, high-speed direct enforcement for WIM could be just around the corner

SUBSCRIBE FREE TO PRINT OR DIGITAL

If you wish to unsubscribe from Traffic Technology International News emails, please click here.
To understand how we process, use & safeguard your data, please read our Privacy Policy. If you would like to update your marketing contact preferences, then please click here.

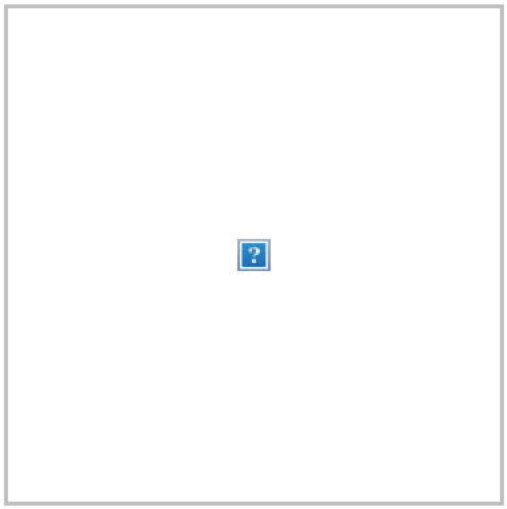
From: Traffic Technology Today
To: zzDowd, Timothy (POL)
Subject: Secretary Chao makes historic announcement on USA's freight system
Date: Friday, September 4, 2020 8:29:46 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

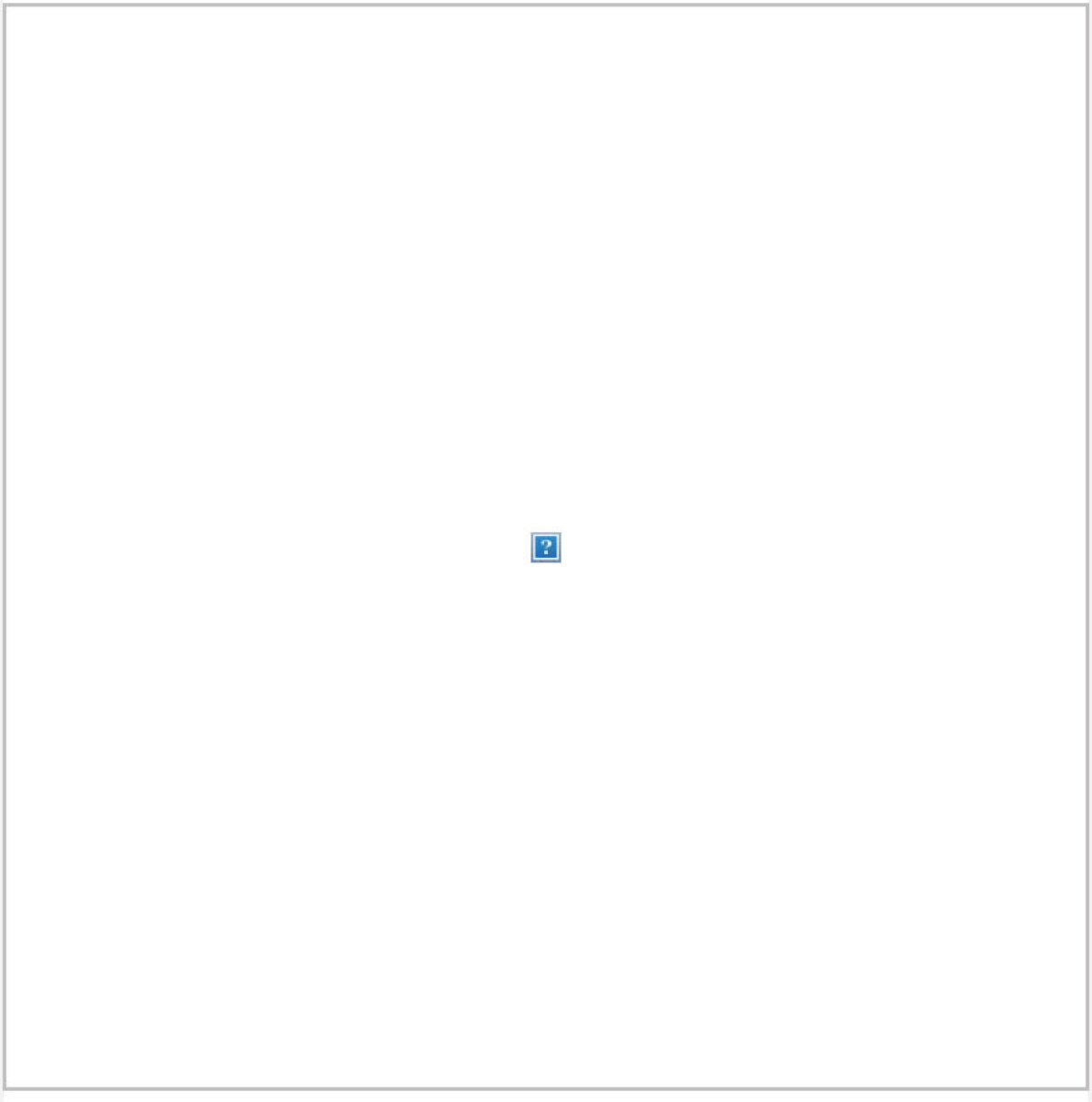
TOP NEWS THIS WEEK

VIDEO: US Transportation Secretary Elaine Chao makes historic announcement on USA's freight system

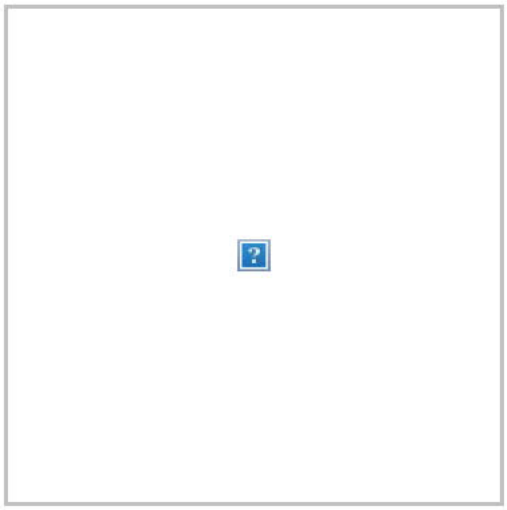
The Transportation Secretary Elaine



Chao has just posted this video announcing the launch of the USA's first ever National Freight Strategic Plan, which will help the nation take full advantage of new technologies such as autonomous vehicles and drones more...

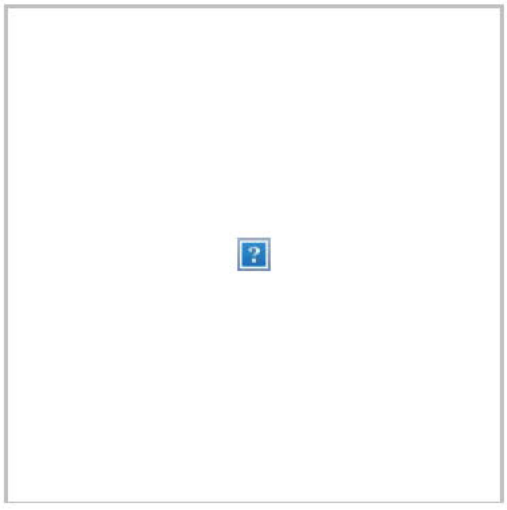


VIDEO: Secretary Chao launches AV test-tracking tool

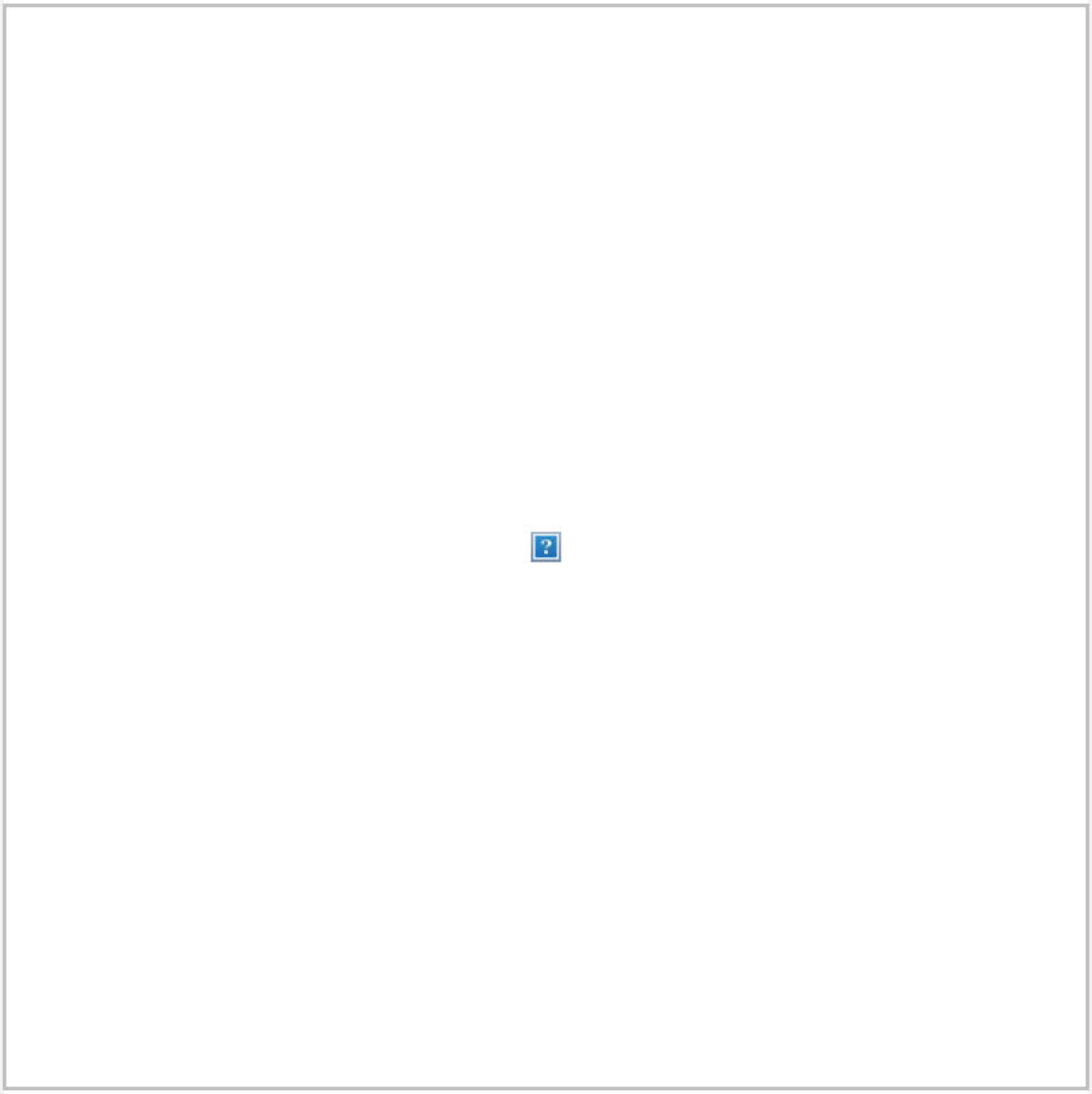


Secretary Chao also this week announced the launch of a new USDOT-backed autonomous vehicle test-tracking tool to enable greater sharing of results and lessons learned about this new technology more...

FEATURE: The impact of Covid-19 on the future of mobility

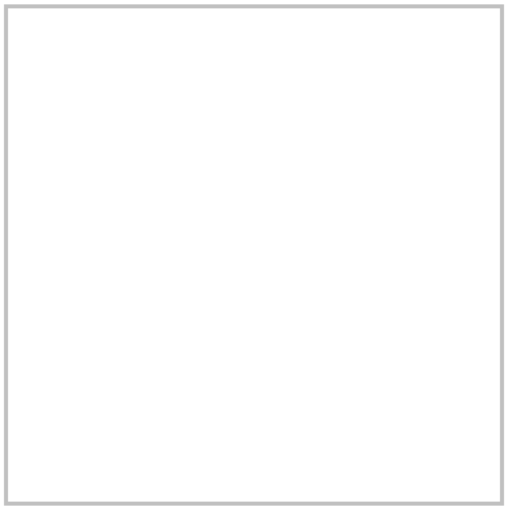


Stephanie Leonard, head of government and regulatory affairs at TomTom, looks at how MaaS, autonomous 'robo-taxis' and electrification could help us to keep moving in the Covid-19 era more...



COVID-19: Smart school-zone beacons help keep students safe from traffic as schedules change

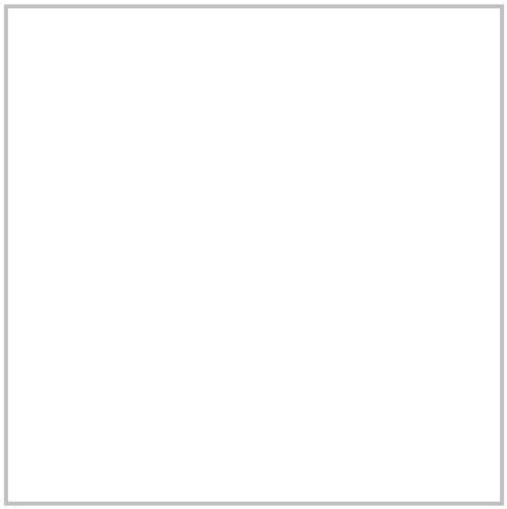
Traffic engineers working with more than 5,000 schools across the US can now use their smartphone or tablet to monitor and control school beacons (the flashing signs intended to slow drivers down as they pass by a school) more...

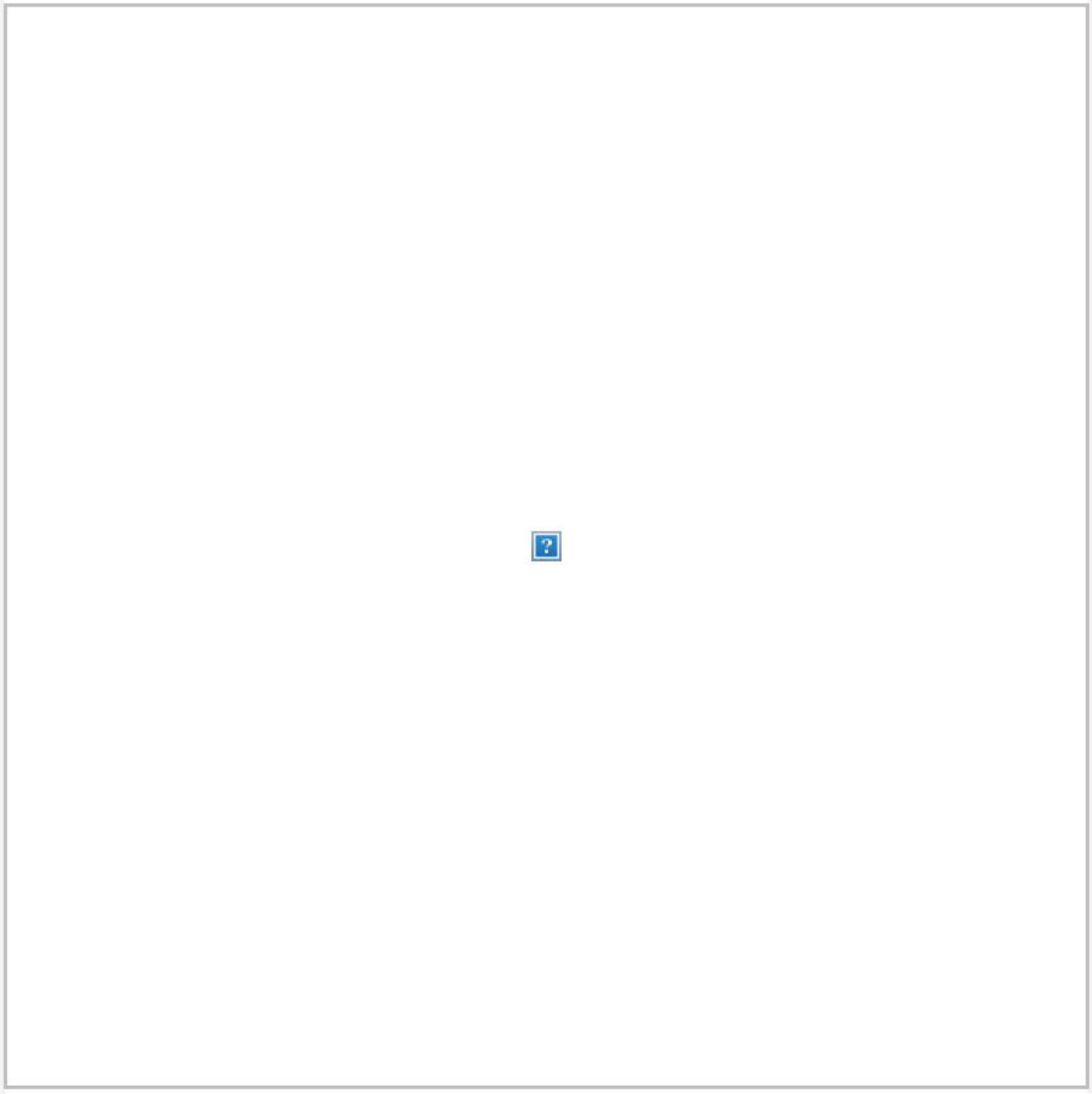


Bookmark our Covid-19 news hub, to stay up-to-date, every day

PTV Group analyses mobility behaviour in Munich to plan potential AV and MaaS deployments

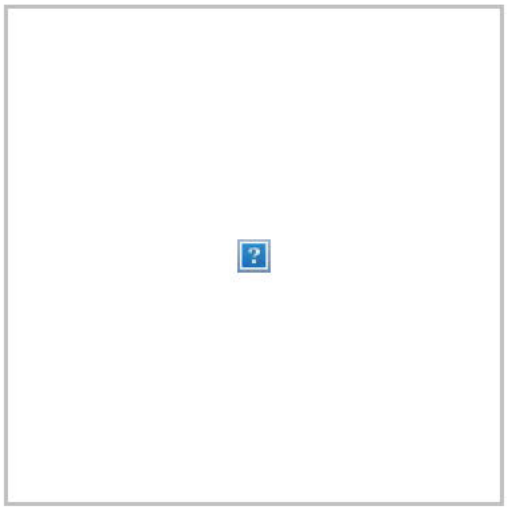
PTV Group, together with a broad-based research team, has been commissioned by the German Federal Ministry of Transport and Digital Infrastructure (BMVI) to analyse mobility behaviour in the city of Munich, with a view to future deployment of autonomous vehicles more...



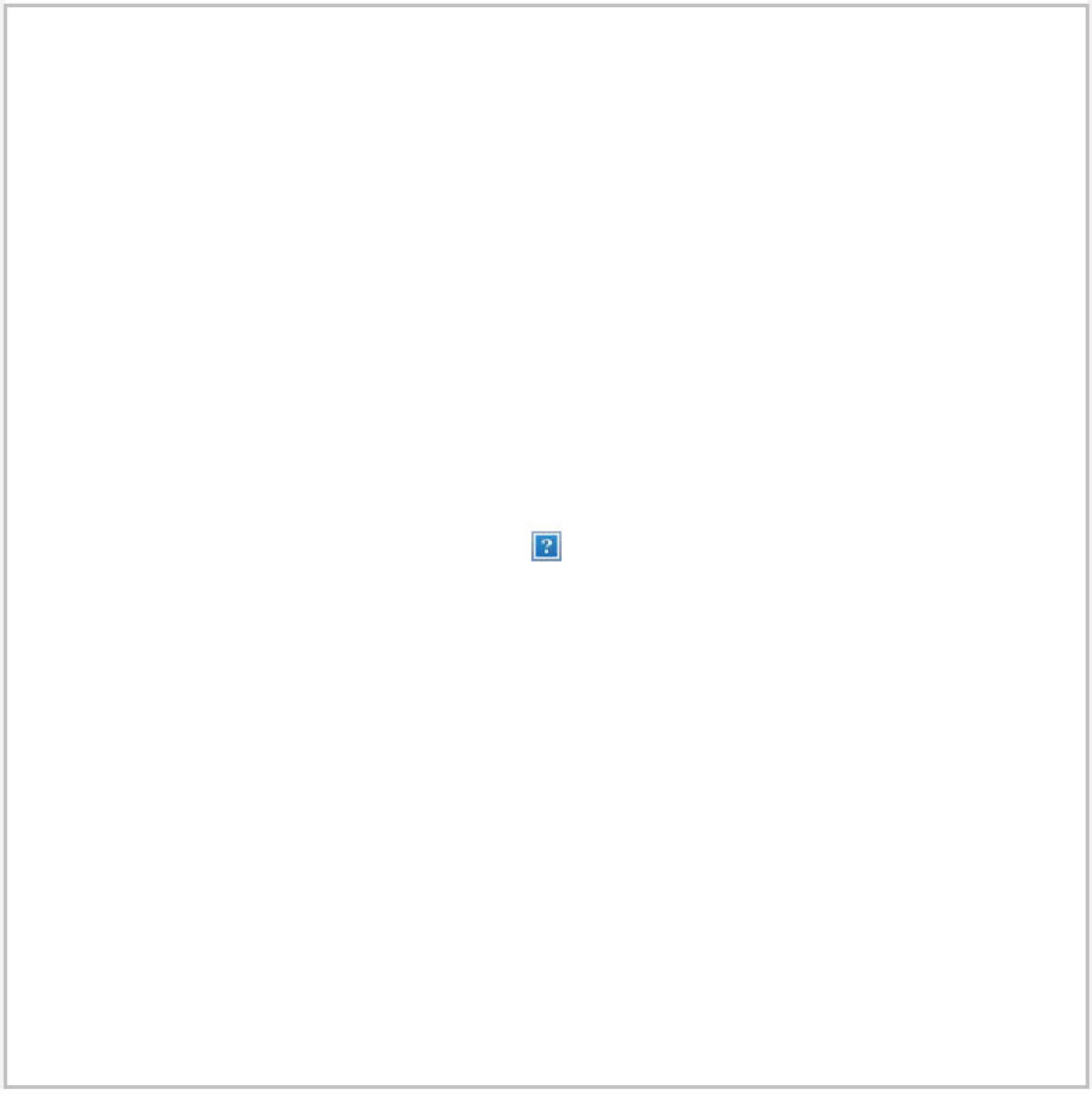


Redflex begins major upgrade of automated enforcement

in Los Angeles

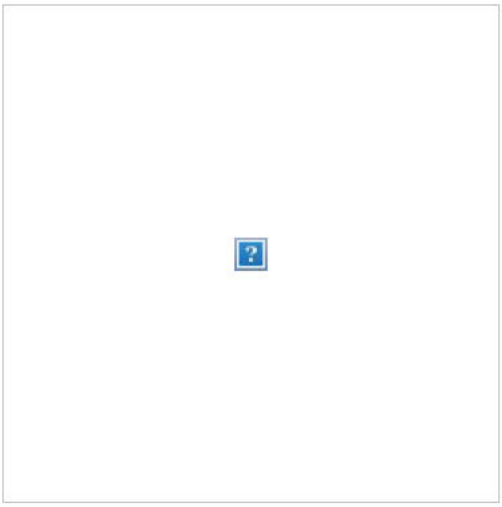


Redflex Traffic Systems is currently in the beginning stages of upgrading 113 automated enforcement camera sites throughout the Los Angeles area that are designed to enhance safety by enforcing traffic laws at bus and rail crossings.
more...



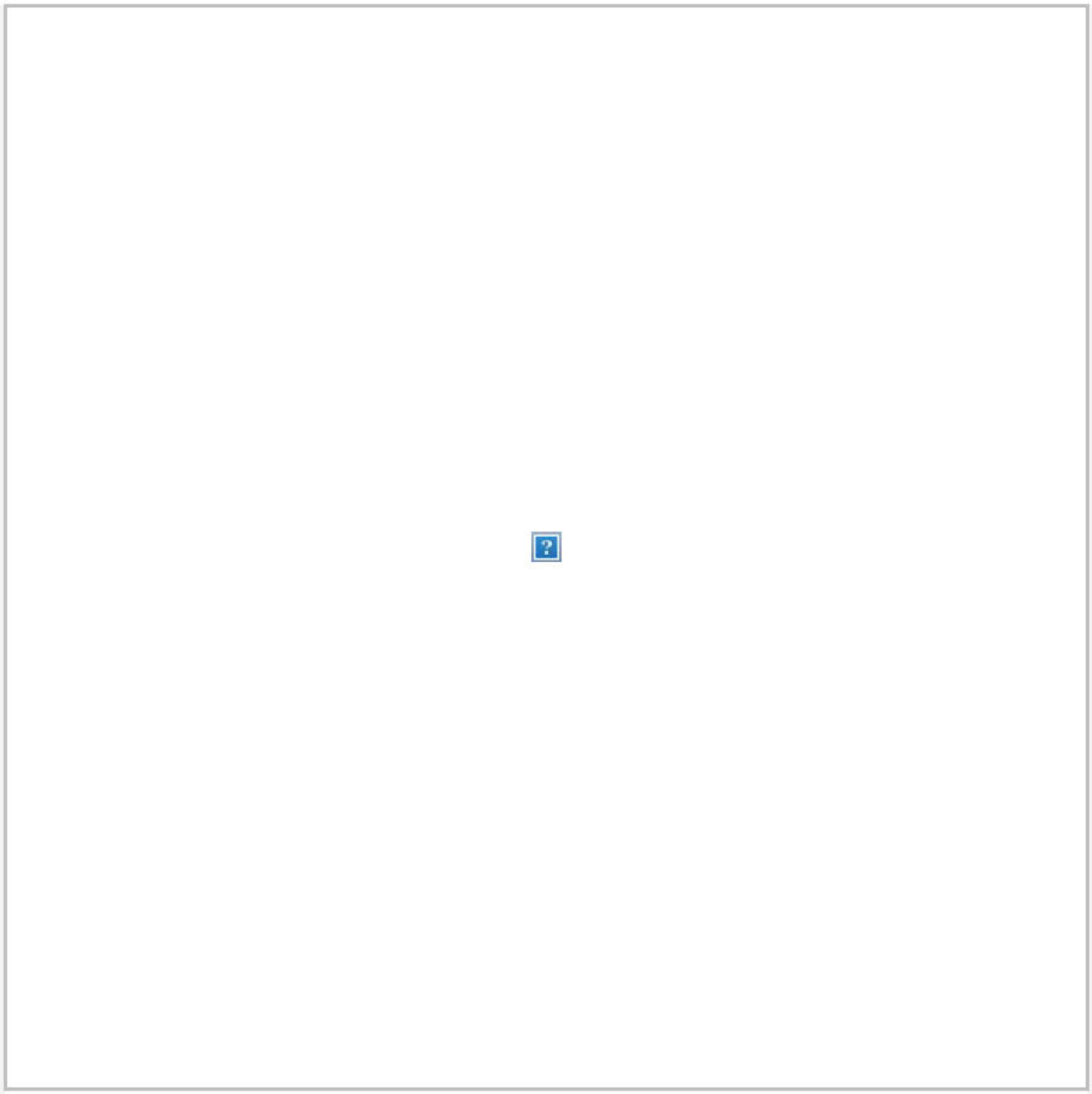
MORE NEWS…

- **Academics at Cal Poly develop system to disable e-scooters if they are ridden on a sidewalk**
- **Millbrook simulator allows real connected vehicles to be tested in virtual world**
- **City of Norwich, England, to launch world's first multi-modal micromobility service**
- **Florida DOT set to deploy near-miss detection system from Iteris and AMAG**
- **Vaisala Digital to deliver real-time weather data to new Hyundai cars**
- **Econolite's Centracs Mobility now able to use crowdsourced traffic data**
- **AMG launches new AMG250 Series Ethernet SFP media converters**

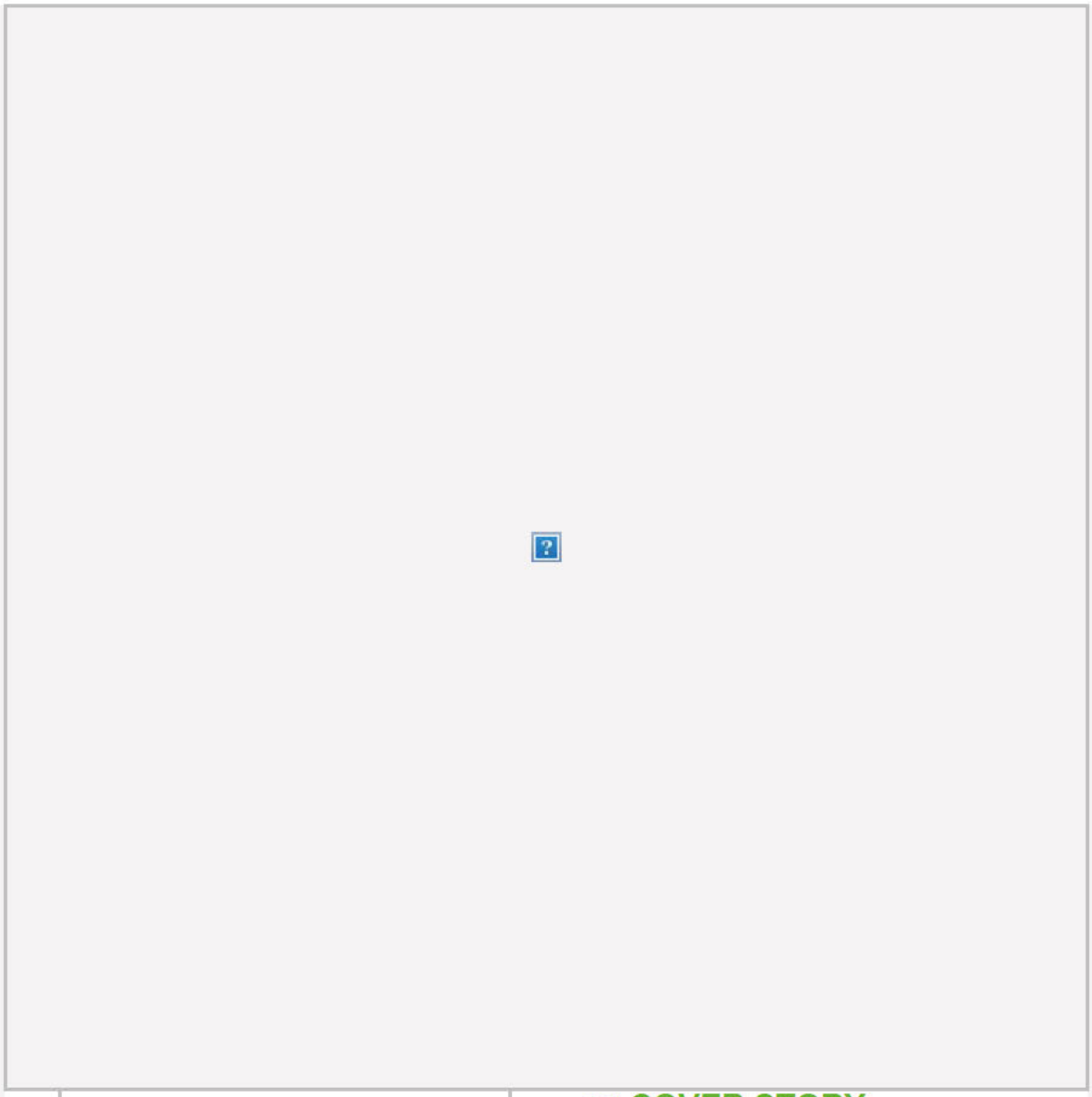


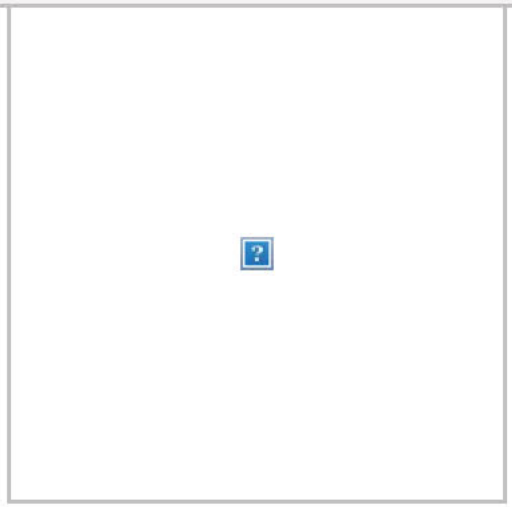
Supplier of the week

CARRIDA Technologies
Your partner for ALPR solutions. CARRIDA Technologies has a simple mission: to detect all cars and licence plates. The root to achieving this goal is the CARRIDA software engine. It is based on modern AI technology and one of world's best recognition software suites. It is designed for all kinds of ALPR/ANPR applications.



BRAND NEW DIGITAL MAGAZINE PLATFORM!





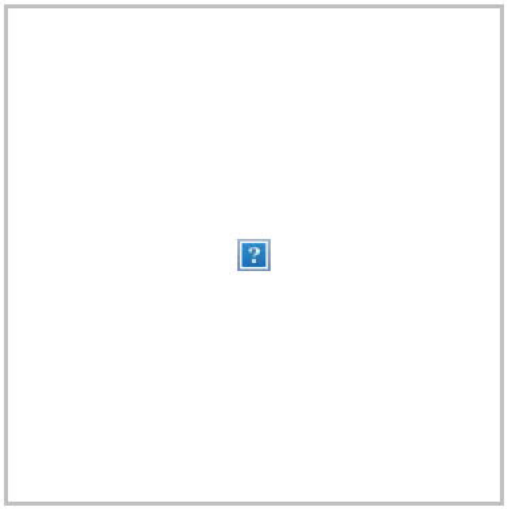
<< COVER STORY

Nineteen ways to start the Covid-19 transport revolution

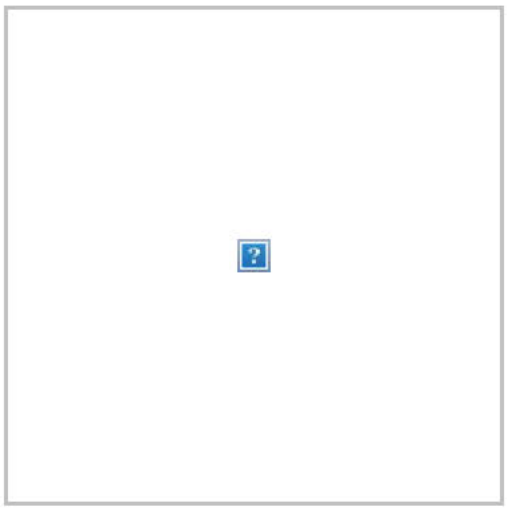
How can we redefine transportation in the 'new normal'? International thought leaders seize the opportunity to create a roadmap to a better future

<< ENFORCEMENT ALPR

Pedal to the metal



Covid-19 lockdowns around the world saw a surge in super-speeders. Saul Wordsworth unpicks the root causes and asks, is the technology up to the task of catching them?



<< WIM INTERVIEW
Chris Koniditsiotis

The president of the International Society for Weigh-in-Motion talks Covid-19, in-vehicle scales and why international, high-speed direct enforcement for WIM could be just around the corner

SUBSCRIBE FREE TO PRINT OR DIGITAL

If you wish to unsubscribe from Traffic Technology International News emails, please click here.
To understand how we process, use & safeguard your data, please read our Privacy Policy. If you would like to update your marketing contact preferences, then please click here.

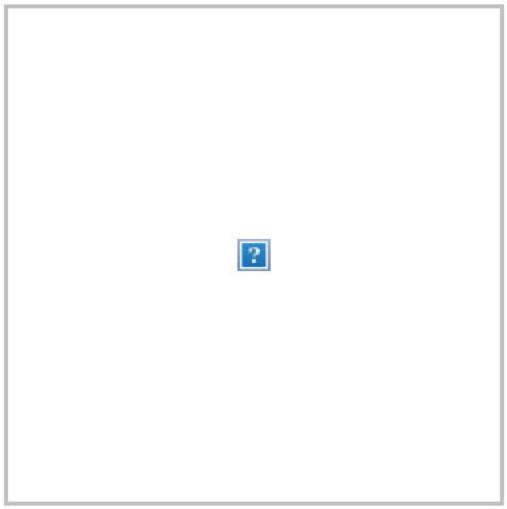
From: Traffic Technology Today
To: Griffin, Daniel (POL)
Subject: Shailen Bhatt says ITS community "open" to 5.9GHz sharing – ONLY if safety is not compromised
Date: Tuesday, September 1, 2020 7:13:46 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

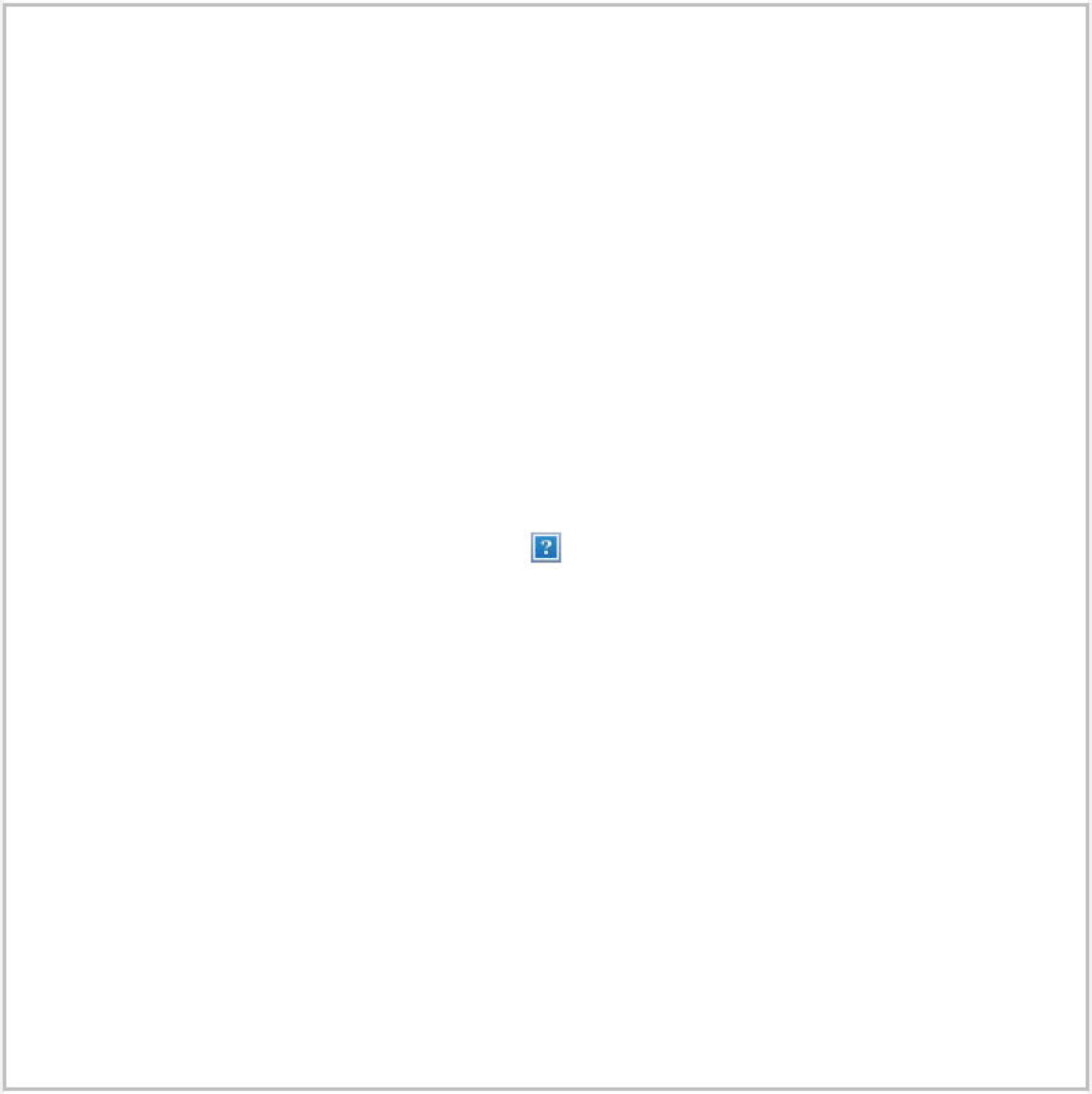
TOP NEWS THIS WEEK

EXCLUSIVE: Shailen Bhatt says ITS community 'open' to 5.9GHz sharing – ONLY if safety is not compromised

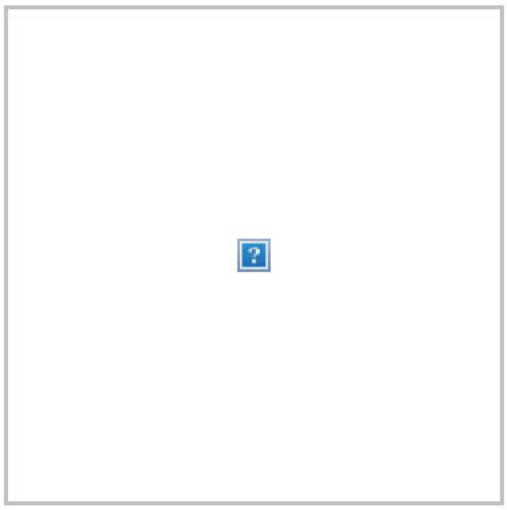
ITS America's president and CEO



Shailen Bhatt has taken a cooperative stance on the controversial issue of spectrum sharing for V2X in the USA – but is still waiting for proof that there will be no detriment to road safety **more...**



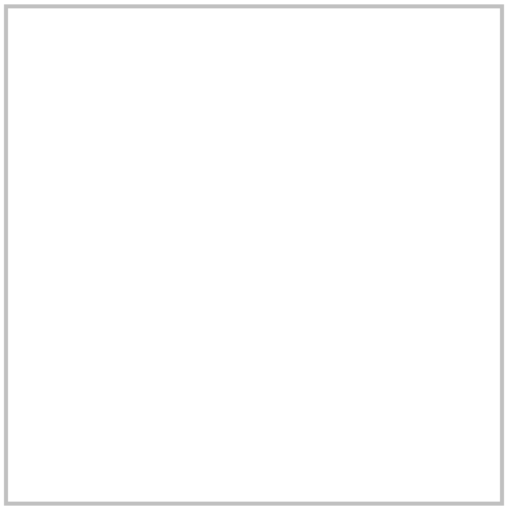
VIDEO: Oxbotica AV platform masters driving on both sides of the road



UK-based autonomous vehicle software developer Oxbotica has mastered driving both on the left and right-hand side of the road on public roads after being granted automated vehicle (AV) permit recommendation by TÜV SÜD to conduct live trials in Germany **more...**

Covid-19: UK government launches Acceleration Unit and £360m extra investment for transportation

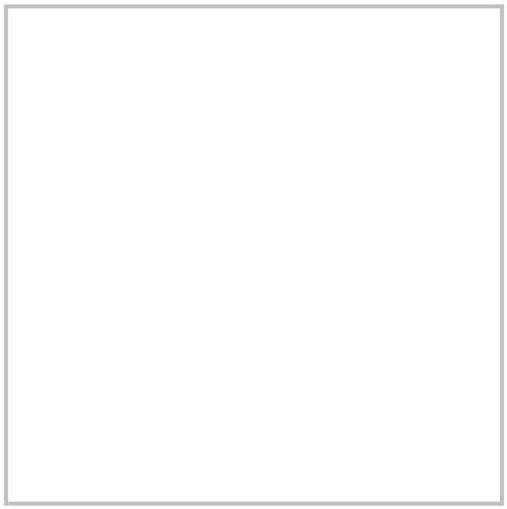
The UK Transport Secretary Grant Shapps has launched a new Acceleration Unit to speed up transport infrastructure projects and build back better from Covid-19. The New unit will boost the delivery times of major transport projects as new funding is announced more...



Bookmark our Covid-19 news hub, to stay up-to-date, every day

Ford, Bedrock and Bosch explore autonomous vehicle parking solution

Ford Motor Company, Bedrock and Bosch are launching a demonstration project with connected Ford Escape test vehicles that can drive and park themselves inside Bedrock's Assembly Garage in Detroit using Bosch smart infrastructure more...



MORE NEWS…

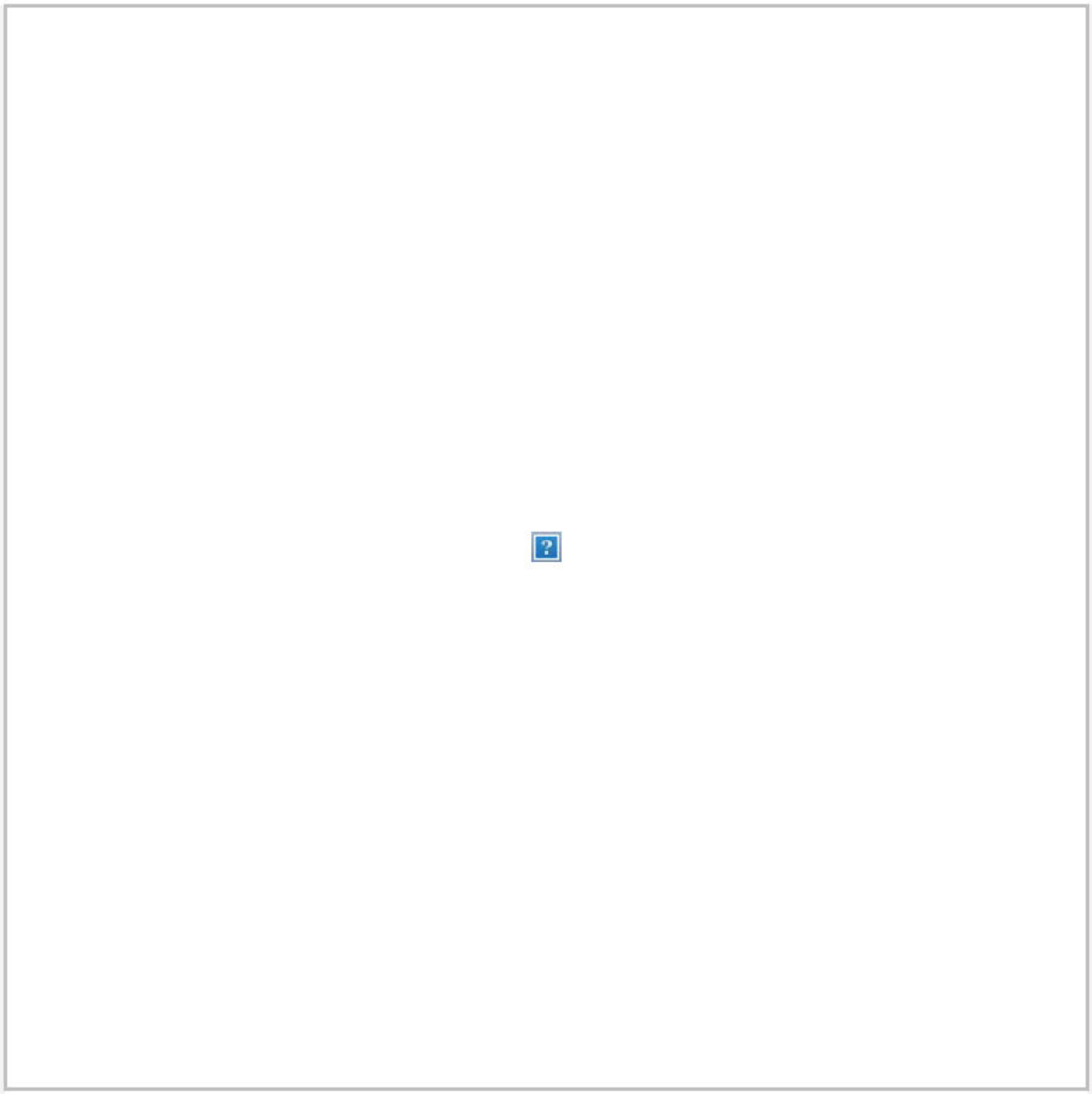
- **Siemens supports New Zealand's low carbon future with ebus charging infrastructure**
- **Highways England installs new, smart, cloud-linked Swarco Traffic prism signage along M6**
- **Cangzhou, China, sees public robotaxi service extended, though safety drivers still monitor**
- **New carpool lane on I-680, California, opens a year ahead of schedule**
- **Highways England chief executive Jim O'Sullivan announces departure**
- **PTV takes to the cloud with realigned business model to deliver positive 2020**



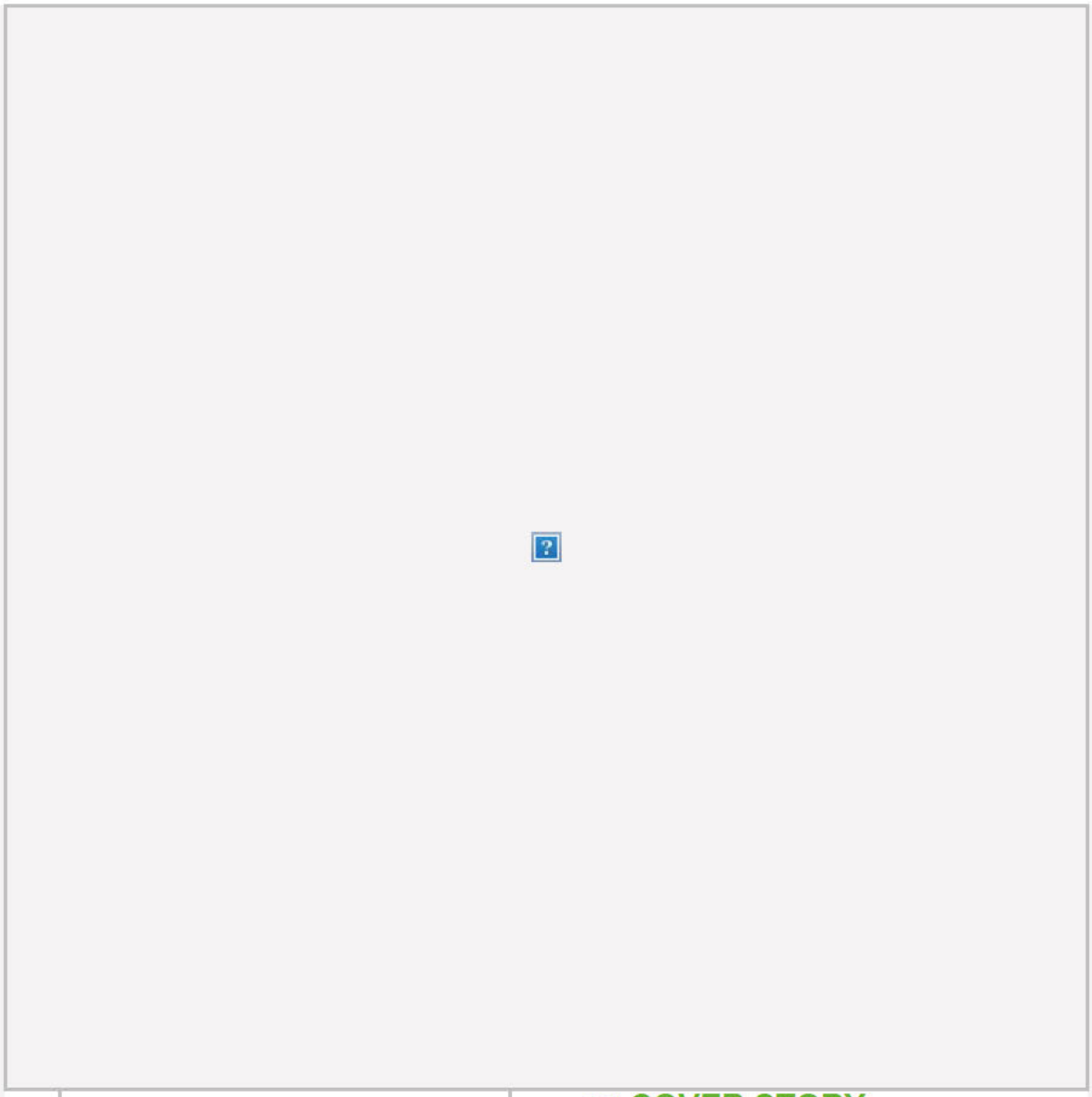


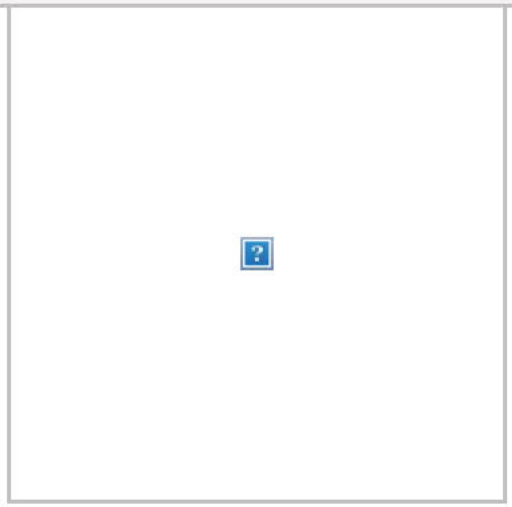
Supplier of the week

Triple Sign System
Triple Sign System AB is a leading producer and developer of Prismatic variable messaging signs, VMS. These signs provide relevant traffic information for safety and efficiency in a cost-effective and sustainable way



BRAND NEW DIGITAL MAGAZINE PLATFORM!





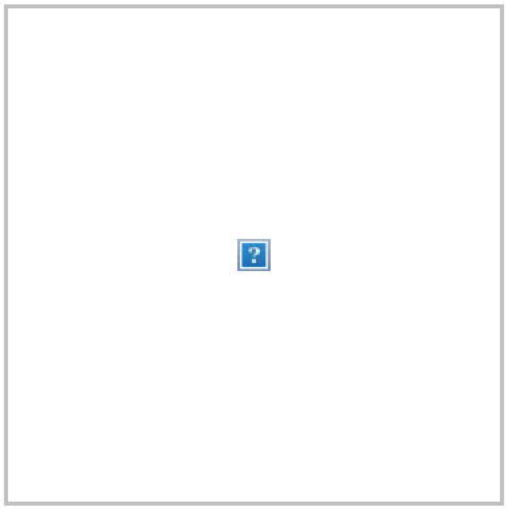
<< COVER STORY

Nineteen ways to start the Covid-19 transport revolution

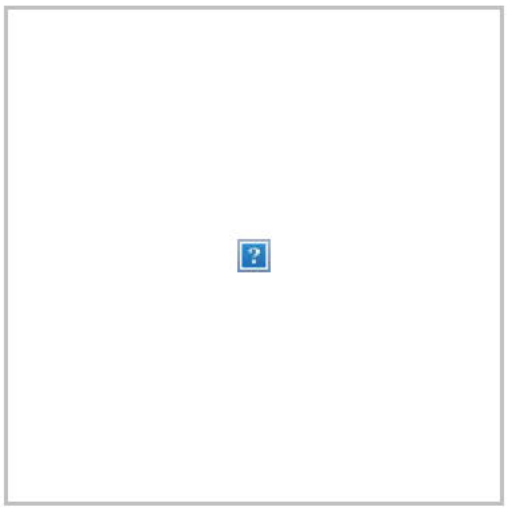
How can we redefine transportation in the 'new normal'? International thought leaders seize the opportunity to create a roadmap to a better future

<< ENFORCEMENT ALPR

Pedal to the metal



Covid-19 lockdowns around the world saw a surge in super-speeders. Saul Wordsworth unpicks the root causes and asks, is the technology up to the task of catching them?



<< WIM INTERVIEW
Chris Koniditsiotis

The president of the International Society for Weigh-in-Motion talks Covid-19, in-vehicle scales and why international, high-speed direct enforcement for WIM could be just around the corner

SUBSCRIBE FREE TO PRINT OR DIGITAL

If you wish to unsubscribe from Traffic Technology International News emails, please click here.
To understand how we process, use & safeguard your data, please read our Privacy Policy. If you would like to update your marketing contact preferences, then please click here.

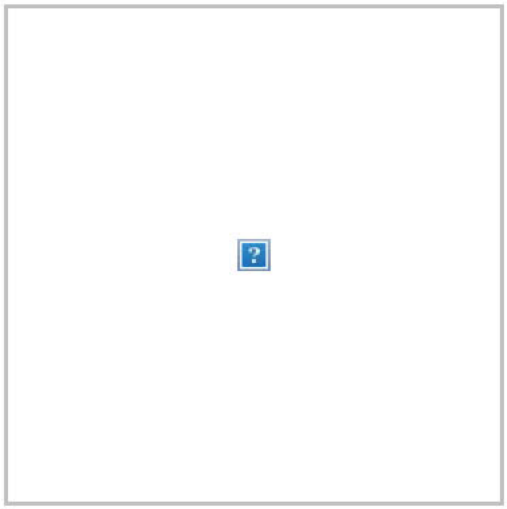
From: Traffic Technology Today
To: zzDowd, Timothy (POL)
Subject: Shailen Bhatt says ITS community "open" to 5.9GHz sharing – ONLY if safety is not compromised
Date: Tuesday, September 1, 2020 7:18:13 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

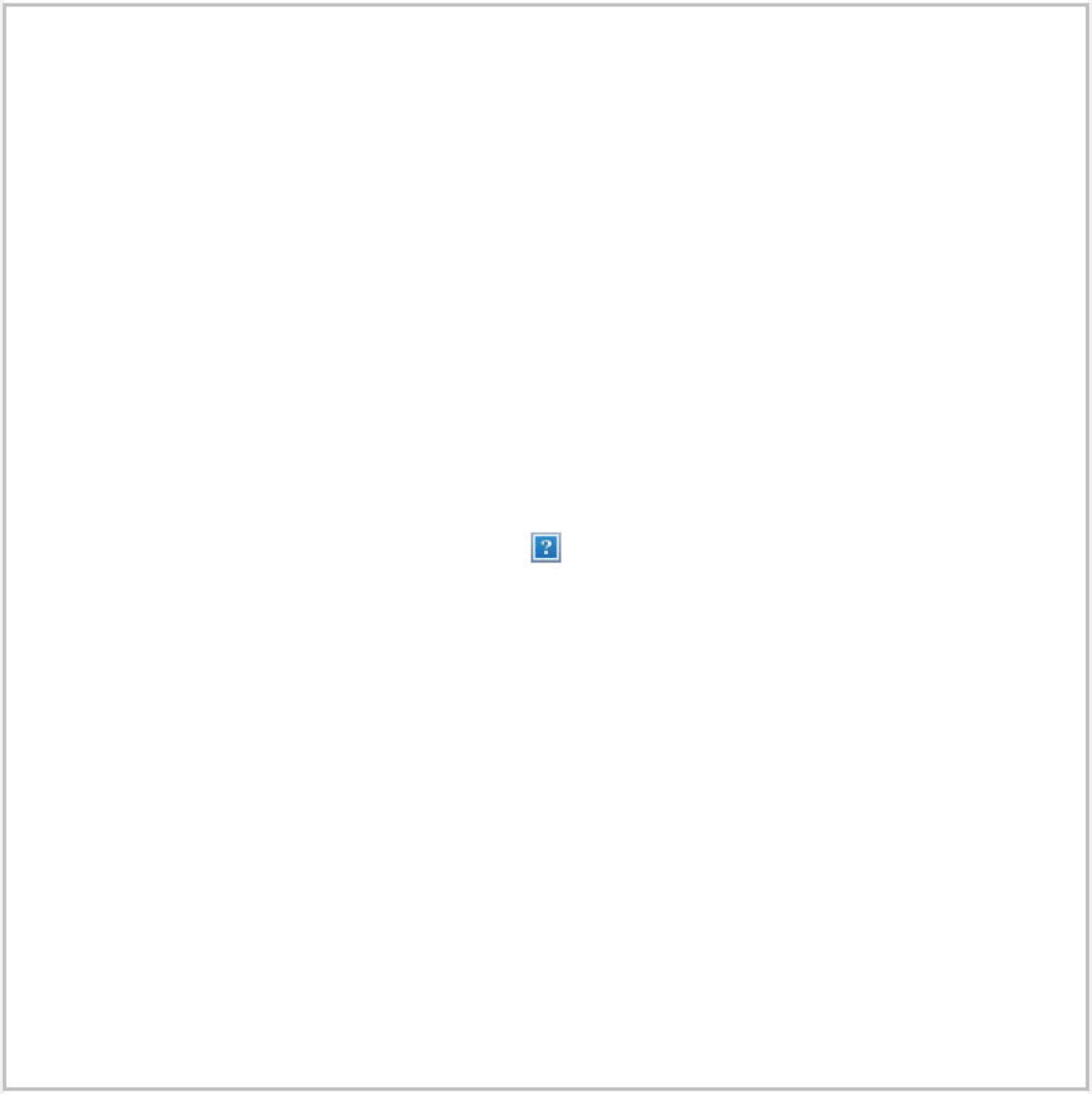
TOP NEWS THIS WEEK

EXCLUSIVE: Shailen Bhatt says ITS community 'open' to 5.9GHz sharing – ONLY if safety is not compromised

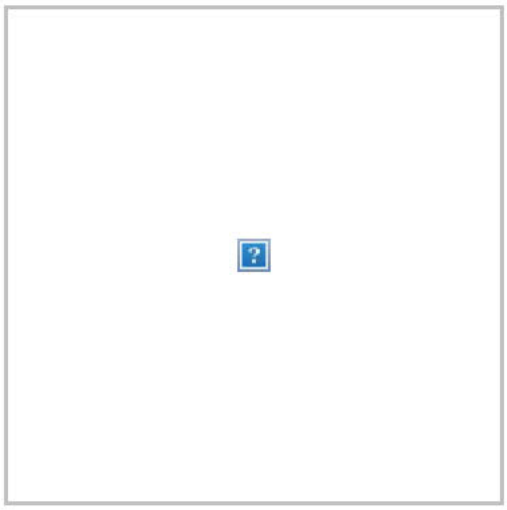
ITS America's president and CEO



Shailen Bhatt has taken a cooperative stance on the controversial issue of spectrum sharing for V2X in the USA – but is still waiting for proof that there will be no detriment to road safety **more...**



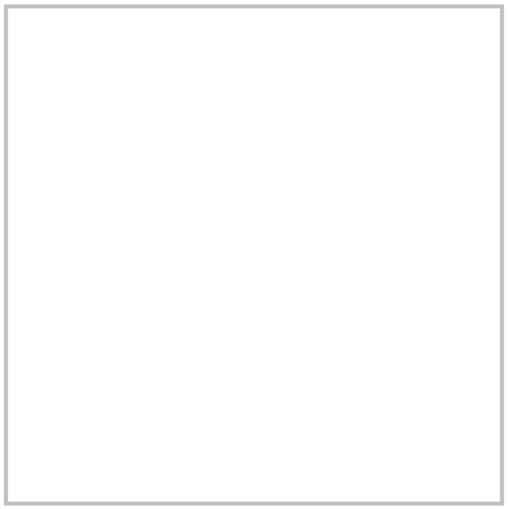
VIDEO: Oxbotica AV platform masters driving on both sides of the road



UK-based autonomous vehicle software developer Oxbotica has mastered driving both on the left and right-hand side of the road on public roads after being granted automated vehicle (AV) permit recommendation by TÜV SÜD to conduct live trials in Germany **more...**

Covid-19: UK government launches Acceleration Unit and £360m extra investment for transportation

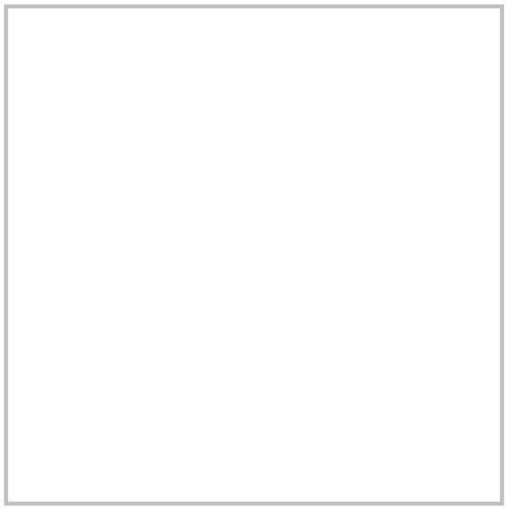
The UK Transport Secretary Grant Shapps has launched a new Acceleration Unit to speed up transport infrastructure projects and build back better from Covid-19. The New unit will boost the delivery times of major transport projects as new funding is announced more...



Bookmark our Covid-19 news hub, to stay up-to-date, every day

Ford, Bedrock and Bosch explore autonomous vehicle parking solution

Ford Motor Company, Bedrock and Bosch are launching a demonstration project with connected Ford Escape test vehicles that can drive and park themselves inside Bedrock's Assembly Garage in Detroit using Bosch smart infrastructure more...

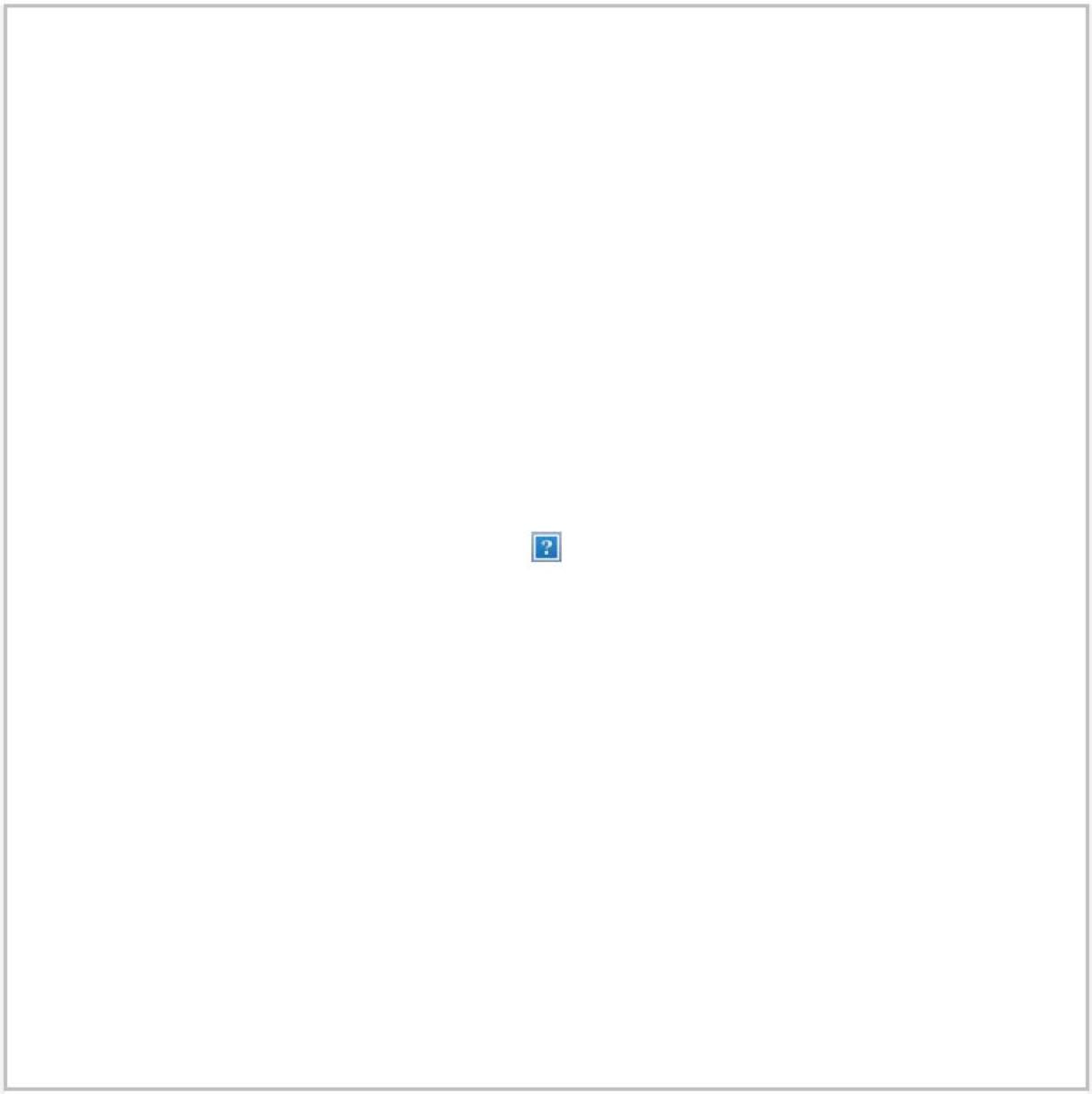


MORE NEWS…

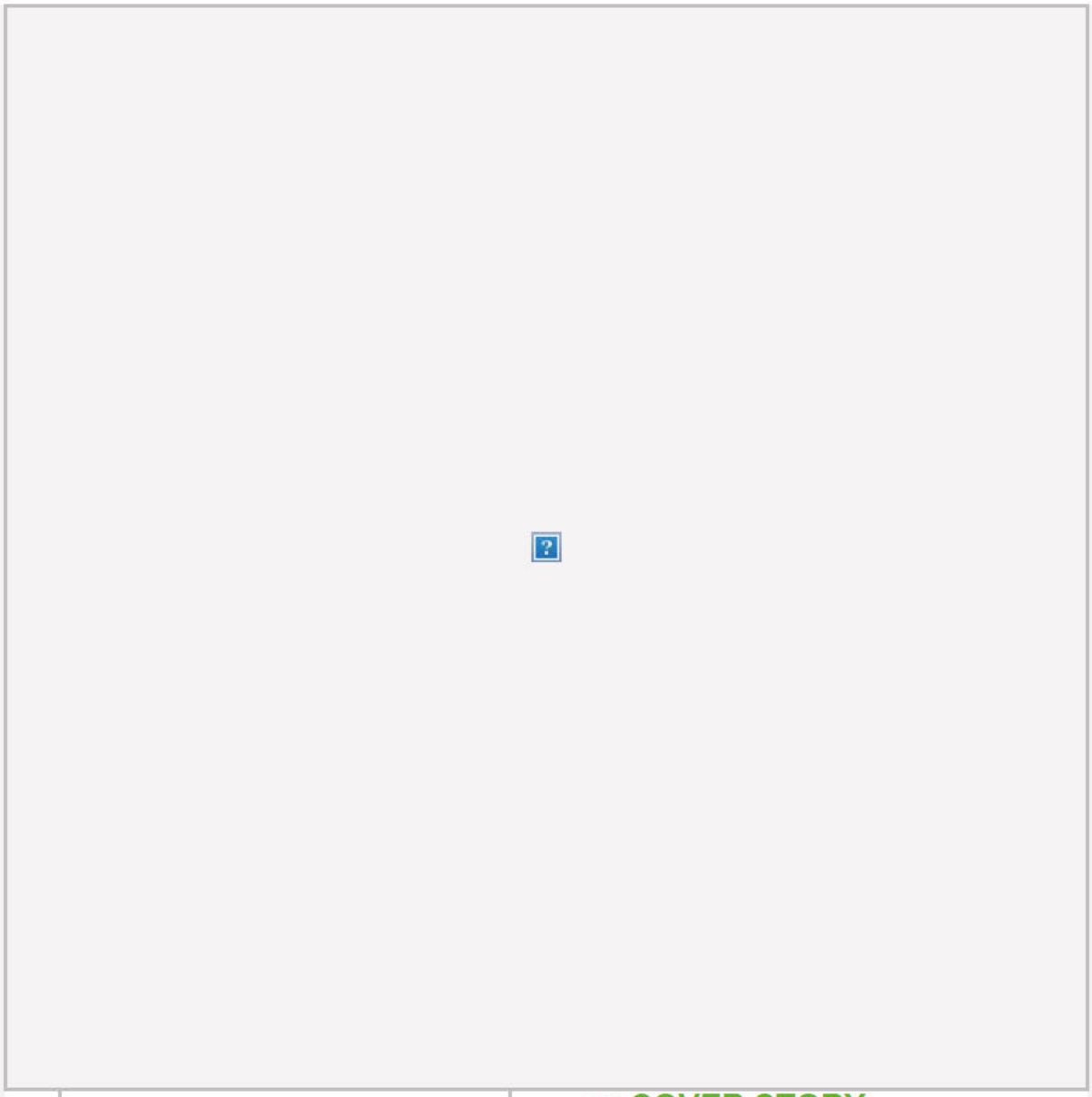
- Siemens supports New Zealand's low carbon future with ebus charging infrastructure
- Highways England installs new, smart, cloud-linked Swarco Traffic prism signage along M6
- Cangzhou, China, sees public robotaxi service extended, though safety drivers still monitor
- New carpool lane on I-680, California, opens a year ahead of schedule
- Highways England chief executive Jim O'Sullivan announces departure
- PTV takes to the cloud with realigned business model to deliver positive 2020

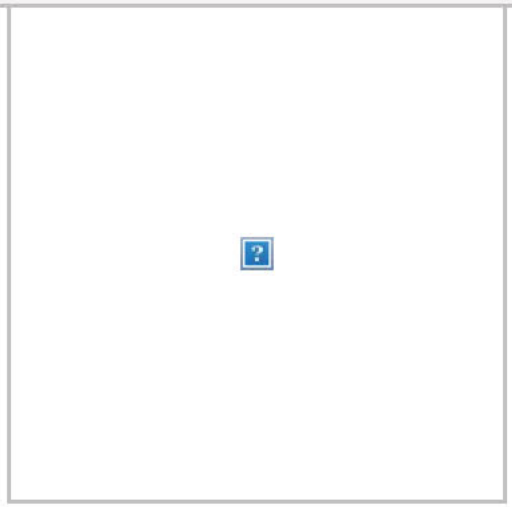
Supplier of the week

Triple Sign System
Triple Sign System AB is a leading producer and developer of Prismatic variable messaging signs, VMS. These signs provide relevant traffic information for safety and efficiency in a cost-effective and sustainable way



BRAND NEW DIGITAL MAGAZINE PLATFORM!





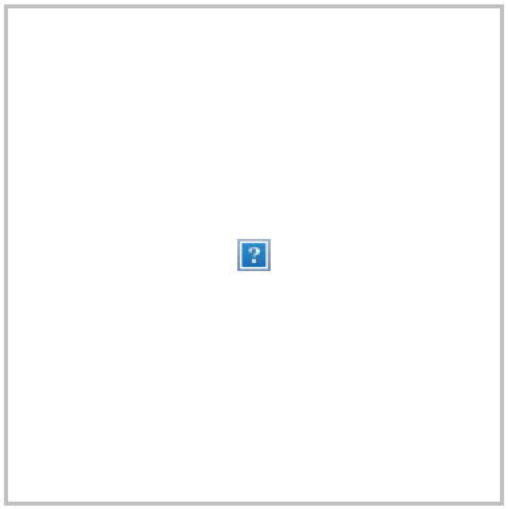
<< COVER STORY

Nineteen ways to start the Covid-19 transport revolution

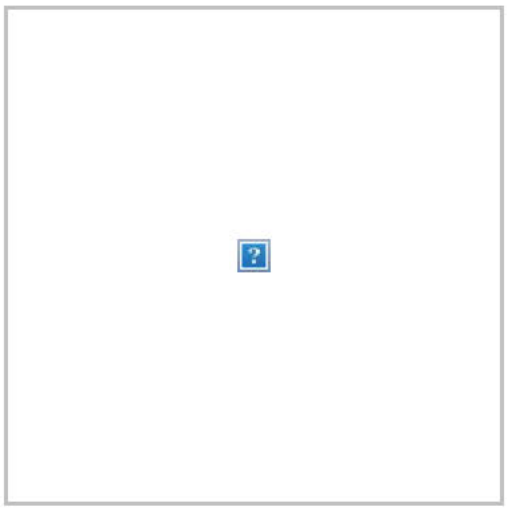
How can we redefine transportation in the 'new normal'? International thought leaders seize the opportunity to create a roadmap to a better future

<< ENFORCEMENT ALPR

Pedal to the metal



Covid-19 lockdowns around the world saw a surge in super-speeders. Saul Wordsworth unpicks the root causes and asks, is the technology up to the task of catching them?



<< WIM INTERVIEW
Chris Koniditsiotis

The president of the International Society for Weigh-in-Motion talks Covid-19, in-vehicle scales and why international, high-speed direct enforcement for WIM could be just around the corner

SUBSCRIBE FREE TO PRINT OR DIGITAL

If you wish to unsubscribe from Traffic Technology International News emails, please click here.
To understand how we process, use & safeguard your data, please read our Privacy Policy. If you would like to update your marketing contact preferences, then please click here.

From: info@lahidtatraining.org
To: Newton, Justin (POL)
Subject: Some Upcoming Training
Date: Tuesday, February 18, 2020 1:55:31 PM

LA HIDTA Sunset Header.png

Here is a very small portion of classes that are listed on the training calendar at LA HIDTA Training. To view all the classes posted on the training calendar or to register for one of these classes, go to www.lahidtatraining.org.

February 20, 2020 - Thursday
Human Trafficking and Child Exploitation Training
Los Angeles, CA
Download Flyer

February 22, 2020 - Saturday
Police Promotion: Oral Interview Dynamics
Chino Hills, CA
Download Flyer

February 25, 2020 - Tuesday
Clandestine Laboratory Safety Recertification Course – *POST Certified*
Anaheim, CA
Download Flyer

February 26, 2020 - Wednesday
Asset Forfeiture Seminar – *POST Certified - Free*
Alhambra, CA
Download Flyer

February 28, 2020 - Friday
Tactical Emergency Casualty Care for Law Enforcement & First Responders Course – *POST & NAEMT Certified*
Commerce, CA
Download Flyer

March 02, 2020 - Monday
Crisis Negotiations - Basic Course – *POST Certified – Free Class*
Los Angeles, CA
Download Flyer

March 03-05, 2020; Tuesday - Thursday
Assertive Supervision: Practical Approaches to Performance Management – *POST & STC Certified*
Camarillo, CA
Download Flyer

March 04, 2020 - Wednesday
Evidence Management for Supervisors
Rialto, Ca
Download Flyer

March 04-06, 2020; Wednesday - Friday
Force Encounters Analysis: Understanding Human Performance in Critical Incidents – *POST & STC Certified*
Newport Beach, CA
Download Flyer

March 04-06, 2020; Wednesday - Friday
Drug Abuse Recognition (DAR)/Drugged Driving Investigations (DDI) – *POST & STC Certified*
French Camp, CA
Download Flyer

March 05, 2020 - Thursday
Workshop: ALPR & Community Policing – *Free Class – For Command Staff*
Commerce, CA
Click to Register
Download Flyer

March 09-11, 2020; Monday - Wednesday
Performance Staff Leadership Training – *POST & STC Certified*
San Bernardino, CA
Download Flyer

March 09-11, 2020; Monday - Wednesday
DUI - Standardized Field Sobriety Testing
Santa Monica, CA
Download Flyer

March 12-13, 2020; Thursday - Friday
Advanced Roadside Impaired Driving Enforcement (ARIDE) – *POST Certified – Free Class*
Santa Monica, CA
Download Flyer

March 13, 2020 - Friday
Use It, Write It, Tell It
Watsonville, CA
Download Flyer

March 16, 2020 - Monday
DUI Checkpoints - Planning & Managing – *POST Certified*
Riverside, Ca
Download Flyer

March 17, 2020 - Tuesday
Clandestine Laboratory Safety Recertification Course – *POST Certified*
Monterey, CA
Download Flyer

March 17, 2020 - Tuesday
Preliminary Alcohol Screening (PAS) Instruments – *POST Certified*
Riverside, Ca
Download Flyer

March 17-18, 2020; Tuesday - Wednesday
Advanced Training Officer – *POST Certified*
Santa Clara, CA
Download Flyer

March 19, 2020 - Thursday
Crisis Communications Skills: Public Safety Dispatcher – *POST Certified*
Fresno, CA
Download Flyer

March 19, 2020 - Thursday
Terrorism Liaison Officer (TLO) Basic *UPDATED COURSE* - *POST & STC Certified – Free Class*
San Bernardino, CA
Apply for Training
Download Flyer

March 20, 2020 - Friday
Tactical Emergency Casualty Care for Law Enforcement & First Responders Course – *POST & NAEMT Certified*
Commerce, CA
Download Flyer

March 20, 2020 - Friday
Call Record Analysis Level I – *Free Class*

Commerce, CA
Download Flyer

March 23, 2020 - Monday
Investigative Genetic Genealogy
Tempe, AZ
Download Flyer

March 23-25, 2020; Monday - Wednesday
Unmanned Aircraft Systems - Basic Operator's Course – *POST Certified*
Chula Vista, CA
Download Flyer

March 24, 2020 - Tuesday
San Bernardino Terrorist Attack: Everything on What Happened to Lessons Learned
Ontario, CA
Download Flyer

March 24, 2020 - Tuesday
Assault Weapon Identification & New and Upcoming CA Gun Laws - AM Session – *Free Class – Good for Officers, Detectives, Evidence, Probation & Parole Officers*
Santa Barbara, CA
Click to Register
Download Flyer

March 24, 2020 - Tuesday
Assault Weapon Identification & New and Upcoming CA Gun Laws - PM Session - *Free Class – Good for Officers, Detectives, Evidence, Probation & Parole Officers*
Santa Barbara, CA
Click to Register
Download Flyer

March 26-27, 2020; Thursday - Friday
Leadership and Accountability: Leading with Influence – *POST & STC Certified*
Corona, CA
Download Flyer

March 27, 2020 - Friday
Covert Methods of Entry - Operators Course
Whittier, CA
Download Flyer

March 30-April 03, 2020; Monday - Friday
Basic Crisis (Hostage) Negotiations – *POST Certified*
Irvine, Ca
Download Flyer

March 31-January 22, 2020; Tuesday - Wednesday
The Illicit Underground – *Free Class*
Los Angeles, Ca
Download Flyer

April 01-03, 2020; Wednesday - Friday
Effective Strategies to Investigate and Prosecute Labor Trafficking in the United States – *Free Class*
Solvang, CA
Download Flyer

April 02, 2020 - Thursday
Cultural Competency for Today's Law Enforcement Professional – *STC Certified*
Seal Beach, Ca
Download Flyer

April 02, 2020 - Thursday

"Close Quarters" Combat Handgun for Law Enforcement
Corona, CA
Download Flyer

April 02-03, 2020; Thursday - Friday
Two-Day Fundamentals of Facilitation
Seal Beach, Ca
Download Flyer

April 06-07, 2020; Monday - Tuesday
Leadership and Accountability: Leading with Influence – *POST & STC Certified*
Fresno, CA
Download Flyer

April 07, 2020 - Tuesday
Counter Ambush Handgun Tactics for Law Enforcement/Military
Camarillo, CA
Download Flyer

April 09-10, 2020; Thursday - Friday
Law Enforcement Pistol Mounted Optics (RDS) Transition Course – *POST Certified*
Chino, CA

Download Flyer

April 13, 2020 - Monday
Tactical Combat Casualty Care
Commerce, CA
Download Flyer

April 13-16, 2020; Monday - Thursday
K9 Team/Bomb Squad Integration Course
Pasadena, CA

Download Flyer

April 13, 2020 - Monday
Funding Terrorism and Domestic Sex Trafficking – *POST & STC Certified – Free Class*
Corona, CA
Apply for Training
Download Flyer

April 14, 2020 - Tuesday
Electronic Surveillance (Wiretap) – *POST Certified – Free for Local POST Agencies*
Commerce, CA
Download Flyer

April 16, 2020 - Thursday
Introduction to Communication Technology for Law Enforcement – *Free Class*
Commerce, CA
Download Flyer

April 20-22, 2020; Monday - Wednesday
Force Encounters Analysis: Understanding Human Performance in Critical Incidents – *POST & STC Certified*
Commerce, CA
Download Flyer

April 20-24, 2020; Monday - Friday
sUnmanned Aircraft Systems - Program Operator's Course – *POST Certified*
Costa Mesa, CA
Download Flyer

April 20-May 01, 2020; Monday - Friday

Crime Scene Investigation – *POST Certified*
Long Beach, CA
Download Flyer

April 21, 2020 - Tuesday
Murder by EME - The Carmen Rodriguez Homicide Study
Fontana, CA
Download Flyer

April 22, 2020 - Wednesday
Behavioral Threat Assessment - Preventing the Active Shooter – *POST & STC Certified – Free Class*
Lancaster, CA
Apply for Training
Download Flyer

April 23-24, 2020; Thursday - Friday
2-Day TCCC Live-Fire
Newark, CA
Download Flyer

April 27-29, 2020; Monday - Wednesday
UAS Crime & Accident Scene – *POST Certified*
Costa Mesa, CA
Download Flyer

April 29, 2020 - Wednesday
Privacy in the Age of the Internet – *POST & STC Certified*
San Diego, CA
Download Flyer

April 29, 2020 - Wednesday
"Narco" Life – *STC Certified*
Modesto, CA
Download Flyer

May 04-06, 2020; Monday - Wednesday
Assertive Supervision: Practical Approaches to Performance Management – *POST & STC Certified*
Morgan Hill, CA
Download Flyer

May 08, 2020 - Friday
Response to the Non-Criminal Barricade: Disengagement & Special Relationships – *POST Certified*
Chino Hills, CA
Download Flyer

May 11, 2020 - Monday
UAS Manager's Course
Mountain View, CA
Download Flyer

May 12-15, 2020; Tuesday - Friday
Tactical Rifle Instructor Course – *POST Certified*
Chino, CA
Download Flyer

May 13, 2020 - Wednesday
License Plate Recognition Technology and Best Practices – *POST Certified – Free Class*
Commerce, CA, CA
Download Flyer

May 14, 2020 - Thursday
Facial Recognition Technology and Best Practices – *POST Certified – Free Class*
Commerce, CA, CA
Download Flyer

May 14-15, 2020; Thursday - Friday
ILGIA 12th Annual Gang Symposium
Ontario, CA
Download Flyer

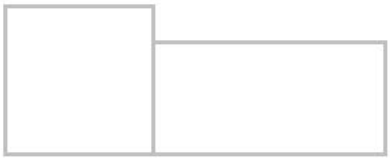
May 18-22, 2020; Monday - Friday
5-Day "Undercover Techniques and Survival" – *Free Class*
Commerce, CA
Click to Register
Download Flyer

May 27, 2020 - Wednesday
Open Source & Social Media Analysis – *Free Class*
Commerce, CA
Download Flyer

May 28, 2020 - Thursday
Open Source & Social Media Analysis – *Free Class*
Commerce, CA
Download Flyer

June 01-03, 2020; Monday - Wednesday
Cellular Technology and Records Analysis
Corona, CA
Download Flyer

June 04, 2020 - Thursday
Alcohol Beverage Control: Enforcement/Stings/Inspections
Ontario, CA
Download Flyer



www.lahidtatraining.org for Training Calendar

info@lahidtatraining.org for info/questions

Kenneth.Cordray@LACLEAR.ca.gov for Trainers and schedule new classes

https://instruq.co for "On-Line Training"

To remove yourself from this mailing list, Click here

From: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: Suspect charged after 2 cops shot at protest; Cop killer granted parole
Date: Thursday, September 24, 2020 6:31:32 PM

September 24, 2020 | View as webpage

TOP STORIES

Suspect who shot Louisville cops at protest charged with assault, wanton endangerment

Larynzo Johnson allegedly fired "multiple bullets" at Louisville police officers amid protests for Breonna Taylor

LEO rescues 14-year-old from Ill. house fire

Protests erupt across America after Breonna Taylor decision

Man convicted in 1971 NYPD cops' slayings granted parole, widow 'heartbroken'

Wash. city opens new police precinct, commits to community-centered policing

St. Louis police chief hopes ending residency rule will net more officers

The ELSAG® VPH900 Low-Cost ALPR System

Build a license plate reader network or expand the one you have with the ELSAG VPH900, the most cost-efficient way to combat vehicle-related crimes. This fixed plate reader system uses select IP cameras to aid real-time policing and investigations.

Find out more

FEATURED CONTENT

The Breonna Taylor grand jury findings: Separating fact from fiction and rhetoric from the rule of law

By Lance J. LoRusso

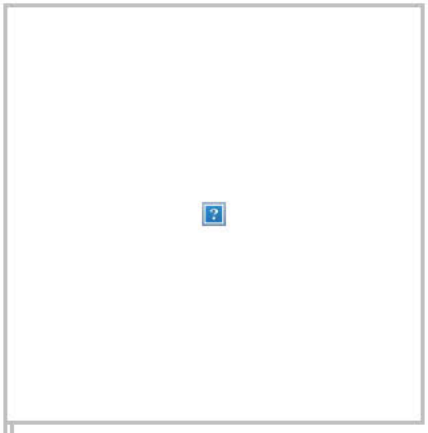
Paramount in the grand jury's findings was that although the warrant contained a 'no-knock' provision, it was not served in that manner



How will the Breonna Taylor case impact law enforcement operations?

By Policing Matters Podcast

'No knock' warrants and department policies regarding drug investigations are under the national spotlight



Connect 2020: Lexipol's Virtual User Conference



Featured speakers include Lexipol co-founders Gordon Graham and Bruce Praet, Chief Ken Wallentine and attorney Laura Scarry. Join us to discuss use of force policy, how to create a high-performing agency and more!

Register for free

OTHER HIGHLIGHTS



Enhancing hands-on training with online learning

By Chief Joel F. Shults, Ed.D.

Online learning can meet many of the demands of the human brain to engage with the material, retain information and ultimately perform better in the real world



How cops can train at home while social distancing

By Ron LaPedis

These new products will not only improve your own skills, but may also get your family off the sofa



IADLEST releases digital report on science-based learning in law enforcement

By Police1 Staff

The report is an informed response to the law enforcement training challenges faced in 2020

SPONSORED CONTENT



4 ways LEOs can protect their personal data

Digital privacy is more important than ever before. Here are four tips to help you take your privacy back online.

FEATURED JOB



Recruit Police Officer/Lateral Police Officer Job

Top Pay: $105,248 annual

FEATURED DEAL



Last Chance to Win a FREE Narcotics Analyzer!

New Rigaku EXCEL Program Contributes FIVE Raman Analyzers!

Apply Now!



Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click **here to unsubscribe.** Visit our **Customer Support** page to report any email problems or **subscribe to our other newsletters.** Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: FBI National Academy Associates, Inc.
To: McCarthy, Steven (POL)
Subject: TRAINING WEBINAR THIS WEEK: Advanced Call Data Record (CDR) Cleansing & Analysis
Date: Monday, June 22, 2020 4:56:35 PM

Discover How to Optimize Call Data Records (CDR) Cleansing and Analysis Which Typically Results in Solving Cases Faster and Saving Analysts 97% of Time Spent on a Case.

Chorus is the leading provider of data cleansing and analysis software in the UK and is used by 80% of regional police forces, all Counter Terror Units and the Home Office. Chorus is now making its software available for North American law enforcement.

Chorus is exceptional at:

- **Rules-based data cleansing.** Taking communications data from providers such as T-Mobile, AT&T, Sprint and Verizon in the USA as well as Bell, Telus and Rogers Communications in Canada, removing the noise and normalizing it ready for analysis.
- **Connecting data.** Combining disparate data such as CDR, ALPR, RF surveys and device downloads and overlaying it with communications data to spot crucial connections using maps and charts.
- **Evidence quality reporting.** Maintaining data integrity so reports and maps can be used in court as evidence.
- **Integration with IBM® i2 products.**

Thursday, June 25, 2020
11:00 am ET | 8:00 am PT

Richard is a law enforcement veteran of 19 years. He will be presenting insights from his work as a Fingerprint Expert, Crime Scene Manager, and Forensics Manager for some of the busiest agencies in the world. Richard is an expert at cleansing, combining and connecting data to create evidence supported reports to close cases at record rates. He has been helping law enforcement solve their biggest challenges with criminal data for over 5 years.

Why Learn From Chorus Intelligence?

Chorus has been used in some of the highest profile operations in the UK, such as the Manchester bombing and the London Bridge attacks, answering key investigation questions and ultimately bringing offenders to justice. Learn from these leading-edge methods from former law enforcement.

Register for this fun and informative session to take your investigations to the next level and close cases faster.

Cannot make it on Thursday, June 25th at 11am EST?
Sign up and we will email an on-demand replay link when available.

Learn More

This Training Webinar was brought to you through collaboration between two leading organizations dedicated to Law Enforcement and the Communities they serve.

FBI National Academy Associates, Inc., FBI Academy, Quantico, VA 22135

SafeUnsubscribe™ steven.mccarthy@pol.state.ma.us

Forward email | Update Profile | About our service provider

Sent by do-not-reply@fbinaa.org in collaboration with

Constant Contact

Try email marketing for free today!

From: FBI National Academy Associates, Inc.
To: McCarthy, Steven (POL)
Subject: TRAINING WEBINAR: Advanced Call Data Record (CDR) Cleansing & Analysis
Date: Thursday, June 18, 2020 1:47:54 PM

Discover How to Optimize Call Data Records (CDR) Cleansing and Analysis Which Typically Results in Solving Cases Faster and Saving Analysts 97% of Time Spent on a Case.

Chorus is the leading provider of data cleansing and analysis software in the UK and is used by 80% of regional police forces, all Counter Terror Units and the Home Office. Chorus is now making its software available for North American law enforcement.

Chorus is exceptional at:

- **Rules-based data cleansing.** Taking communications data from providers such as T-Mobile, AT&T, Sprint and Verizon in the USA as well as Bell, Telus and Rogers Communications in Canada, removing the noise and normalizing it ready for analysis.
- **Connecting data.** Combining disparate data such as CDR, ALPR, RF surveys and device downloads and overlaying it with communications data to spot crucial connections using maps and charts.
- **Evidence quality reporting.** Maintaining data integrity so reports and maps can be used in court as evidence.
- **Integration with IBM® i2 products.**

Thursday, June 25, 2020
11:00 am ET | 8:00 am PT



Richard is a law enforcement veteran of 19 years. He will be presenting insights from his work as a Fingerprint Expert, Crime Scene Manager, and Forensics Manager for some of the busiest agencies in the world. Richard is an expert at cleansing, combining and connecting data to create evidence supported reports to close cases at record rates. He has been helping law enforcement solve their biggest challenges with criminal data for over 5 years.



Why Learn From Chorus Intelligence?

Chorus has been used in some of the highest profile operations in the UK, such as the Manchester bombing and the London Bridge attacks, answering key investigation questions and ultimately bringing offenders to justice. Learn from these leading-edge methods from former law enforcement.

Register for this fun and informative session to take your investigations to the next level and close cases faster.

Cannot make it on Thursday, June 25th at 11am EST?
Sign up and we will email an on-demand replay link when available.

Learn More

This Training Webinar was brought to you through collaboration between two leading organizations dedicated to Law Enforcement and the Communities they serve.

FBI National Academy Associates, Inc., FBI Academy, Quantico, VA 22135

SafeUnsubscribe™ steven.mccarthy@pol.state.ma.us

Forward email | Update Profile | About our service provider

Sent by do-not-reply@fbinaa.org in collaboration with

Constant Contact

Try email marketing for free today!

From: FBI National Academy Associates, Inc.
To: McCarthy, Steven (POL)
Subject: TRAINING WEBINAR: Advanced Call Data Record (CDR) Cleansing & Analysis
Date: Tuesday, June 16, 2020 9:09:51 AM

Discover How to Optimize Call Data Records (CDR) Cleansing and Analysis Which Typically Results in Solving Cases Faster and Saving Analysts 97% of Time Spent on a Case.

Chorus is the leading provider of data cleansing and analysis software in the UK and is used by 80% of regional police forces, all Counter Terror Units and the Home Office. Chorus is now making its software available for North American law enforcement.

Chorus is exceptional at:

- **Rules-based data cleansing.** Taking communications data from providers such as T-Mobile, AT&T, Sprint and Verizon in the USA as well as Bell, Telus and Rogers Communications in Canada, removing the noise and normalizing it ready for analysis.
- **Connecting data.** Combining disparate data such as CDR, ALPR, RF surveys and device downloads and overlaying it with communications data to spot crucial connections using maps and charts.
- **Evidence quality reporting.** Maintaining data integrity so reports and maps can be used in court as evidence.
- **Integration with IBM® i2 products.**

Thursday, June 25, 2020
11:00 am ET | 8:00 am PT



Richard is a law enforcement veteran of 19 years. He will be presenting insights from his work as a Fingerprint Expert, Crime Scene Manager, and Forensics Manager for some of the busiest agencies in the world. Richard is an expert at cleansing, combining and connecting data to create evidence supported reports to close cases at record rates. He has been helping law enforcement solve their biggest challenges with criminal data for over 5 years.



Why Learn From Chorus Intelligence?

Chorus has been used in some of the highest profile operations in the UK, such as the Manchester bombing and the London Bridge attacks, answering key investigation questions and ultimately bringing offenders to justice. Learn from these leading-edge methods from former law enforcement.

Register for this fun and informative session to take your investigations to the next level and close cases faster.

Cannot make it on Thursday, June 25th at 11am EST?
Sign up and we will email an on-demand replay link when available.

Learn More

This Training Webinar was brought to you through collaboration between two leading organizations dedicated to Law Enforcement and the Communities they serve.

FBI National Academy Associates, Inc., FBI Academy, Quantico, VA 22135

SafeUnsubscribe™ steven.mccarthy@pol.state.ma.us

Forward email | Update Profile | About our service provider

Sent by do-not-reply@fbinaa.org in collaboration with

Constant Contact

Try email marketing for free today!

From: FBI National Academy Associates, Inc.
To: McCarthy, Steven (POL)
Subject: TRAINING WEBINAR: Advanced Call Data Record (CDR) Cleansing & Analysis
Date: Friday, June 12, 2020 9:28:00 AM

Discover How to Optimize Call Data Records (CDR) Cleansing and Analysis Which Typically Results in Solving Cases Faster and Saving Analysts 97% of Time Spent on a Case.

Chorus is the leading provider of data cleansing and analysis software in the UK and is used by 80% of regional police forces, all Counter Terror Units and the Home Office. Chorus is now making its software available for North American law enforcement.

Chorus is exceptional at:

- **Rules-based data cleansing.** Taking communications data from providers such as T-Mobile, AT&T, Sprint and Verizon in the USA as well as Bell, Telus and Rogers Communications in Canada, removing the noise and normalizing it ready for analysis.
- **Connecting data.** Combining disparate data such as CDR, ALPR, RF surveys and device downloads and overlaying it with communications data to spot crucial connections using maps and charts.
- **Evidence quality reporting.** Maintaining data integrity so reports and maps can be used in court as evidence.
- **Integration with IBM® i2 products.**

Thursday, June 25, 2020
11:00 am ET | 8:00 am PT

Richard is a law enforcement veteran of 19 years. He will be presenting insights from his work as a Fingerprint Expert, Crime Scene Manager, and Forensics Manager for some of the busiest agencies in the world. Richard is an expert at cleansing, combining and connecting data to create evidence supported reports to close cases at record rates. He has been helping law enforcement solve their biggest challenges with criminal data for over 5 years.

Why Learn From Chorus Intelligence?

Chorus has been used in some of the highest profile operations in the UK, such as the Manchester bombing and the London Bridge attacks, answering key investigation questions and ultimately bringing offenders to justice. Learn from these leading-edge methods from former law enforcement.

Register for this fun and informative session to take your investigations to the next level and close cases faster.

Cannot make it on Thursday, June 25th at 11am EST?
Sign up and we will email an on-demand replay link when available.

Learn More

This Training Webinar was brought to you through collaboration between two leading organizations dedicated to Law Enforcement and the Communities they serve.

FBI National Academy Associates, Inc., FBI Academy, Quantico, VA 22135

SafeUnsubscribe™ steven.mccarthy@pol.state.ma.us

Forward email | Update Profile | About our service provider

Sent by do-not-reply@fbinaa.org in collaboration with

Constant Contact

Try email marketing for free today!

From: FBI National Academy Associates, Inc.
To: McCarthy, Steven (POL)
Subject: TRAINING WEBINAR: Advanced Call Data Record (CDR) Cleansing & Analysis
Date: Wednesday, June 24, 2020 8:07:42 AM

Discover How to Optimize Call Data Records (CDR) Cleansing and Analysis Which Typically Results in Solving Cases Faster and Saving Analysts 97% of Time Spent on a Case.

Chorus is the leading provider of data cleansing and analysis software in the UK and is used by 80% of regional police forces, all Counter Terror Units and the Home Office. Chorus is now making its software available for North American law enforcement.

Chorus is exceptional at:

- **Rules-based data cleansing.** Taking communications data from providers such as T-Mobile, AT&T, Sprint and Verizon in the USA as well as Bell, Telus and Rogers Communications in Canada, removing the noise and normalizing it ready for analysis.
- **Connecting data.** Combining disparate data such as CDR, ALPR, RF surveys and device downloads and overlaying it with communications data to spot crucial connections using maps and charts.
- **Evidence quality reporting.** Maintaining data integrity so reports and maps can be used in court as evidence.
- **Integration with IBM® i2 products.**

Thursday, June 25, 2020
11:00 am ET | 8:00 am PT



Richard is a law enforcement veteran of 19 years. He will be presenting insights from his work as a Fingerprint Expert, Crime Scene Manager, and Forensics Manager for some of the busiest agencies in the world. Richard is an expert at cleansing, combining and connecting data to create evidence supported reports to close cases at record rates. He has been helping law enforcement solve their biggest challenges with criminal data for over 5 years.



Why Learn From Chorus Intelligence?

Chorus has been used in some of the highest profile operations in the UK, such as the Manchester bombing and the London Bridge attacks, answering key investigation questions and ultimately bringing offenders to justice. Learn from these leading-edge methods from former law enforcement.

Register for this fun and informative session to take your investigations to the next level and close cases faster.

Cannot make it on Thursday, June 25th at 11am EST?
Sign up and we will email an on-demand replay link when available.

Learn More

This Training Webinar was brought to you through collaboration between two leading organizations dedicated to Law Enforcement and the Communities they serve.

FBI National Academy Associates, Inc., FBI Academy, Quantico, VA 22135

SafeUnsubscribe™ steven.mccarthy@pol.state.ma.us

Forward email | Update Profile | About our service provider

Sent by do-not-reply@fbinaa.org in collaboration with

Constant Contact

Try email marketing for free today!

From: Traffic Technology Today
To: Griffin, Daniel (POL)
Subject: UK road building set to continue in Covid-19 pandemic
Date: Thursday, March 26, 2020 8:03:17 AM

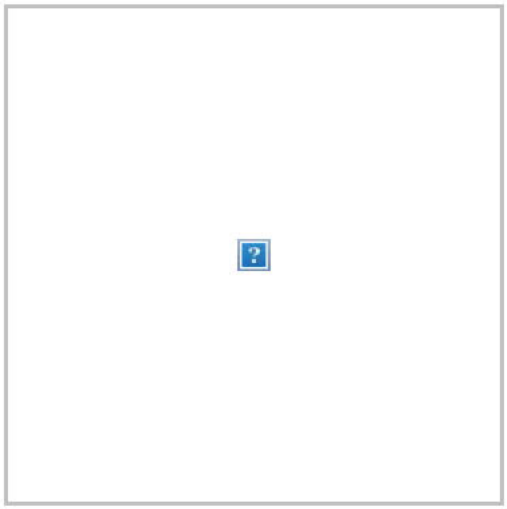
CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

View this email online

TOP NEWS THIS WEEK

Highways England aims to continue construction activity during Covid-19 pandemic

Highways England is doing all it can

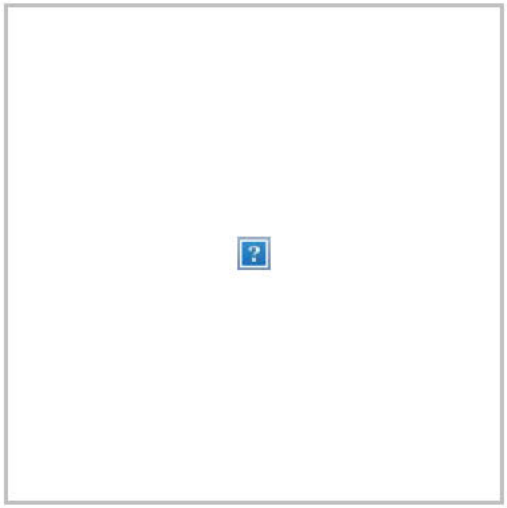


to ensure operations continue as usual in an effort to help traffic technology suppliers weather the Covid-19 storm more...

MORE COVID-19 NEWS...

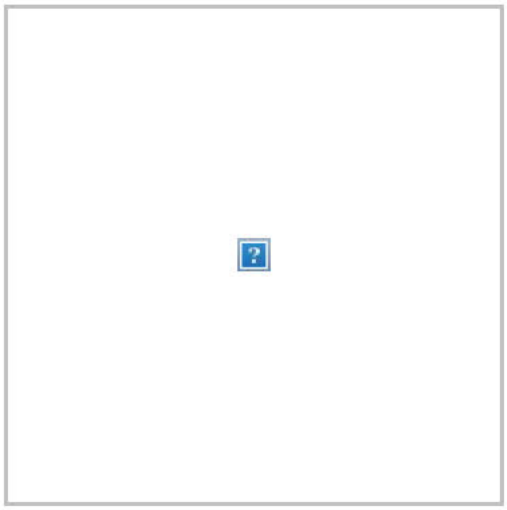
- **DfT urgently seeking transport data to tackle Covid-19**
- **London road user charging schemes suspended to fight Covid-19**
- **LADOT relaxes parking restrictions in wake of Covid-19**
- **AI sensors reveal early Covid-19 advice produced only small traffic reductions**
- **Ride-sharing firm to support essential Covid-19 response healthcare workers**

NEW VIDEO What you need to know about C-V2X



Nokia's head of disruptive innovation and vice chair of the 5G Automotive Association, Thierry Klein, answers the important questions regarding Cellular-Vehicle-to-Everything technology **more...**

NEW TECHNOLOGY The basics of coordinating traffic signals



Applied informatics firm, Iteris, explain the benefits and challenges of coordinating traffic signals as well as how consolidated metrics can help improve coordination more...

MORE NEWS

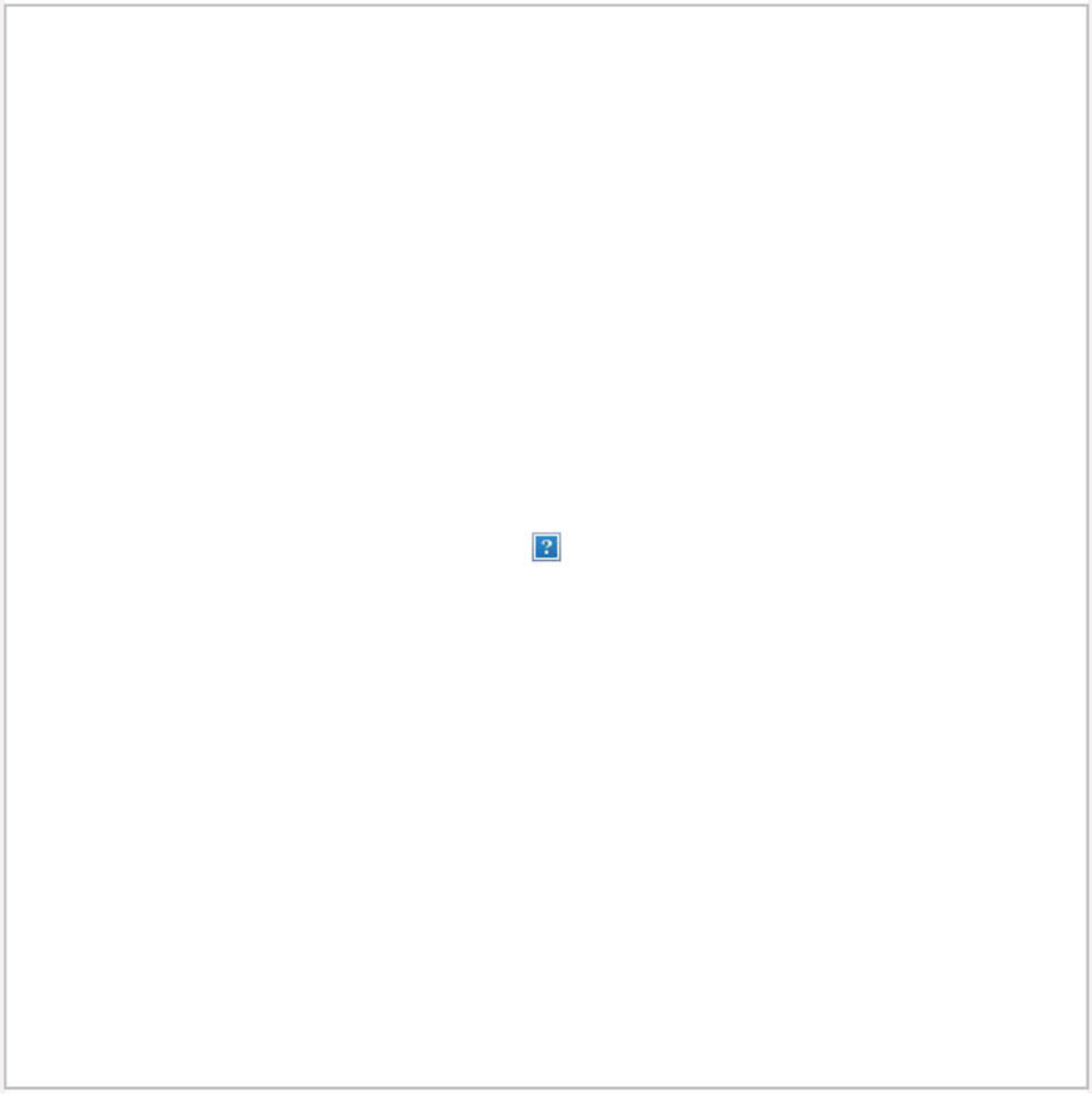
- ‘Supercab’ to patrol M25 to cut driver smartphone use
- Edge-based ALPR system offers greater awareness and analytics
- Bluetooth ‘tags’ trialled to warn drivers about highway workzones
- Nokia delivers smart landslide alert system for Chinese highway operator
- Greek islands enhance public transport with solar-powered travel information
- London residential parking strategy needs an overhaul, says think tank

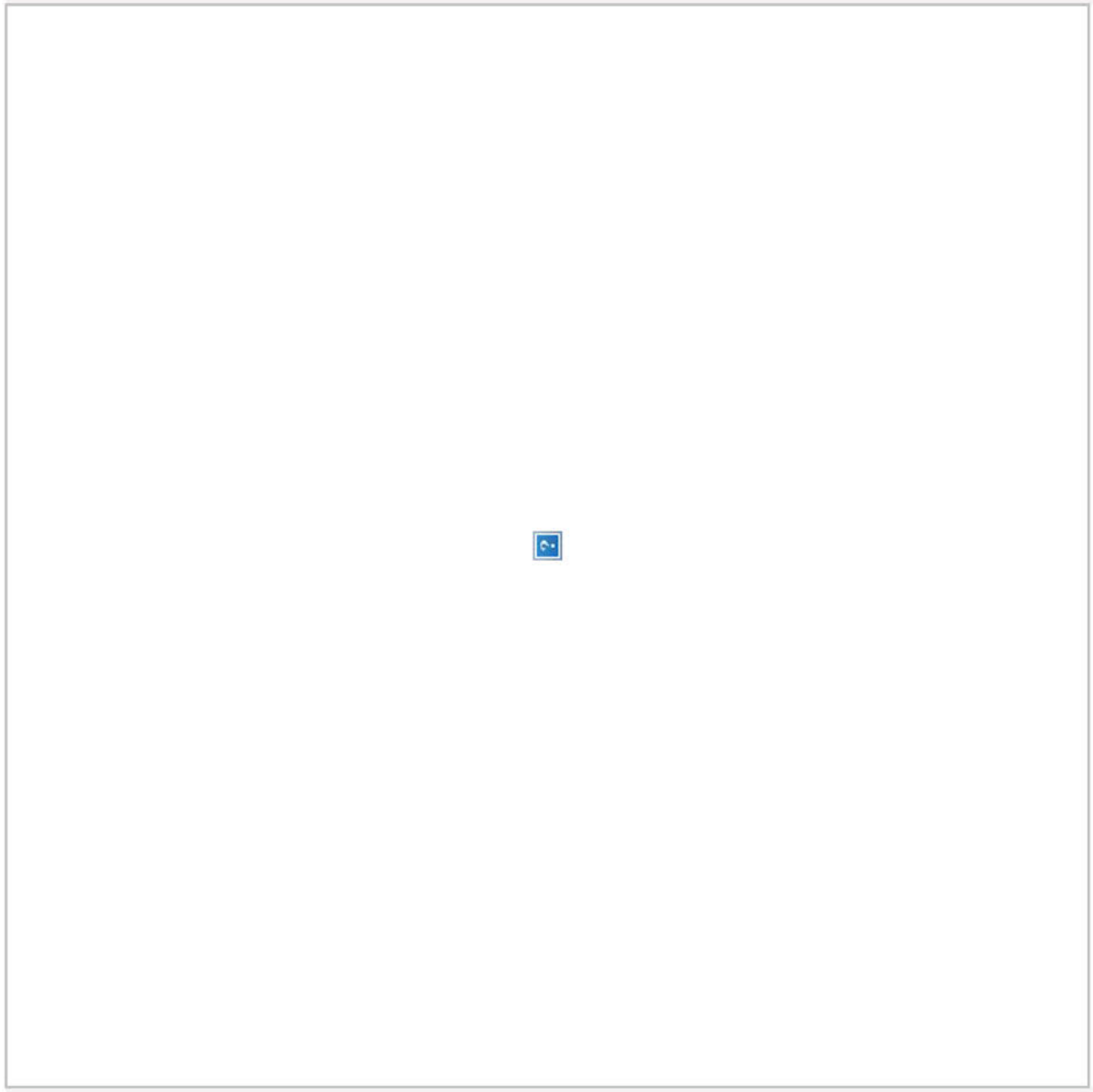


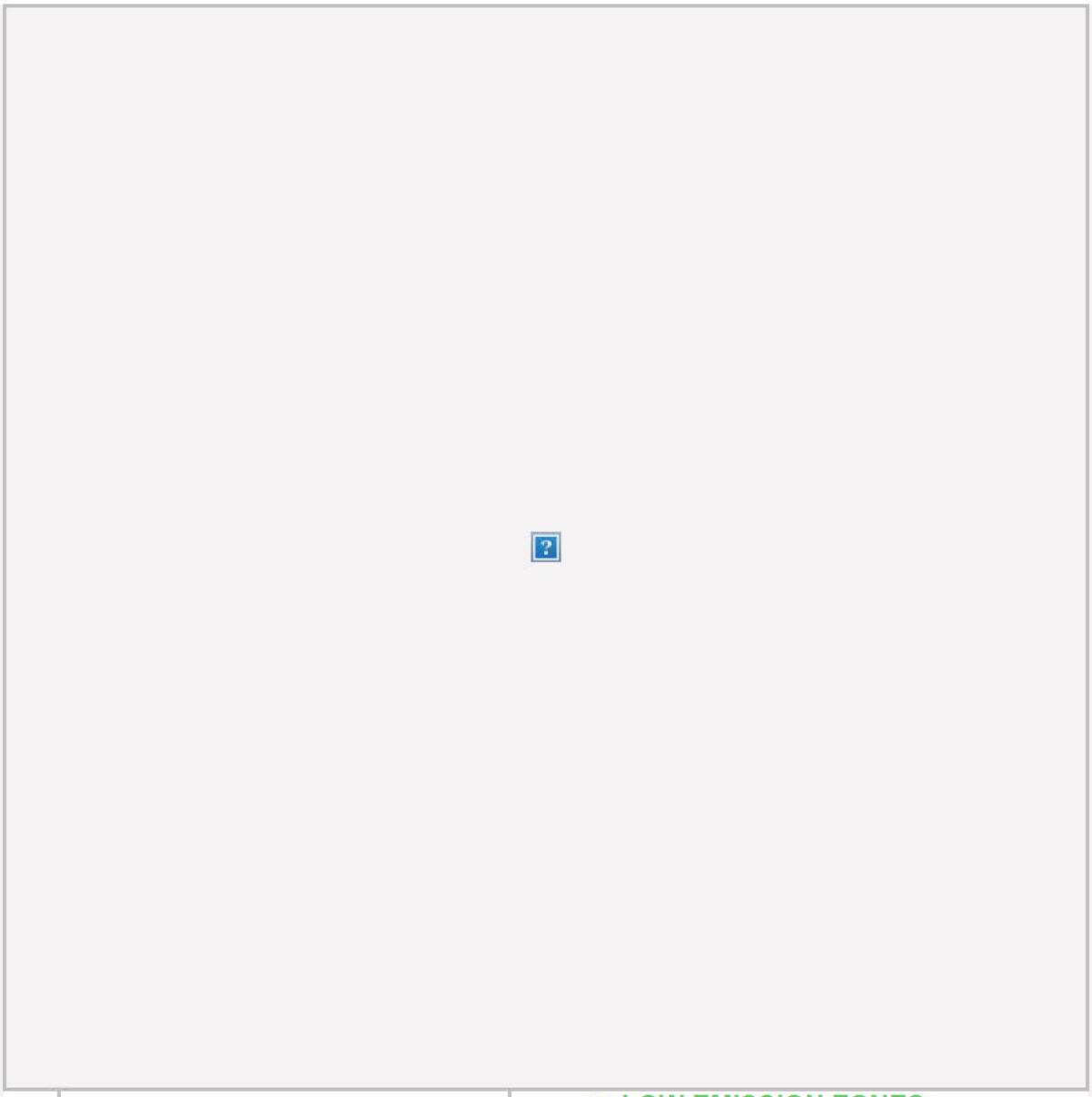
NEW FEATURE Reducing distraction with vehicle activated signs

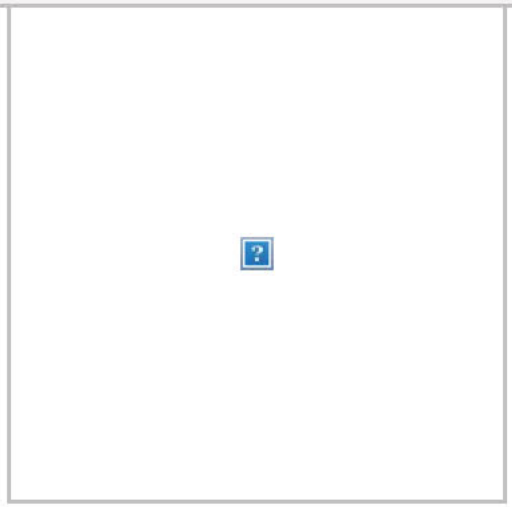


The dangers of distraction are a real concern for any driver, irrespective of their experience on the road. Find out how signage can address the issue **more...**





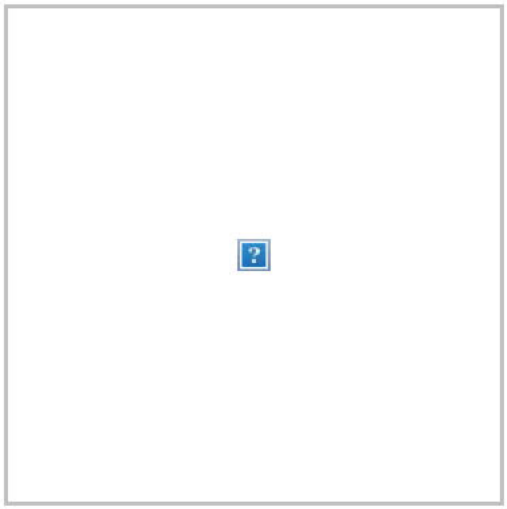




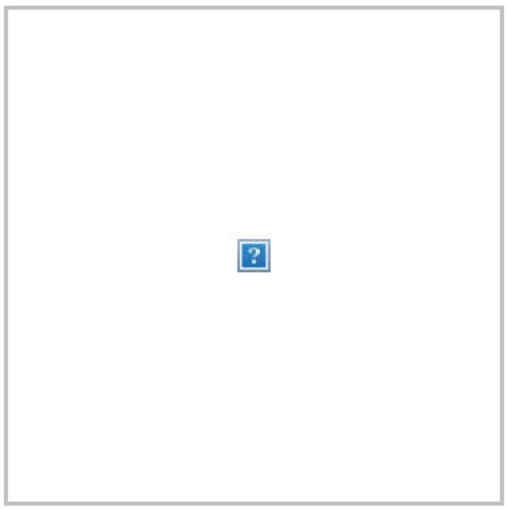
<< LOW EMISSION ZONES
JUST BE CAZ

How the city of Birmingham's emissions-based private-car restrictions (the first in the UK outside London) will be enforced

<< WORKZONES
SMART WORKZONES AHEAD



Workzones are notoriously dangerous for those driving or working in them, but research into connected and automated technologies is helping to rectify this situation



<< COVID-19

GREG WINFREE

The Mode Warrior begins the debate on ways transportation in our interconnected world should change in order to better protect public health, in light of the coronavirus pandemic

CLICK HERE TO RECEIVE YOUR FREE COPY

If you wish to unsubscribe from Traffic Technology International News emails, please click here.

To understand how we process, use & safeguard your data, please read our Privacy Policy. If you would like to update your marketing contact preferences, then please click here.

From: Traffic Technology Today
To: zzDowd, Timothy (POL)
Subject: UK road building set to continue in Covid-19 pandemic
Date: Thursday, March 26, 2020 8:06:03 AM

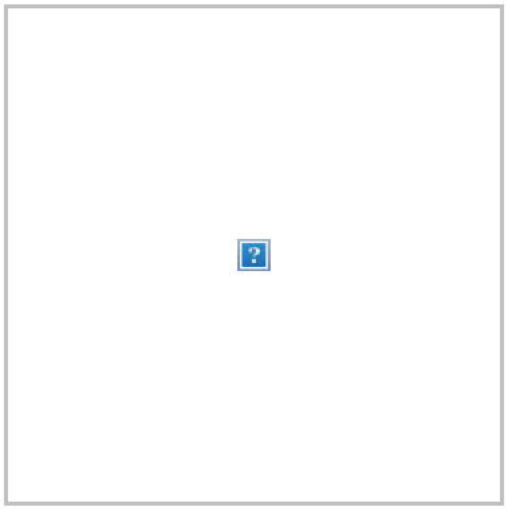
CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

View this email online

TOP NEWS THIS WEEK

Highways England aims to continue construction activity during Covid-19 pandemic

Highways England is doing all it can

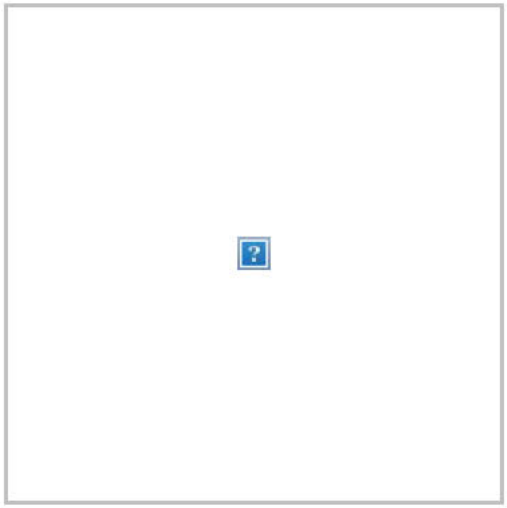


to ensure operations continue as usual in an effort to help traffic technology suppliers weather the Covid-19 storm more...

MORE COVID-19 NEWS...

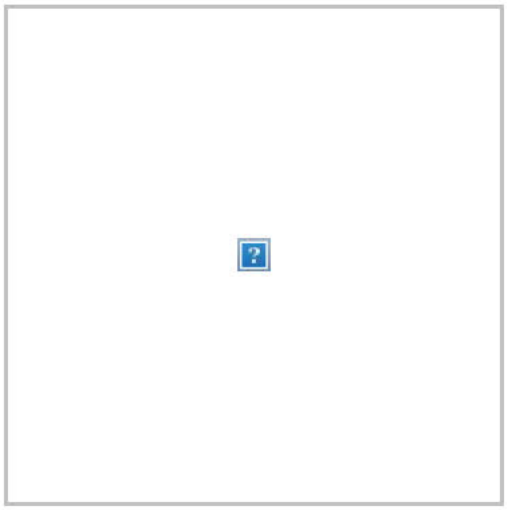
- **DfT urgently seeking transport data to tackle Covid-19**
- **London road user charging schemes suspended to fight Covid-19**
- **LADOT relaxes parking restrictions in wake of Covid-19**
- **AI sensors reveal early Covid-19 advice produced only small traffic reductions**
- **Ride-sharing firm to support essential Covid-19 response healthcare workers**

NEW VIDEO What you need to know about C-V2X



Nokia's head of disruptive innovation and vice chair of the 5G Automotive Association, Thierry Klein, answers the important questions regarding Cellular-Vehicle-to-Everything technology **more...**

NEW TECHNOLOGY The basics of coordinating traffic signals



Applied informatics firm, Iteris, explain the benefits and challenges of coordinating traffic signals as well as how consolidated metrics can help improve coordination more...

MORE NEWS

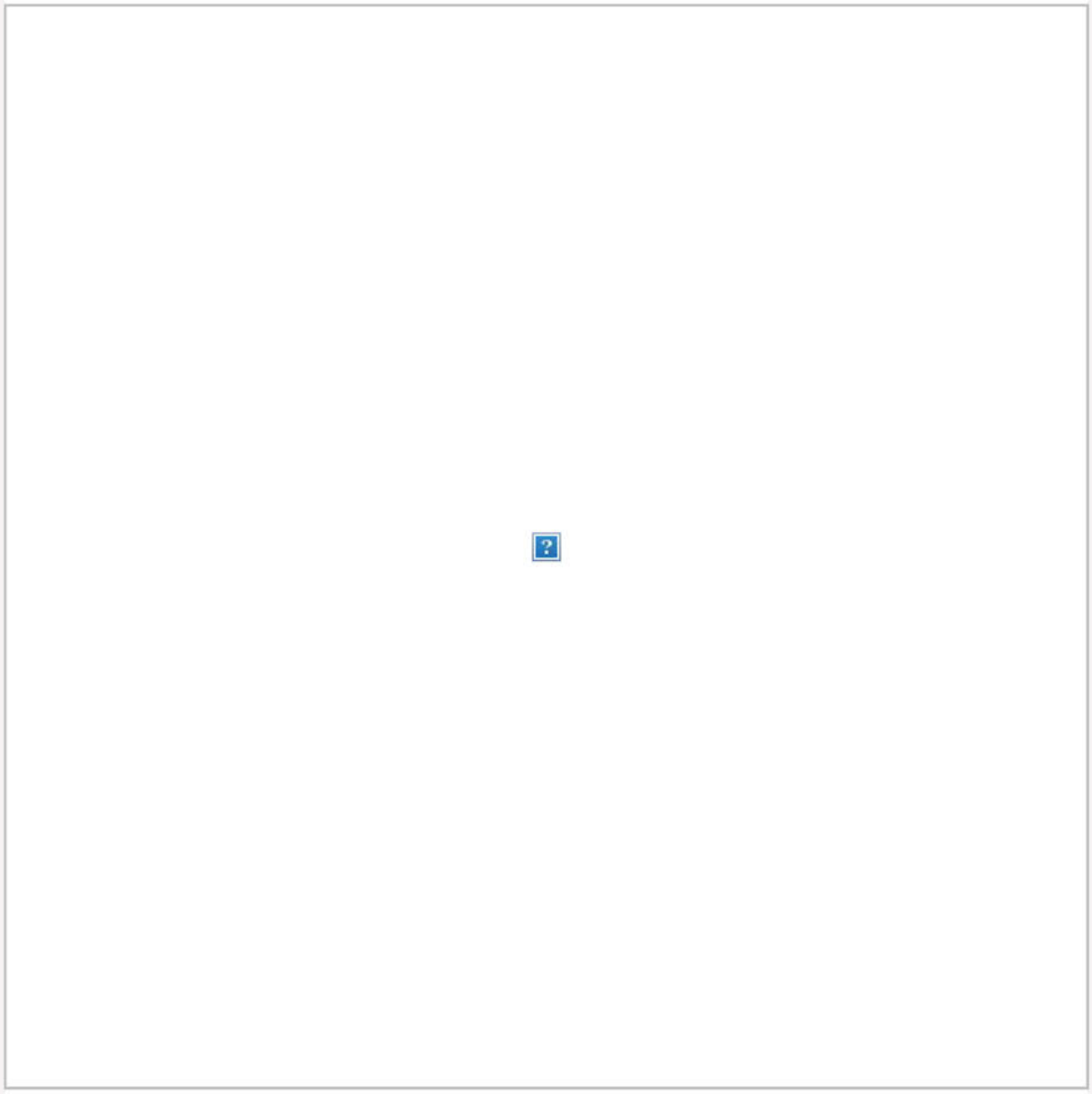
- ‘Supercab’ to patrol M25 to cut driver smartphone use
- Edge-based ALPR system offers greater awareness and analytics
- Bluetooth ‘tags’ trialled to warn drivers about highway workzones
- Nokia delivers smart landslide alert system for Chinese highway operator
- Greek islands enhance public transport with solar-powered travel information
- London residential parking strategy needs an overhaul, says think tank

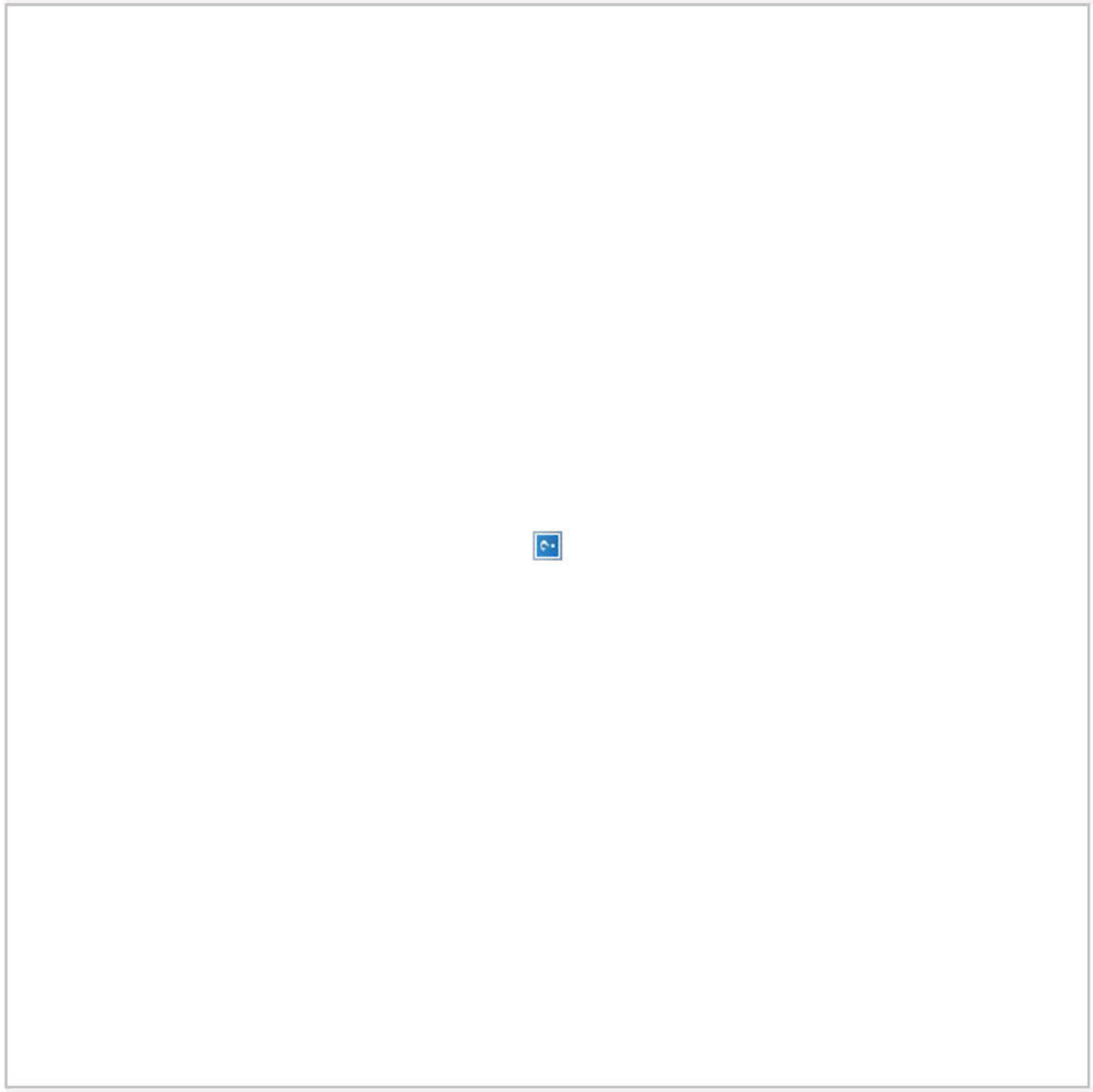


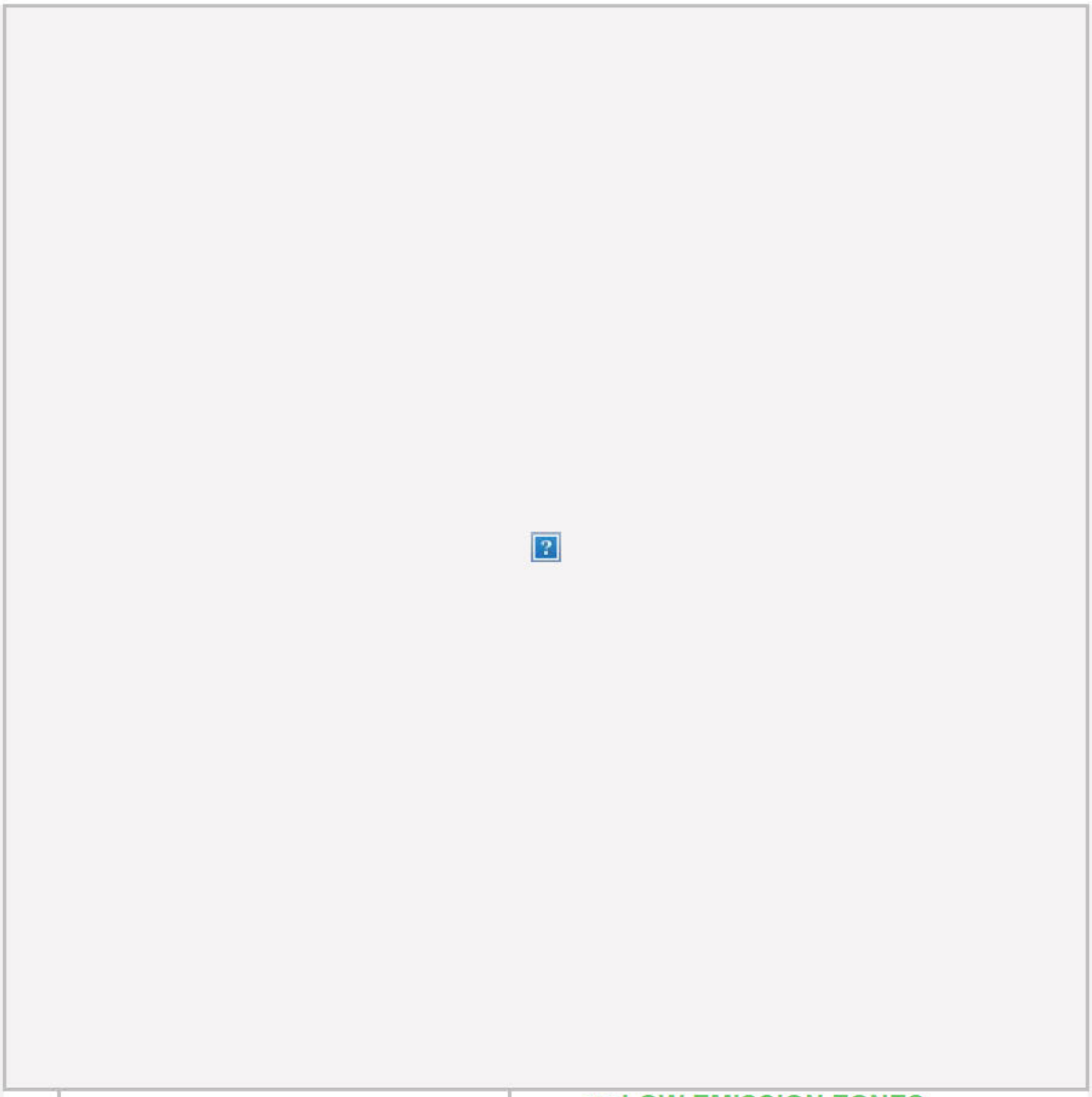
NEW FEATURE Reducing distraction with vehicle activated signs

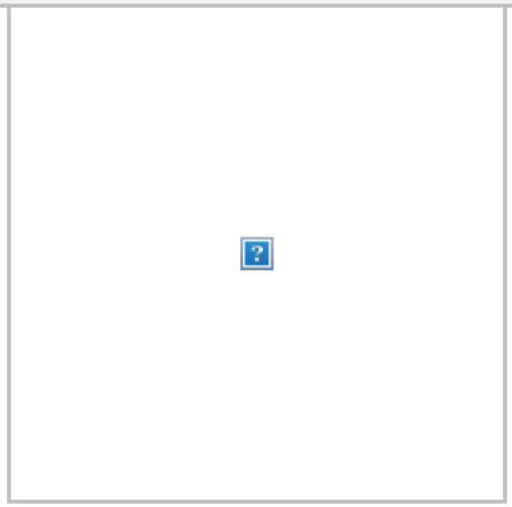


The dangers of distraction are a real concern for any driver, irrespective of their experience on the road. Find out how signage can address the issue **more...**





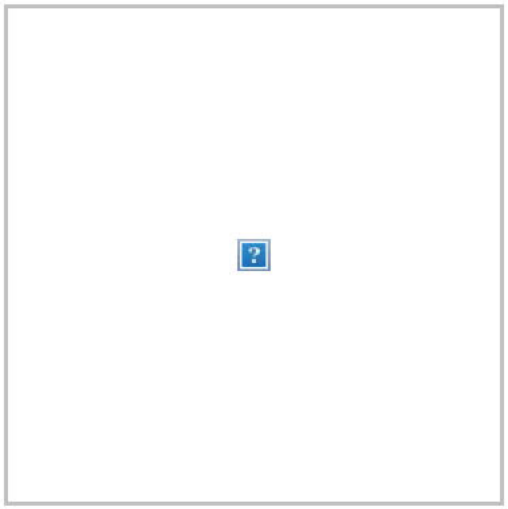




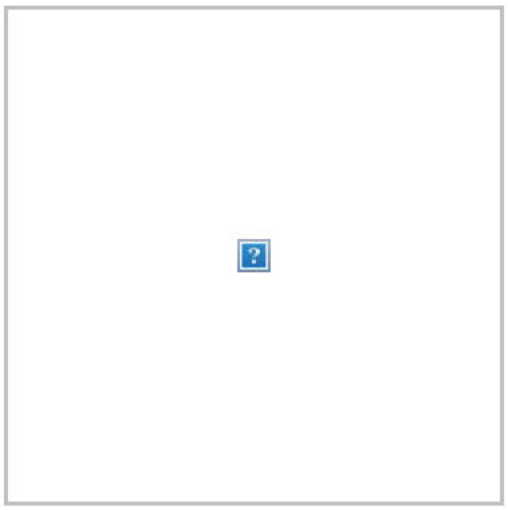
<< LOW EMISSION ZONES
JUST BE CAZ

How the city of Birmingham's emissions-based private-car restrictions (the first in the UK outside London) will be enforced

<< WORKZONES
SMART WORKZONES AHEAD



Workzones are notoriously dangerous for those driving or working in them, but research into connected and automated technologies is helping to rectify this situation



<< COVID-19

GREG WINFREE

The Mode Warrior begins the debate on ways transportation in our interconnected world should change in order to better protect public health, in light of the coronavirus pandemic

CLICK HERE TO RECEIVE YOUR FREE COPY

If you wish to unsubscribe from Traffic Technology International News emails, please click here.

To understand how we process, use & safeguard your data, please read our Privacy Policy. If you would like to update your marketing contact preferences, then please click here.

From: Mail Delivery Subsystem
To: Victorioscause@gmail.com; info@macdle.com; Patrick.O.Bomberg@massmail.state; Franklinbar@publiccounsel.net
Subject: Undeliverable: ALPR Camera Notice
Date: Wednesday, December 23, 2020 11:47:41 AM

The original message was received at Wed, 23 Dec 2020 11:46:56 -0500
from sdc-ppmailsec-002.state.ma.us [10.255.145.135]
  ----- The following addresses had permanent fatal errors -----
<Victorioscause@gmail.com>
  (reason: 550-5.1.1 The email account that you tried to reach does not exist. Please try)
<info@macdle.com>
  (reason: 550 Host unknown)
<Patrick.O.Bomberg@massmail.state>
  (reason: 550 Host unknown)
<Franklinbar@publiccounsel.net>
  (reason: 550 5.4.1 Recipient address rejected: Access denied. AS(201806281) [BL0GCC02FT009.eop-gcc02.prod.protection.outlook.com])
  ----- Transcript of session follows -----
... while talking to gmail-smtp-in.l.google.com.:
>>> DATA
<<< 550-5.1.1 The email account that you tried to reach does not exist. Please try
<<< 550-5.1.1 double-checking the recipient's email address for typos or
<<< 550-5.1.1 unnecessary spaces. Learn more at
<<< 550 5.1.1 https://support.google.com/mail/?p=NoSuchUser 10si27638857qvs.129 - gsmtp
550 5.1.1 <Victorioscause@gmail.com>... User unknown
<<< 503 5.5.1 RCPT first. 10si27638857qvs.129 - gsmtp
550 5.1.2 <info@macdle.com>... Host unknown (Name server: macdle.com: host not found)
550 5.1.2 <Patrick.O.Bomberg@massmail.state>... Host unknown (Name server: massmail.state: host not found)
... while talking to d189465a.ess.barracudanetworks.com.:
>>> DATA
<<< 451 temporary failure for one or more recipients (franklinbar@publiccounsel.net:550 5.4.1 Recipient address rejected: Access denied.
AS(201806281) [BL0GCC02FT009.eop-g...)
... while talking to d189465b.ess.barracudanetworks.com.:
>>> DATA
<<< 550 5.4.1 Recipient address rejected: Access denied. AS(201806281) [BL0GCC02FT009.eop-gcc02.prod.protection.outlook.com]
550 5.1.1 <Franklinbar@publiccounsel.net>... User unknown

From: Police1 Investigations
To: Grassia, Michael (POL)
Subject: Using open-source intel to tackle extremists; Fighting child abuse
Date: Tuesday, August 25, 2020 4:40:18 PM

August 25, 2020 | View as webpage

Dear Police1 Member,

While technology has brought great benefits to our daily lives it has also facilitated the growth of digital crime. From ransomware to human trafficking, technology is being used for nefarious purposes in an online world that knows no borders. It can be challenging for police investigators to stay informed of trends and equipped with the products and software to apprehend online criminals.

With that in mind, here are two steps to take to combat cybercrime:

- Read our digital edition to find out how AI can improve investigations
- Download our "How to Buy Investigation Software" guide to help procure the latest investigation tech

How is technology helping or hindering your investigations? Email editor@police1.com.

— *The Police1 Team*

FEATURED CONTENT

Using WEBINT and OSINT to tackle extremist groups

By Johnmichael O'Hare

Agencies that familiarize themselves with extremists' cyber haunts stand a better chance of uncovering potential problems before they materialize



How police can embrace the cloud to fight child sexual abuse

By Johann Hofmann

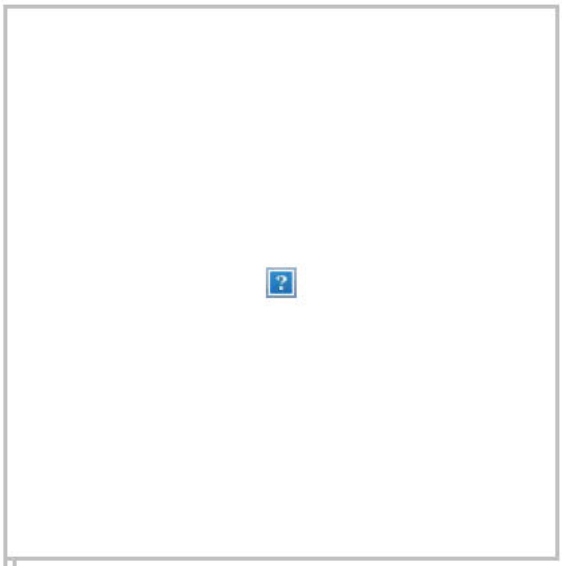
On-premise technology is increasingly inadequate for handling the scale of material associated with these cases



Guilty by association: How data linking strengthens investigations

By Joshua Lee, MLS, CFE, CCCI, CTFI, CCIE

With a few clicks of the mouse, an internet connection and the right know-how, police investigators can find crucial connections



Got Cameras? Get LPR



Your agency may be eligible for two free trial software licenses to add vehicle recognition capabilities to IP cameras in your jurisdiction.

Find out how

OTHER HIGHLIGHTS



How contactless technology

can help reduce bias, increase efficiencies and bolster safety

By Robert Berman

Real-time intelligence makes it easier for officers to be more strategic and safer in how they engage with suspects

Research review: Identifying the benefits of ALPR systems

By Tim Dees

How law enforcement agencies can use research findings to get community support and funding for ALPR systems

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Investigations
To: benesh, meghann E (POL)
Subject: Using open-source intel to tackle extremists; Fighting child abuse
Date: Tuesday, August 25, 2020 4:30:53 PM

August 25, 2020 | View as webpage

Dear Police1 Member,

While technology has brought great benefits to our daily lives it has also facilitated the growth of digital crime. From ransomware to human trafficking, technology is being used for nefarious purposes in an online world that knows no borders. It can be challenging for police investigators to stay informed of trends and equipped with the products and software to apprehend online criminals.

With that in mind, here are two steps to take to combat cybercrime:

- Read our digital edition to find out how AI can improve investigations
- Download our "How to Buy Investigation Software" guide to help procure the latest investigation tech

How is technology helping or hindering your investigations? Email editor@police1.com.

— *The Police1 Team*

FEATURED CONTENT

Using WEBINT and OSINT to tackle extremist groups

By Johnmichael O'Hare

Agencies that familiarize themselves with extremists' cyber haunts stand a better chance of uncovering potential problems before they materialize



How police can embrace the cloud to fight child sexual abuse

By Johann Hofmann

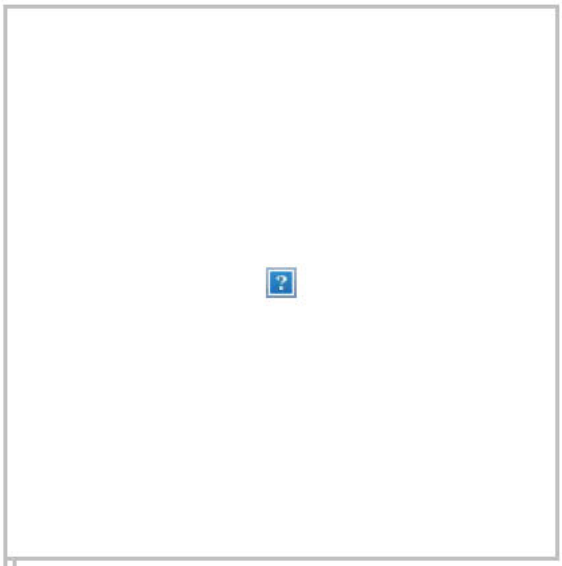
On-premise technology is increasingly inadequate for handling the scale of material associated with these cases



Guilty by association: How data linking strengthens investigations

By Joshua Lee, MLS, CFE, CCCI, CTFI, CCIE

With a few clicks of the mouse, an internet connection and the right know-how, police investigators can find crucial connections



Got Cameras? Get LPR



Your agency may be eligible for two free trial software licenses to add vehicle recognition capabilities to IP cameras in your jurisdiction.

Find out how

OTHER HIGHLIGHTS



How contactless technology

can help reduce bias, increase efficiencies and bolster safety

By Robert Berman

Real-time intelligence makes it easier for officers to be more strategic and safer in how they engage with suspects



Research review: Identifying the benefits of ALPR systems

By Tim Dees

How law enforcement agencies can use research findings to get community support and funding for ALPR systems



Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Investigations
To: zzLeVangie, Dean (POL)
Subject: Using open-source intel to tackle extremists; Fighting child abuse
Date: Tuesday, August 25, 2020 4:10:02 PM

August 25, 2020 | View as webpage

Dear Police1 Member,

While technology has brought great benefits to our daily lives it has also facilitated the growth of digital crime. From ransomware to human trafficking, technology is being used for nefarious purposes in an online world that knows no borders. It can be challenging for police investigators to stay informed of trends and equipped with the products and software to apprehend online criminals.

With that in mind, here are two steps to take to combat cybercrime:

- Read our digital edition to find out how AI can improve investigations
- Download our "How to Buy Investigation Software" guide to help procure the latest investigation tech

How is technology helping or hindering your investigations? Email editor@police1.com.

— *The Police1 Team*

FEATURED CONTENT

Using WEBINT and OSINT to tackle extremist groups

By Johnmichael O'Hare

Agencies that familiarize themselves with extremists' cyber haunts stand a better chance of uncovering potential problems before they materialize



How police can embrace the cloud to fight child sexual abuse

By Johann Hofmann

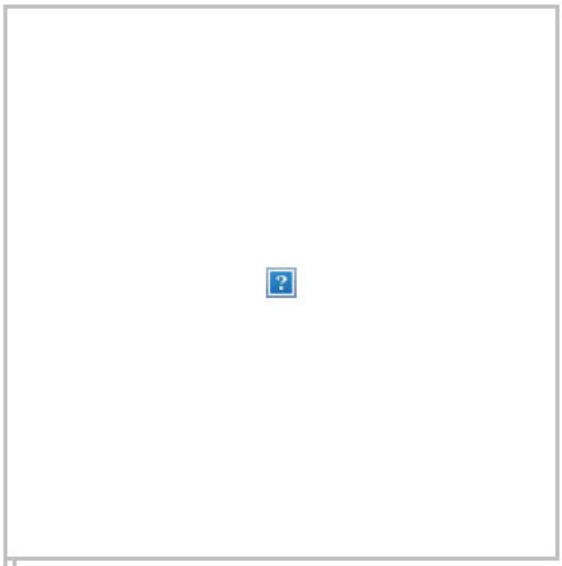
On-premise technology is increasingly inadequate for handling the scale of material associated with these cases



Guilty by association: How data linking strengthens investigations

By Joshua Lee, MLS, CFE, CCCI, CTFI, CCIE

With a few clicks of the mouse, an internet connection and the right know-how, police investigators can find crucial connections



Got Cameras? Get LPR



Your agency may be eligible for two free trial software licenses to add vehicle recognition capabilities to IP cameras in your jurisdiction.

Find out how

OTHER HIGHLIGHTS



How contactless technology

can help reduce bias, increase efficiencies and bolster safety

By Robert Berman

Real-time intelligence makes it easier for officers to be more strategic and safer in how they engage with suspects

Research review: Identifying the benefits of ALPR systems

By Tim Dees

How law enforcement agencies can use research findings to get community support and funding for ALPR systems

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Investigations
To: Tapis, Stephen C (POL)
Subject: Using open-source intel to tackle extremists; Fighting child abuse
Date: Tuesday, August 25, 2020 4:09:53 PM

August 25, 2020 | View as webpage

Dear Police1 Member,

While technology has brought great benefits to our daily lives it has also facilitated the growth of digital crime. From ransomware to human trafficking, technology is being used for nefarious purposes in an online world that knows no borders. It can be challenging for police investigators to stay informed of trends and equipped with the products and software to apprehend online criminals.

With that in mind, here are two steps to take to combat cybercrime:

- Read our digital edition to find out how AI can improve investigations
- Download our "How to Buy Investigation Software" guide to help procure the latest investigation tech

How is technology helping or hindering your investigations? Email editor@police1.com.

— *The Police1 Team*

FEATURED CONTENT

Using WEBINT and OSINT to tackle extremist groups

By Johnmichael O'Hare

Agencies that familiarize themselves with extremists' cyber haunts stand a better chance of uncovering potential problems before they materialize



How police can embrace the cloud to fight child sexual abuse

By Johann Hofmann

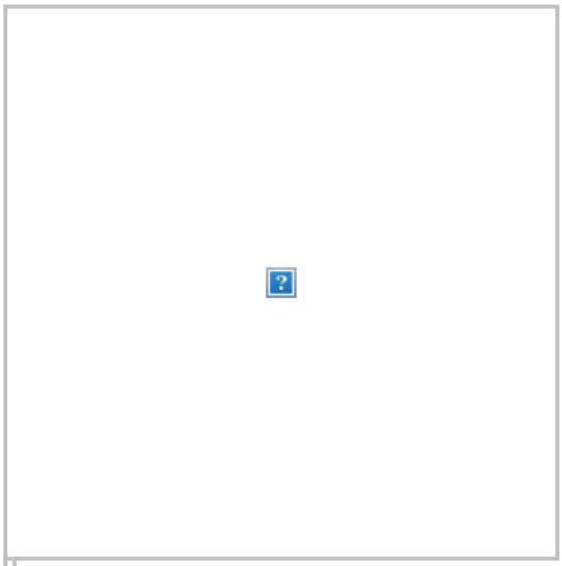
On-premise technology is increasingly inadequate for handling the scale of material associated with these cases



Guilty by association: How data linking strengthens investigations

By Joshua Lee, MLS, CFE, CCCI, CTFI, CCIE

With a few clicks of the mouse, an internet connection and the right know-how, police investigators can find crucial connections



Got Cameras? Get LPR



Your agency may be eligible for two free trial software licenses to add vehicle recognition capabilities to IP cameras in your jurisdiction.

Find out how

OTHER HIGHLIGHTS



How contactless technology

can help reduce bias, increase efficiencies and bolster safety

By Robert Berman

Real-time intelligence makes it easier for officers to be more strategic and safer in how they engage with suspects



Research review: Identifying the benefits of ALPR systems

By Tim Dees

How law enforcement agencies can use research findings to get community support and funding for ALPR systems



Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Investigations
To: Paquette, Brian (POL)
Subject: Using open-source intel to tackle extremists; Fighting child abuse
Date: Tuesday, August 25, 2020 4:09:42 PM

August 25, 2020 | View as webpage

Dear Police1 Member,

While technology has brought great benefits to our daily lives it has also facilitated the growth of digital crime. From ransomware to human trafficking, technology is being used for nefarious purposes in an online world that knows no borders. It can be challenging for police investigators to stay informed of trends and equipped with the products and software to apprehend online criminals.

With that in mind, here are two steps to take to combat cybercrime:

- Read our digital edition to find out how AI can improve investigations
- Download our "How to Buy Investigation Software" guide to help procure the latest investigation tech

How is technology helping or hindering your investigations? Email editor@police1.com.

— *The Police1 Team*

FEATURED CONTENT

Using WEBINT and OSINT to tackle extremist groups

By Johnmichael O'Hare

Agencies that familiarize themselves with extremists' cyber haunts stand a better chance of uncovering potential problems before they materialize



How police can embrace the cloud to fight child sexual abuse

By Johann Hofmann

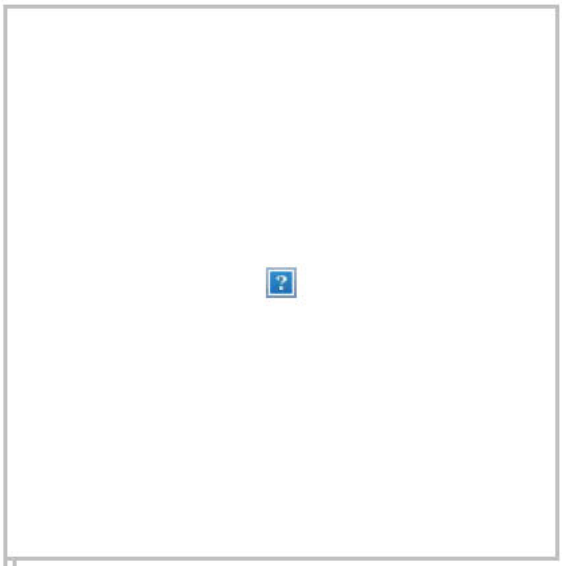
On-premise technology is increasingly inadequate for handling the scale of material associated with these cases



Guilty by association: How data linking strengthens investigations

By Joshua Lee, MLS, CFE, CCCI, CTFI, CCIE

With a few clicks of the mouse, an internet connection and the right know-how, police investigators can find crucial connections



Got Cameras? Get LPR



Your agency may be eligible for two free trial software licenses to add vehicle recognition capabilities to IP cameras in your jurisdiction.

Find out how

OTHER HIGHLIGHTS



How contactless technology

can help reduce bias, increase efficiencies and bolster safety

By Robert Berman

Real-time intelligence makes it easier for officers to be more strategic and safer in how they engage with suspects

Research review: Identifying the benefits of ALPR systems

By Tim Dees

How law enforcement agencies can use research findings to get community support and funding for ALPR systems

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Investigations
To: McCarthy, Steven (POL)
Subject: Using open-source intel to tackle extremists; Fighting child abuse
Date: Tuesday, August 25, 2020 4:01:05 PM

August 25, 2020 | View as webpage

Dear Police1 Member,

While technology has brought great benefits to our daily lives it has also facilitated the growth of digital crime. From ransomware to human trafficking, technology is being used for nefarious purposes in an online world that knows no borders. It can be challenging for police investigators to stay informed of trends and equipped with the products and software to apprehend online criminals.

With that in mind, here are two steps to take to combat cybercrime:

- Read our digital edition to find out how AI can improve investigations
- Download our "How to Buy Investigation Software" guide to help procure the latest investigation tech

How is technology helping or hindering your investigations? Email editor@police1.com.

— *The Police1 Team*

FEATURED CONTENT

Using WEBINT and OSINT to tackle extremist groups

By Johnmichael O'Hare

Agencies that familiarize themselves with extremists' cyber haunts stand a better chance of uncovering potential problems before they materialize



How police can embrace the cloud to fight child sexual abuse

By Johann Hofmann

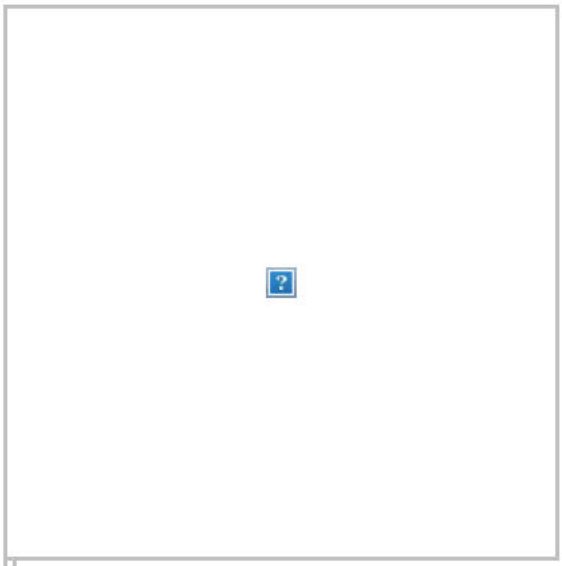
On-premise technology is increasingly inadequate for handling the scale of material associated with these cases



Guilty by association: How data linking strengthens investigations

By Joshua Lee, MLS, CFE, CCCI, CTFI, CCIE

With a few clicks of the mouse, an internet connection and the right know-how, police investigators can find crucial connections



Got Cameras? Get LPR



Your agency may be eligible for two free trial software licenses to add vehicle recognition capabilities to IP cameras in your jurisdiction.

Find out how

OTHER HIGHLIGHTS



How contactless technology

can help reduce bias, increase efficiencies and bolster safety

By Robert Berman

Real-time intelligence makes it easier for officers to be more strategic and safer in how they engage with suspects

Research review: Identifying the benefits of ALPR systems

By Tim Dees

How law enforcement agencies can use research findings to get community support and funding for ALPR systems

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Investigations
To: Doyle, Paul (POL)
Subject: Using open-source intel to tackle extremists; Fighting child abuse
Date: Tuesday, August 25, 2020 4:00:10 PM

August 25, 2020 | View as webpage

Dear Police1 Member,

While technology has brought great benefits to our daily lives it has also facilitated the growth of digital crime. From ransomware to human trafficking, technology is being used for nefarious purposes in an online world that knows no borders. It can be challenging for police investigators to stay informed of trends and equipped with the products and software to apprehend online criminals.

With that in mind, here are two steps to take to combat cybercrime:

- Read our digital edition to find out how AI can improve investigations
- Download our "How to Buy Investigation Software" guide to help procure the latest investigation tech

How is technology helping or hindering your investigations? Email editor@police1.com.

— *The Police1 Team*

FEATURED CONTENT

Using WEBINT and OSINT to tackle extremist groups

By Johnmichael O'Hare

Agencies that familiarize themselves with extremists' cyber haunts stand a better chance of uncovering potential problems before they materialize



How police can embrace the cloud to fight child sexual abuse

By Johann Hofmann

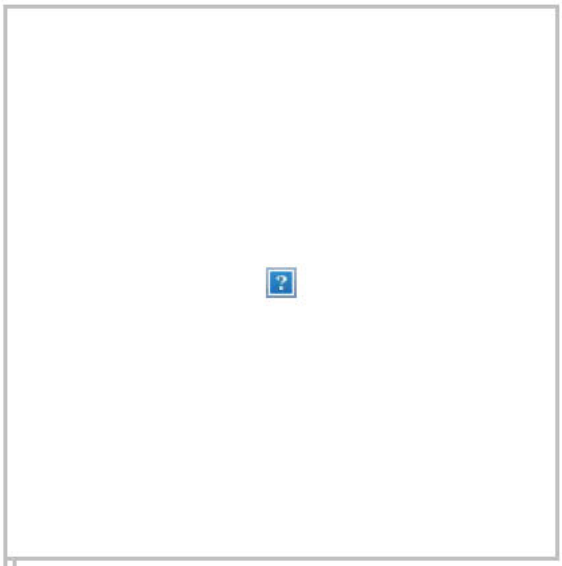
On-premise technology is increasingly inadequate for handling the scale of material associated with these cases



Guilty by association: How data linking strengthens investigations

By Joshua Lee, MLS, CFE, CCCI, CTFI, CCIE

With a few clicks of the mouse, an internet connection and the right know-how, police investigators can find crucial connections



Got Cameras? Get LPR



Your agency may be eligible for two free trial software licenses to add vehicle recognition capabilities to IP cameras in your jurisdiction.

Find out how

OTHER HIGHLIGHTS



How contactless technology

can help reduce bias, increase efficiencies and bolster safety

By Robert Berman

Real-time intelligence makes it easier for officers to be more strategic and safer in how they engage with suspects

Research review: Identifying the benefits of ALPR systems

By Tim Dees

How law enforcement agencies can use research findings to get community support and funding for ALPR systems

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Investigations
To: Procopio, David (POL)
Subject: Using open-source intel to tackle extremists; Fighting child abuse
Date: Tuesday, August 25, 2020 3:49:51 PM

August 25, 2020 | View as webpage

Dear Police1 Member,

While technology has brought great benefits to our daily lives it has also facilitated the growth of digital crime. From ransomware to human trafficking, technology is being used for nefarious purposes in an online world that knows no borders. It can be challenging for police investigators to stay informed of trends and equipped with the products and software to apprehend online criminals.

With that in mind, here are two steps to take to combat cybercrime:

- Read our digital edition to find out how AI can improve investigations
- Download our "How to Buy Investigation Software" guide to help procure the latest investigation tech

How is technology helping or hindering your investigations? Email editor@police1.com.

— *The Police1 Team*

FEATURED CONTENT

Using WEBINT and OSINT to tackle extremist groups

By Johnmichael O'Hare

Agencies that familiarize themselves with extremists' cyber haunts stand a better chance of uncovering potential problems before they materialize



How police can embrace the cloud to fight child sexual abuse

By Johann Hofmann

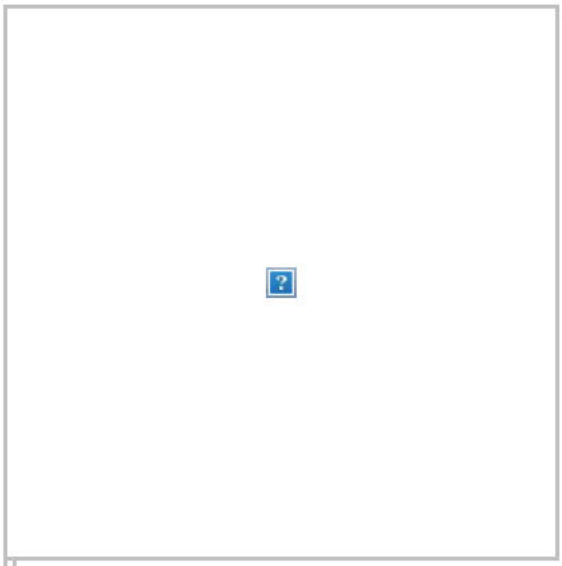
On-premise technology is increasingly inadequate for handling the scale of material associated with these cases



Guilty by association: How data linking strengthens investigations

By Joshua Lee, MLS, CFE, CCCI, CTFI, CCIE

With a few clicks of the mouse, an internet connection and the right know-how, police investigators can find crucial connections



Got Cameras? Get LPR



Your agency may be eligible for two free trial software licenses to add vehicle recognition capabilities to IP cameras in your jurisdiction.

Find out how

OTHER HIGHLIGHTS



How contactless technology

can help reduce bias, increase efficiencies and bolster safety

By Robert Berman

Real-time intelligence makes it easier for officers to be more strategic and safer in how they engage with suspects

Research review: Identifying the benefits of ALPR systems

By Tim Dees

How law enforcement agencies can use research findings to get community support and funding for ALPR systems

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Investigations
To: Loiselle, Rachel (POL)
Subject: Using open-source intel to tackle extremists; Fighting child abuse
Date: Tuesday, August 25, 2020 3:49:46 PM

August 25, 2020 | View as webpage

Dear Police1 Member,

While technology has brought great benefits to our daily lives it has also facilitated the growth of digital crime. From ransomware to human trafficking, technology is being used for nefarious purposes in an online world that knows no borders. It can be challenging for police investigators to stay informed of trends and equipped with the products and software to apprehend online criminals.

With that in mind, here are two steps to take to combat cybercrime:

- Read our digital edition to find out how AI can improve investigations
- Download our "How to Buy Investigation Software" guide to help procure the latest investigation tech

How is technology helping or hindering your investigations? Email editor@police1.com.

— *The Police1 Team*

FEATURED CONTENT

Using WEBINT and OSINT to tackle extremist groups

By Johnmichael O'Hare

Agencies that familiarize themselves with extremists' cyber haunts stand a better chance of uncovering potential problems before they materialize



How police can embrace the cloud to fight child sexual abuse

By Johann Hofmann

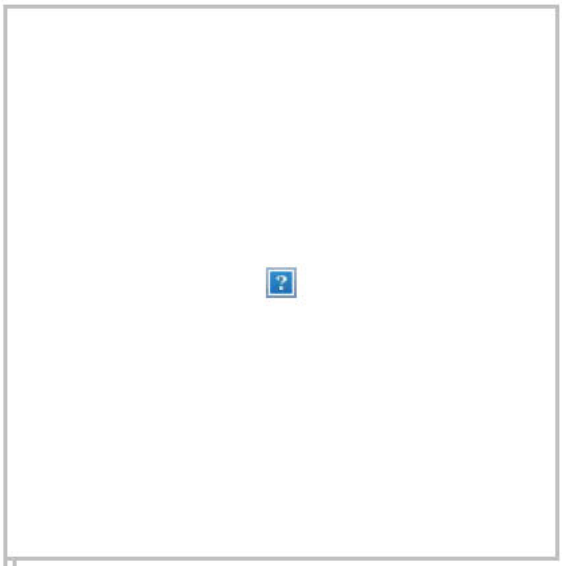
On-premise technology is increasingly inadequate for handling the scale of material associated with these cases



Guilty by association: How data linking strengthens investigations

By Joshua Lee, MLS, CFE, CCCI, CTFI, CCIE

With a few clicks of the mouse, an internet connection and the right know-how, police investigators can find crucial connections



Got Cameras? Get LPR



Your agency may be eligible for two free trial software licenses to add vehicle recognition capabilities to IP cameras in your jurisdiction.

Find out how

OTHER HIGHLIGHTS



How contactless technology

can help reduce bias, increase efficiencies and bolster safety

By Robert Berman

Real-time intelligence makes it easier for officers to be more strategic and safer in how they engage with suspects

Research review: Identifying the benefits of ALPR systems

By Tim Dees

How law enforcement agencies can use research findings to get community support and funding for ALPR systems

Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: Police1 Investigations
To: Davis, Matthew (POL)
Subject: Using open-source intel to tackle extremists; Fighting child abuse
Date: Tuesday, August 25, 2020 4:40:26 PM

August 25, 2020 | View as webpage

Dear Police1 Member,

While technology has brought great benefits to our daily lives it has also facilitated the growth of digital crime. From ransomware to human trafficking, technology is being used for nefarious purposes in an online world that knows no borders. It can be challenging for police investigators to stay informed of trends and equipped with the products and software to apprehend online criminals.

With that in mind, here are two steps to take to combat cybercrime:

- Read our digital edition to find out how AI can improve investigations
- Download our "How to Buy Investigation Software" guide to help procure the latest investigation tech

How is technology helping or hindering your investigations? Email editor@police1.com.

— *The Police1 Team*

FEATURED CONTENT

Using WEBINT and OSINT to tackle extremist groups

By Johnmichael O'Hare

Agencies that familiarize themselves with extremists' cyber haunts stand a better chance of uncovering potential problems before they materialize



How police can embrace the cloud to fight child sexual abuse

By Johann Hofmann

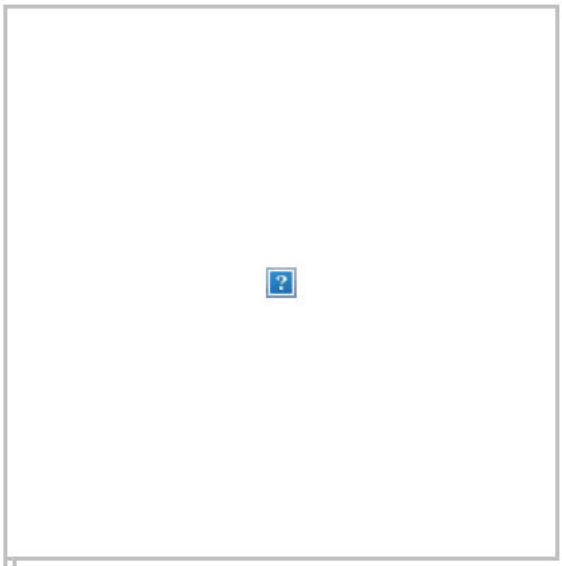
On-premise technology is increasingly inadequate for handling the scale of material associated with these cases



Guilty by association: How data linking strengthens investigations

By Joshua Lee, MLS, CFE, CCCI, CTFI, CCIE

With a few clicks of the mouse, an internet connection and the right know-how, police investigators can find crucial connections



Got Cameras? Get LPR



Your agency may be eligible for two free trial software licenses to add vehicle recognition capabilities to IP cameras in your jurisdiction.

Find out how

OTHER HIGHLIGHTS



How contactless technology

can help reduce bias, increase efficiencies and bolster safety

By Robert Berman

Real-time intelligence makes it easier for officers to be more strategic and safer in how they engage with suspects

Research review: Identifying the benefits of ALPR systems

By Tim Dees

How law enforcement agencies can use research findings to get community support and funding for ALPR systems

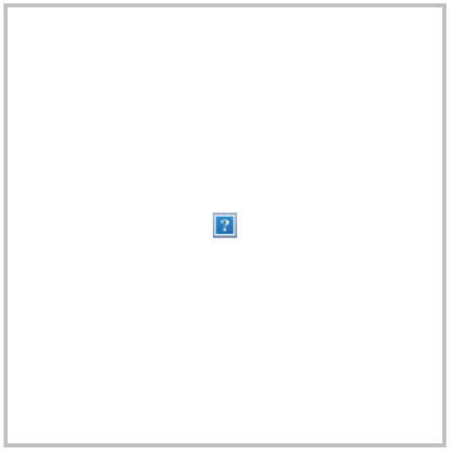
Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

From: PoliceOne Roll Call
To: Breton, Benjamin (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:40:31 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

April 30, 2020 | View as webpage

TOP STORIES



LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

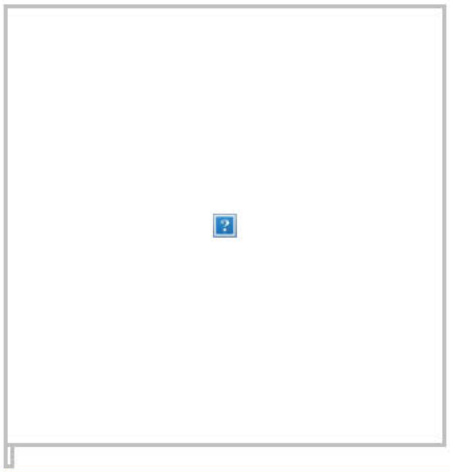
New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral



Real-Time Threats. Real-Time Detection.



The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE

5 steps to refine your COVID-19 social media strategy

By Cole Zercoe
Social media is the most effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall
When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed
While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer

3257

course

By Sean Curtis
A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt
Follow these report-writing tips to improve the outcomes of your cases



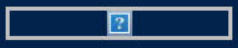
SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.





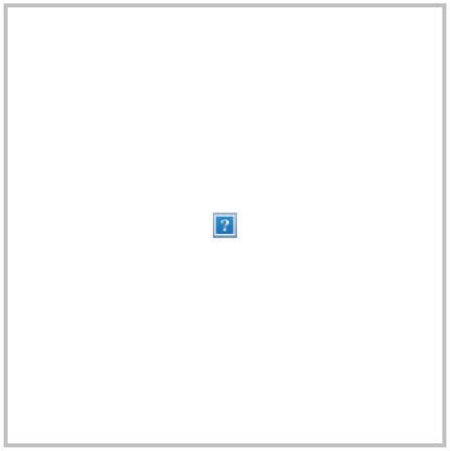
PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: Irwin, Patrick (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:40:23 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

April 30, 2020 | View as webpage

TOP STORIES



LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

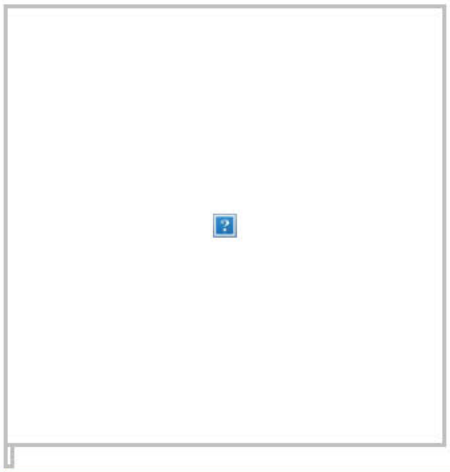
New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral



Real-Time Threats. Real-Time Detection.



The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE



5 steps to refine your COVID-19 social media strategy

By Cole Zercoe
Social media is the most effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall
When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed
While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer

course

By Sean Curtis

A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt

Follow these report-writing tips to improve the outcomes of your cases



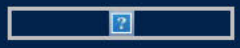
SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.





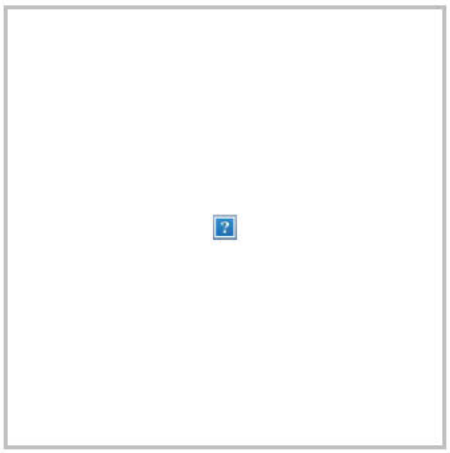
PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: Mcdonald, Scott (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:40:13 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

April 30, 2020 | View as webpage

TOP STORIES



LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

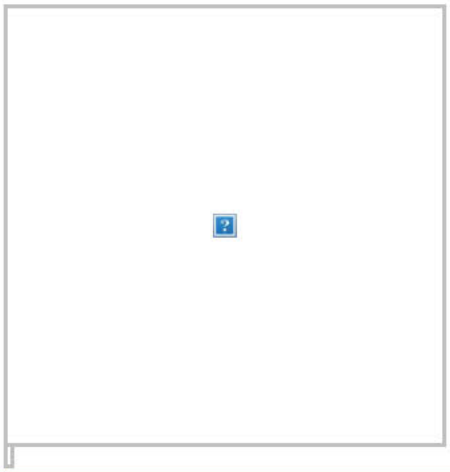
New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral



Real-Time Threats. Real-Time Detection.



The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE



5 steps to refine your COVID-19 social media strategy

By Cole Zercoe
Social media is the most effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall
When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed
While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer

course

By Sean Curtis

A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt

Follow these report-writing tips to improve the outcomes of your cases



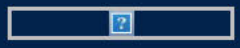
SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.



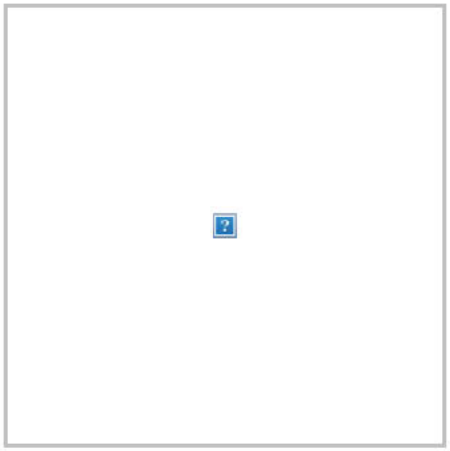


PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: Keville, Robert (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:39:57 PM

April 30, 2020 | View as webpage

TOP STORIES



LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

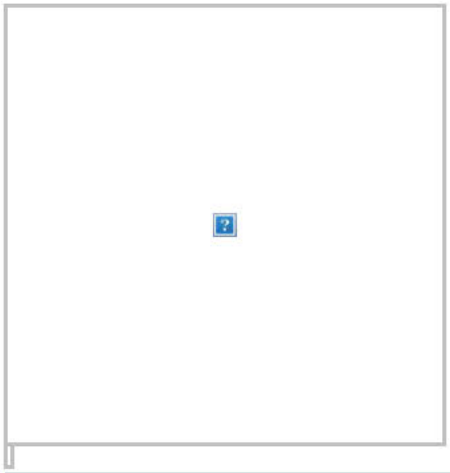
New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral



Real-Time Threats. Real-Time Detection.



The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE



5 steps to refine your COVID-19 social media strategy

By Cole Zercoe

Social media is the most

effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall

When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed

While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer course

By Sean Curtis
A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt
Follow these report-writing tips to improve the outcomes of your cases



SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.





PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: Goonan, Michael D (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:39:43 PM

April 30, 2020 | View as webpage

TOP STORIES

LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral

Real-Time Threats. Real-Time Detection.

The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE

5 steps to refine your COVID-19 social media strategy

By Cole Zercoe

Social media is the most

effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall

When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed

While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer course

By Sean Curtis
A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt
Follow these report-writing tips to improve the outcomes of your cases



SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.



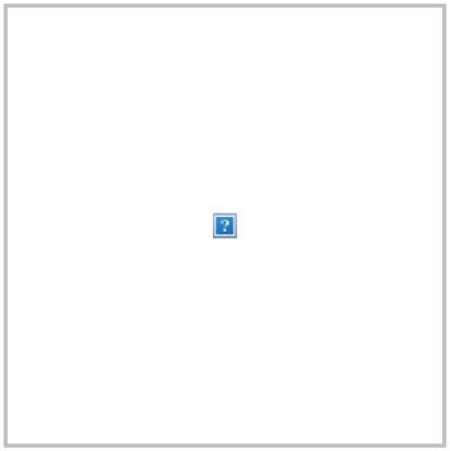


PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: Cannon, Brian (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:39:38 PM

April 30, 2020 | View as webpage

TOP STORIES



LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

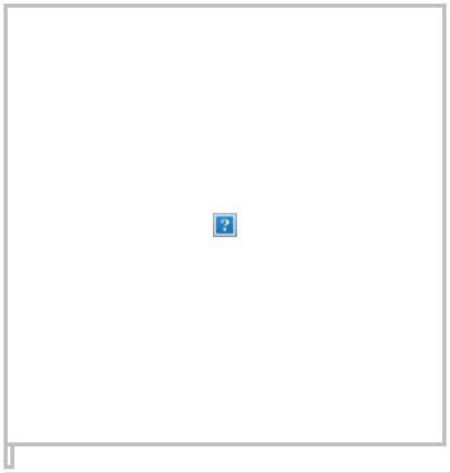
New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral



Real-Time Threats. Real-Time Detection.



The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE



5 steps to refine your COVID-19 social media strategy

By Cole Zercoe

Social media is the most

effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall

When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed

While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer course

By Sean Curtis
A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt
Follow these report-writing tips to improve the outcomes of your cases



SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.





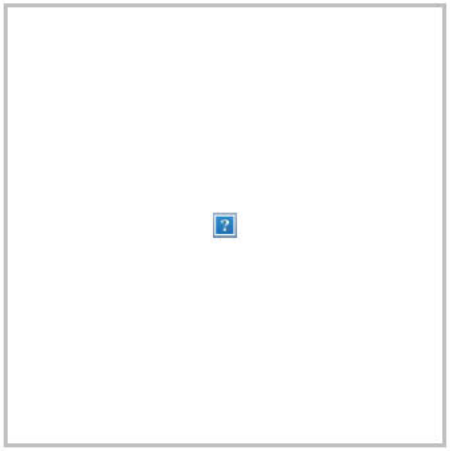
PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: Seymour, Alexander P (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:39:30 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

April 30, 2020 | View as webpage

TOP STORIES



LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

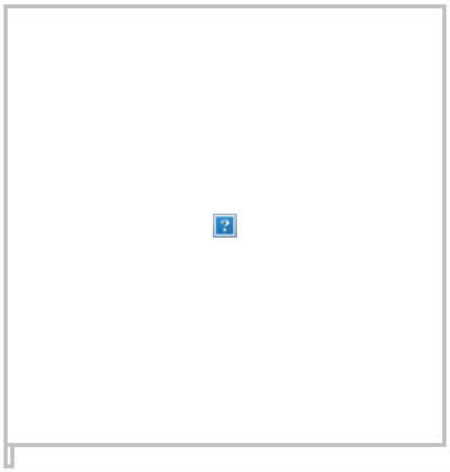
New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral



Real-Time Threats. Real-Time Detection.



The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE

5 steps to refine your COVID-19 social media strategy

By Cole Zercoe
Social media is the most effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall
When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed
While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer

course

By Sean Curtis

A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt

Follow these report-writing tips to improve the outcomes of your cases



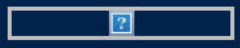
SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.



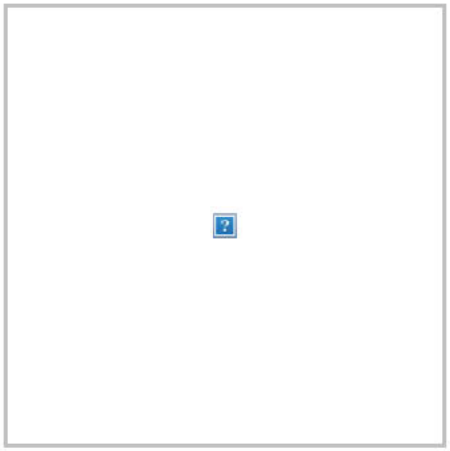


PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: Lee, Brian (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:39:17 PM

April 30, 2020 | View as webpage

TOP STORIES



LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

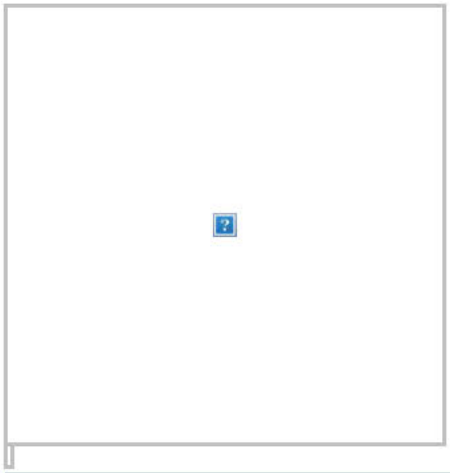
New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral



Real-Time Threats. Real-Time Detection.



The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE



5 steps to refine your COVID-19 social media strategy

By Cole Zercoe

Social media is the most

effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall

When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed

While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer course

By Sean Curtis
A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt
Follow these report-writing tips to improve the outcomes of your cases



SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.



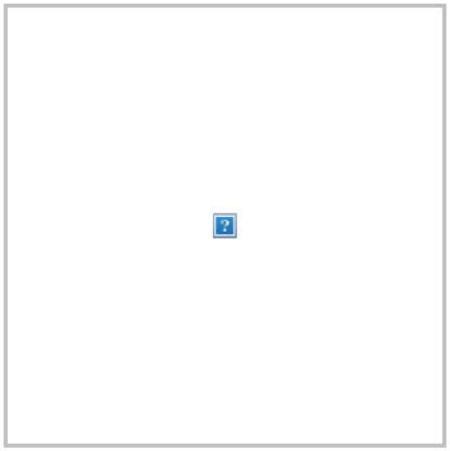


PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: zzMullaney, Stephen (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:39:05 PM

April 30, 2020 | View as webpage

TOP STORIES



LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

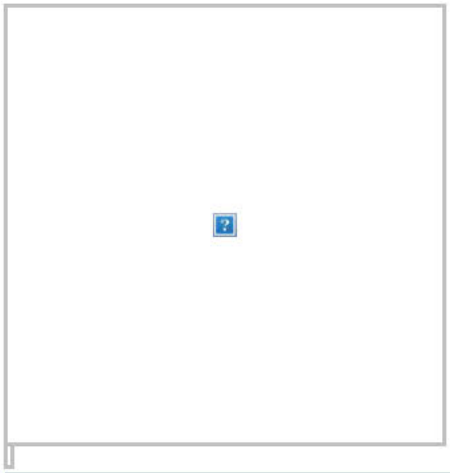
New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral



Real-Time Threats. Real-Time Detection.



The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE



5 steps to refine your COVID-19 social media strategy

By Cole Zercoe

Social media is the most

effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall

When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed

While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer course

By Sean Curtis
A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt
Follow these report-writing tips to improve the outcomes of your cases



SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.





PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: zzLeVangie, Dean (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:39:02 PM

April 30, 2020 | View as webpage

TOP STORIES

LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral

Real-Time Threats. Real-Time Detection.

The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE

5 steps to refine your COVID-19 social media strategy

By Cole Zercoe

Social media is the most

effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall

When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed

While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer course

By Sean Curtis
A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt
Follow these report-writing tips to improve the outcomes of your cases



SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.





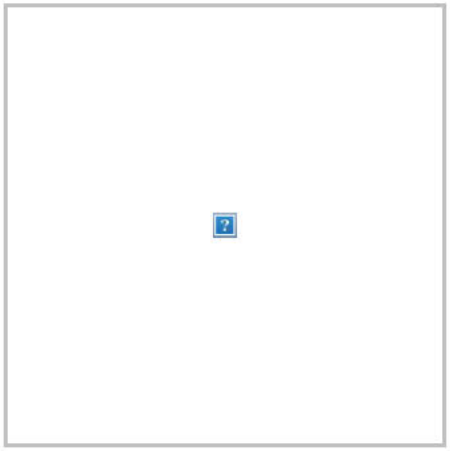
PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: Grassia, Michael (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:39:00 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

April 30, 2020 | View as webpage

TOP STORIES



LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

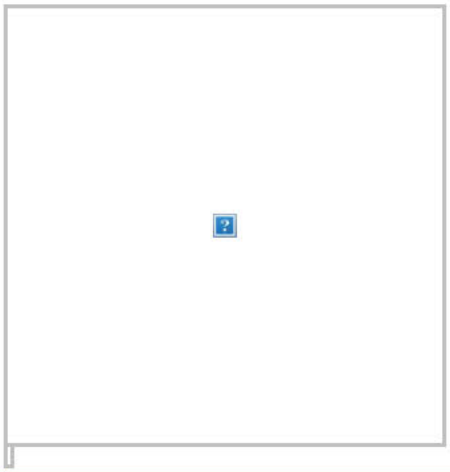
New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral



Real-Time Threats. Real-Time Detection.



The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE

5 steps to refine your COVID-19 social media strategy

By Cole Zercoe
Social media is the most effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall
When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed
While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer

course

By Sean Curtis
A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt
Follow these report-writing tips to improve the outcomes of your cases



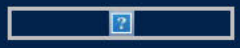
SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.



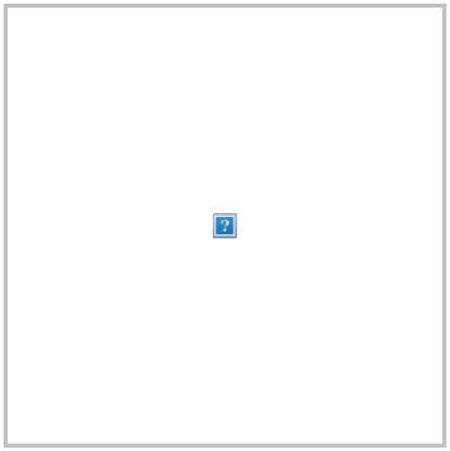


PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: Davis, Matthew (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:38:52 PM

April 30, 2020 | View as webpage

TOP STORIES



LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

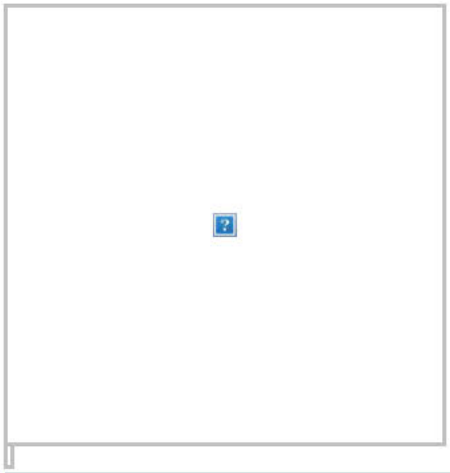
New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral



Real-Time Threats. Real-Time Detection.



The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE



5 steps to refine your COVID-19 social media strategy

By Cole Zercoe

Social media is the most

effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall

When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed

While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer course

By Sean Curtis
A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt
Follow these report-writing tips to improve the outcomes of your cases



SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.





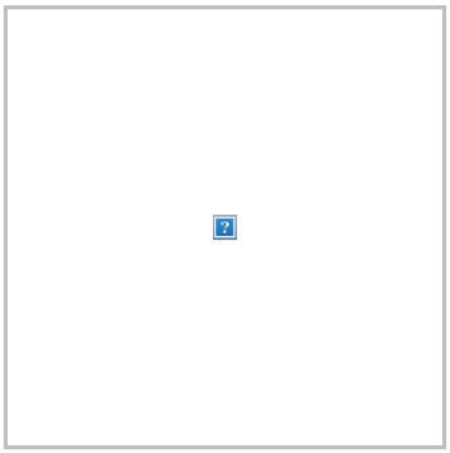
PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: Rizos, Byron (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:38:39 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

April 30, 2020 | View as webpage

TOP STORIES



LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

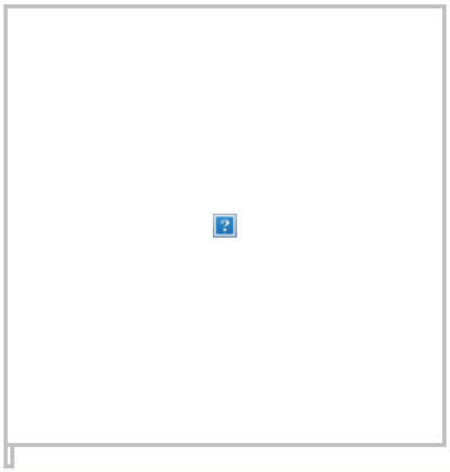
New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral



Real-Time Threats. Real-Time Detection.



The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE



5 steps to refine your COVID-19 social media strategy

By Cole Zercoe
Social media is the most effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall
When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed
While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer

course

By Sean Curtis

A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt

Follow these report-writing tips to improve the outcomes of your cases



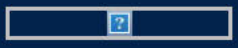
SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.





PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: Seymour, Alexander P (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:38:23 PM

April 30, 2020 | View as webpage

TOP STORIES

LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral

Real-Time Threats. Real-Time Detection.

The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE

5 steps to refine your COVID-19 social media strategy

By Cole Zercoe

Social media is the most

effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall

When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed

While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer course

By Sean Curtis
A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt
Follow these report-writing tips to improve the outcomes of your cases



SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.



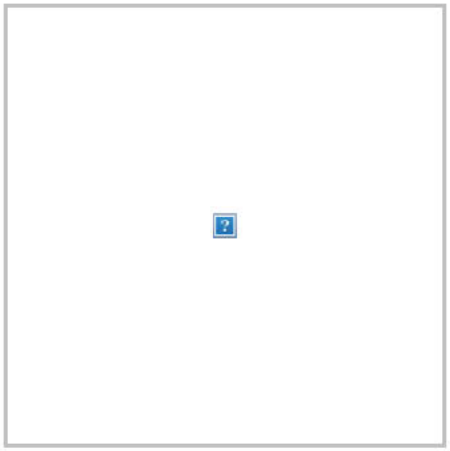


PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: Golenski, Michael (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:38:23 PM

April 30, 2020 | View as webpage

TOP STORIES



LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

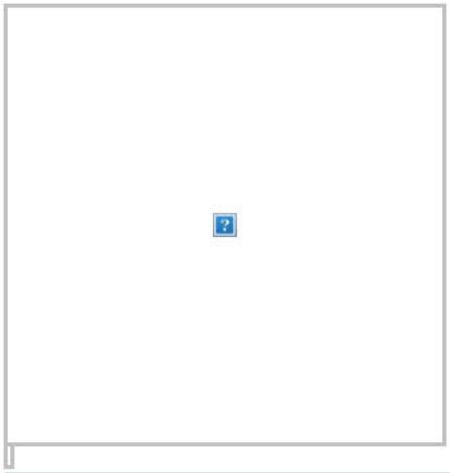
New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral



Real-Time Threats. Real-Time Detection.



The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE



5 steps to refine your COVID-19 social media strategy

By Cole Zercoe

Social media is the most

effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall

When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed

While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer course

By Sean Curtis
A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt
Follow these report-writing tips to improve the outcomes of your cases



SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.





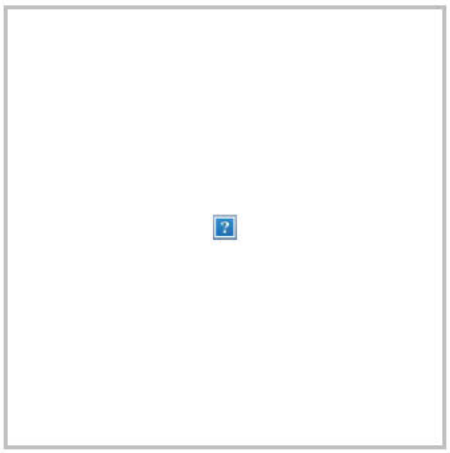
PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: wanagel@bu.edu
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:38:21 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

April 30, 2020 | View as webpage

TOP STORIES



LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

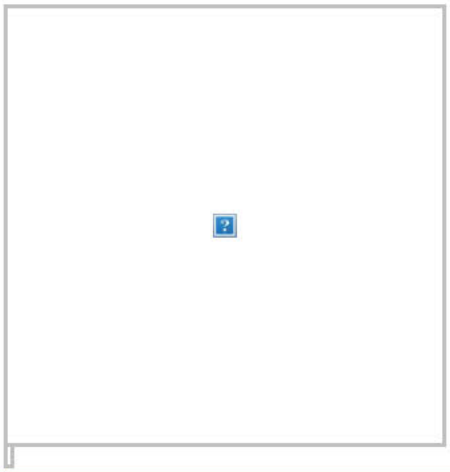
New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral



Real-Time Threats. Real-Time Detection.



The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE



5 steps to refine your COVID-19 social media strategy

By Cole Zercoe
Social media is the most effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall
When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed
While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer

3302

course

By Sean Curtis

A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt

Follow these report-writing tips to improve the outcomes of your cases



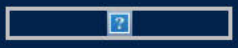
SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.



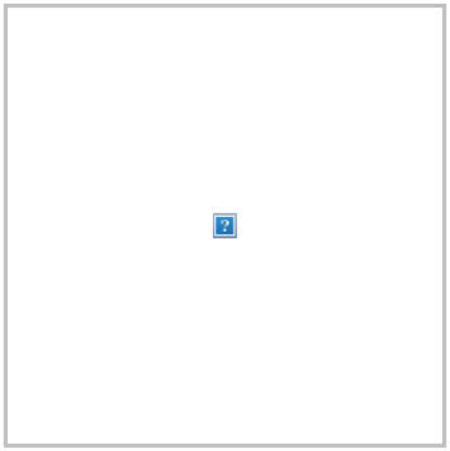


PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: benesh, meghann E (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:38:17 PM

April 30, 2020 | View as webpage

TOP STORIES



LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

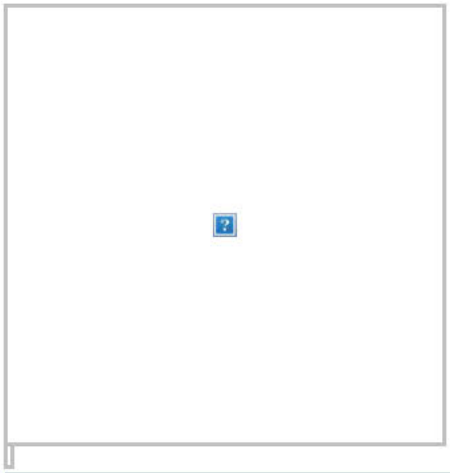
New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral



Real-Time Threats. Real-Time Detection.



The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE



5 steps to refine your COVID-19 social media strategy

By Cole Zercoe

Social media is the most

effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall

When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed

While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer course

By Sean Curtis
A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt
Follow these report-writing tips to improve the outcomes of your cases



SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.



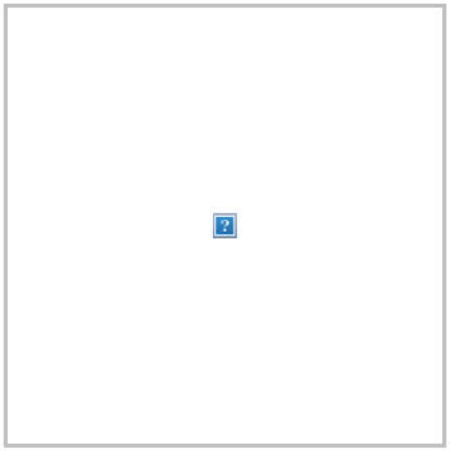


PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: Williams, Keller (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:38:12 PM

April 30, 2020 | View as webpage

TOP STORIES



LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

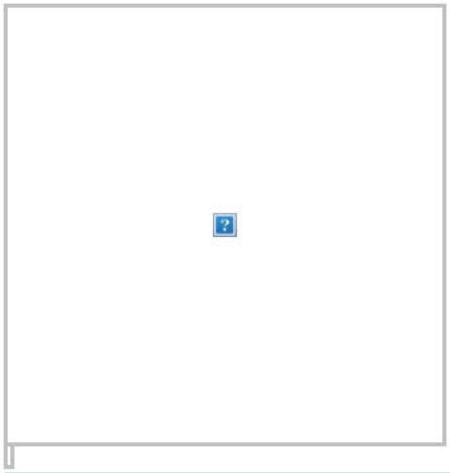
New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral



Real-Time Threats. Real-Time Detection.



The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE



5 steps to refine your COVID-19 social media strategy

By Cole Zercoe

Social media is the most

effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall

When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed

While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer course

By Sean Curtis
A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt
Follow these report-writing tips to improve the outcomes of your cases



SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.



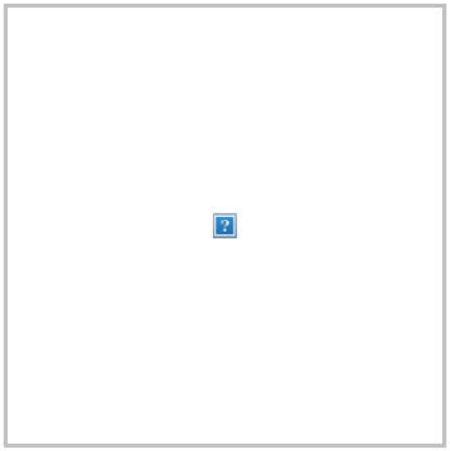


PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: Silva, Patrick (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:38:05 PM

April 30, 2020 | View as webpage

TOP STORIES



LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

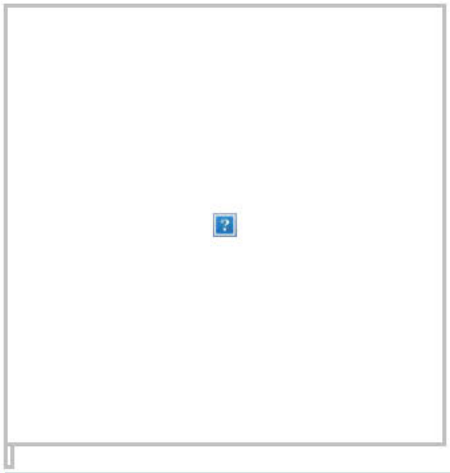
New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral



Real-Time Threats. Real-Time Detection.



The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE



5 steps to refine your COVID-19 social media strategy

By Cole Zercoe

Social media is the most

effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall

When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed

While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer course

By Sean Curtis
A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt
Follow these report-writing tips to improve the outcomes of your cases



SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.





PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: McCarthy, Steven (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:37:46 PM

April 30, 2020 | View as webpage

TOP STORIES

LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral

Real-Time Threats. Real-Time Detection.

The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE

5 steps to refine your COVID-19 social media strategy

By Cole Zercoe

Social media is the most

effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall

When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed

While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer course

By Sean Curtis
A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt
Follow these report-writing tips to improve the outcomes of your cases



SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.



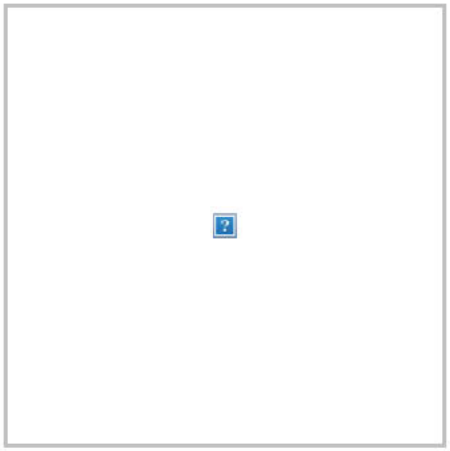


PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: Paquette, Brian (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:37:43 PM

April 30, 2020 | View as webpage

TOP STORIES



LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

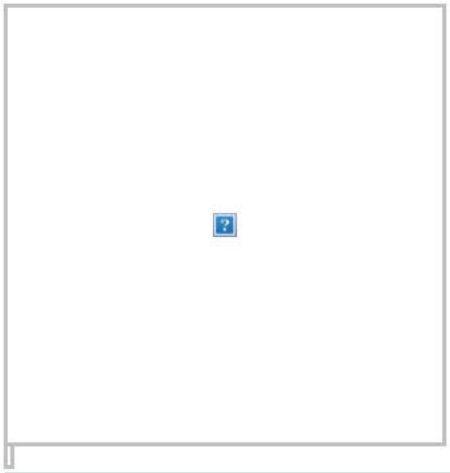
New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral



Real-Time Threats. Real-Time Detection.



The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE



5 steps to refine your COVID-19 social media strategy

By Cole Zercoe

Social media is the most

effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall

When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed

While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer course

By Sean Curtis
A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt
Follow these report-writing tips to improve the outcomes of your cases



SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.





PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: Spencer, Jonathan (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:37:37 PM

April 30, 2020 | View as webpage

TOP STORIES

LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral

Real-Time Threats. Real-Time Detection.

The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE

5 steps to refine your COVID-19 social media strategy

By Cole Zercoe

Social media is the most

effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall

When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed

While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer course

By Sean Curtis
A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt
Follow these report-writing tips to improve the outcomes of your cases



SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.



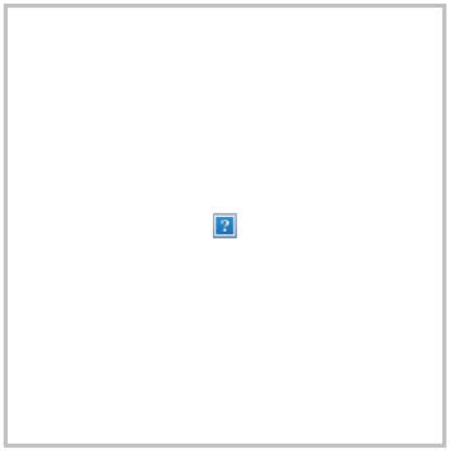


PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: Griffin, Daniel (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:37:28 PM

April 30, 2020 | View as webpage

TOP STORIES



LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

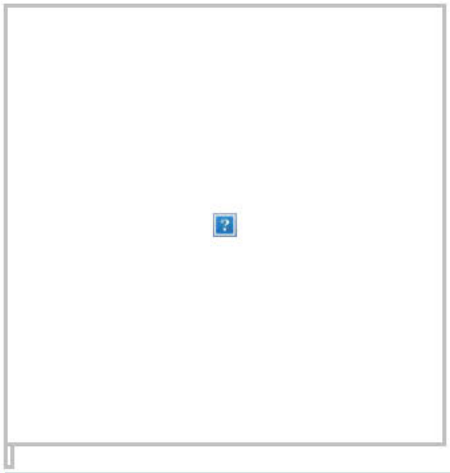
New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral



Real-Time Threats. Real-Time Detection.



The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE



5 steps to refine your COVID-19 social media strategy

By Cole Zercoe

Social media is the most

effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall

When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed

While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer course

By Sean Curtis
A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt
Follow these report-writing tips to improve the outcomes of your cases



SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.





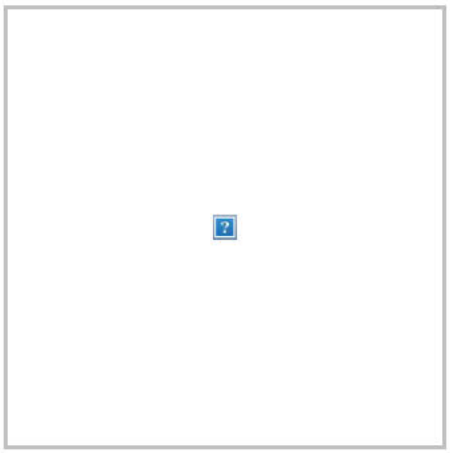
PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: Conneely, Paul (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:37:23 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

April 30, 2020 | View as webpage

TOP STORIES



LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

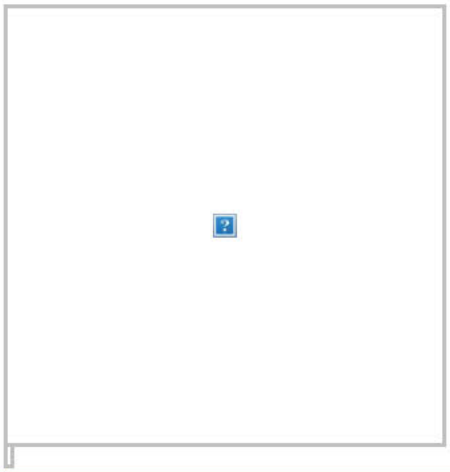
New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral



Real-Time Threats. Real-Time Detection.



The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE



5 steps to refine your COVID-19 social media strategy

By Cole Zercoe
Social media is the most effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall
When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed
While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer

course

By Sean Curtis

A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt

Follow these report-writing tips to improve the outcomes of your cases



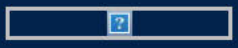
SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.





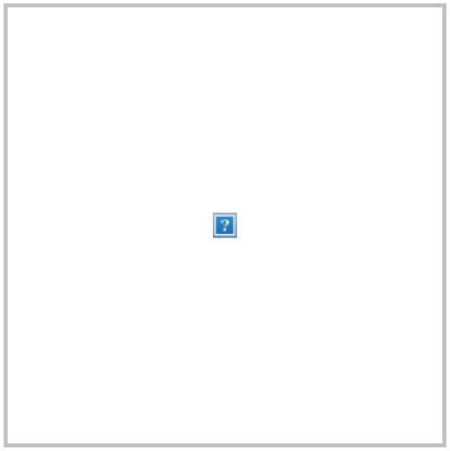
PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: Johnson, Robert - Captain (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:37:21 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

April 30, 2020 | View as webpage

TOP STORIES



LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

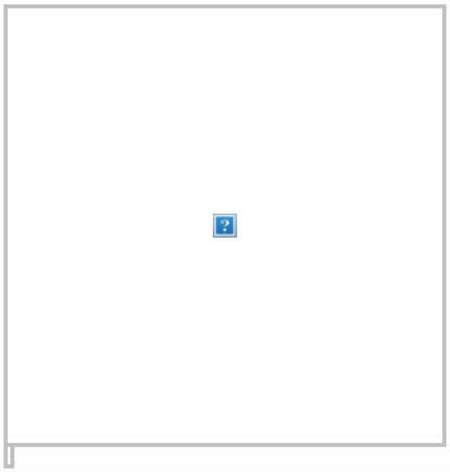
New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral



Real-Time Threats. Real-Time Detection.



The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE

5 steps to refine your COVID-19 social media strategy

By Cole Zercoe
Social media is the most effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall
When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed
While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer

course

By Sean Curtis

A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt

Follow these report-writing tips to improve the outcomes of your cases



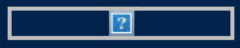
SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.





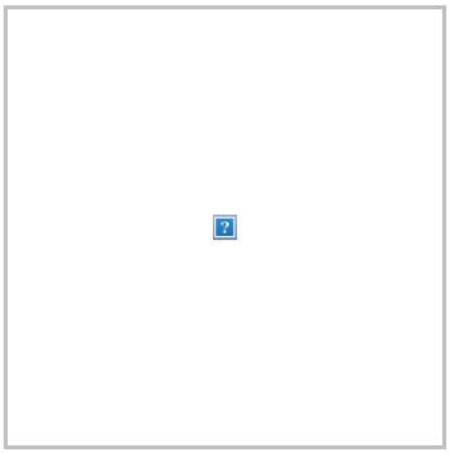
PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: Lyver, Michael (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:37:05 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

April 30, 2020 | View as webpage

TOP STORIES



LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

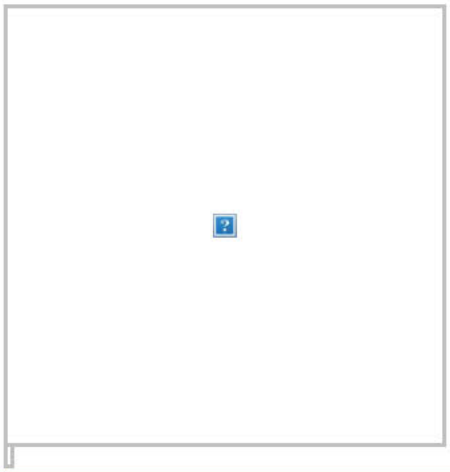
New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral



Real-Time Threats. Real-Time Detection.



The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE

5 steps to refine your COVID-19 social media strategy

By Cole Zercoe
Social media is the most effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall
When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed
While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer

course

By Sean Curtis

A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt

Follow these report-writing tips to improve the outcomes of your cases



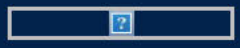
SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.





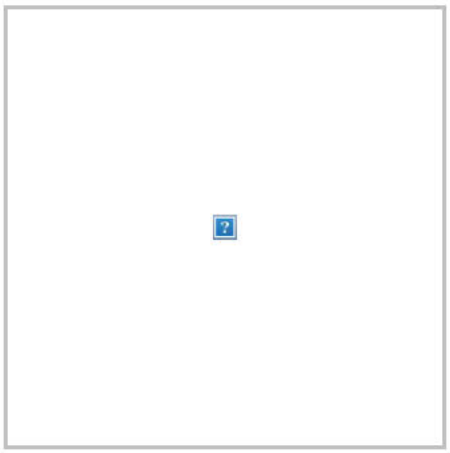
PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: Cronin, John E (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:36:59 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

April 30, 2020 | View as webpage

TOP STORIES



LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

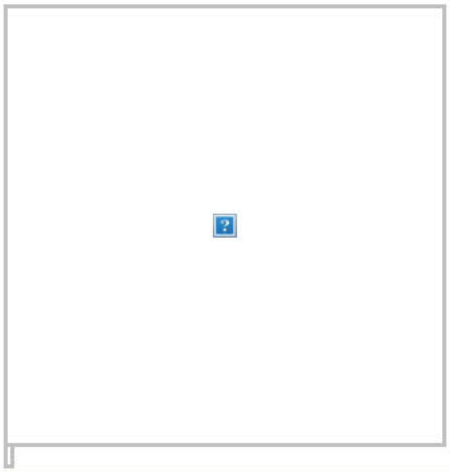
New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral



Real-Time Threats. Real-Time Detection.



The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE

5 steps to refine your COVID-19 social media strategy

By Cole Zercoe
Social media is the most effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall
When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed
While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer

3335

course

By Sean Curtis
A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt
Follow these report-writing tips to improve the outcomes of your cases



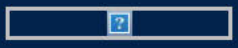
SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.





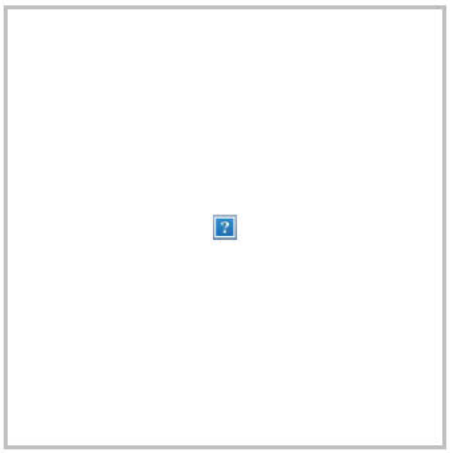
PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: Lawlor Jr, Daniel (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:36:57 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

April 30, 2020 | View as webpage

TOP STORIES



LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

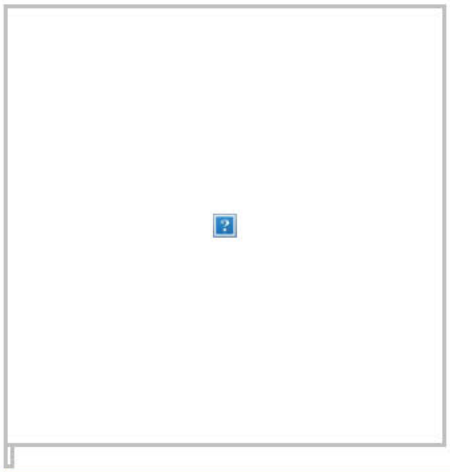
New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral



Real-Time Threats. Real-Time Detection.



The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE

5 steps to refine your COVID-19 social media strategy

By Cole Zercoe
Social media is the most effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall
When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed
While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer

3338

course

By Sean Curtis

A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt

Follow these report-writing tips to improve the outcomes of your cases



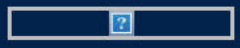
SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.





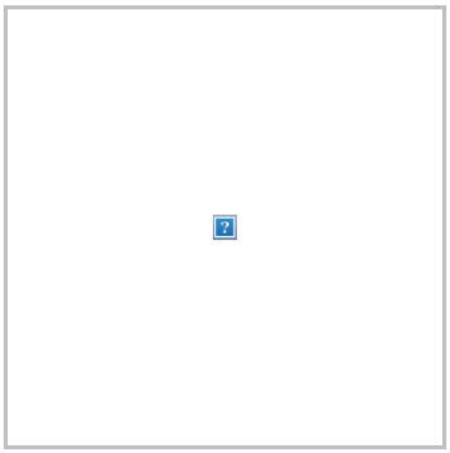
PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: Nee, William (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:36:39 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

April 30, 2020 | View as webpage

TOP STORIES



LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

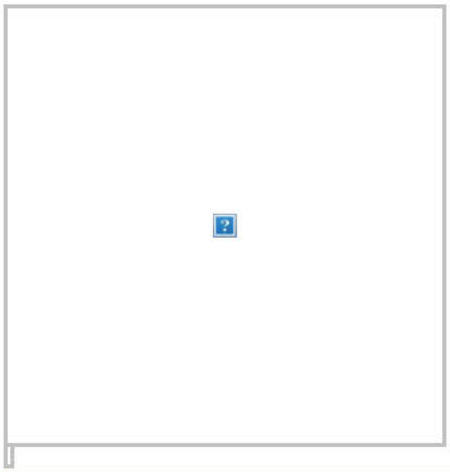
New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral



Real-Time Threats. Real-Time Detection.



The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE



5 steps to refine your COVID-19 social media strategy

By Cole Zercoe
Social media is the most effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall
When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed
While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer

3341

course

By Sean Curtis

A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt

Follow these report-writing tips to improve the outcomes of your cases



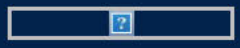
SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.





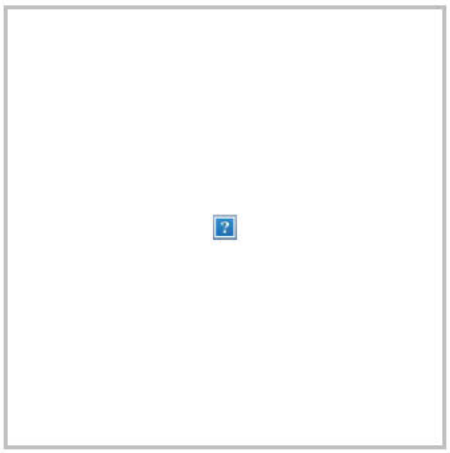
PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: Willhite, Michael (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:36:19 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

April 30, 2020 | View as webpage

TOP STORIES



LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

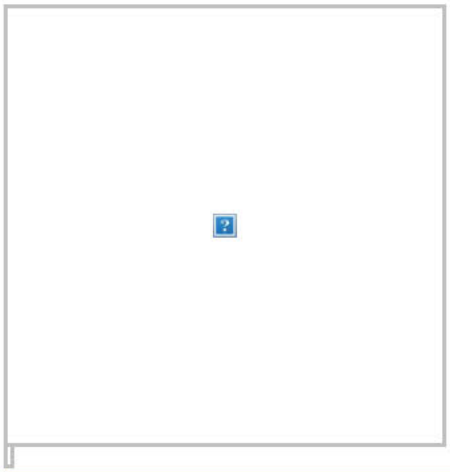
New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral



Real-Time Threats. Real-Time Detection.



The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE

5 steps to refine your COVID-19 social media strategy

By Cole Zercoe
Social media is the most effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall
When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed
While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer

course

By Sean Curtis

A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt

Follow these report-writing tips to improve the outcomes of your cases



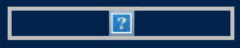
SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.





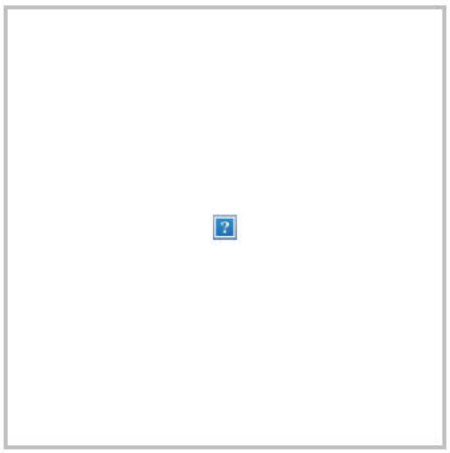
PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: Doyle, Paul (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:36:11 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

April 30, 2020 | View as webpage

TOP STORIES



LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

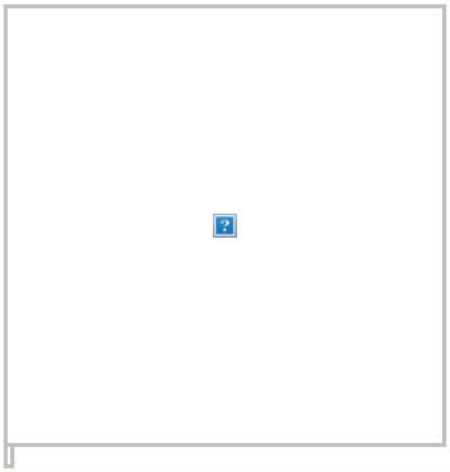
New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral



Real-Time Threats. Real-Time Detection.



The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE



5 steps to refine your COVID-19 social media strategy

By Cole Zercoe
Social media is the most effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall
When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed
While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer

course

By Sean Curtis

A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt

Follow these report-writing tips to improve the outcomes of your cases



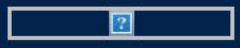
SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.



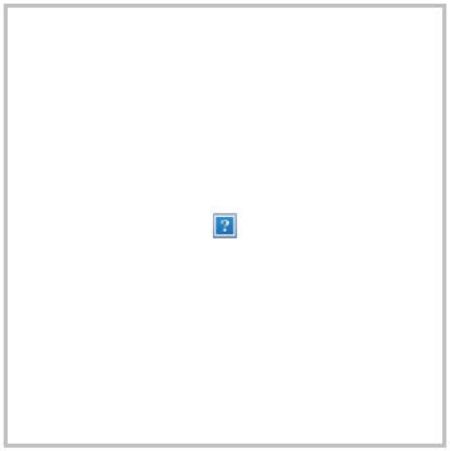


PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: Upton, Paul (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:36:07 PM

April 30, 2020 | View as webpage

TOP STORIES



LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

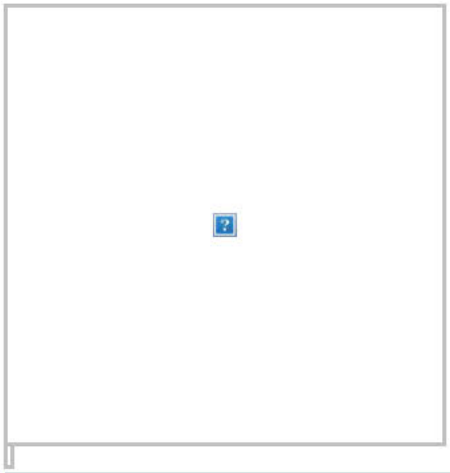
New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral



Real-Time Threats. Real-Time Detection.



The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE



5 steps to refine your COVID-19 social media strategy

By Cole Zercoe

Social media is the most

effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall

When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed

While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer course

By Sean Curtis
A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt
Follow these report-writing tips to improve the outcomes of your cases



SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.





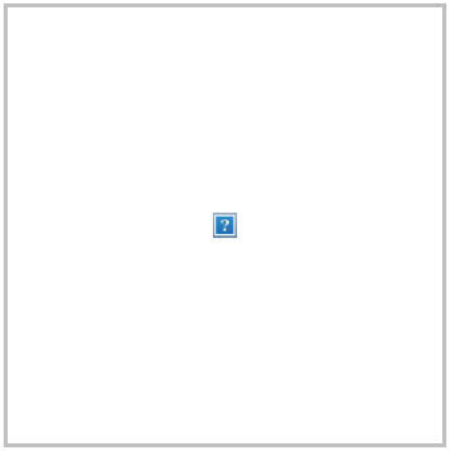
PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: Barry, Sean (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:36:06 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

April 30, 2020 | View as webpage

TOP STORIES



LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

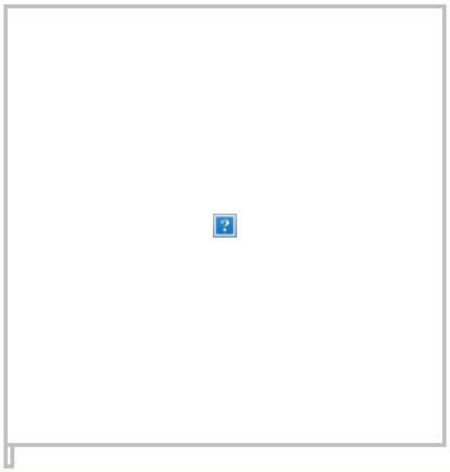
New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral



Real-Time Threats. Real-Time Detection.



The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE



5 steps to refine your COVID-19 social media strategy

By Cole Zercoe
Social media is the most effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall
When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed
While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer

3353

course

By Sean Curtis

A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt

Follow these report-writing tips to improve the outcomes of your cases



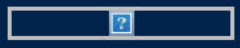
SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.





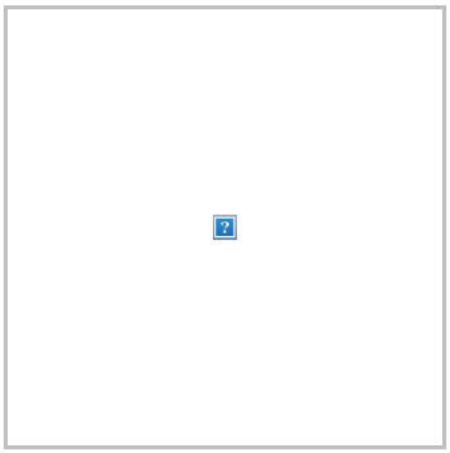
PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: Lenti, Jeffrey (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:35:32 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

April 30, 2020 | View as webpage

TOP STORIES



LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

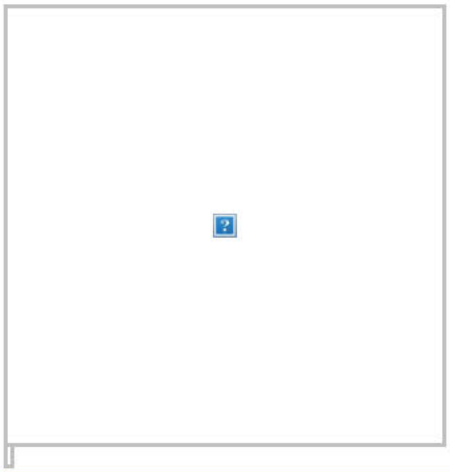
New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral



Real-Time Threats. Real-Time Detection.



The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE

5 steps to refine your COVID-19 social media strategy

By Cole Zercoe
Social media is the most effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall
When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed
While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer

3356

course

By Sean Curtis
A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt
Follow these report-writing tips to improve the outcomes of your cases



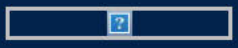
SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.





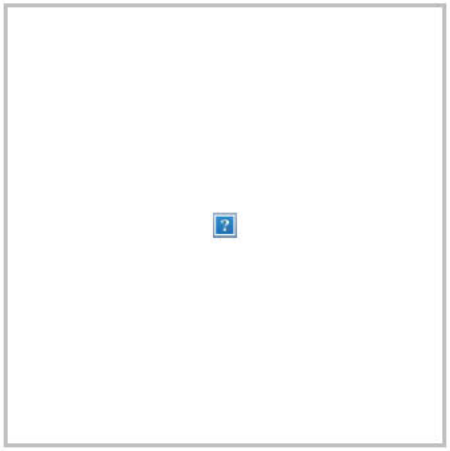
PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: Tapis, Stephen C (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:35:08 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

April 30, 2020 | View as webpage

TOP STORIES



LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

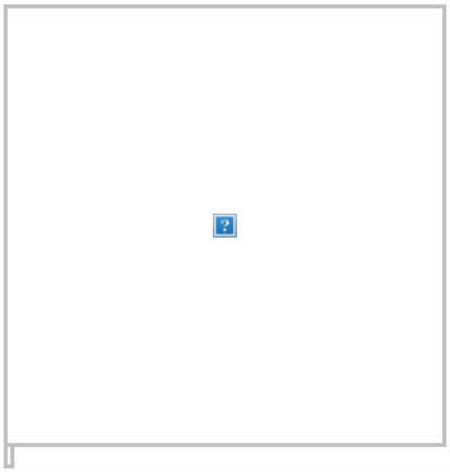
New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral



Real-Time Threats. Real-Time Detection.



The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE

5 steps to refine your COVID-19 social media strategy

By Cole Zercoe
Social media is the most effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall
When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed
While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer

3359

course

By Sean Curtis

A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt

Follow these report-writing tips to improve the outcomes of your cases



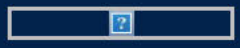
SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.



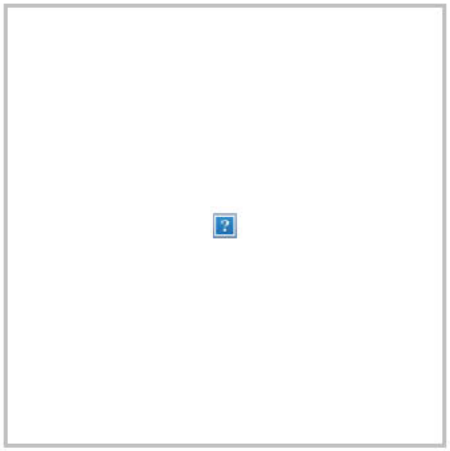


PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: PoliceOne Roll Call
To: Loiselle, Rachel (POL)
Subject: Video shows controversial Chicago OIS; Zero bail policy increasing offenses
Date: Thursday, April 30, 2020 5:40:46 PM

April 30, 2020 | View as webpage

TOP STORIES



LA police blame zero bail for rise in repeat offenders

In the first 30 days of the policy, the Los Angeles Police Department has arrested 213 individuals multiple times, with 23 being arrested three or more times

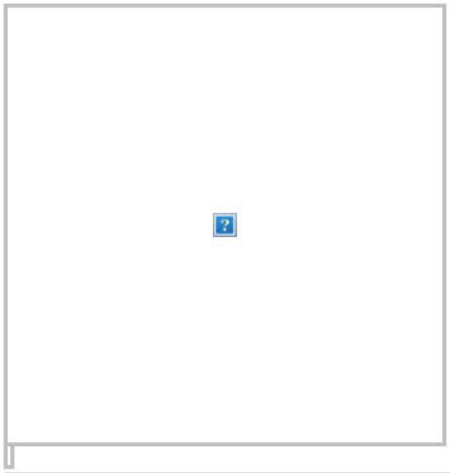
New video shows controversial Chicago OIS — and cops' scramble to tend to wounded man

NYPD disperses crowd of hundreds gathered for rabbi's funeral

Baltimore turns to aerial surveillance as homicides continue

Judge rules forced catheterizations unconstitutional

Boston cop's rendition of 'America the Beautiful' goes viral



Real-Time Threats. Real-Time Detection.



The MX908® is a multi-mission trace detection tool used for HazMat operations around the world to detect and identify toxic industrial chemicals, chemical warfare agents, drugs of abuse and explosives.

See it in action

COVID-19 SPECIAL COVERAGE



5 steps to refine your COVID-19 social media strategy

By Cole Zercoe

Social media is the most

effective community outreach tool PDs have during this pandemic, but online messaging comes with several challenges



How ALPRs can be a force multiplier for law enforcement in times of crisis

By Susan Crandall

When resources are limited, and human interaction should be kept at a minimum for the betterment of public health, ALPR technology can help



Police composite sketches & COVID-19

By Michael W. Streed

While the coronavirus pandemic has forced LE to alter the way it does business, technology is already enabling forensic artists to work remotely

Arm Yourself Properly



StrongArm® is a powerful yet portable, battery-powered rescue tool. It helps heroes cut, spread and breach doors with ease.

Learn more

How to ID Drugs Without Opening Packages



With a handheld narcotics analyzer, officers can scan the contents of suspicious bags and bottles to find out what's inside, enhancing scene safety.

Learn more

OTHER HIGHLIGHTS



What I learned from attending a red dot sights train-the-trainer course

By Sean Curtis
A 2-day course from NLEFIA shows why your department should adopt RDS for duty pistols



Let's be S.A.F.E. out there

By Steve Pratt
Follow these report-writing tips to improve the outcomes of your cases



SPONSORED CONTENT



Autism awareness: why it matters for law enforcement

Find out what police need to know about people with autism and what you can expect to learn from a new training course.





PoliceOne does not send unsolicited messages. You are receiving this email because you have signed up for PoliceOne and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters.

From: Police1 Roll Call
To: McCarthy, Steven (POL)
Subject: Video: Cop saves suicidal man; Viral police graduation ceremony
Date: Tuesday, October 20, 2020 1:45:56 PM

October 20, 2020 | View as webpage

Dear Police1 Member,

In the wake of the death of George Floyd, law enforcement has been inundated with demands for 'reform' with public officials nationwide reimagining public safety.

In Wednesday's Leadership Briefing newsletter, Police1 columnist Booker Hodges, who currently serves as assistant commissioner of law enforcement for the Minnesota Department of Public Safety, writes about the need to replace the term 'reform' with 'alignment' and shares three steps to help police departments better align with their communities.

Sign up today to ensure you receive a copy of the newsletter in your inbox.

Stay safe,

— *The Police1 Team*

TOP STORIES

Video: NJ cop stops man from jumping off building

"I love you," Officer Eric Knuttel told the complete stranger after rescuing him on top of a 13-story parking garage

DA: No charges for NY cops in fatal OIS that sparked protests

Acrobatic graduation ceremony for Egyptian Police goes viral

Police: NC cop hospitalized after he's beaten during arrest

Video: Atlanta Police use drone to arrest suspect in actor's shooting death

Mich. police chiefs' leader: Cops can't enforce open carry ban at polls

Where Officers in Crisis Can Get the Help They Need

A treatment center designed by first responders for first responders takes a medical, clinical and peer support approach to help police officers overcome addiction.

Read more

Get more than 20% OFF on Prisoner Training Manikin

The Ruth Lee Prisoner is a realistically sized & weighted training manikin. Its PVC reinforced wrists easily accommodate handcuffs & it's made with the same flame-retardant polyester as police vests, making it perfect for a variety of training scenarios.

Get discount from Alternate Force

FEATURED CONTENT

Opinion: Why the next generation of cops need a criminal justice degree

By Janay Gasparini, Ph.D.

Forging partnerships with faculty members at local colleges and universities can have a direct impact on the quality of officer candidates in your region

Comparing student and police chief executive views on drug use disqualifiers

for hiring

By A Johannes Bottema & Cody Telep

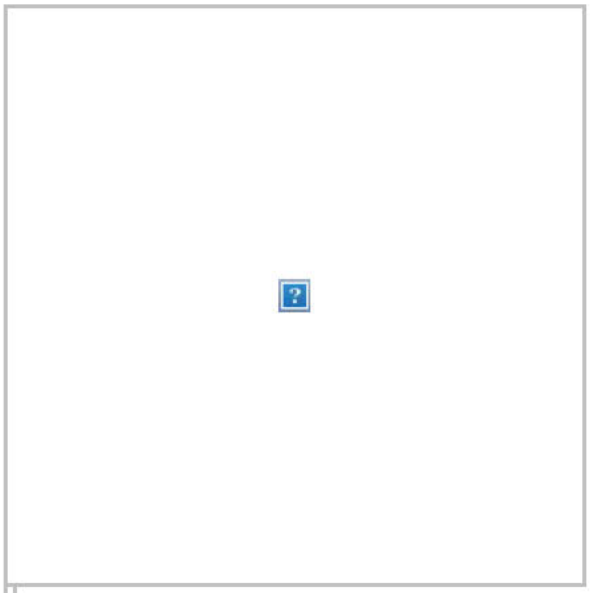
Overall, police leaders and students have different views about how drugs should be treated for hiring officers

Calling all Podcast Fans!



Our podcast, dubbed Hazard Class, covers all things related to the first response mission. Each week we'll bring listeners interesting stories, educational topics, and tips from the field. You don't want to miss this!

Check out the episodes today



OTHER HIGHLIGHTS



7 unusual police agencies you've probably never heard of

By Police1 Staff

From the police force that protects our nation's marine wildlife to

the New York cops who deal exclusively in sanitation issues



5 benefits of networking with your local game warden

By Steven Beltran

Conservation officers can be an invaluable resource for police investigations

FEATURED DEAL



Pangaro Training Guide - The Interview

Use POC10 for a 10% discount

FEATURED JOB



3211 - Deputy Sheriff (Lateral)

Pima County Sheriff's Department - Tuscon, Arizona

Entry Level: $25.50 hourly



Police1 does not send unsolicited messages. You are receiving this email because you have signed up for Police1 and subscribed to this newsletter. Click here to unsubscribe. Visit our Customer Support page to report any email problems or subscribe to our other newsletters. Copyright © 2020 Lexipol. 2611 Internet Blvd., Ste. 100, Frisco, TX 75034.

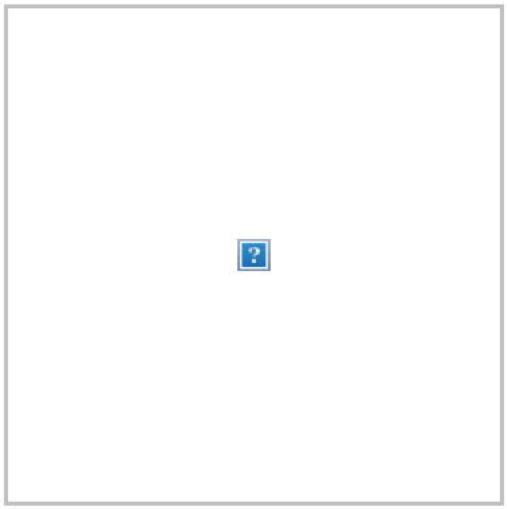
From: Traffic Technology Today
To: Griffin, Daniel (POL)
Subject: War of words erupts over Transport for London's £1.6bn government bailout
Date: Thursday, May 21, 2020 11:53:54 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

View this email online

TOP NEWS THIS WEEK

Covid-19: War of words erupts over Transport for London's £1.6bn government bailout



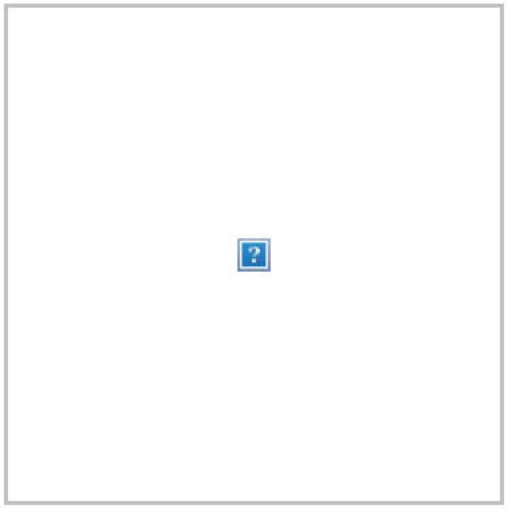
Transport for London (TfL) has secured a £1.6bn (US$2bn) bailout after passenger numbers on the capital's Underground and buses crashed by 90% at the height of the ongoing coronavirus lockdown. But now a war of words has erupted as to the state of TfL's underlying finances **more...**

More Covid-19 news...

- **Cargo bikes could help ease congestion in UK city post-lockdown**
- **Social distancing car park solution enables in-vehicle queuing**
- **ITS (UK) survey shows members finding new business opportunities**
- **ViaVan launches on-demand bus service for health workers in UK**

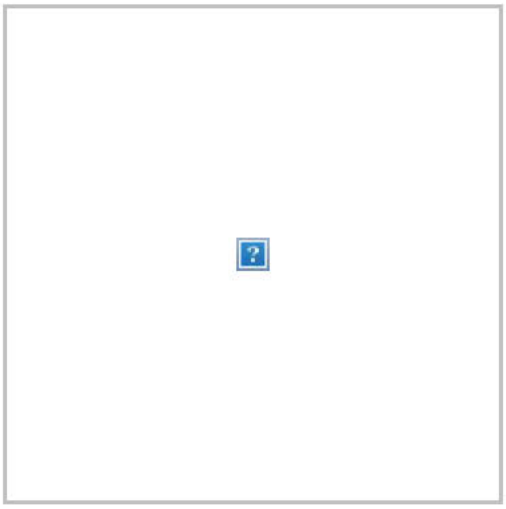
Bookmark our Covid-19 news hub, to stay up-to-date, every day

NEW AUDIO: Where should infrastructure investment be focused?



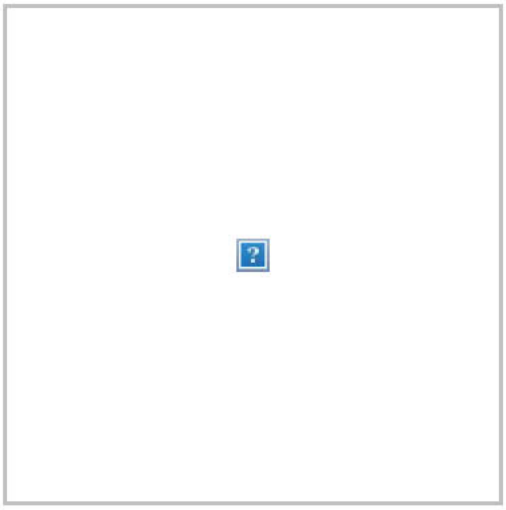
As the world looks toward economic recovery strategies to address the Covid-19 fallout, transportation infrastructure investment is high on the list of potential areas for growth. Bernie Wagenblast talks to Allie Kelly, executive director of Georgia transportation testbed The Ray, about some of the innovative, sustainable, ways in which officials should consider investing in the coming months **more...**

OPINION: What lessons have we learned from Covid-19?

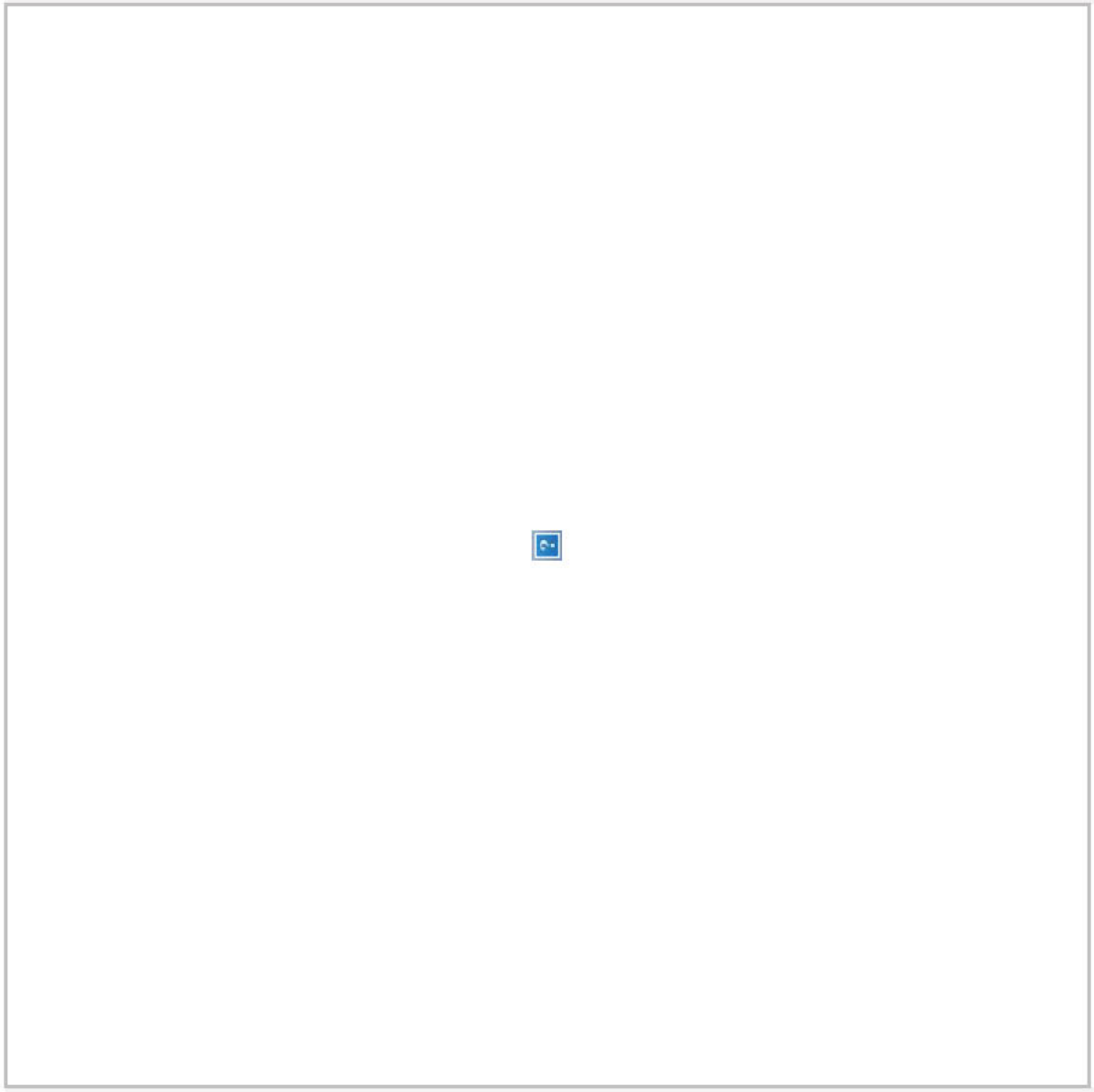


Paul Campion, CEO of the UK's TRL (Transport Research Laboratory) gives his opinion on the lessons we have learnt from the changes in transport use over the last couple of months and how they can inform future strategies.
"One of the things that makes it hard to think about how transport can change for the better, is that everything is hypothetical: it is usually impossible to experiment at scale" more...

OPINION: The challenges of CAVs and how to overcome them



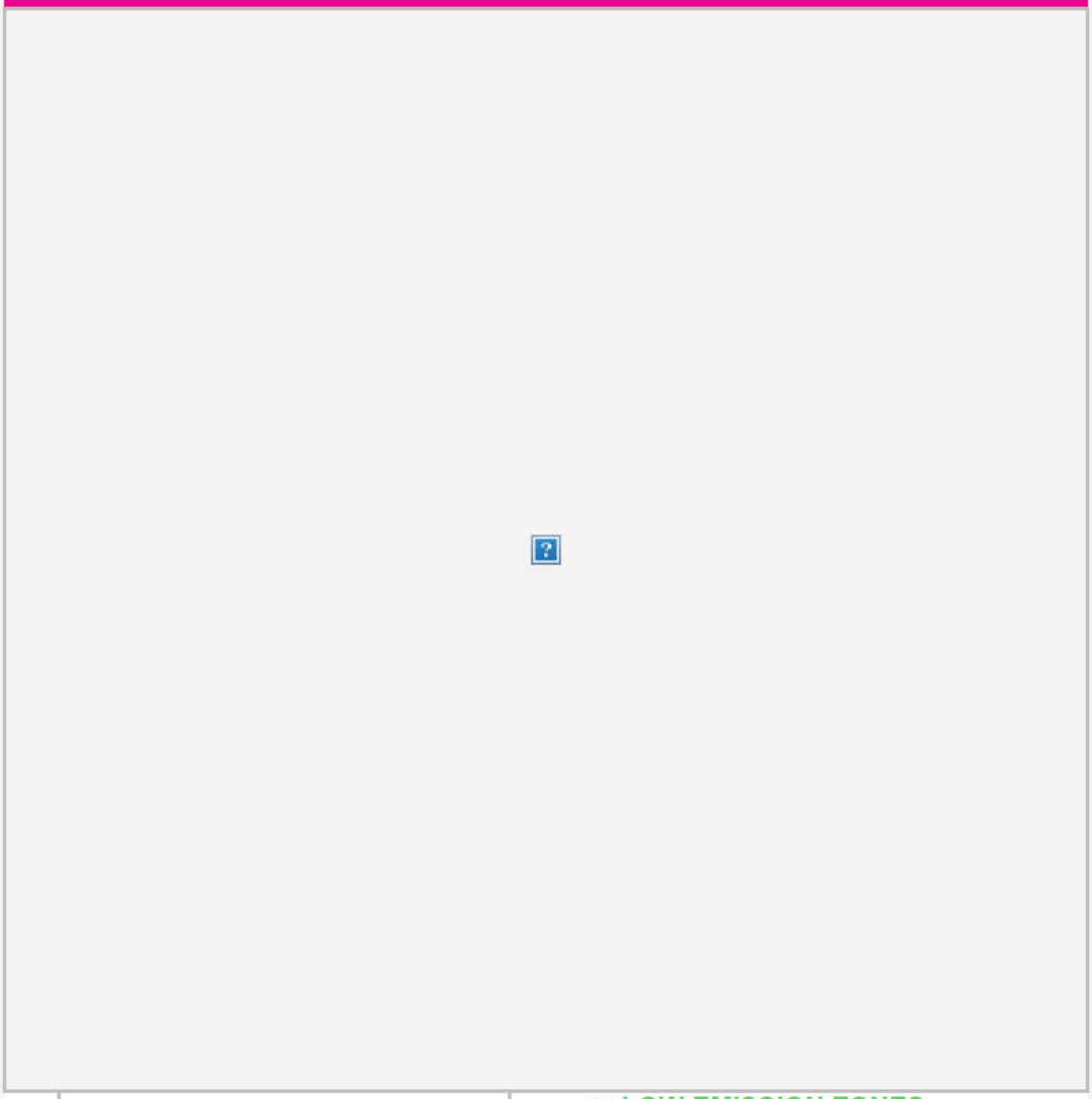
Matt D'Angelo PE, Transportation Systems Management and Operations (TSMO) practice leader at architecture and engineering consultancy Gresham Smith, gives his insight into the evolving world of connected and automated vehicles (CAVs) and gives his opinion on how we might overcome some of the challenges that lie ahead – from public acceptance to 5.9Ghz spectrum sharing. more...



MORE NEWS…

- Siemens wins major UK traffic signal equipment and ITS contract
- Q-Free developing new machine learning tech for ALPR
- Smart truck parking system rolled out in Calais, France
- The USA's National Operations Center of Excellence (NOCoE) announces TSMO Resource Connect Service
- South Carolina DOT upgrades traffic analysis with Iteris ClearGuide

NEW: DOWNLOAD FULL MAGAZINE PDF HERE

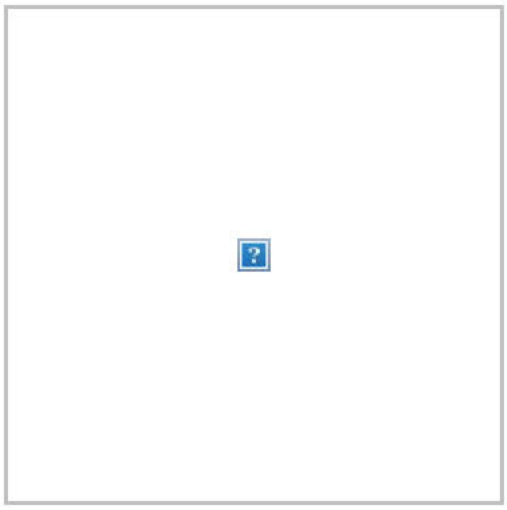




<< LOW EMISSION ZONES

JUST BE CAZ

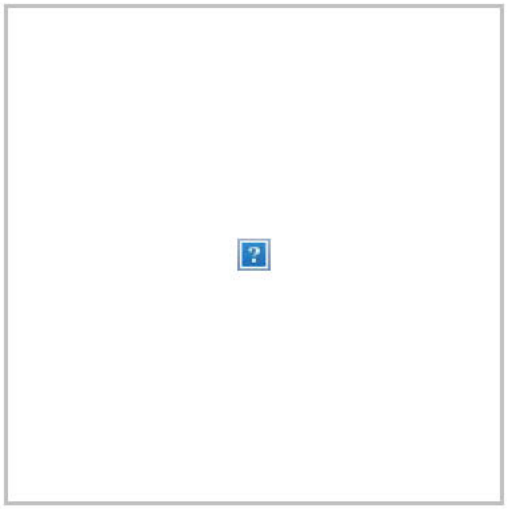
How the city of Birmingham's emissions-based private-car restrictions (the first in the UK outside London) will be enforced



<< WORKZONES

SMART WORKZONES AHEAD

Workzones are notoriously dangerous for those driving or working in them, but research into connected and automated technologies is helping to rectify this situation



<< COVID-19

GREG WINFREE

The Mode Warrior begins the debate on ways transportation in our interconnected world should change in order to better protect public health, in light of the coronavirus pandemic

CLICK HERE TO RECEIVE YOUR FREE COPY

If you wish to unsubscribe from Traffic Technology International News emails, please click here.

To understand how we process, use & safeguard your data, please read our Privacy Policy. If you would like to update your marketing contact preferences, then please click here.

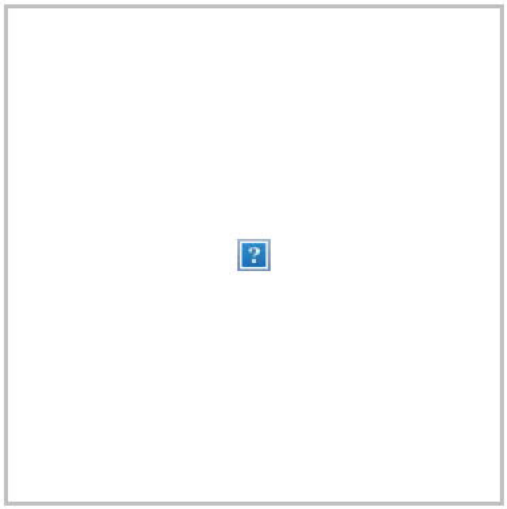
From: Traffic Technology Today
To: zzDowd, Timothy (POL)
Subject: War of words erupts over Transport for London's £1.6bn government bailout
Date: Thursday, May 21, 2020 11:55:45 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

View this email online

TOP NEWS THIS WEEK

Covid-19: War of words erupts over Transport for London's £1.6bn government bailout



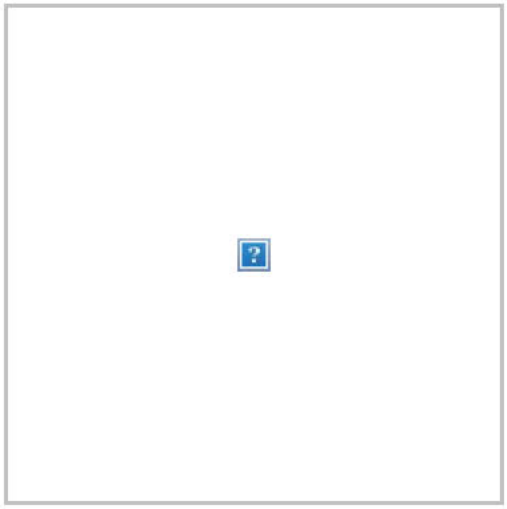
Transport for London (TfL) has secured a £1.6bn (US$2bn) bailout after passenger numbers on the capital's Underground and buses crashed by 90% at the height of the ongoing coronavirus lockdown. But now a war of words has erupted as to the state of TfL's underlying finances **more...**

More Covid-19 news...

- **Cargo bikes could help ease congestion in UK city post-lockdown**
- **Social distancing car park solution enables in-vehicle queuing**
- **ITS (UK) survey shows members finding new business opportunities**
- **ViaVan launches on-demand bus service for health workers in UK**

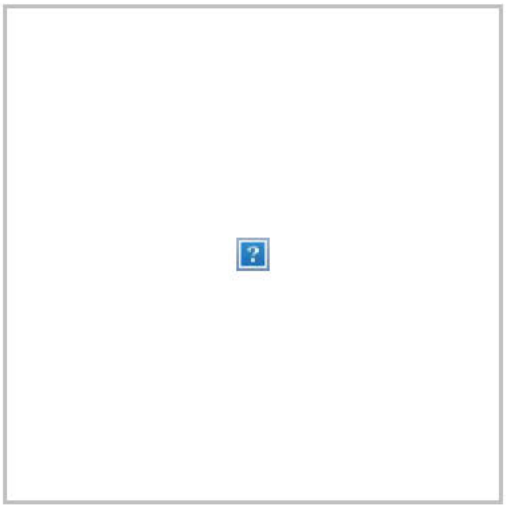
Bookmark our Covid-19 news hub, to stay up-to-date, every day

NEW AUDIO: Where should infrastructure investment be focused?



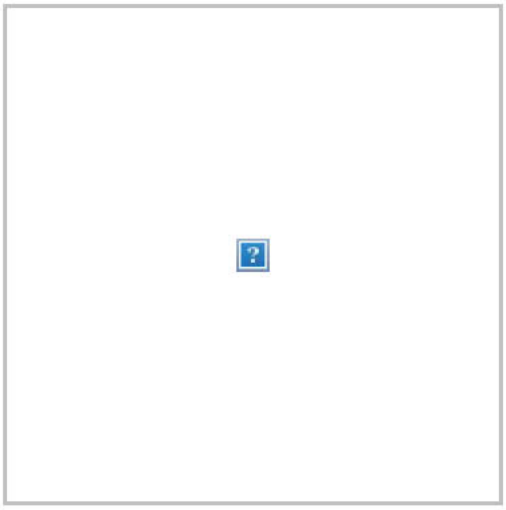
As the world looks toward economic recovery strategies to address the Covid-19 fallout, transportation infrastructure investment is high on the list of potential areas for growth. Bernie Wagenblast talks to Allie Kelly, executive director of Georgia transportation testbed The Ray, about some of the innovative, sustainable, ways in which officials should consider investing in the coming months **more...**

OPINION: What lessons have we learned from Covid-19?

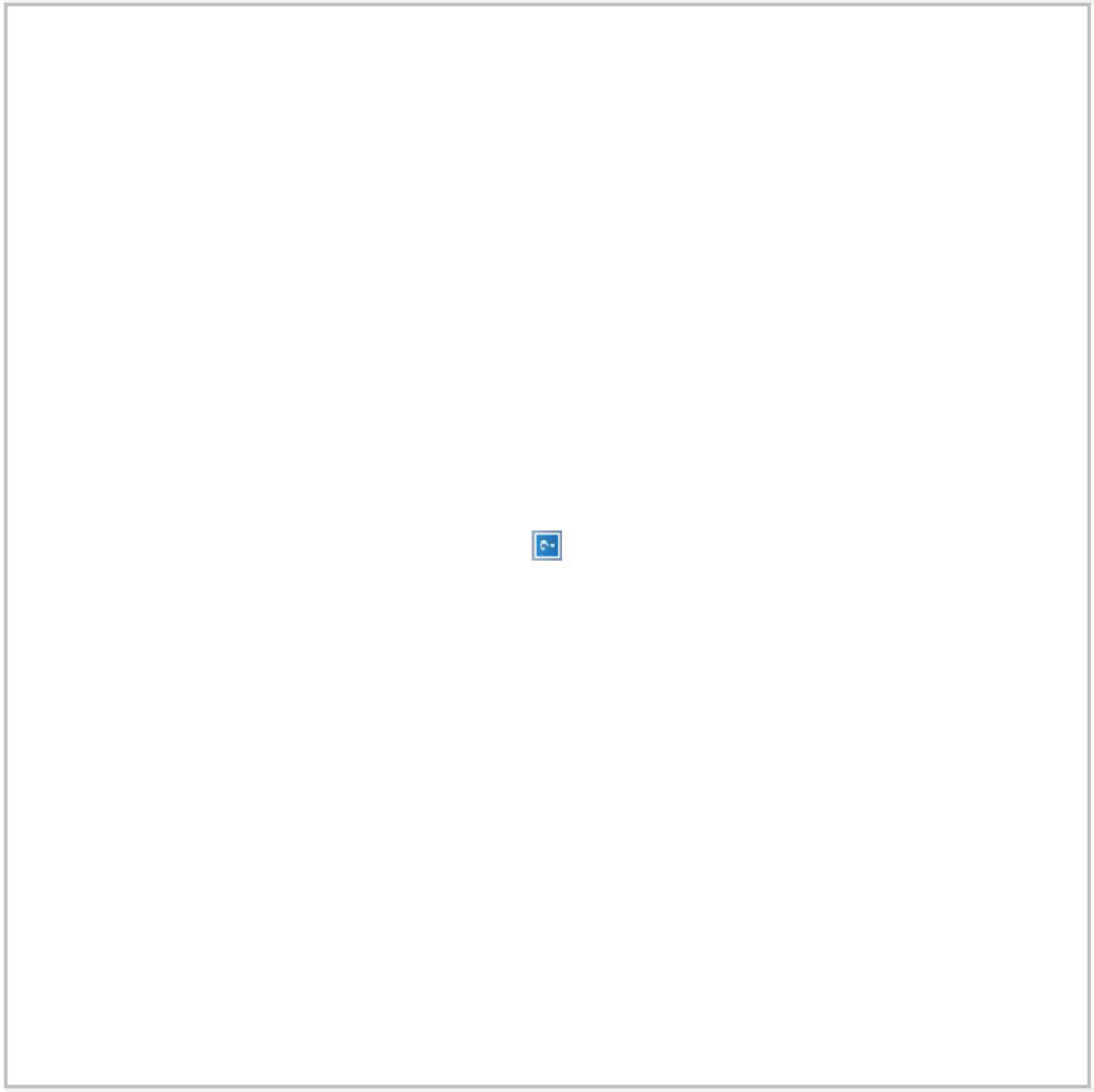


Paul Campion, CEO of the UK's TRL (Transport Research Laboratory) gives his opinion on the lessons we have learnt from the changes in transport use over the last couple of months and how they can inform future strategies.
"One of the things that makes it hard to think about how transport can change for the better, is that everything is hypothetical: it is usually impossible to experiment at scale" more...

OPINION: The challenges of CAVs and how to overcome them



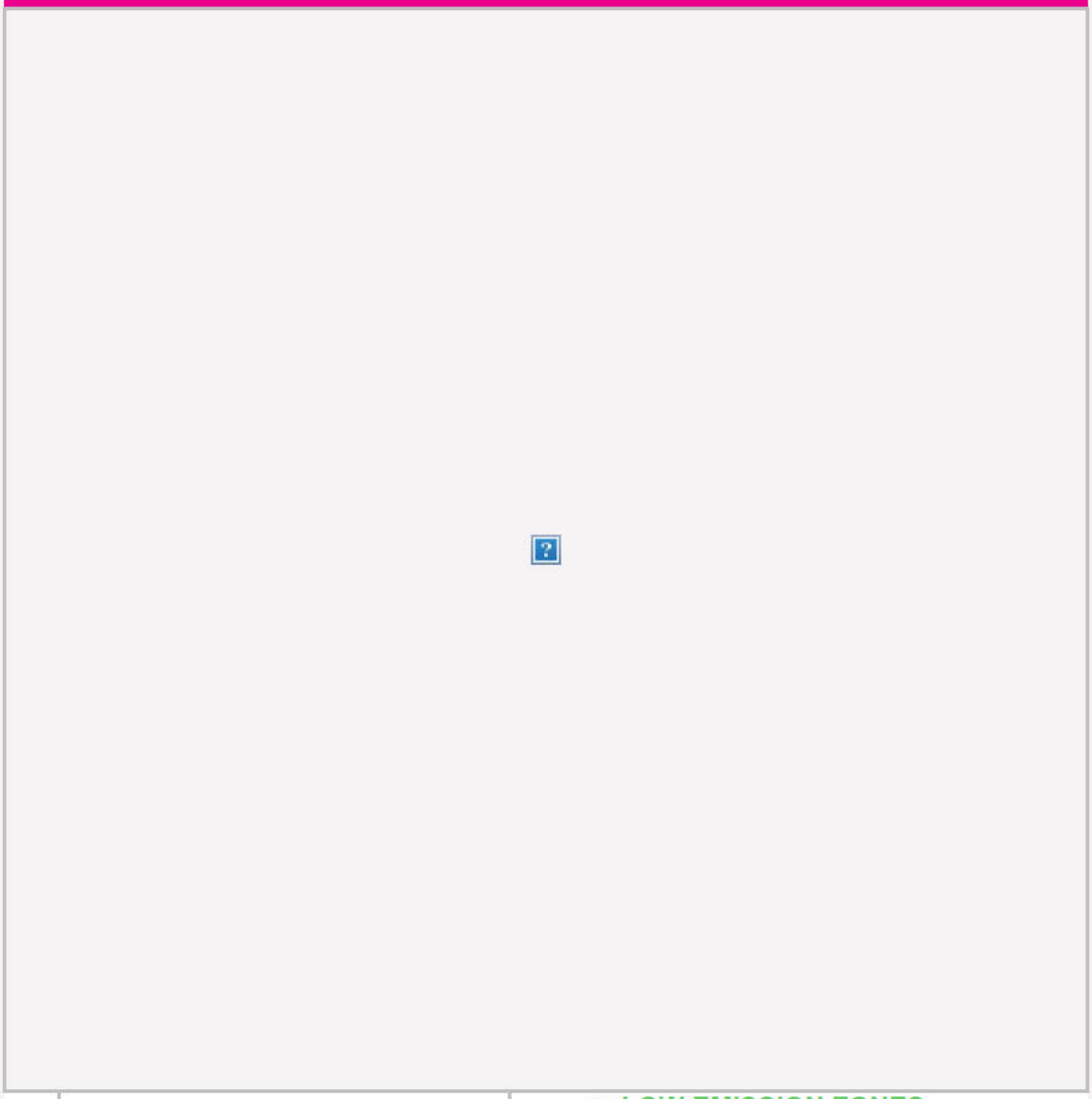
Matt D'Angelo PE, Transportation Systems Management and Operations (TSMO) practice leader at architecture and engineering consultancy Gresham Smith, gives his insight into the evolving world of connected and automated vehicles (CAVs) and gives his opinion on how we might overcome some of the challenges that lie ahead – from public acceptance to 5.9Ghz spectrum sharing. more...



MORE NEWS…

- Siemens wins major UK traffic signal equipment and ITS contract
- Q-Free developing new machine learning tech for ALPR
- Smart truck parking system rolled out in Calais, France
- The USA's National Operations Center of Excellence (NOCoE) announces TSMO Resource Connect Service
- South Carolina DOT upgrades traffic analysis with Iteris ClearGuide

NEW: DOWNLOAD FULL MAGAZINE PDF HERE

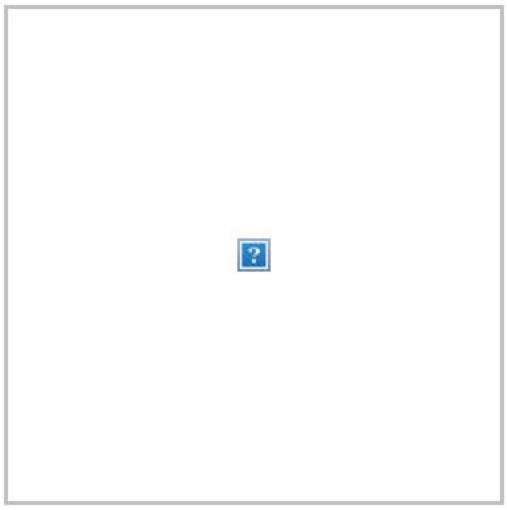




<< LOW EMISSION ZONES

JUST BE CAZ

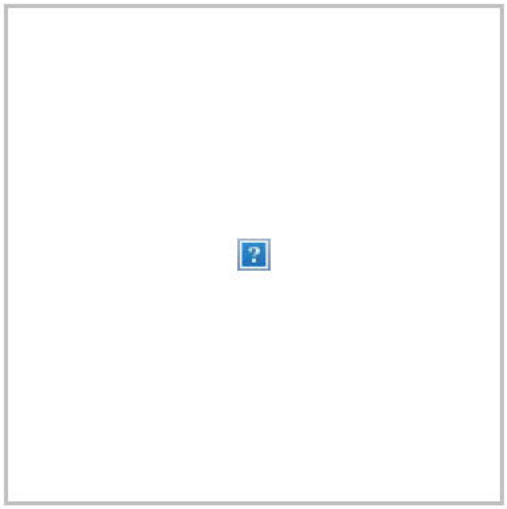
How the city of Birmingham's emissions-based private-car restrictions (the first in the UK outside London) will be enforced



<< WORKZONES

SMART WORKZONES AHEAD

Workzones are notoriously dangerous for those driving or working in them, but research into connected and automated technologies is helping to rectify this situation



<< COVID-19

GREG WINFREE

The Mode Warrior begins the debate on ways transportation in our interconnected world should change in order to better protect public health, in light of the coronavirus pandemic

CLICK HERE TO RECEIVE YOUR FREE COPY

If you wish to unsubscribe from Traffic Technology International News emails, please click here.

To understand how we process, use & safeguard your data, please read our Privacy Policy. If you would like to update your marketing contact preferences, then please click here.

From: Apple News
To: Gamache, Alan (POL)
Subject: What"s in the new stimulus deal, West Point accuses 70 cadets of cheating, and more from Apple News
Date: Tuesday, December 22, 2020 7:55:11 AM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Good Morning From Apple News

It's December 22, 2020.

Here's what you need to know.

Good Morning From Apple News

It's December 22, 2020.

Here's what you need to know.

TOP STORIES

TOP STORIES

CONGRESS PASSED a $900 billion pandemic-relief package after months of haggling, and President Trump should sign the bill in the coming days. Here's what's in the deal, and when stimulus checks are expected to arrive. NBC NEWS

Congress passed a $900 billion pandemic-relief package after months of haggling, and President Trump should sign the bill in the coming days. Here's what's in the deal, and when stimulus checks are expected to arrive. NBC NEWS

PRESIDENT-ELECT BIDEN received his first dose of Pfizer's COVID-19 vaccine on live TV. Meanwhile, Moderna's shot arrived at hospitals around the country. CBS NEWS

President-elect Biden received his first dose of Pfizer's COVID-19 vaccine on live TV. Meanwhile, Moderna's shot arrived at hospitals around the country. CBS NEWS

THE SPRAWLING RECENT CYBERATTACK on U.S. agencies compromised the email accounts of several top Treasury Department officials, one senior senator said. Investigators are still scrambling to understand the scope of the suspected Russian hack. THE WALL STREET JOURNAL

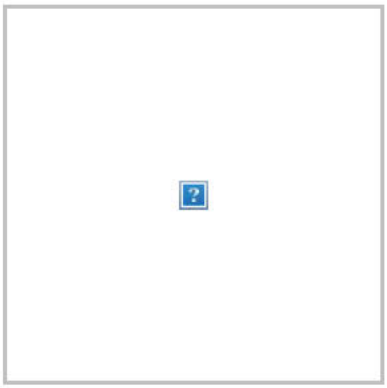
The sprawling recent cyberattack on U.S. agencies compromised the email accounts of several top Treasury Department officials, one senior senator said. Investigators are still scrambling to understand the scope of the suspected Russian hack. THE WALL STREET JOURNAL

ATTORNEY GENERAL WILLIAM BARR said he saw no reason to appoint a special counsel to investigate charges of voter fraud, breaking with Trump, who continues to contest the election results without evidence. POLITICO

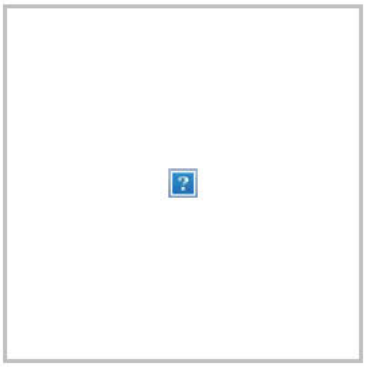
Attorney General William Barr said he saw no reason to appoint a special counsel to investigate charges of voter fraud, breaking with Trump, who continues to contest the election results without evidence. POLITICO

LISTEN NOW

LISTEN NOW

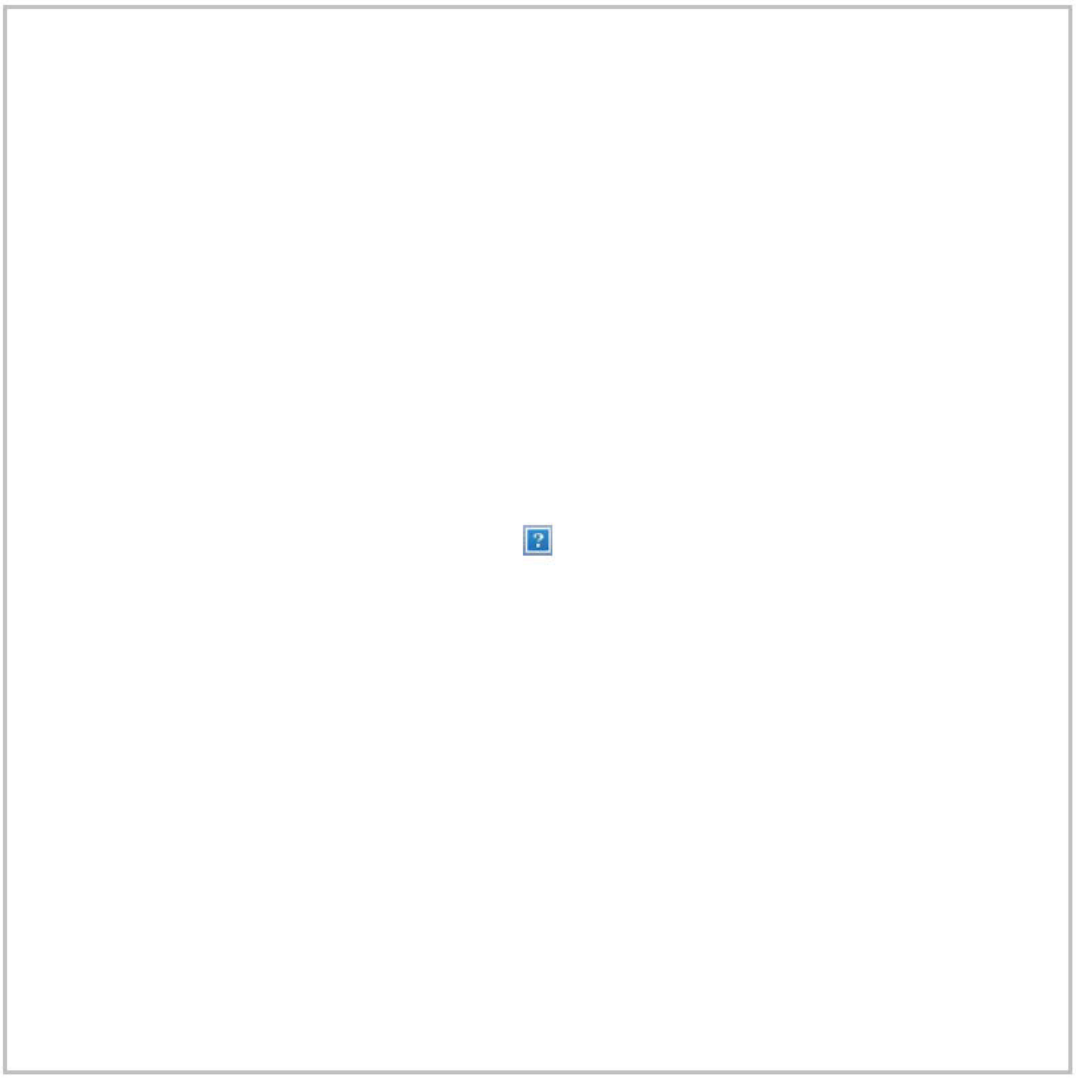


Inside the 5,593-page relief bill, the history of the Christmas tree, and more on today's podcast. APPLE NEWS TODAY



Inside the 5,593-page relief bill, the history of the Christmas tree, and more on today's podcast. APPLE NEWS TODAY

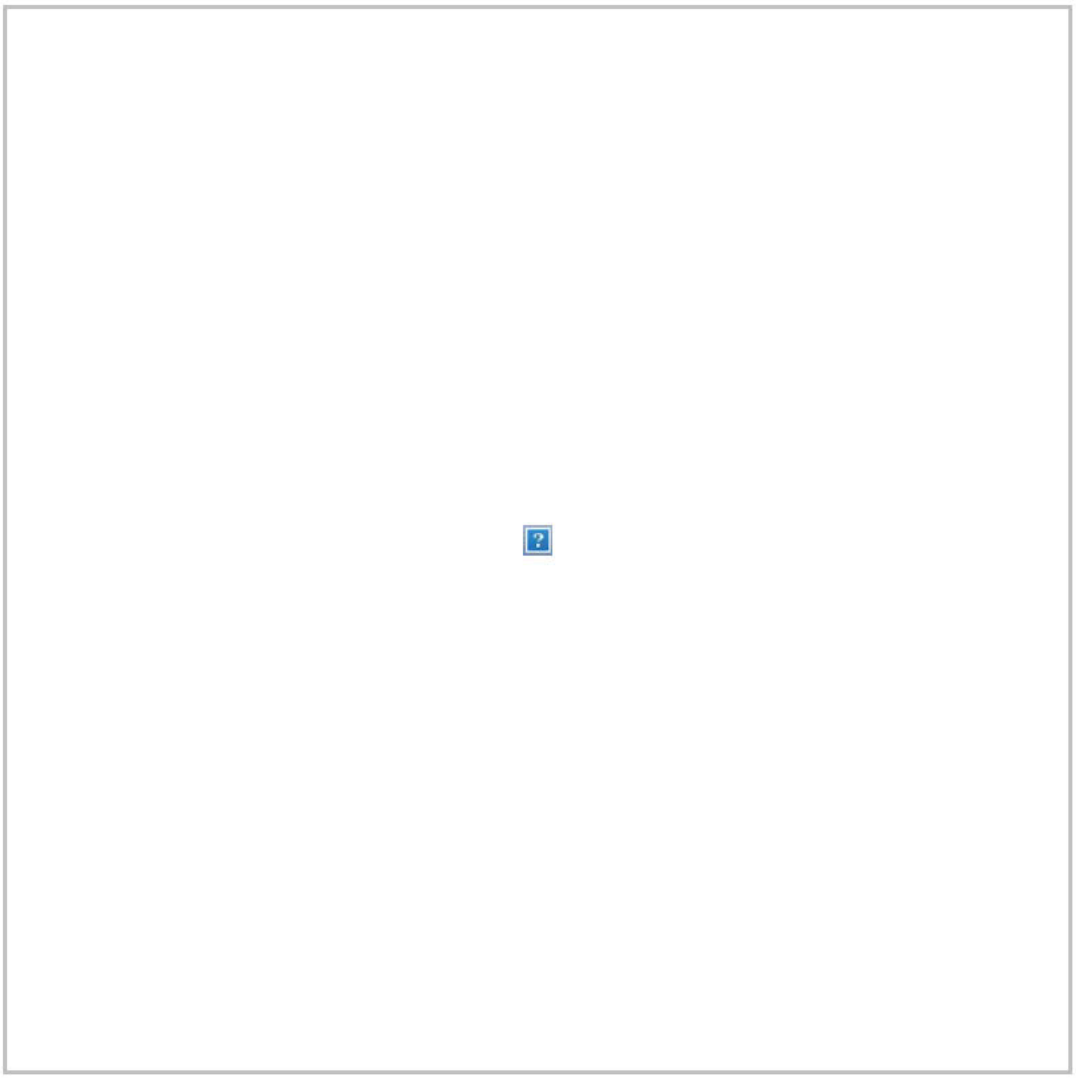
YEAR IN REVIEW



The Most Scandalous Stories of the Year

Featuring Jeffrey Epstein's closest confidant, the pool attendant who took down the Falwells, the spring breakers who sparked a COVID-19 outbreak, and more. APPLE NEWS SPOTLIGHT

YEAR IN REVIEW



The Most Scandalous Stories of the Year

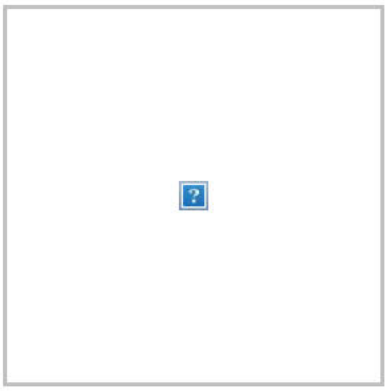
Featuring Jeffrey Epstein's closest confidant, the pool attendant who took down the Falwells, the spring breakers who sparked a COVID-19 outbreak, and more. APPLE NEWS SPOTLIGHT

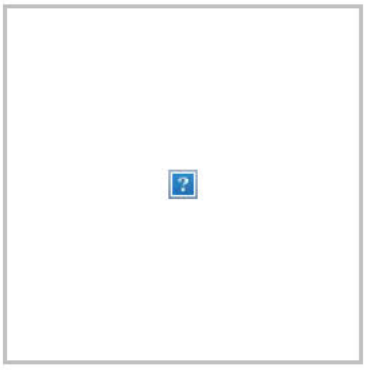


FIVE STORIES WE'RE TALKING ABOUT

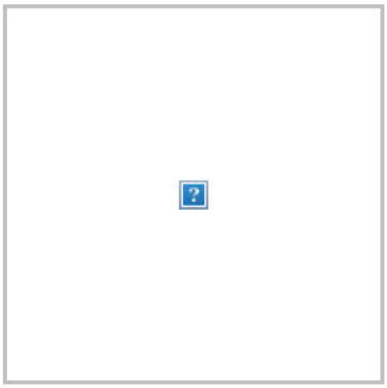
FIVE STORIES WE'RE TALKING ABOUT

Everything we know about the new coronavirus variant in the UK. STAT





Everything we know about the new coronavirus variant in the UK. STAT

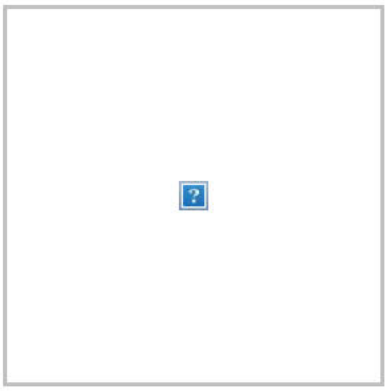


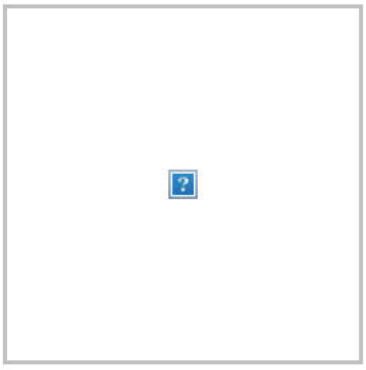
The Putin critic who was poisoned in August says he duped a Russian spy into revealing the details of the operation. CNN



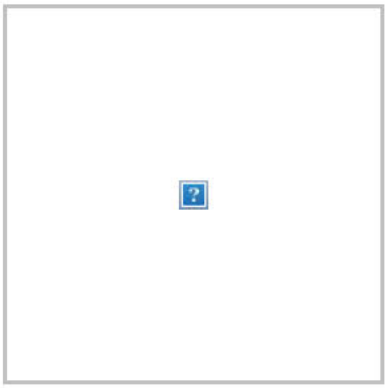
The Putin critic who was poisoned in August says he duped a Russian spy into revealing the details of the operation. CNN

West Point accused 70 cadets of cheating on an online math exam. USA TODAY

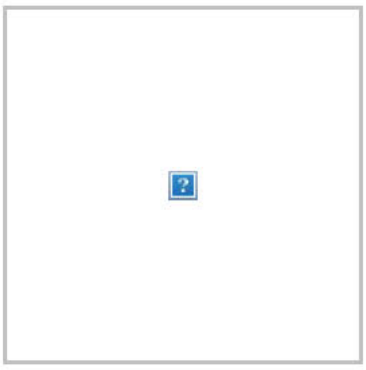




West Point accused 70 cadets of cheating on an online math exam. USA TODAY

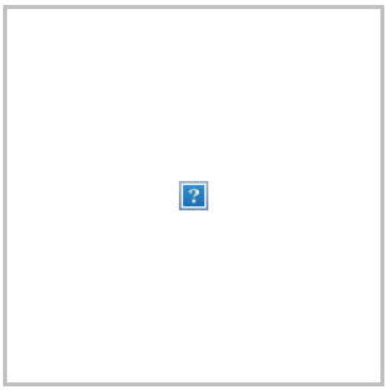


In a quest to find her birth family, a woman made a life-altering discovery: She's a princess. NBC NEWS



In a quest to find her birth family, a woman made a life-altering discovery: She's a princess. NBC NEWS

For all the procrastinators out there: Here's the ultimate last-minute holiday gift guide. APPLE NEWS



SPOTLIGHT



For all the procrastinators out there: Here's the ultimate last-minute holiday gift guide. APPLE NEWS SPOTLIGHT

THE LAST WORD

"People are shaking their heads wondering what in the world has gotten into this man."

Senator Mitt Romney called Trump's ongoing efforts to overturn the election results "sad" and "embarrassing." BUSINESS INSIDER

THE LAST WORD

"People are shaking their heads wondering what in the world has gotten into this man."

Senator Mitt Romney called Trump's ongoing efforts to overturn the election results "sad" and "embarrassing." BUSINESS INSIDER

Try Apple News+ for Free



Try Apple News+ for Free

Some content requires specific hardware or software. Internet access required; data fees may apply. Content availability is subject to change. For more information, click here.

Copyright © 2020 Apple Inc. One Apple Park Way, Cupertino, California 95014 USA

Privacy Policy | Terms and Conditions | Support | Account

Unsubscribe

Some content requires specific hardware or software. Internet access required; data fees may

apply. Content availability is subject to change. For more information, click here.

Copyright © 2020 Apple Inc. One Apple Park Way, Cupertino, California 95014 USA

Privacy Policy | Terms and Conditions | Support | Account

Unsubscribe

From: Axon Enterprise, Inc.
To: McCarthy, Steven (POL)
Subject: You're Invited: CEO Roundtables on ALPR Policy and The Future of UAV's
Date: Thursday, July 30, 2020 5:20:02 PM

Axon

CEO Roundtables on ALPR Policy and The Future of UAV's

Our AI Ethics Board is preparing to release its recommendations on best practices and model policies for ALPR systems. This is your chance to get a preview of their recommendations — and, more importantly, to give your feedback on these important issues.

Rick Smith, Axon CEO and Founder, is hosting back-to-back technology roundtables on August 11th to share the draft report on ALPR best practices from our AI Ethics Board, followed by a session on the future of Unmanned Aerial Vehicles in Public Safety.

- **ALPR Ethics, Policy and Best Practices: August 11, 9 a.m. PT**
  Rick will discuss ethics-first design of ALPRs and how that aligns with police reform efforts and where the technology is going. Joining him will be Flock Safety CEO and Founder, Garret Langley. The Axon AI Ethics Board is an independent body that is rapidly gaining influence among both law enforcement and community/justice reform communities. This is a chance to make sure your voice is heard before their final report is issued.

- **Future of UAV's: August 11, 10:30 a.m. PT**
  Rick will be joined by Aydin Ghajar, who ran Uber's premium ride business before joining Axon as GM of Axon Air. This session will include a survey of emerging UAV technologies including potential partners that could be integrated into the Axon ecosystem.

These roundtables will run back-to-back for people interested in attending both sessions. There is a single registration link here:

Register Now

One registration gives you access to both events - simply join at 9 or 10:30 based on your interest area.

These sessions are closed to only sworn law enforcement attendees.

If you have any questions, please contact Jack Nolan at Axon.

Stay safe,
Axon

Axon Enterprise, Inc. | 17800 N. 85th St. | Scottsdale, AZ 85255-6311, USA

Your privacy is important to us. You are receiving this email either because you are a customer of Axon or because you have opted in to receive communications from us. If you prefer not to receive updates, you can unsubscribe here. The 'Delta Axon' logo, Axon Citizen and Axon are trademarks of Axon Enterprise, Inc., some of which are registered in the US and other countries.

All Rights Reserved. © 2020 Axon Enterprise, Inc.

Privacy Policy

Contact Us

Unsubscribe





From: Serra, Anthony F (POL)
To: 91111-33928506@requests.muckrock.com
Subject: Your Request
Date: Thursday, May 7, 2020 9:29:00 AM

Good Morning,

The Department of State Police ("Department") has received your request for the following records:

1. All use of force reports from Troop E and A at Westfield Massachusetts [S]tate [P]olice barracks, from January 1, 2017 until the date that this request is processed;
2. The names of agencies and organizations with which the Agency shares ALPR data;
3. The names of agencies and organizations with which the Agency receives ALPR data;
4. The names of agencies and organizations with which the Agency shares "hot list" information
5. What is "hot list" information and I would like my personal record of what shows up when my license plate is scanned – License Plate 289ve4, by MSP.

The Department considers your request as a submission under M.G.L. c. 66, §10, the Public Records Law. As you recall, the Department responded to your first request on April 21, 2020 and provided you with a fee estimate. The Department submits the following in response to requests 2-5. Please be advised that the Department does not use the system referenced in your request, however please note the following responses:

- #2 – The Agency shares ALPR data with State, Local, and Federal law enforcement agencies that are approved to access Public Safety data.
- #3 – The Agency shares data with any law enforcement agency that submits information to the server.
- #4 – The Agency shares Hotlist data, when appropriate, to State, Local, and Federal law enforcement Agencies that are approved to access Public Safety data.

As for request #5, the Department has identified the following definition as responsive:

> Hotlists are lists containing "[l]icense plate numbers of vehicles of interest, such as stolen vehicles, unregistered vehicles, vehicles owned by persons of interest, and vehicles associated with AMBER Alerts, Missing Child Alerts, Missing College Student Bulletins, Silver Alerts, Incapacitated or Endangered Persons, Be On Look Out (BOLO), Attempt To Locate (ATL), and Wanted or Missing Person broadcasts or bulletins in which a license plate number is included, or other license plate numbers of interest entered by the Department or an authorized officer."

As for your request for "[your] personal record of what shows up when [your] license plate is scanned," the Department asserts that this information is exempt under G.L. c. 4, §7 cl. 26(f) (investigative exemption), which specifically exempts from public disclosure investigatory materials necessarily compiled out of the public view by law enforcement or other investigatory officials the disclosure of which materials would probably so prejudice the possibility of effective law enforcement that such disclosure would not be in the public interest. The policy considerations underlying the exemption are well settled. *See Bougas v. Chief of Police*, 371 Mass. 59, 62 (1976) (among them "avoidance of premature disclosure of the Commonwealth's case prior to trial, the prevention of the disclosure of confidential investigative techniques, procedures, or sources of information, the encouragement of individual citizens to come forward and speak freely with police concerning matters under investigation, and the creation of initiative that police officers might be completely candid in recording their observations, hypotheses and interim conclusions"). The

general rule is that investigative materials may only be withheld if disclosure will affect investigative efforts in general.

Although under M.G.L. c. 66, § 6A, a records access officer is not "required to create a new public record in order to comply with a request," the Department asserts that the hotlist information is compiled out of the public view by law enforcement officials for the purpose of aiding in the investigation of the above-referenced situations and the entry of information in the hot file is based on the need identified by a criminal justice agency for purposes of investigation, promoting the situational awareness of law enforcement officers and addressing public safety issues. Similarly, the database in which this information is kept is investigative in nature. By disclosing "what shows up when [your] license plate is scanned," the Department is, in effect, disclosing whether or not your license plate number has been entered into the list by the Department or an authorized officer. Generally speaking, this type of disclosure would affect investigatory efforts in general in that it would allow any individual to determine whether a vehicle they are associated with is a vehicle of interest by simply submitting this type of request. With knowledge of this information, it would aid the individual's ability to circumvent law enforcement efforts and impede all types of investigations.

If you wish to challenge any aspect of this response, you may appeal to the Supervisor of Public Records following the procedure set forth in 950 C.M.R. 32.08, a copy of which is available at http://www.mass.gov/courts/case-legal-res/law-lib/laws-by-source/cmr/. You may also file a civil action in accordance with M.G.L. c. 66, § 10A. Please contact me if you have any questions or concerns. Thank you for your attention in this matter.

Anthony Serra
Staff Legal Counsel
Office of Chief Legal Counsel
Massachusetts State Police
470 Worcester Road
Framingham, MA 01702
Telephone: (508) 820-2391

The preceding email message (including any attachments) contains information that may be confidential, may be protected by the attorney-client or other applicable privileges, or may constitute non-public information. It is intended to be conveyed only to the designated recipient(s) named above. If you are not an intended recipient of this message, please notify the sender by replying to this message and then delete all copies of it from your computer system. Any use, dissemination, distribution, or reproduction of this message by unintended recipients is not authorized and may be unlawful.

From: WatchGuard
To: McCarthy, Steven (POL)
Subject: Your Technology Should Do More
Date: Monday, March 23, 2020 7:13:07 PM

CAUTION: This email originated from a sender outside of the Commonwealth of Massachusetts mail system. Do not click on links or open attachments unless you recognize the sender and know the content is safe.

Not rendering correctly? View this email as a web page here.

ALPR-in-car-1with WG Logos-blur-email-600

Your Technology Should Do More

Your first responders do more — why shouldn't your technology? By joining the power of license plate recognition to a WatchGuard 4RE In-Car system, your team can turn static data into actionable intelligence.

Several subscription options are available to maximize your current investments all while increasing your in-field data capturing capabilities. Choose the subscription that fits your agency's needs. Whether simply activating a current 4RE In-Car system with LPR capabilities, purchasing a new 4RE system with LPR, or adding Vigilant mobile LPR cameras to the system, your team can significantly enhance data capture, gain automated alerts, and leverage your technology to do more.



WatchGuard Video
415 E Exchange Parkway
Allen, TX 75002
USA

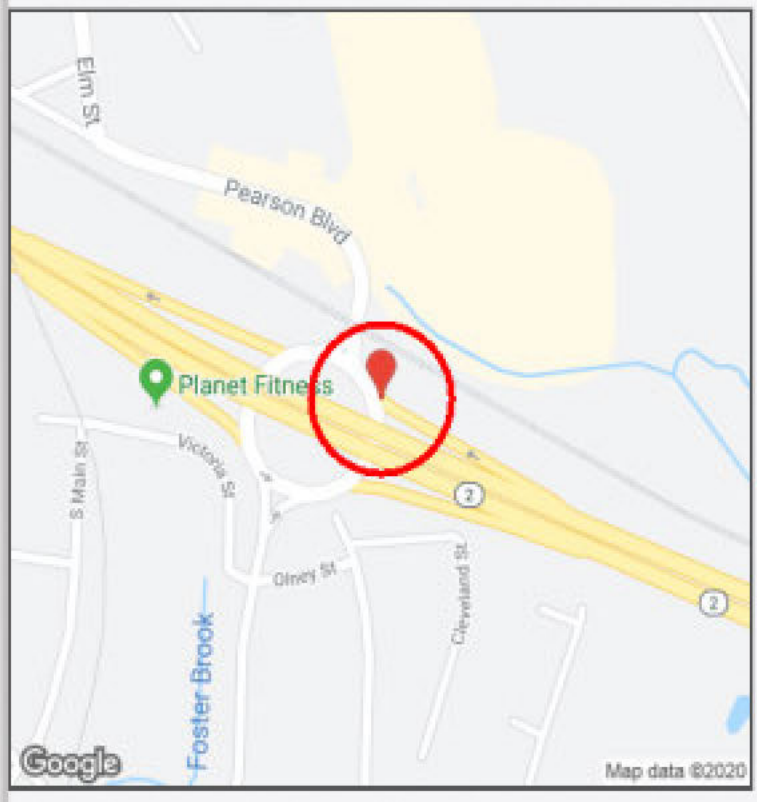
You received this email because you are subscribed to Products from WatchGuard Video.

Update your email preferences to choose the types of emails you receive.

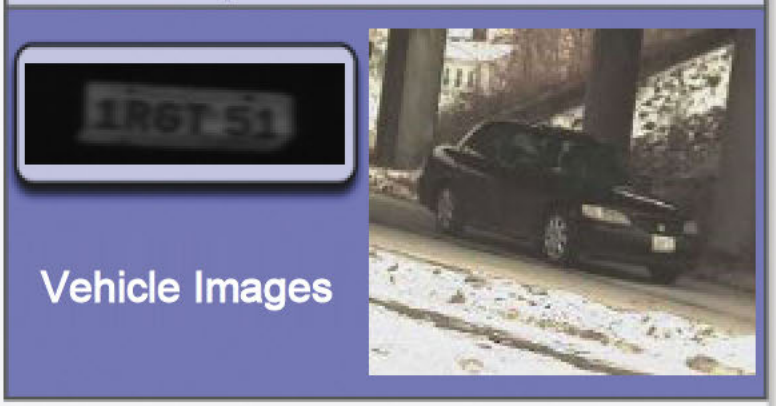
Unsubscribe from all future emails

Vehicle Detection Report

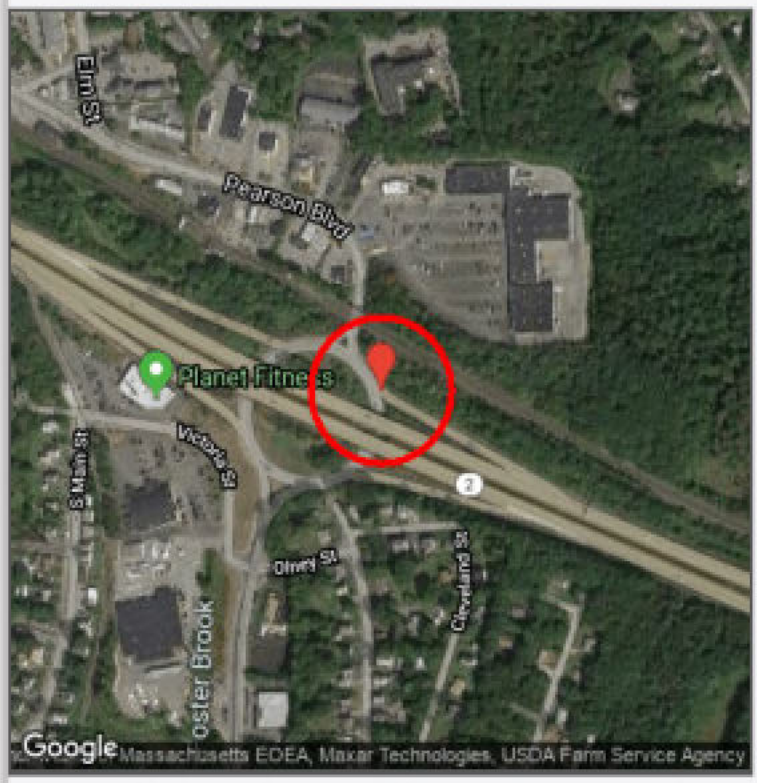
License Plate Number: 1RGT51



Powered By: VIGILANT SOLUTIONS



Vehicle Spotted:
01-07-20 at 3:45:43 PM EST



Detection Data

Vehicle Info

Plate # 1:	1RGT51
Plate # 2:	1RG151
Date:	01-07-20
Time:	3:45:43 PM
Longitude:	-71.978381
Latitude:	42.564358

Camera Info

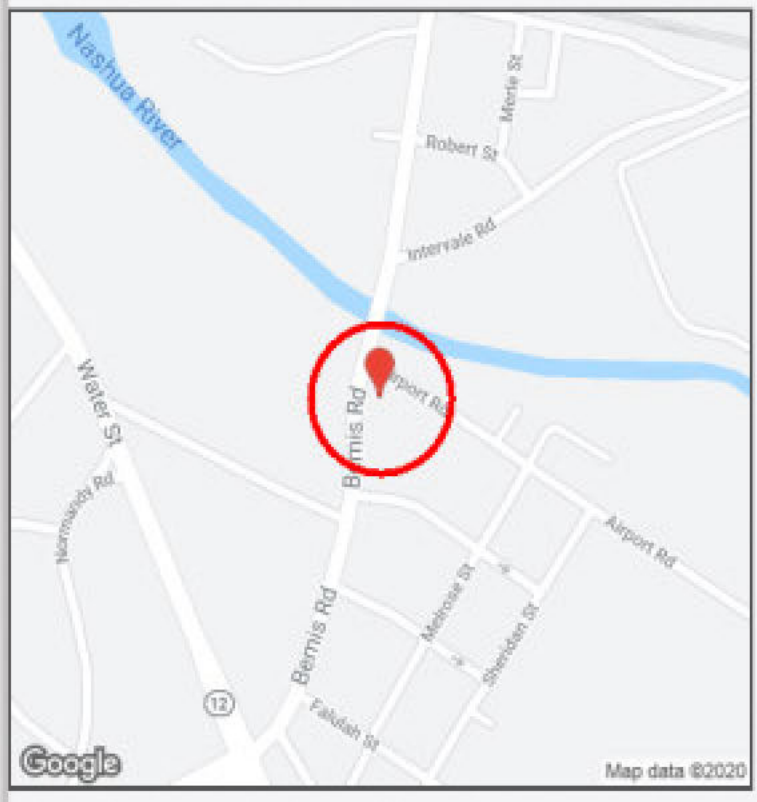
Agency:	N/A
User:	Commercial Data
System:	Commercial System
Camera:	N/A
Type:	N/A

Nearest Address:	Vfw Cir Gardner, MA 01440
Nearest Intersection:	Vfw Cir George W Stanton Hwy

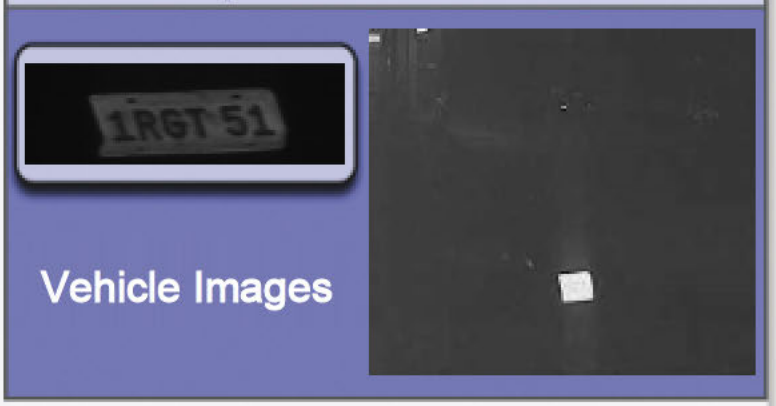
Disclaimer: The address listed above is ONLY an estimate.

Vehicle Detection Report

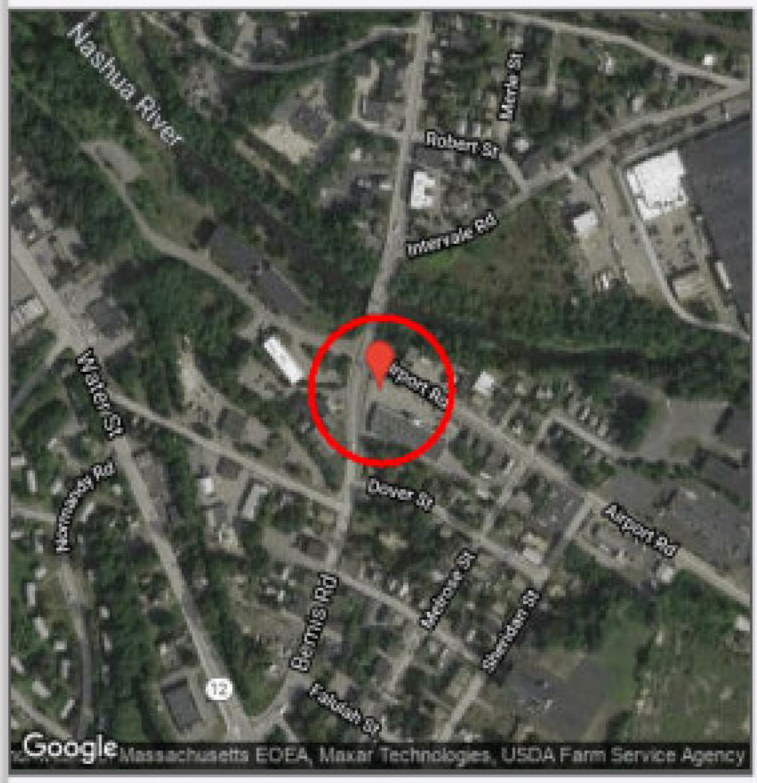
License Plate Number: 1RGT51



Powered By: VIGILANT SOLUTIONS



Vehicle Spotted:
09-24-19 at 11:58:06 PM EDT



Detection Data

Vehicle Info

Plate # 1:	1RGT51
Plate # 2:	1RG151
Date:	09-24-19
Time:	11:58:06 PM
Longitude:	-71.778901
Latitude:	42.567072

Camera Info

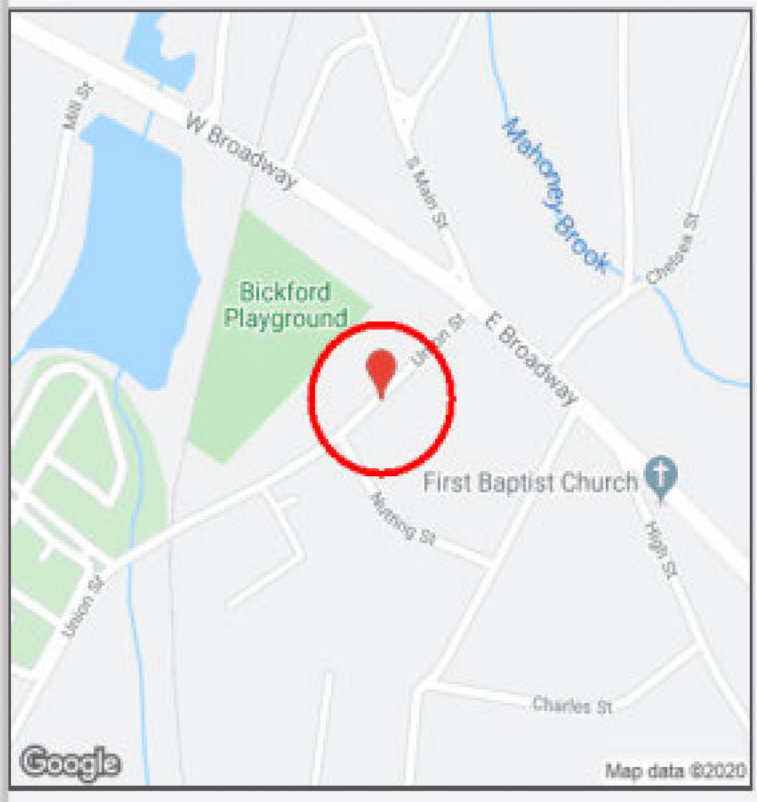
Agency:	N/A
User:	Commercial Data
System:	Commercial System
Camera:	N/A
Type:	N/A

Nearest Address:	23 Airport Rd Fitchburg, MA 01420
Nearest Intersection:	Airport Rd Bemis Rd

Disclaimer: The address listed above is ONLY an estimate.

Vehicle Detection Report

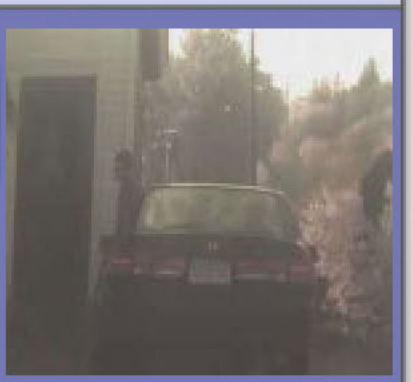
License Plate Number: 1RGT51



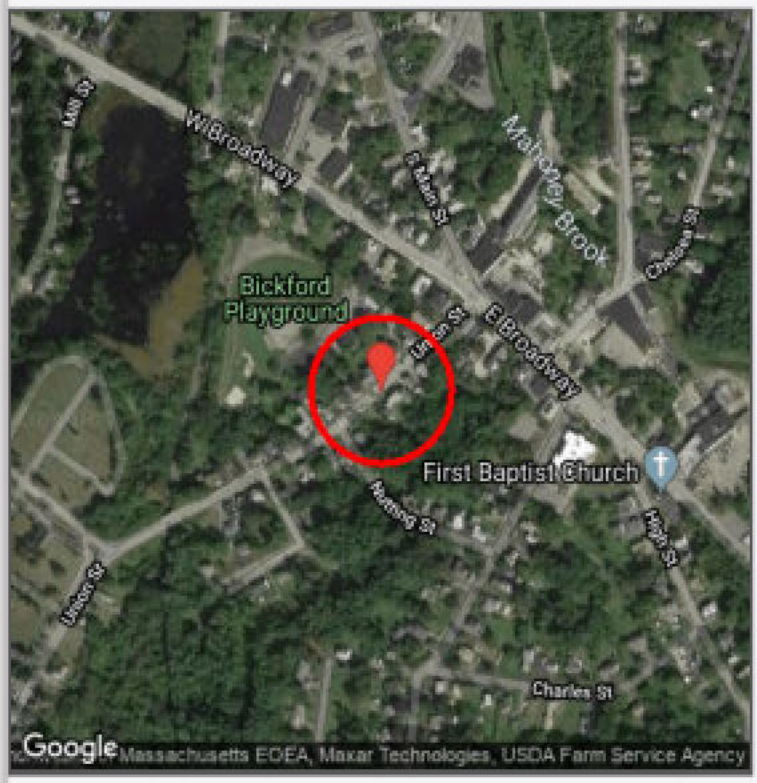
Powered By: VIGILANT SOLUTIONS



Vehicle Images



Vehicle Spotted:
09-11-19 at 4:56:42 PM EDT



Detection Data

Vehicle Info

Plate # 1:	1RGT51
Plate # 2:	1R6T51
Date:	09-11-19
Time:	4:56:42 PM
Longitude:	-71.981584
Latitude:	42.556760

Camera Info

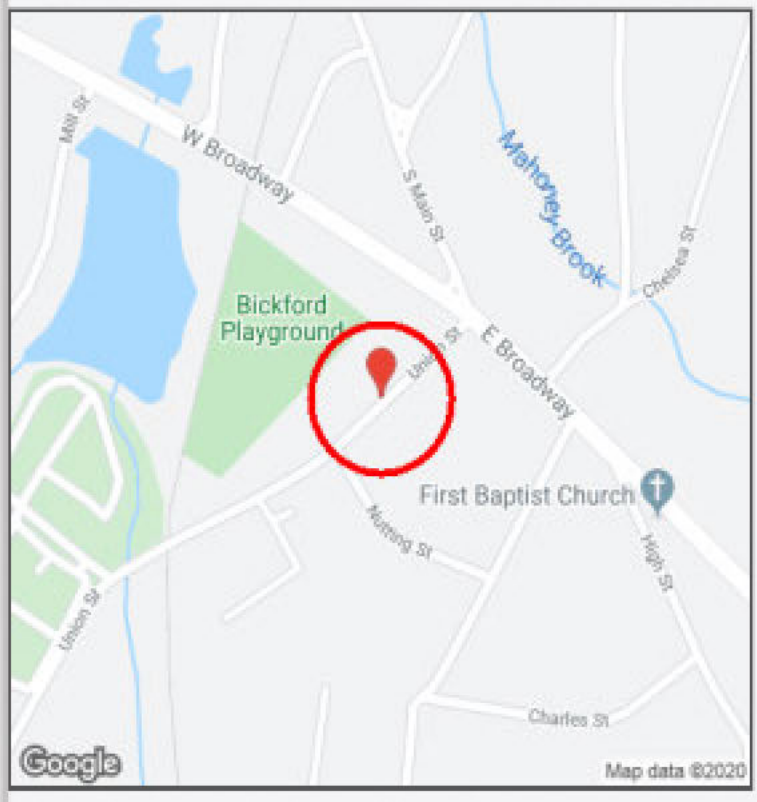
Agency:	N/A
User:	Commercial Data
System:	Commercial System
Camera:	N/A
Type:	N/A

Nearest Address:	32 Union St Gardner, MA 01440
Nearest Intersection:	Union St Nutting St

Disclaimer: The address listed above is ONLY an estimate.

Vehicle Detection Report

License Plate Number: 1RGT51



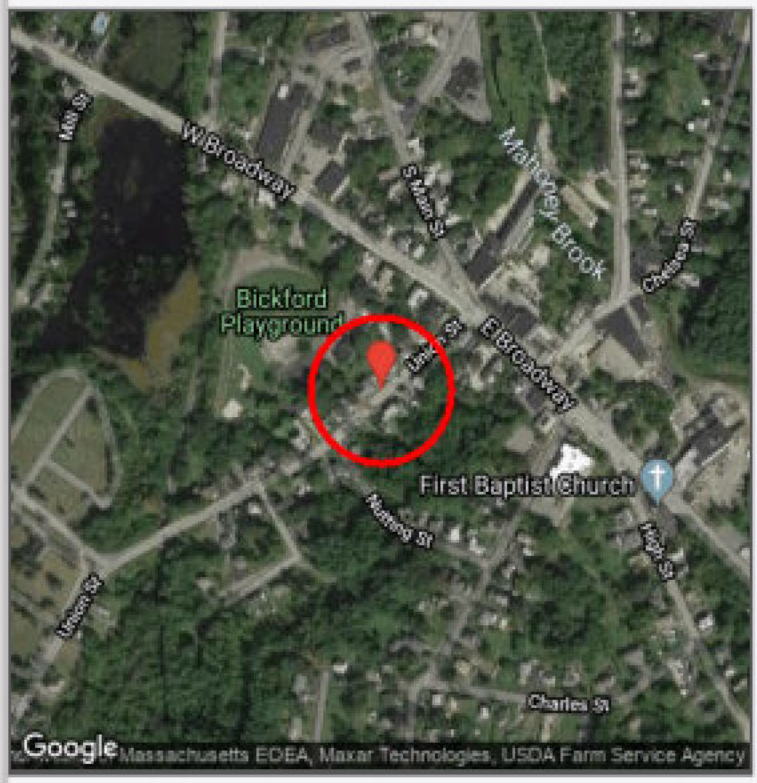
Powered By: VIGILANT SOLUTIONS



Vehicle Images



Vehicle Spotted:
08-22-19 at 8:14:24 PM EDT



Detection Data

Vehicle Info

Plate # 1:	1RGT51
Plate # 2:	1RGY51
Date:	08-22-19
Time:	8:14:24 PM
Longitude:	-71.981541
Latitude:	42.556878

Camera Info

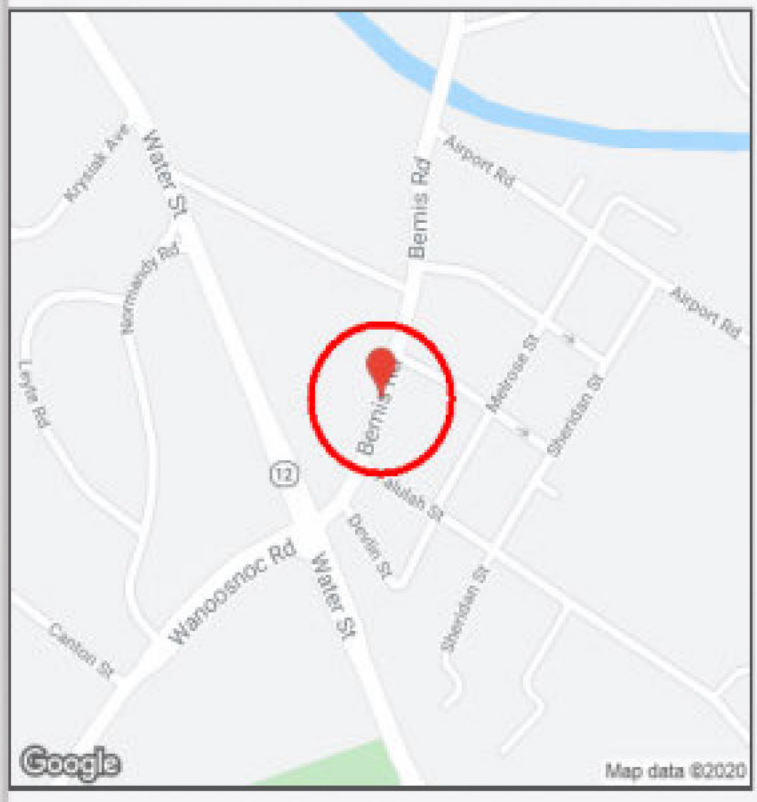
Agency:	N/A
User:	Commercial Data
System:	Commercial System
Camera:	N/A
Type:	N/A

Nearest Address:	32 Union St Gardner, MA 01440
Nearest Intersection:	Union St Nutting St

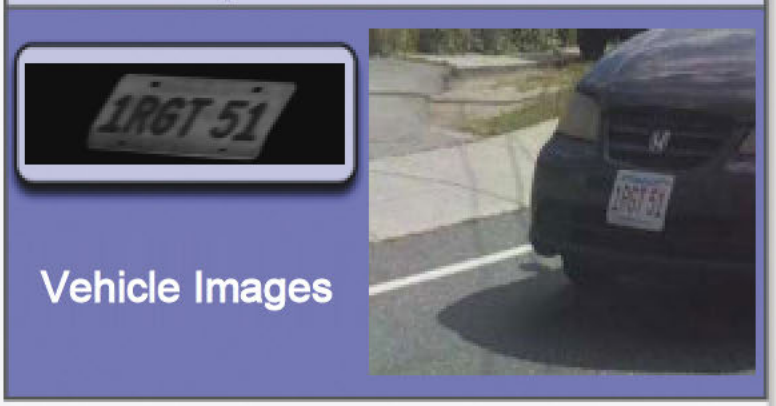
Disclaimer: The address listed above is ONLY an estimate.

Vehicle Detection Report

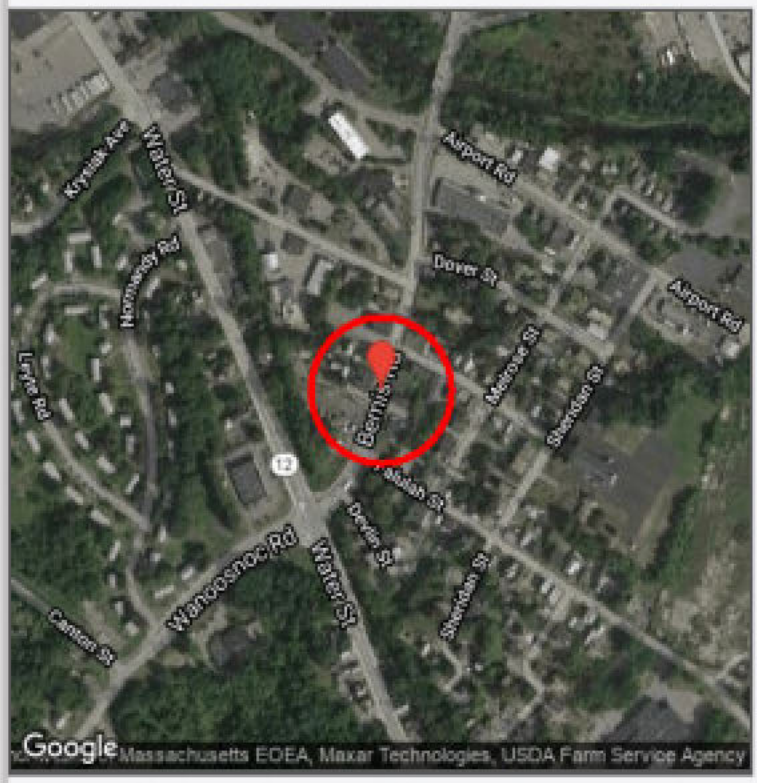
License Plate Number: 1RGT51



Powered By: VIGILANT SOLUTIONS



Vehicle Spotted:
08-15-19 at 2:23:28 PM EDT



Detection Data

Vehicle Info

Plate # 1:	1RGT51
Plate # 2:	1RG151
Date:	08-15-19
Time:	2:23:28 PM
Longitude:	-71.779689
Latitude:	42.565127

Camera Info

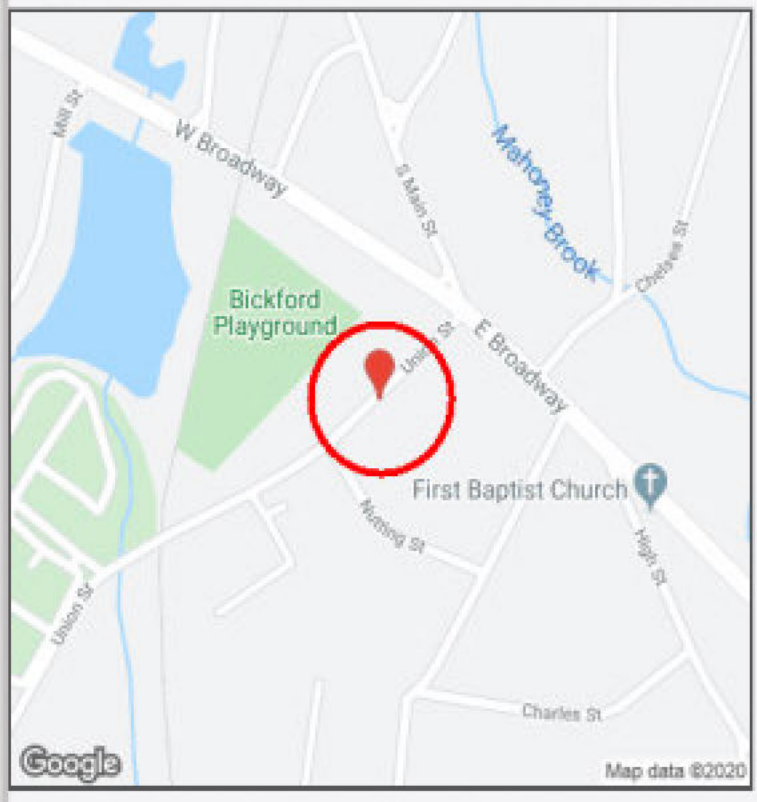
Agency:	N/A
User:	Commercial Data
System:	Commercial System
Camera:	N/A
Type:	N/A

Nearest Address:	40 Bemis Rd Fitchburg, MA 01420
Nearest Intersection:	Bemis Rd Market St

Disclaimer: The address listed above is ONLY an estimate.

Vehicle Detection Report

License Plate Number: 1RGT51



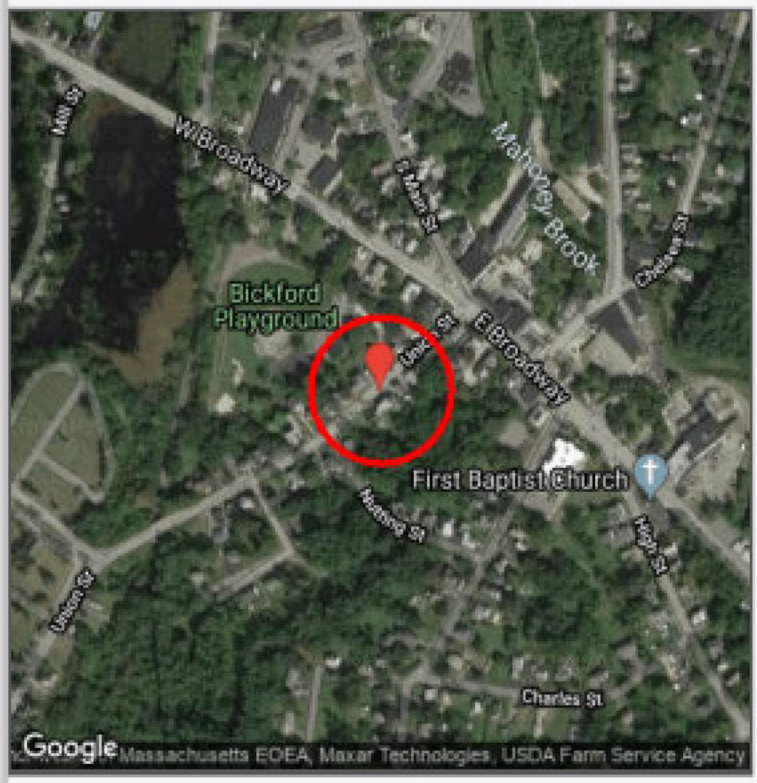
Powered By: VIGILANT SOLUTIONS



Vehicle Images



Vehicle Spotted:
07-02-19 at 7:16:42 AM EDT



Detection Data

Vehicle Info

Plate # 1:	1RGT51
Plate # 2:	1RG151
Date:	07-02-19
Time:	7:16:42 AM
Longitude:	-71.981466
Latitude:	42.556824

Camera Info

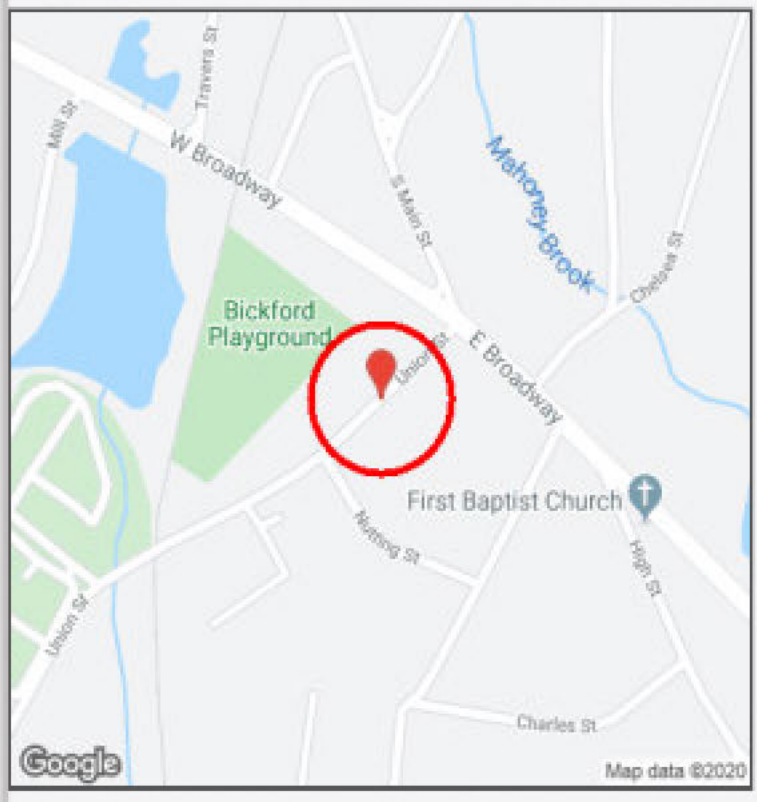
Agency:	N/A
User:	Commercial Data
System:	Commercial System
Camera:	N/A
Type:	N/A

Nearest Address:	32 Union St Gardner, MA 01440
Nearest Intersection:	Union St Nutting St

Disclaimer: The address listed above is ONLY an estimate.

Vehicle Detection Report

License Plate Number: 1RGT51



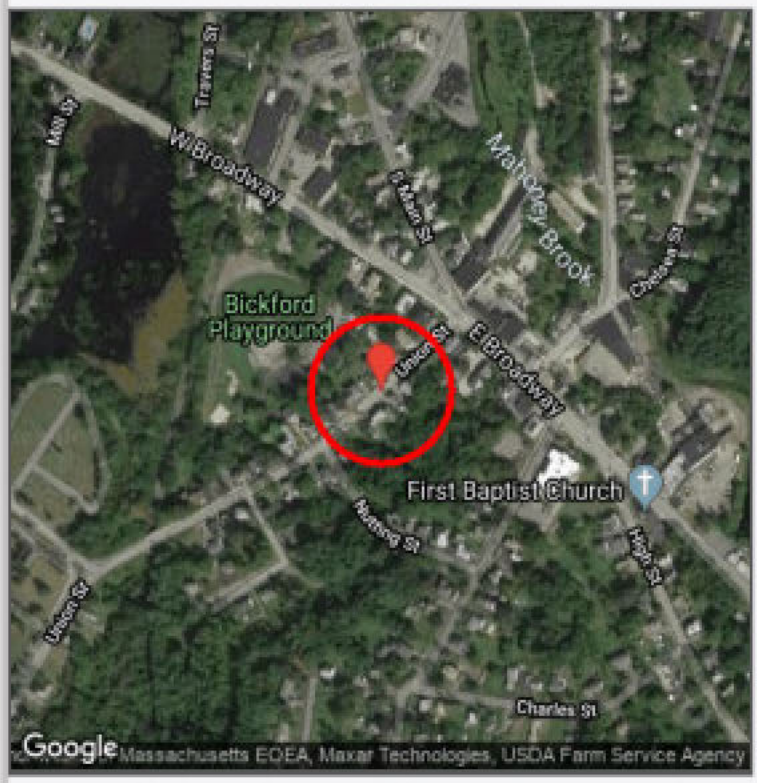
Powered By: VIGILANT SOLUTIONS



Vehicle Images



Vehicle Spotted:
04-06-19 at 12:03:16 PM EDT



Detection Data

Vehicle Info

Plate # 1:	1RGT51
Plate # 2:	1RG151
Date:	04-06-19
Time:	12:03:16 PM
Longitude:	-71.981383
Latitude:	42.556919

Camera Info

Agency:	N/A
User:	Commercial Data
System:	Commercial System
Camera:	N/A
Type:	N/A

Nearest Address:	28 Union St Gardner, MA 01440
Nearest Intersection:	Union St Nutting St

Disclaimer: The address listed above is ONLY an estimate.

Department of State Police
Special Order

Effective Date	Number
October 1, 2019	**19-SO-12**

Subject

Distribution of General Orders

I. DISTRIBUTION OF GENERAL ORDER

Policy and Procedure
TRF-11 Automatic License Plate Recognition

The requirements for the distribution of the above listed General Order are:

√ Each employee shall follow the instructions within this Special Order.

√ Supervisors shall obtain a signature receipt from each employee acknowledging this General Order has been promulgated and posted on DocuShare.

√ Troop/Station/Section/Unit Commanders shall forward the *completed* signature receipt forms through channels to their respective Division Commanders on or before: November 1, 2019.

√ Division Commanders shall:

- Ensure that employees under their command have been notified of this General Order; and
- Maintain a file of all completed signature receipt forms for their Division.

II. DISTRIBUTION OF GENERAL ORDER INSTRUCTIONS

A. Instructions

Each employee shall acknowledge that the following General Order has been rescinded:

Policy and Procedure		Effective Date
TRF-11	Automatic License Plate Recognition	06/14/2018

III. DISTRIBUTION OF GENERAL ORDER INSTRUCTIONS

A. Instructions

It is the responsibility of each sworn and civilian employee to read promulgated directives. Sworn and civilian employees shall read and become familiar with the contents of all posted written directives.

Each employee shall acknowledge the following General Order has been promulgated and posted to DocuShare. Each employee is responsible for reading and becoming familiar with the following General Order:

Policy and Procedure		Effective Date
TRF-11	Automatic License Plate Recognition	10/01/2019

OFFICIAL:

KERRY A. GILPIN
Colonel/Superintendent





PIPS TECHNOLOGY™
DETECTION INNOVATION

Back Office System Software

User's Manual
Version 3.5 or above

NEOLOGY™ MOBILITY TECHNOLOGIES

Table of Contents

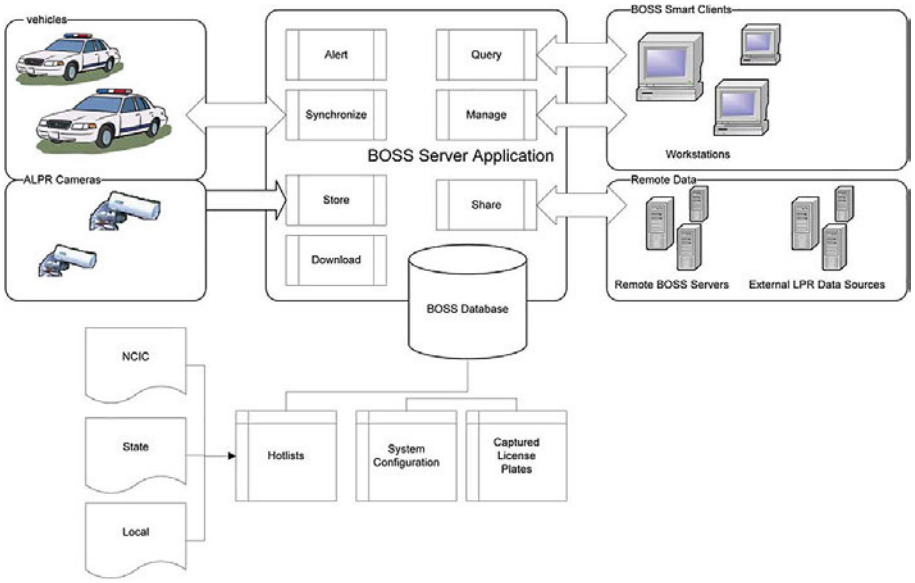
1 Introduction 4
1.1 The Design of PIPS Back Office System Software Version
2 Logging In 5
2.1 PIPS Back Office System Software Administrator Login 5
2.2 User Login 5
2.3 Login Dialog 5
2.3.1 Storing Username and Password 6
2.3.2 BOSS Client Connection Settings 6
3 Application Layout 7
3.1 Components of the BOSS Application Screen 7
3.2 The BOSS Home Screen 8
3.3 Help Documentation 9
3.4 Minimizing the BOSS Application 9
4 BOSS Access Permissions: Users/Groups/Roles 10
4.1 Permission Levels 10
4.2 Permissions 10
4.3 Roles 11
4.4 Groups 12
4.4.1 Creating a New Group 12
4.4.2 Parent Groups 13
4.4.3 Deleting a Group 13
4.5 Users 14
4.5.1 Creating a New User 14
4.5.2 Deleting a User 15
4.5.3 Importing Users from Active Directory 16
4.6 Access Permission Example 17
4.7 Preferences 18
4.7.1 Changing User Preferences 18
5 Devices and Sites 19
5.1 Devices 19
5.1.1 Device Status 20
5.1.2 Defining a Device 20
5.1.3 Editing a Device 21
5.1.4 Enabling and Disabling a Device 21
5.1.5 Deleting a Device 22
5.2 Sites 22
5.2.1 Default Sites 22
5.2.2 Creating a Site 23
5.2.3 Deleting a Site 23
6 BOSS Data Sharing 24
6.1 Configuring BOSS to Allow Remote BOSS Queries 24
6.2 Configuring BOSS to Access a Remote BOSS Server 24
7 Hotlists 25
7.1 Creating a New Hotlist 25
7.1.1 Configuring Basic Hotlist Settings 25
7.1.2 Defining the Hotlist Data Source 27
7.1.3 ZIP Compressed Hotlist Files 29
7.1.4 Defining Hotlist Source Credentials 29
7.1.5 Defining Hotlist Advanced Options 31
7.2 Enabling and Disabling a Hotlist 32
7.3 Modifying Hotlist Entries 32
7.3.1 Querying Hotlist Entries 33
7.3.2 Editing a Hotlist Entry 34
7.3.3 Adding a Hotlist Entry Manually 34
7.3.4 Deleting a Hotlist Entry 35
7.4 Targets 35
7.4.1 Creating a New Target 36
7.4.2 Deleting a Target 36
8 Hotlist Formatters 37
8.1 Creating a New Formatter for Hotlists 37
9 Alerts 38
10 Dispatch 39
10.1 Dispatch Settings 40
10.2 Dispatch Hits 41
10.3 Dispatch Reads 41
10.4 Manual Entries 41
10.4.1 Adding a Manual Read 42
10.4.2 Correcting Reads 42
11 Querying Stored Data 43
11.1 Wildcards 43
11.2 Quick Search Bar 43
11.2.1 Quick Search Fields 43
11.3 Query Result Navigation Icons 43
11.4 Advanced Reads Queries 44
11.4.1 Performing an Advanced Reads Query 44
11.4.2 Entering Advanced Reads Query Criteria 45
11.4.3 Managing Query Results 46
11.5 Multiple Query Tabs 46
11.6 Cross-Referencing External Data 47
11.7 Working with Queried Reads. 48
11.7.1 Viewing Query Results 48
11.7.2 Query Results Actions 49
11.7.3 Viewing Read Details 49
11.8 Favorites 52
11.8.1 Creating a New Favorite 52
11.8.2 Activating a Favorite 52
11.8.3 Deleting a Favorite 53
12 Reports 54
12.1 Running a System Report 54
12.2 Viewing and Printing Reports 54
12.2.1 Viewing the Login Statistics Report 55
13 Client Tools 56
14 Archiving Data 57
15 System Settings 58
15.1 Sessions 58
15.1.1 Viewing and Disconnecting Sessions 58
15.1.2 Workstation Power Management and Sessions 58
15.2 Dispositions 59
15.2.1 Defining a New Disposition 59
15.2.2 Deleting a Disposition 59
15.3 System Parameters 60
15.3.1 Editing System Parameters 60
15.3.2 List of BOSS System Parameters 60
15.3.3 Branding 62
15.4 Roles 63
15.4.1 Adding New Roles 63
15.4.2 Deleting Roles 63

15.5 Report Management ... 64
15.5.1 Assigning Permissions to Access Reports ... 64
15.6 Translations ... 64
15.6.1 Entering a New Translation ... 65
15.7 Justifications ... 66
15.7.1 Entering a New Justification ... 66
15.7.2 Deleting Justifications ... 66
17 Appendix: Installation and Configuration Guide ... 67
17.1 Installing the BOSS Server Application Files ... 68
17.1.1 Running the Installer ... 68
17.1.2 PIPS License Agreement ... 69
17.2 BOSS Version 3.2 and Above License Key Management ... 70
17.2.1 Activating the License Key ... 70
17.2.1.1 Activating the License Key over the Internet ... 71
17.2.1.2 Activating the Software with a License File. ... 72
17.2.1.3 Request a License File to Activate the License ... 72
17.2.2 Updating a License Key ... 73
17.3 Map Display Options with BOSS ... 74
17.3.1 U.S. Census Bureau TIGER Maps ... 74
17.3.2 Advanced Mapping with Microsoft Bing Maps ... 74
17.4 Configuring the BOSS Server Application ... 74
17.4.1 The BOSS Controller Application ... 74
17.4.1.1 Starting the BOSS Controller ... 74
17.4.1.2 Status Colors ... 74
17.4.1.3 Right-Click Menu ... 75
17.4.1.4 Starting the BOSS Service ... 75
17.4.1.5 Stopping the BOSS Service ... 75
17.4.2 BOSS Configuration ... 76
17.4.2.1 Activating the Configuration Wizard ... 76
17.4.2.2 BOSS Configuration Wizard ... 76
17.4.2.3 SQL Server Configuration ... 77
17.4.2.4 Resetting the Administrator Password ... 78
17.4.2.5 Network Port Settings ... 78
17.4.2.6 Regional Hotlist Formatters ... 80
17.4.2.7 NCIC Hotlist Formatters ... 80
17.4.2.8 TIGER Maps Configuration ... 81
17.4.2.9 Finishing Configuration ... 81
17.5 Installing the BOSS Smart Client Application ... 82
17.5.1 Installation over the Web ... 82
17.5.2 Stand-Alone Installation ... 82
17.6 Configuring Client Tools ... 82
18 Troubleshooting ... 84
19 Appendix: Plug-Ins ... 87
19.1 The BOSS Truck Drayage Utility ... 87
19.2 The BOSS LPRD Plug-In ... 87
19.3 The BOSS DEA Plug-In ... 87
20 Appendix: BOSS Mantis ... 88
20.1 How Dose Mantis Work ... 88
20.2 Mantis Security and Encryption ... 89
20.3 Mantis Requirements ... 90
20.4 Mantis Installation ... 90
20.5 Mantis Configurations ... 90
20.6 Mantis Search Features. ... 91
20.6.1 Mantis Search Definitions ... 91
20.7 Additional Mantis Parameters ... 92
20.8 Mantis Configuration Troubleshoot ... 92
20.8.1 Mantis Log Messages Catalog ... 93
Glossary ... 95

1 INTRODUCTION

This document serves as a user's manual for the PIPS Back Office System Software (BOSS) version 3.5 or above and describes the various features and functionality of the application. BOSS is a management and administration tool for the PIPS Automatic License Plate Recognition (ALPR; also known as ANPR, or Automatic License Number Recognition) systems. The BOSS server application provides an interface for user maintenance, data queries, import and export of data, and dispatch functions. BOSS lets an Administrator specify the databases used by both mobile and fixed camera installations. BOSS retrieves these databases on a regular schedule; manages the users of the PIPS PAGIS systems and BOSS Smart Client workstations; provides a central repository for data collected by mobile PAGIS deployments and fixed camera installation; provides reporting and data management tools; provides hit detection and dispatch functions for fixed camera installations; and allows for data mining and data sharing with other agencies.

The following schematic shows how the BOSS server application works together with Smart Client workstations, various data sources, PAGIS, and the full line of ALPR cameras to create a comprehensive solution.



1.1 The Design of PIPS Back Office System Software Version 3.5 and Above

The design of BOSS version 3.5 or above offers ease of accessibility with a user-friendly look and feel. Large, easy-to-identify icons provide intuitive navigation, and the frequently used elements are readily available. The user interface (UI) is very recognizable and comfortable, particularly for users already familiar with Windows-based applications, including Microsoft® Office software, or the Mobile Pagis Software. In addition, users can enter a minimum amount of information to add a data object, with the ability to include more details if needed.

2 LOGGING IN

2.1. PIPS Back Office System Software Administrator Login

During each new installation of the PIPS Back Office System Software, a default user of “admin” is created, with the password of “admin1.” The installer or designated BOSS Administrator can log in with this account to create additional users and otherwise configure the system. It is important that the “admin” password be changed to protect the system’s security. Likewise, it is equally as important to keep this and all passwords confidential to protect the security of the BOSS system. Section 17, Installation and Configuration, offers more information on setting up users and passwords.

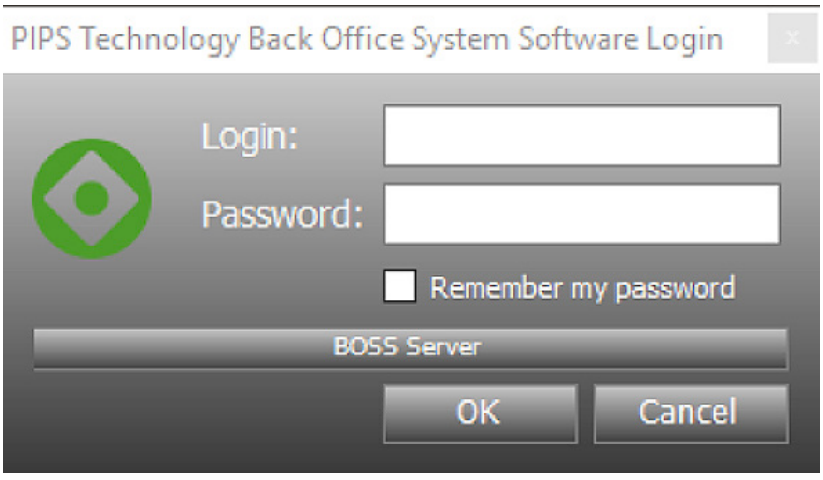
2.2 User Logins

The PIPS Back Office System Software will require a user to log in with a username and password only if there is no BOSS user matching the current Active Directory user login. In other words, if the username currently logged into Windows matches a username in the BOSS system, the user is automatically logged into the application when it is started, and no login screen will appear.

For example, if user “bsmith” is logged in using Windows Domain Authentication through Active Directory (“logged into Windows”), when the BOSS Smart Client is started, and a “bsmith” user exists within the BOSS system, no login screen will appear; the application will authenticate the user and load automatically. If a user logs onto Windows with a name that is not an exact match to a username in the BOSS system, or is not logged into the same Windows Domain, a login screen will appear. The user will then need to enter a correct BOSS user name and password in order to enter the application.

Note: In order for a user to be automatically logged into BOSS, the Active Directory user must be in the same Windows domain as the PIPS™ Back Office System Software server.

2.3 Login Dialog



1. Enter your username in the Login field.

2. Enter the correct password in the Password field.
Note: Passwords are case sensitive.

3. Click OK to complete the login process.

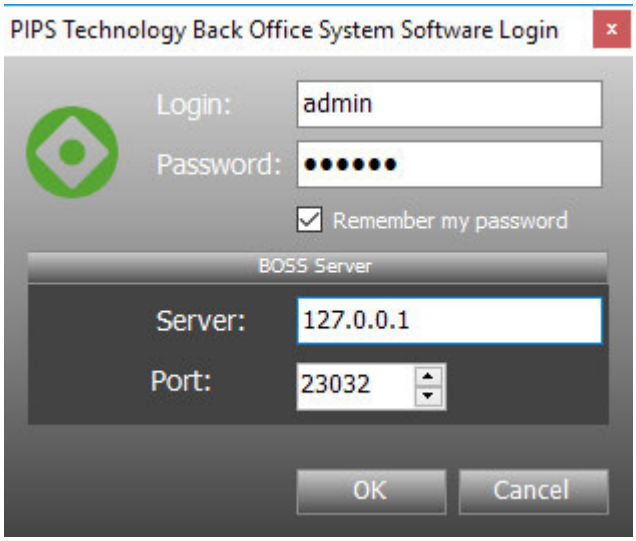
2.3.1 Storing Username and Password

Select the Remember my password option to save the password to the computer's local Windows registry and automatically fill in both Login and Password fields on subsequent logins.
Selecting this option only remembers the login information for the current Windows User on the local computer. It will not apply to a different Windows user logged in the same computer and will not apply to the same user logging in a different computer. This option need not be checked every time. Once checked, the option will stay that way until it is deselected during a login.

Note: The username and the password are stored in the Windows Registry. This can be a security risk. It is recommended that you not use the Remember my password option unless the Windows workstation can be secured against unauthorized access.

2.3.2 BOSS Client Connection Settings

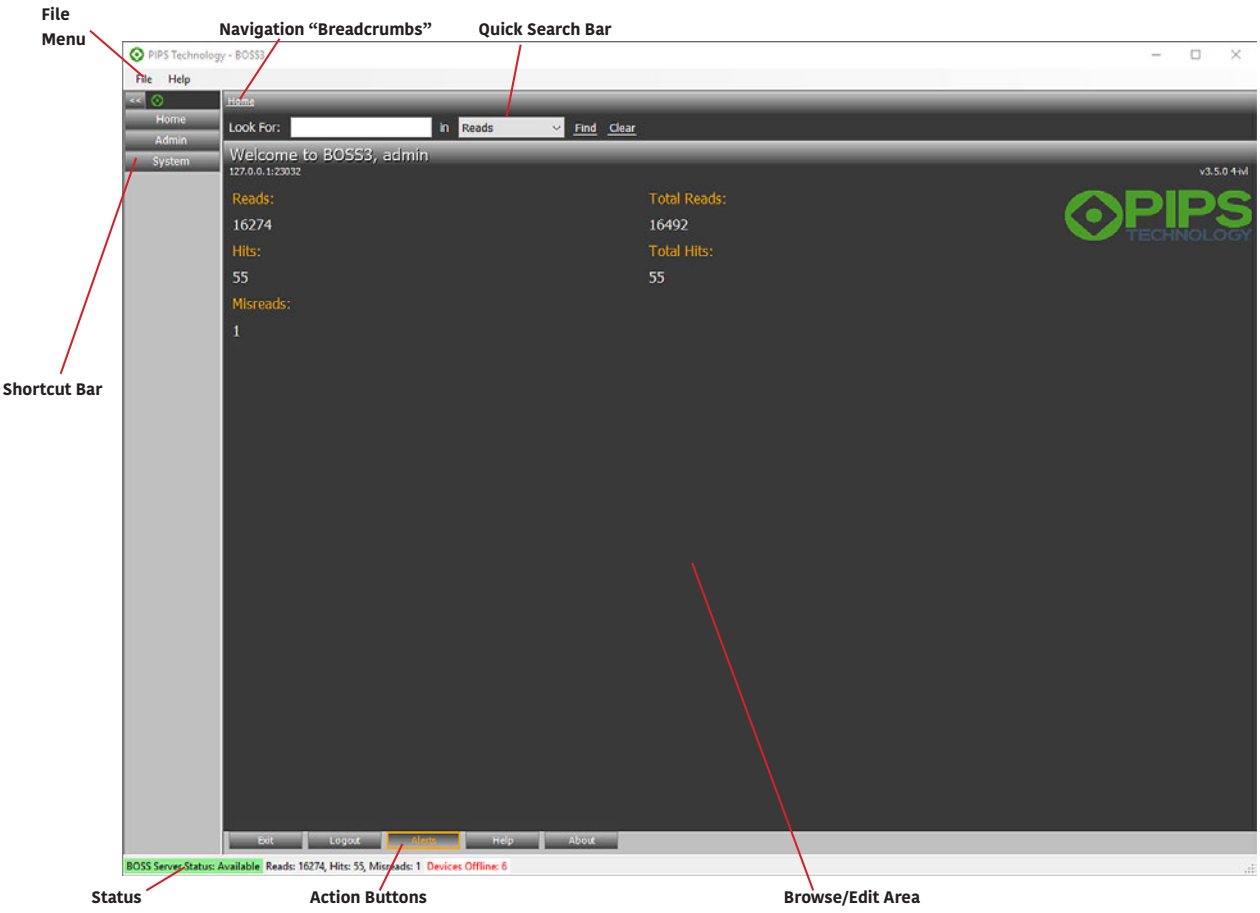
Click the BOSS Server button on the Login screen to view or change the client connection settings.



Server – IP address, computer name, or DNS address can be used in the Server field as long as the client can reach the server using the value entered.
Port – The default port used for connecting to the BOSS server is 23032. This should only be changed here if the BOSS server has been configured to use a non-default port.

3 APPLICATION LAYOUT

3.1 Components of the BOSS Application Screen



File Menu – The File menu of the application resides in the very top left of the application window. The File menu is always visible and available regardless of the screen or shortcut selected. The Exit option is available through this menu.

Navigation – The navigation "breadcrumbs" appear at the top of the BOSS screen as different actions are selected. By clicking on the links it is possible to backtrack to a previous screen.

Shortcut Bar –The Shortcut bar (the panel on the left of the screen) contains icon buttons for the various operations available. The shortcut icons are divided into three categories: Home, Admin, and System. Each time the application is started, all of the categories are closed with no shortcuts displayed. Click on any of the three headings to access the shortcuts within that category. The actual categories and shortcuts that appear depend on the logged-in user's privileges.

The Shortcut bar can be collapsed entirely to provide a larger space for the Browse/Edit area by clicking the << button at the top left of the screen. To expand the Shortcut bar again, click the >> button.

Browse/Edit Area – The widest portion of the application window, the Browse/Edit area is where data is displayed for viewing or editing. The actual data displayed here depends upon the shortcut icon that is selected from the Shortcut bar.

Quick Search Bar – Directly above the Browse/Edit Area, the Quick Search bar allows for simple, immediate queries of BOSS data. Using the Quick Search bar simply involves typing the text to query in the Look For field and selecting the type of data (reads, hits, etc.) to search in the drop-down box.

Action Buttons – These are the buttons directly below the Browse/Edit area. These buttons will differ depending on the shortcut icon selected. The actual buttons that appear will also vary depending upon the user's privileges.

Status Bar – This is the area along the very bottom of the application window that displays the following system information:

- **BOSS System State (Available or Offline):** "Available" status indicates that the client is currently communicating with the BOSS server application and the server is running. This status is highlighted with a green background. "Offline" status indicates that the client is currently not able to communicate with the BOSS server and is highlighted with a red background. In this event, the BOSS UI will continue to check for the BOSS server to become available again. After three attempts to reconnect, the user will be notified that the connection could not be re-established and will be provided further instructions on how to proceed.
- **Reads:** The total number of reads currently contained in the BOSS system.
- **Hits:** The total number of hits currently contained in the BOSS system.
- **Misreads:** The total number of misreads currently contained in the BOSS system.
- **Devices Offline:** The number of fixed camera devices that are currently identified as offline.

3.2 The BOSS Home Screen

The BOSS Home screen is displayed within the Browse/Edit area upon login. The top banner displays the username of the current BOSS user, the BOSS server address, and current system statistics. Statistics may take a few moments to update after login. The action buttons, described below, are displayed along the bottom of the screen. The actual buttons that display will vary depending upon the user's privileges.

Exit – Exit the BOSS application.

Logout – Log out from the current session to the Login screen.

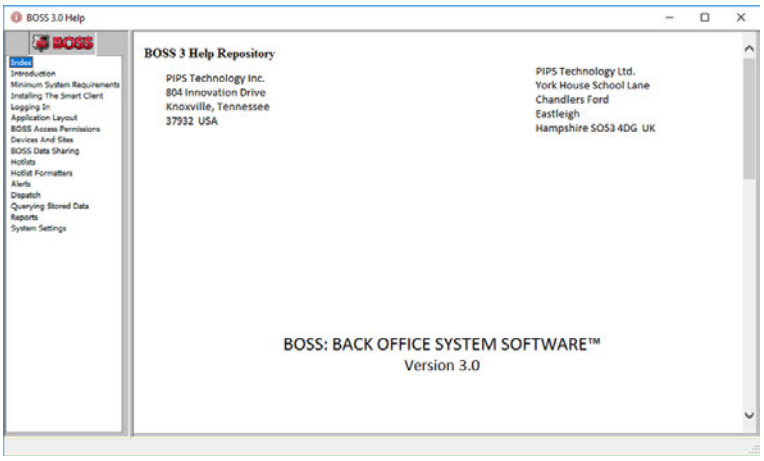
Alerts – Toggle dispatch alerts on (orange highlight) and off. This button will not be displayed if the user is not authorized to access the dispatch screen, or if the user has not chosen to receive dispatch alerts in Preferences (Section 5.3).

Help – Activate the help system.

About – Display application information.

3.3 Help Documentation

BOSS provides a help document accessible in the client application. To access help, select Help in the File menu area or press the F1 button. A help document will be displayed in a browser window and is indexed and searchable for ease of use.



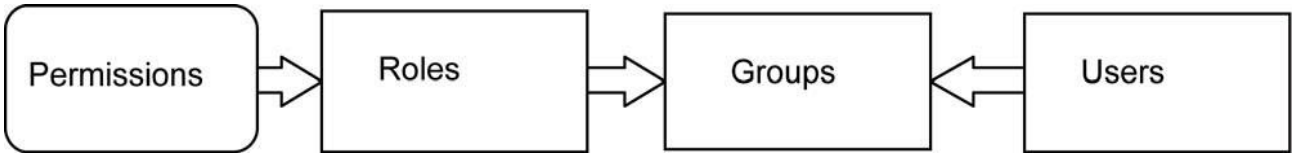
3.4 Minimizing the BOSS Application

The BOSS application can be minimized to the Windows System Tray using the Windows minimize button on the right upper corner of the BOSS application window. To restore the BOSS application, click on the BOSS PIPS icon. When the application is minimized, real-time alerts will still be displayed.



4 BOSS ACCESS PERMISSIONS: USERS/GROUPS/ROLES

Access permissions to various functions (such as reports or dispatches) in BOSS are administered through users, groups, and roles. Each individual who will use the BOSS software must log in via a user account. Each user account is assigned to a group. Every group is assigned a role (such as Administrator or Dispatcher), which determines the set of functionality to which the group's members will have access:



The security parameters defined in a role apply to a user via the group to which the user belongs.

4.1 Permission Levels

The following table lists the levels that apply to permissions:

LEVEL	EXPLANATION
No Access*	No permissions to the function
Read Only	View-only permissions to the function. Add/Change/Delete are not permitted.
Full Access	Complete permissions to the function. View/Add/Change/Delete are permitted.

**When a user's effective permissions to a function are No Access, the function is not visible to the user. For example, if a user has No Access privileges to the System function, the System category is not displayed.*

4.2 Permissions

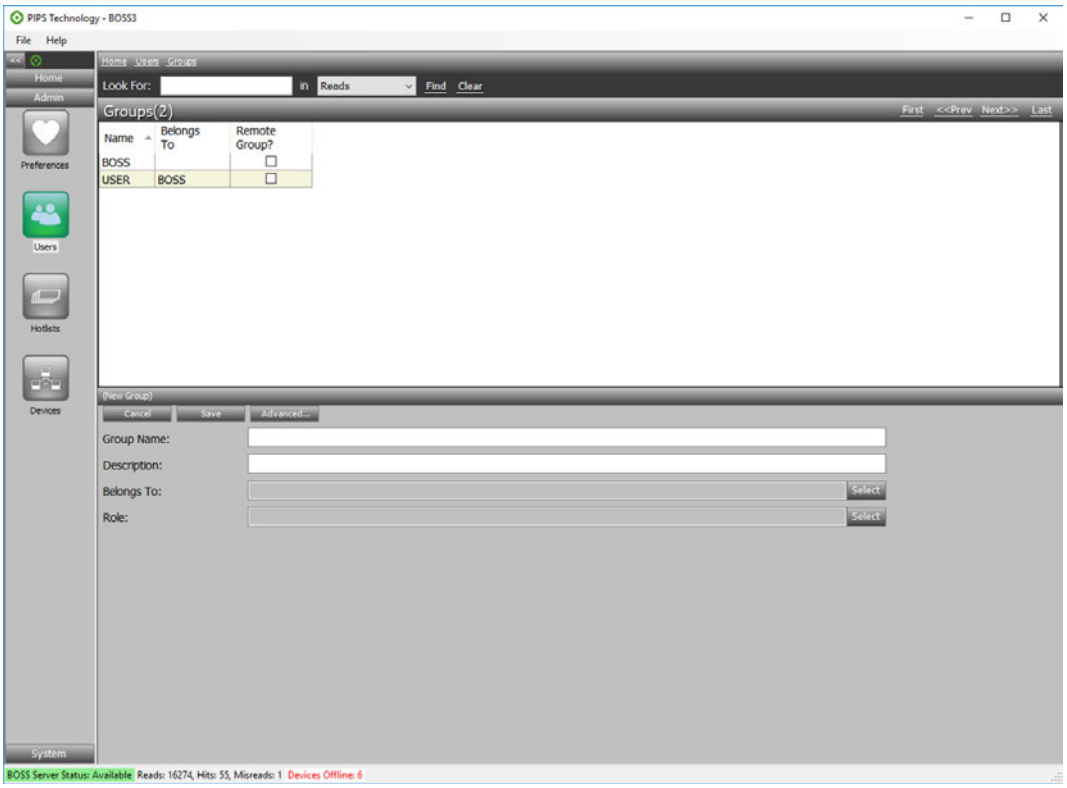
The following table lists the functions that are controlled by permissions levels:

PERMISSION	EXPLANATION
Reads	Plate read information
Dispatch	Real-time monitoring and hit alerts
Users	Groups and user accounts
Hotlists	Hotlists (plates of interest)
Devices	Sites and ALPR camera devices
System	System configuration options

See Section 15.4, Roles, for more information on setting permissions.

4.3 Roles

Roles are access permission profiles. BOSS comes with several predefined roles. A BOSS Administrator is able to add additional roles to the system. A BOSS Administrator is also able to alter and delete any roles. Roles define a permission level for different functions of the system. See Section 15.4, Roles, for additional information.



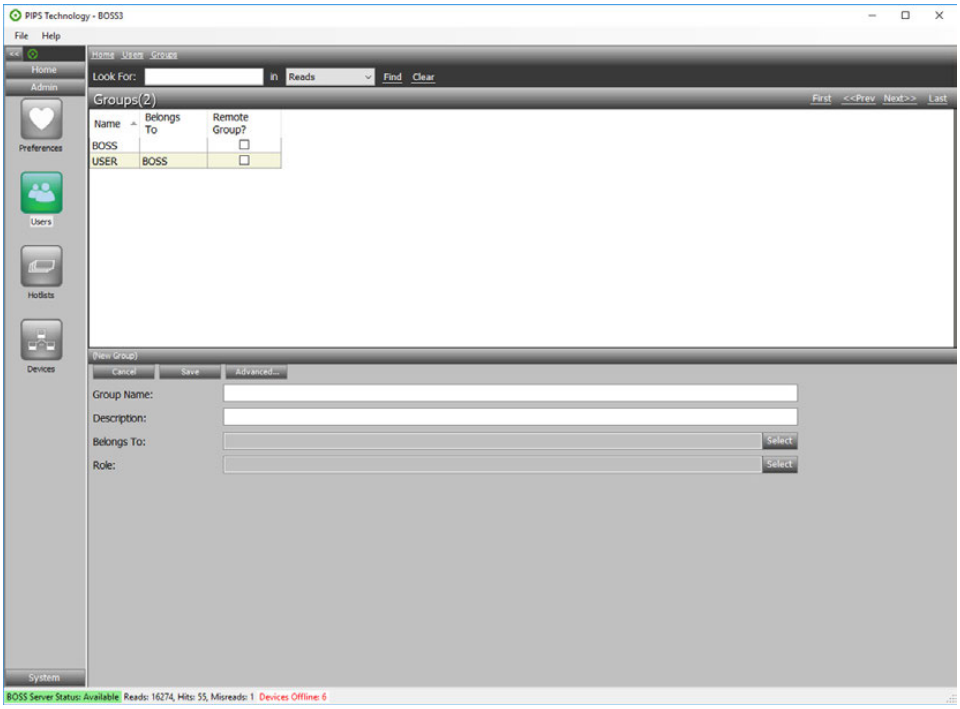
The following roles are installed by default in a BOSS system:

- System Administrators
- User
- Dispatcher
- Group Administrators
- Device Administrators
- Hotlist Administrators

See System Settings section for Role definitions and changes.

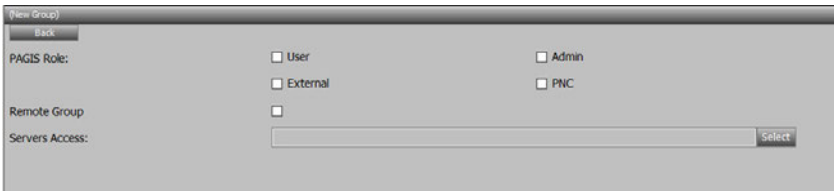
4.4 Groups

Groups are collections of users that have the same permissions. Groups provide an efficient way to organize users, for example by organizational units, and easily assign permissions to those users. Using groups is optional. A default group named “BOSS” automatically exists within a BOSS system, and user accounts will belong to the “BOSS” group by default. The BOSS group cannot be deleted.



4.4.1 Creating a New Group

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Users** shortcut. A list of all current users will display in the Browse/Edit area.
3. Click the **Groups** button at the bottom of the Browse/Edit area. A list of all current groups will display in the Browse/Edit area.
4. Click the **New** button. The New Group Entry screen will display.
5. In the Group Name text box enter a name for the group. (**Note:** The group name must have a minimum of three characters.)
6. In the Group **Description** text box enter a description of the group (optional).
7. Each group, except for the default BOSS group, is required to have a parent group. In the Belongs To field, click the **Select** button to view a list of all existing groups. Click on the desired group and click the **Save** button to select. The name of the selected group will display in the Belongs To field as the parent group.
8. Assign a role to the group. In the Role field, click the **Select** button to select from the existing roles. Click the desired role from the list and click the **Save** button to make the selection. The name of the selected role will appear in the field.
9. Click the **Advanced**... button to access additional, optional settings for the new group.



4.4.1 Creating a New Group (continued)

PAGIS Role (User/Admin/External/PNC) – Check desired PAGIS roles to grant the new group for the associated permissions in Pagis. Please refer to the Pagis User's Manual for more information.

Remote Group – Select this option to designate the group as remote. When a BOSS Administrator wants to give access to another BOSS system for remote queries ("data sharing," see Section 6), a login must be created and assigned to a group that is flagged as a remote group. The remote BOSS Administrator will then create a remote site with credentials for that login.
Servers Access – This option allows for defining which, if any, sites will be accessible by this group. Click the Select button to access a list of sites.

Note: There are two sites defined by default: Manual Entries and Unassigned. If no additional sites have been defined, only the default values are available in this field. Click each desired site and click the **Save** button to complete the selection process. If one site is selected the name of that system will appear in the Server Access field. More than one site can be selected.

Log Queries – This option, when selected, will result in the logging of all queries made by all users of the group. This information is then available via the audits report. **WARNING:** *This can potentially be a very large amount of data. Select this option with care.*

a. Configure these Advanced User settings as desired.

b. Click the **Back** button to return to the main New Group Entry screen

10. Click **Save** to complete creating the new group, or click **Cancel** to clear the new group.

4.4.2 Parent Groups

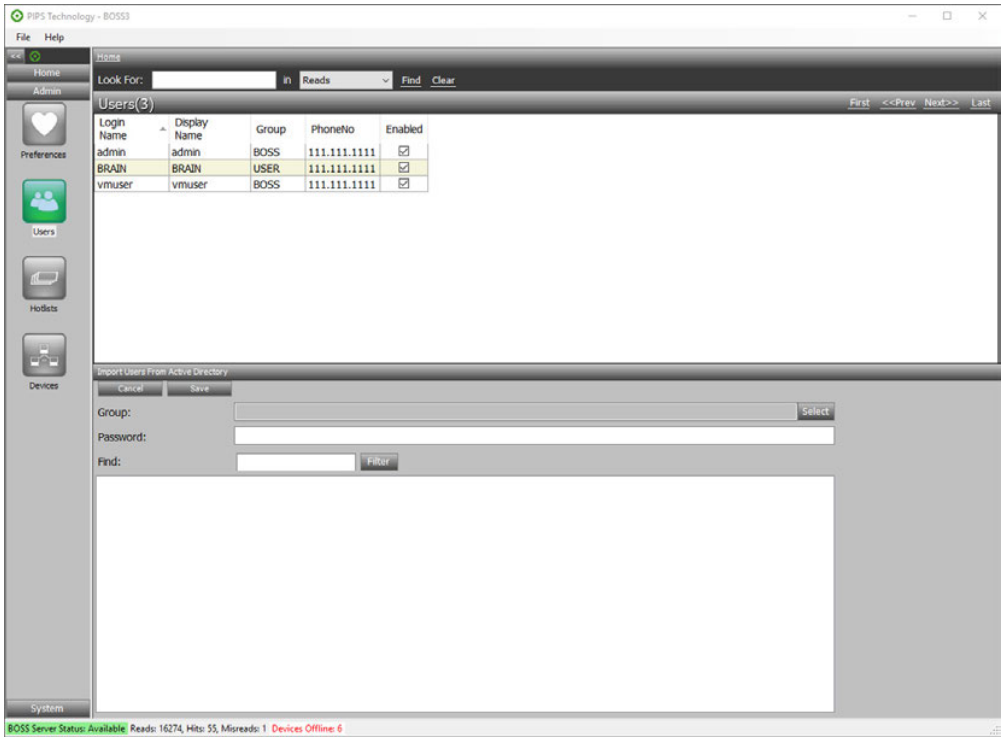
When creating a new group, you must select a parent group (the Belongs To field). BOSS uses a parent-child group structure as an organizational mechanism. This allows the BOSS Administrator to arrange groups into collections based on location, job role, or any other applicable criteria. In BOSS, the parent group can be selected in order to easily reach the entire collection of groups under that parent. This can be especially helpful in large installations with a large number of groups.

4.4.3 Deleting a Group

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Users** shortcut.
3. Click the **Groups** button at the bottom of the Browse/Edit area. A list of all existing groups will display in the Browse/Edit area.
4. Click to select the desired group from the list.
5. Click the **Delete** button.
6. Click **OK** in the confirmation dialog to complete the operation.

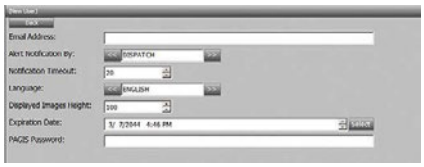
WARNING: Any users currently assigned to the deleted group will be assigned to the default "BOSS" group. You should empty the group by assigning all of its users to different groups prior to deleting it.

4.5 Users



4.5.1 Creating a New User

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Users** shortcut. A list of all existing users will display in the Browse/Edit area.
3. Click the **New** button at the bottom of the Browse/Edit area. The New User Entry screen appears.
4. Enter a **Login Name** for the new user. This is the name the user will enter when logging into the BOSS application. (The login name must be at least three characters.)
5. Enter a **Display Name** for the new user (optional).
6. Enter a **Password** for the new user. (The password must be at least six characters with one Cap, one number and one special symbol.) The strong password requirement cannot be disabled.
7. Select a **Group** for the user. Click the **Select** button to access a list of all groups. Click on the desired group and click the **Save** button to complete the selection.
8. Enter a contact **Phone Number** for the user (optional). This field is for informational purposes only; in case the BOSS Administrator needs to contact the user.
9. Click the **Advanced**... button to access additional, optional settings for the new user. Configure these advanced user settings as desired.



4.4.1 Creating a New Group (continued)

Email Address – Email address or addresses associated with the user. BOSS alerts for the user are sent to the email addresses specified here. Multiple addresses should be separated with a comma.
Alert Notification By – A user can be configured to receive BOSS alerts through the Dispatch application, email, or both. Click the <<
or >> buttons to cycle through the options, stopping at the desired selection.
Notification Timeout – The cutoff time from the time when a hit occurred after which an alert will no longer be sent to the user. For example, if the notification timeout is 20 minutes and a plate of interest is detected at 12:00 pm, notification is not sent to the user after 12:20 pm. This timeout prevents alerts being sent for events that are delayed in arrival to BOSS.
Language – The language preference for the user. The default value is English.
Displayed Images Height – This setting defines the vertical size in pixels of the images (reads and hits) that will display for the user on the Dispatch and Reads screens.
Expiration Date – Date for the user account to automatically be disabled. If no expiration is desired, simply leave this field at its default value (30 years from current date).
PAGIS Password – The user's Pagis password. Strong password requirement not utilized for this field.

Note: The user must be in a group that has been granted PAGIS permissions in order for the user to log in to PAGIS.

---

10. Click the **Back** button to return to the main New User Entry screen.
11. Click the **Save** button to complete creating the new user.

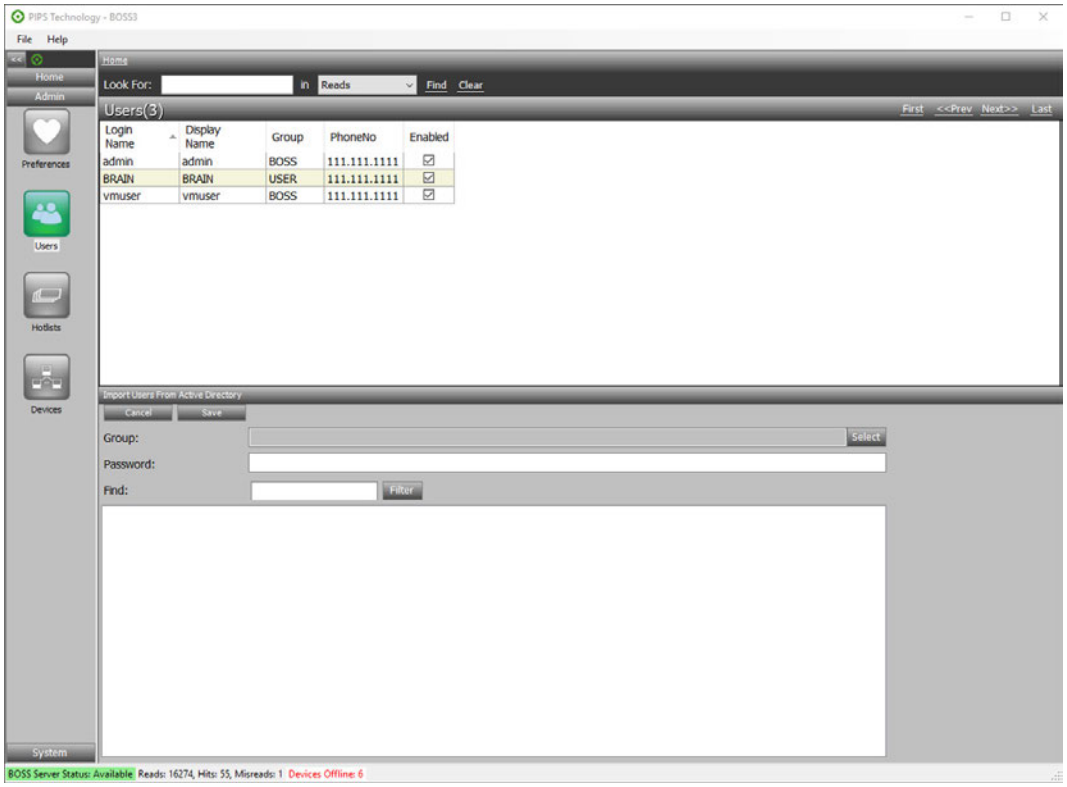
4.5.2 Deleting a User

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Users** shortcut. A list of all existing Users will display in the Browse/Edit area.
3. Click the desired user in the list.
4. Click the **Delete** button at the bottom of the Browse/Edit area.
5. Click **Yes** to confirm the operation.

4.5.3 Importing Users from Active Directory

BOSS allows user logins to be imported from Microsoft Active Directory (AD) service.

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Users** shortcut.
3. Click on the **Import** button.



4. Select the BOSS group that will receive the imported logins. Click the **Select** button to display available groups and **Save** to commit the selection.
5. Enter the default password for the imported logins in the Password field.
6. Browse for the desired users, **or** type in the desired login name (full or partial) in the Find field and press the **Filter** button.
7. Click on the checkbox in front of the desired usernames to select users to be imported to BOSS.
8. Click on **Save** to import the users from Active Directory.

Note: A Windows login cannot have any punctuation included or problems will occur with reads queries being performed.

4.6 Access Permissions Example

The previous sections have described how BOSS user security is designed, using roles, groups, and user accounts. This section presents a working example that integrates the information in this chapter.

A BOSS Administrator creates a role, names the role “Temporary Workers,” and defines the new role to have very limited permissions, as follows:

Reads	Read Only
Dispatch	Read Only
Users	No Access
Hotlists	No Access
Devices	No Access
System	No Access

Then the Administrator creates a group called “Temps.” When creating the group, a role is required. The Administrator selects the new role just created “Temporary Workers,” which assigns the permissions, defined above, to the new group.

Next, the Administrator creates a user account, “Jsmith,” for a temporary worker. While creating the new user, the Administrator is required to select a group for the user, and assigns the user to the “Temps” group just created. The user “Jsmith” has now been created with the permissions shown above because he belongs to the group called “Temps” and that group was assigned the “Temporary Workers” role.

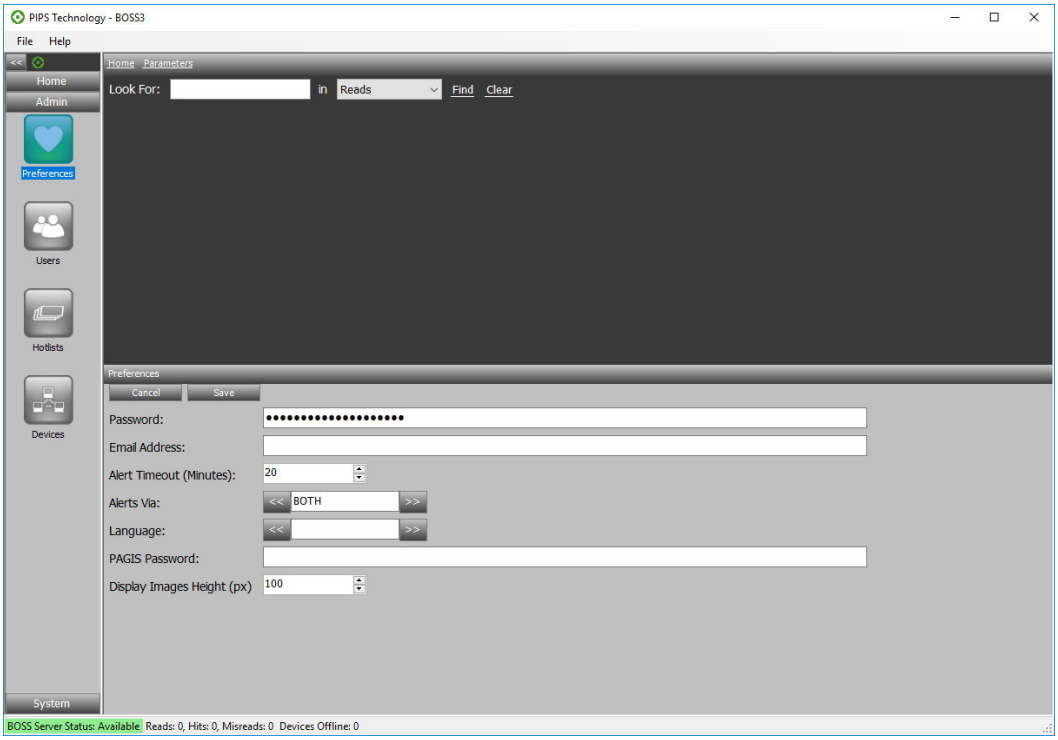
As this example shows, this security design allows reusability of security roles because a BOSS Administrator can define a set of permissions in a role, and that role can be assigned to multiple groups.

4.7 Preferences

The Preferences section allows for changing settings for the currently logged-on BOSS user, such as the password and email addresses.

4.7.1 Changing User Preferences

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Preferences** shortcut. The Preferences Entry screen appears at the bottom of the Browse/Edit area.
3. Modify the preferences settings as desired and click the **Save** button.



Password – Login password for the BOSS user. For security purposes, the existing password does not display on screen.
Email Address – Email address or addresses associated with the user. BOSS alerts for the user are sent to the email addresses specified here. Multiple addresses should be separated with a comma.
Alert Timeout (Minutes) –The cutoff time for older hits to alert the user.
Alerts Via – A user can elect to receive BOSS alerts through the Dispatch screen, emails, or both.
Language – Language preference for the user. The default value is English.
PAGIS Password (PAGIS Password) – The Pagis Software password for the user.

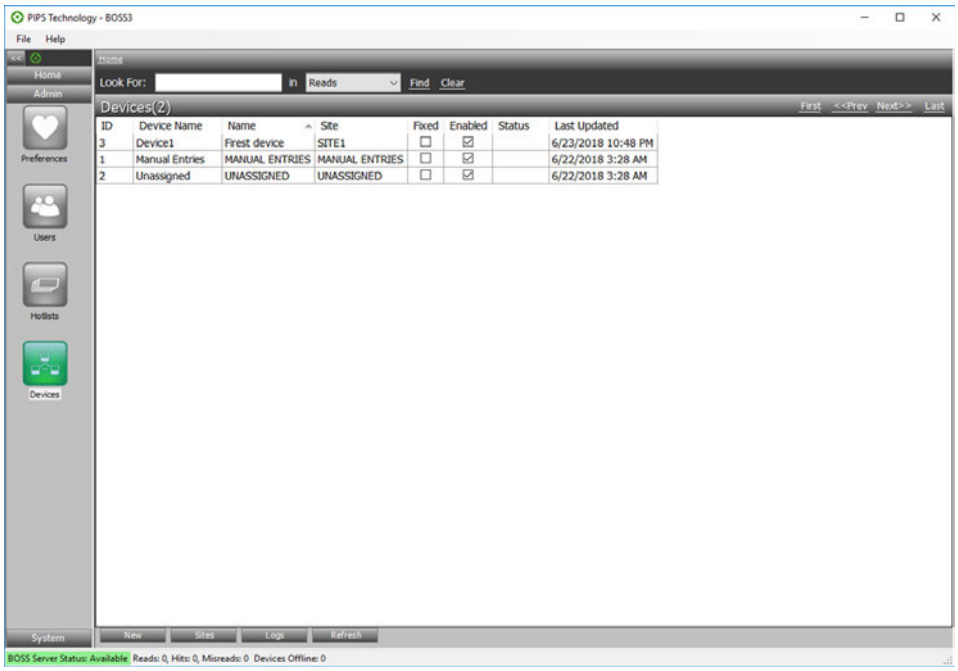
Note: The user must be in a group that has been granted PAGIS permissions in order for the user to log in to PAGIS.

Display Images Height (px) – This setting defines the size in vertical pixels of the images (reads and hits) that will display for the user in the Dispatch and Reads Query sections.

5 DEVICES AND SITES

5.1 Devices

A BOSS device is any source that can input reads into the system. Typically, a device is a camera—either fixed or mobile. Another source for reads is manual entry, in which a BOSS user types the information for a read into the BOSS Dispatch screen .A new BOSS installation automatically contains two default devices, Manual Entries and Unassigned. A BOSS Administrator creates additional devices applicable to his/her organization.



5.1.1 Device Status

To see the current devices in your system with information about their status:

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Devices** shortcut.

The devices will be listed in rows with the following column headings:

Device Name – The name assigned to the device, used in the device selections and is the description of the device. The list will always include Manual Entries and Unassigned.

Name – The name that is given to the device.

Site – The group of devices to which this device belongs. Sites can be grouped by geographical location or other criteria.

See Section 5.2, Sites.

Fixed – This box will be checked if the device is fixed camera, rather than a mobile camera. Enabled – This box will be checked if the device is currently enabled (see Section 5.1.4). Status – The Status field can display the following messages:

Device Added – If the device is newly added to the list, this message will display.

5.1.1 Default Devices (continued)

Offline – This device is a previously connected fixed camera that is not currently connected to BOSS.
Online Heartbeat – BOSS has detected a ping from a fixed camera.
Online Synced – The device's connection with BOSS has been established. This is shown for PAGIS mobile devices only and may not change when the device is offline.
Updated – Information has been sent from BOSS to the device, and the device is up to date.
Received Logins – Updates to the device included logins that were successfully sent to the device.
Received Source – BOSS has found the hotlist source file that it needs in order to send the updated hotlist to the device. Received Source may not be displayed due to timing or events.
Received Hotlist – The hotlist scheduled to be successfully sent has been sent to the device.
Received Hotplates – BOSS is sending "pages" of hotplates for a large hotlist, and the last page was successfully received.
Received Targets – The update to the device included targets that were successfully sent.

5.1.2 Defining a Device

Note: Devices will be defined automatically when a PIPS device, such as an ALPR camera, connects to BOSS the first time. Normally, there is no need to define devices in advance.

---

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Devices** shortcut. A list of existing devices will appear in the Browse/Edit area.
3. Click the **New** button.
4. Enter a name for the new device. (The name must be at least three characters long.) Note that the name **CANNOT BE CHANGED** once the device has been created.
5. Enter a **Description** for the new device. (The description must be at least three characters long.)
6. Select **Mobile** or **Fixed** in the Type field. By default, **Fixed** is selected. To change the current selection, click the **left** or **right** arrow.
7. Select a **Site**. Click the **Select** button next to the Site field to display a list of all available sites. Click on the desired site in the list and click the **Save** button.

Note: In addition to the two default sites, Manual Entries and Unassigned, which are created automatically when a new BOSS system is installed, other sites can be created by an authorized BOSS user. See Section 5.2, Sites, for more information.

---

8. Select **Owners**. Owners are groups that can access this device. For PAGIS units, user logins are sent only to devices where the group is an owner of the device. Click the **Select** button next to the Owners field to display a list of all BOSS groups. Select each desired group by clicking the checkbox. When the desired groups are selected, click the **Save** button. The group name(s) selected will be displayed in the Owners field.

9. Select **Latitude** and **Longitude** values for the geographical location of a device by typing in a value or using the up and down controls on each field to increase or decrease the value. Note that some devices, such as PAGIS units with a GPS attached, will automatically send the latitude and longitude of the device to BOSS.
10. Click the **Advanced** button to display additional options for the device.
    No Reads Alert – Defines how long the device must remain with no reads coming in before the system shows the device as offline.
    Alert Email – The email address or addresses to which alerts associated with this device should be sent.
    Retain Reads – The length of time that reads from this device should be saved in the BOSS database. The Retain Reads setting must be longer or equal to the Retain Images setting.
    Retain Images – The length of time that pictures captured by this device should be saved in the BOSS database.
    Retain Hits – The length of time that hits captured by this device should be saved in the BOSS database.
    SpikeStore – The PIPS High Resolution ANPR/ALPR Camera P382 and the PIPS Compact ANPR/ALPR Camera P372 (formerly the Spike P382 and P372 cameras) allow captured images to be stored in an on-board USB flash drive to be retrieved on demand. Setting a device as a SpikeStore device causes BOSS to attempt to retrieve images from the storage device when the read is requested for viewing.
11. When Advanced Options have been set as desired, click **Back** to return to the New Device screen.
12. Click the **Save** button to complete creation of the new device. The new device will now appear in the devices list above.

5.1.3 Editing a Device

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Devices** shortcut. A listing of all devices appears in the Browse/Edit area.
3. Click the desired device to select it. Details for the selected device appear in the Browse/Edit area.
4. Click the **Edit** button.
5. The Device Edit screen appears in the lower portion of the screen.
6. Modify fields as desired and click the **Save** button.

5.1.4 Enabling and Disabling a Device

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Devices** shortcut. A listing of all devices appears in the Browse/Edit area.
3. Click the desired device to select it. Details for the selected device appear in the Browse/Edit area.
4. Click the **Edit** button.
5. The **Device** Edit screen appears in the lower half of the screen.
6. Click the **Disable/Enable** button. The change will immediately close the edit window and return to the Devices screen. It will also take effect immediately.

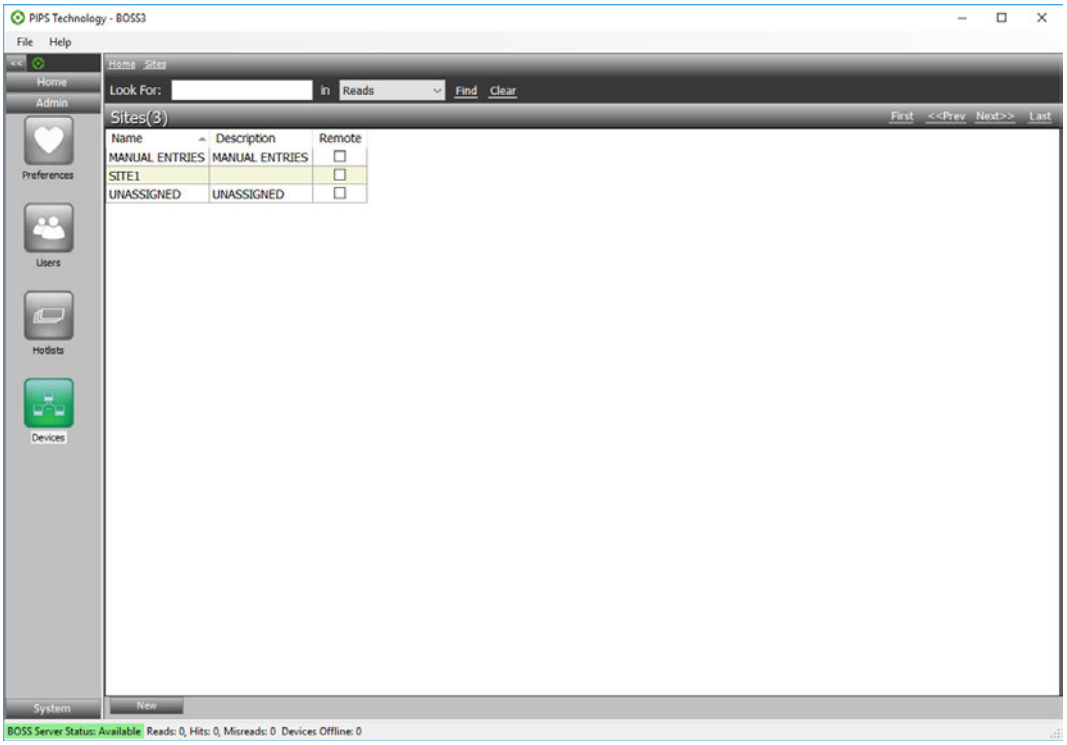
5.1.5 Deleting a Device

Note: It is strongly recommended that **devices are never deleted.** If a device is deleted, queries can no longer be performed using the device as a criterion. Instead of deleting a device, it should be disabled or given a new description.

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Devices** shortcut. (A listing of all existing devices will display in the Browse/Edit area).
3. Click the desired device in the listing.
4. Click the **Edit** button.
5. Click the **Delete** button at the bottom of the Browse/Edit area.
6. Click **Yes** to confirm the operation.

5.2 Sites

A site is a mechanism for organizing devices. This allows a BOSS Administrator to arrange devices into groups according to convenience, such as geographical area or a facility. The ability to group or arrange devices can be quite useful in large installations where there are many devices. Each device created must be assigned to a site.



5.2.1 Default Sites

A new BOSS site automatically contains two default sites, Manual Entries and Unassigned. Normally, a BOSS Administrator will want to create additional sites applicable to an organization.

5.2.2 Creating a Site

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Devices** shortcut.
3. Click the **Sites** button at the bottom of the screen. A list of existing sites will appear in the Browse/Edit area.
4. Click the **New** button at the bottom of the screen.
5. Enter a name for the new site. (The name must be at least three characters long.) Note that the name cannot be changed once the site is created.
6. Enter a description for the site. (The description must be at least three characters long.)
7. Select the parent site for the site. BOSS allows organizing sites into tree-like hierarchies. Click the **Select** button next to the Belongs To field, and select one site from the list. Click the **Save** button to complete the selection. The site name will appear in the Belongs to field.
8. Check the **Remote** option to designate the site as a remote site. (Remote sites are explained in Section 6, BOSS Data Sharing.)

5.2.3 Deleting a Site

Note: It is strongly recommended that sites are never deleted. If a site is deleted, queries can no longer be performed using the site as a criterion. Instead of deleting a site, it is recommended that devices assigned to it should be moved to another site.

---

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Devices** shortcut. A listing of all existing devices will display in the Browse/Edit area.
3. Click the **Sites** button at the bottom of the screen. A listing of existing sites will appear in the Browse/Edit area.
4. Click the desired site in the listing and click the **Edit** button.
5. Click the **Delete** button at the bottom of the Browse/Edit area. Click **Yes** to confirm the operation.

6 BOSS DATA SHARING

BOSS allows "linking" of multiple BOSS systems for data-sharing purposes. When a user issues a query from the Smart Client application that includes a remote site, the query is submitted to the local BOSS server, which in turn makes a query to the remote BOSS server(s). The combined results from all the sites are then returned to the Smart Client. **Data from remote sites is not stored in the local BOSS server.**

The following configuration steps need to be taken to permit BOSS data sharing:

6.1 Configuring BOSS to Allow Remote BOSS Queries

1. Create a BOSS user for remote access. This user account is a "proxy" the local BOSS server will use for all requests from a remote site. This user account will have "Reads" privileges by default; no other privileges need to be given. The user must be assigned to a remote group. (See Section 4.4, Groups, for information about flagging a group as remote.)
2. Give the username and password for this "proxy" user to the BOSS Administrator at the remote BOSS system. The remote BOSS will need to be configured to access this BOSS system, described in the next section.

Note: It is best to create a dedicated user account for remote sites—one that will not be used by an actual user to log in and access the application.

6.2 Configuring BOSS to Access a Remote BOSS Server

1. Obtain username and password from BOSS Administrator at the remote site.
2. Create a site for the remote BOSS server and select the **Remote** option.
3. Enter the remote site IP address and BOSS service port (23032 by default).
4. Add the username and password provided.
5. For each group that is allowed to query the remote BOSS server, assign the remote server to the user via the **Servers Access** option. (See Section 4.4, Groups, for information on selecting Servers Access.)
6. Log out of the application.
7. Log back on using the provided username and password. The Remote BOSS server can then be queried by selecting the desired servers in the Reads Query screen.

Note: BOSS version 3.2 and above only supports data sharing with servers running BOSS 3.0 and above.

---

7 HOTLISTS

A hotlist is a database that contains license plates of interest. When reads from license plate readers arrive at the BOSS server application, they are compared against hotlist records to find matches. Various hotlists can be enabled on a BOSS system and used in this comparison. In addition, hotlists can be assigned individually to specific devices. Only reads from those devices will be compared against these hotlist records. Typical hotlists include stolen vehicles, amber alerts, wants and warrants, etc. When the system reads in a plate that is determined to be a match to a hotlist entry in a hotlist, the BOSS application informs the user either with an alert sound and a pop-up window displaying a picture of the vehicle, or via email, depending on the user's preferences (see "Alerts via" in Section 5.3, Preferences).

A hotlist can be a database imported from an external source, such as another law enforcement agency. It can also be a list created by the local BOSS Administrator. For the BOSS server application to be able to understand how to import the hotlist records into the database, there are three different format types that exist in a BOSS system. In addition, there are several specific formats that are pre-defined and available by default when a new BOSS system is installed (see Section 8, Hotlist Formatters).

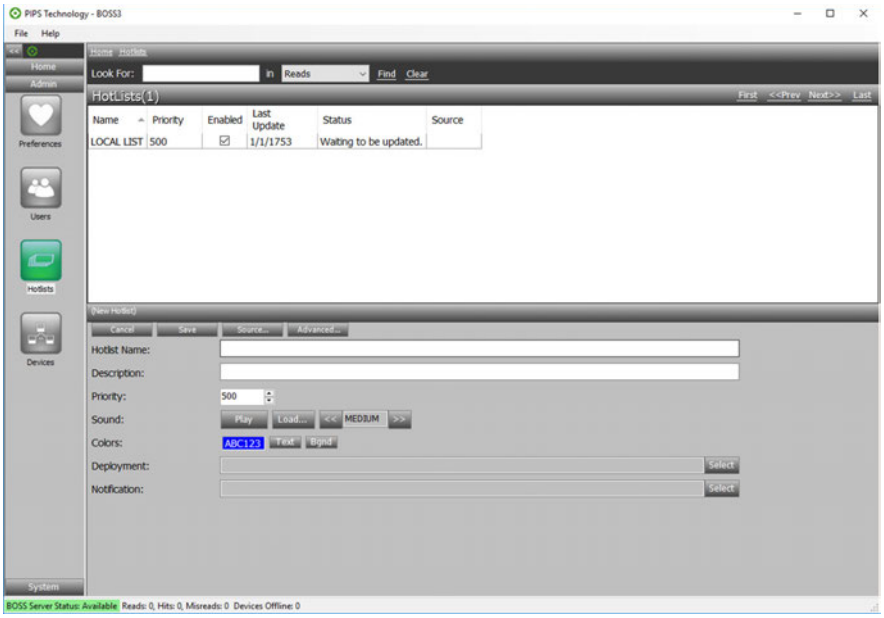
7.1 Creating a New Hotlist

There are three general areas to complete when creating a new hotlist:

- Configure basic settings
- Define a source file location with credentials when necessary.
- Define advanced settings (optional).

7.1.1 Configuring Basic Hotlist Settings

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Hotlists** button. Currently existing Hotlists appear in the Browse/Edit area.
3. Click the **New** button at the bottom of the Browse/Edit area. The New Hotlist Entry form appears.



4. Enter a **Hotlist Name** for the hotlist. It must be at least three alphanumeric characters, and it cannot be an existing hotlist name.
5. Enter a **Description** for the hotlist (optional).

6. Select a **Priority** for the hotlist. When there are multiple hits/alerts, the priority determines which alert will occur first. (The lower the number, the higher the priority.)
7. Select a **Sound** for alerts resulting from this hotlist (optional). Click the **Load** button to select a wave sound file (*.wav). To test the selected sound, click the Play button. Optionally, one of the three default sounds may be selected, **Low, Medium**, or **High** alert.
8. Select **Colors** for the alert if desired (optional). The default is white text on a royal blue background. Custom color settings affect the entries in dispatch. The background color also applies to alerts given in PAGIS.
9. Click the **Text** button to select a color for the text.
10. Click the **Bgnd** (Background) button to select a color for the background.

Note: Currently selected text and background colors are displayed in the sample box (showing “ABC123”).

---

11. Select devices for **Deployment**. Click the **Select** button to select devices from the list of those currently available. Click the checkbox next to a device in order to select it. When desired devices are checked, click the **Save** button to make the selection. One or more devices can be selected, and they will be displayed in the Deployment field.

Note: Deployment means distributing the hotlist to a device or devices. Only the devices where a hotlist is deployed will produce hits from the hotlist.

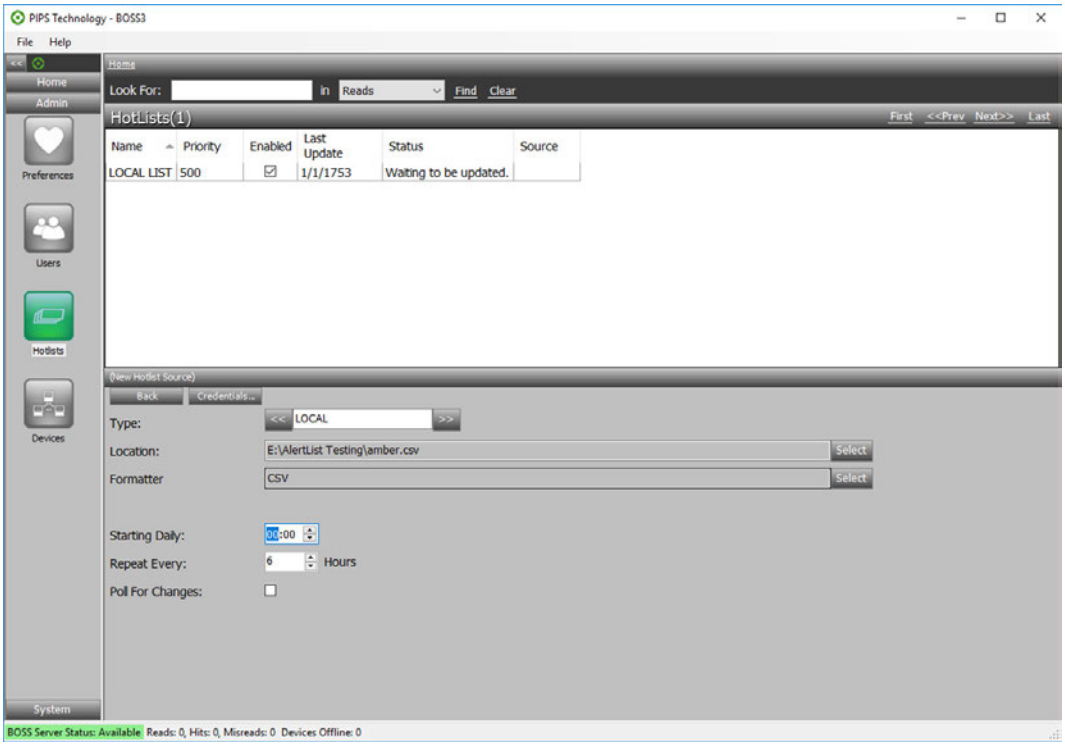
---

12. Select groups for Notification. Click the **Select** button to see a list of all BOSS groups. Click the checkbox next to a group to select the group. When you select a parent group, child groups are automatically selected. When desired groups are checked, click the **Save** button to make the selection.

Note: In order to receive alerts for hits on the hotlist, the user must be in the notification list of the hotlist. For more information see Section 7.1.5, Defining Hotlist Advanced Options.

7.1.2 Defining the Hotlist Data Source

1. On the New Hotlist Entry screen, click the **Source**... button to open the screen shown in the lower half of the following image:

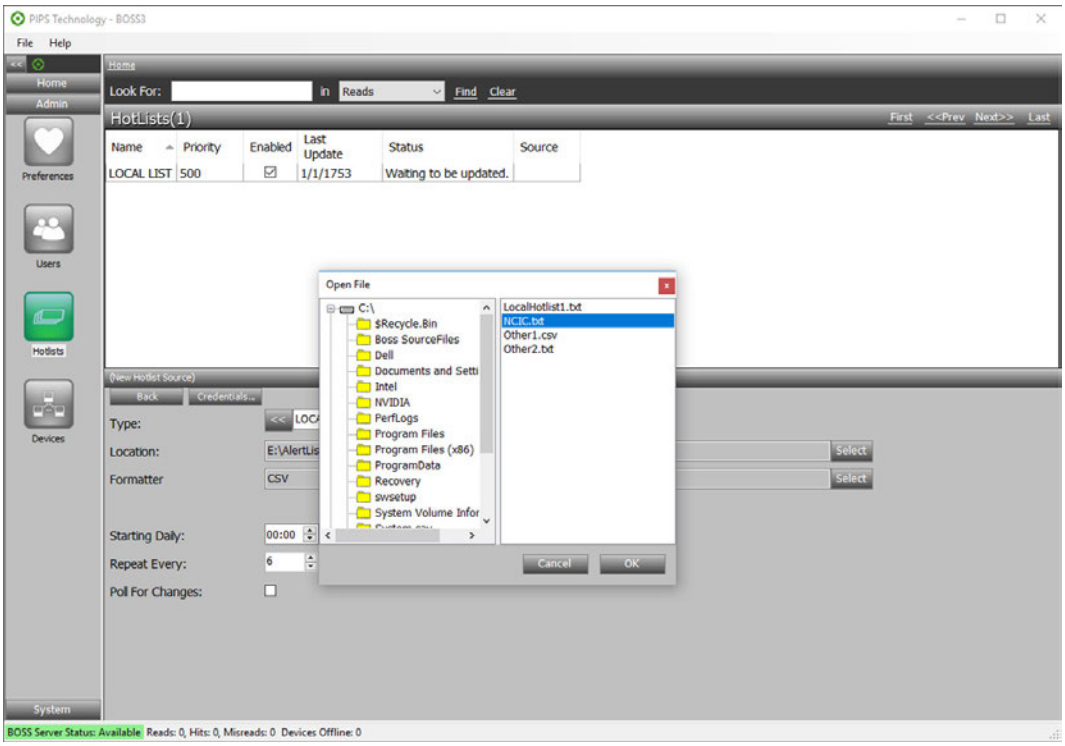


2. Choose the appropriate entries for each of the fields that describe the new hotlist:
   Type (**Network** or **Local**) – A local source means that the file is stored on the BOSS server's Windows file system. A network source means that the hotlist source resides outside the BOSS server.

Note: If a Local source is selected, the source file location (folder) must be accessible to the Windows process running the BOSS server application ("PIPS BOSS3" Windows service).

Location – Enter the location of the hotlist file. Click the **Select** button to the right of the location field.

For a local source, a file dialog will display, allowing you to navigate to a path and select a file.



For a network source, select one of the default locations displayed (if applicable), **or** type in the location of the source:

HTTP – The location format must be in Hypertext Transfer Protocol (HTTP) format: “http://server:port/path.” There are a few predefined HTTP locations (such as CA DOJ) included in BOSS. These locations can be accessed with the **Select** button. Boss also supports FTP & SFTP, examples : “ftp://server:21/path” , : ftp://server:22/path.

Remote BOSS System – The location format must be “boss://server:port/hotlist,” where “hotlist” is the hotlist name on the remote system.

Note: The remote system hotlist name **MUST** be alphanumeric and **CANNOT** contain any spaces.

Formatter – Formatter defines the way a hotlist database file is parsed into discrete fields. Click the **Select** button next to the Formatter field. A list of available formatters appears. Click on the desired formatter and click the **Save** button to make the selection. The name of the selected formatter will appear in the field.

Note: Normally one of the several default formatters included with BOSS is sufficient. A new custom formatter can be created if necessary. See Section 8.1, Creating a New Formatter for Hotlists, for more information.

7.1.2 Defining the Hotlist Data Source (continued)

Starting Daily – Specify the time of day the hotlist should begin updating each day. The time is formatted as hours:minutes in the 24-hour clock, i.e., between 00:00 and 24:00 can be selected.
Repeat Every – Specify the time interval, in hours (1 – 24), between updates.

OR

Poll for Changes – If you choose this setting, BOSS will check for updates to the hotlist approximately every 30 seconds. When this option is selected, the **Starting Daily** and **Repeat Every** options are disabled.

Note: If **Poll for Changes** is selected, and the hotlist source resides on the network, BOSS will attempt to make a network connection every 30 seconds. This frequency may add significantly to network traffic. Use with caution.

7.1.3 ZIP Compressed Hotlist Files

BOSS will automatically recognize and extract a hotlist data file contained in a ZIP archive file, such as Windows Explorer compressed (zipped) folder.

Note: There can be only one file in the ZIP archive.

7.1.4 Defining Hotlist Source Credentials

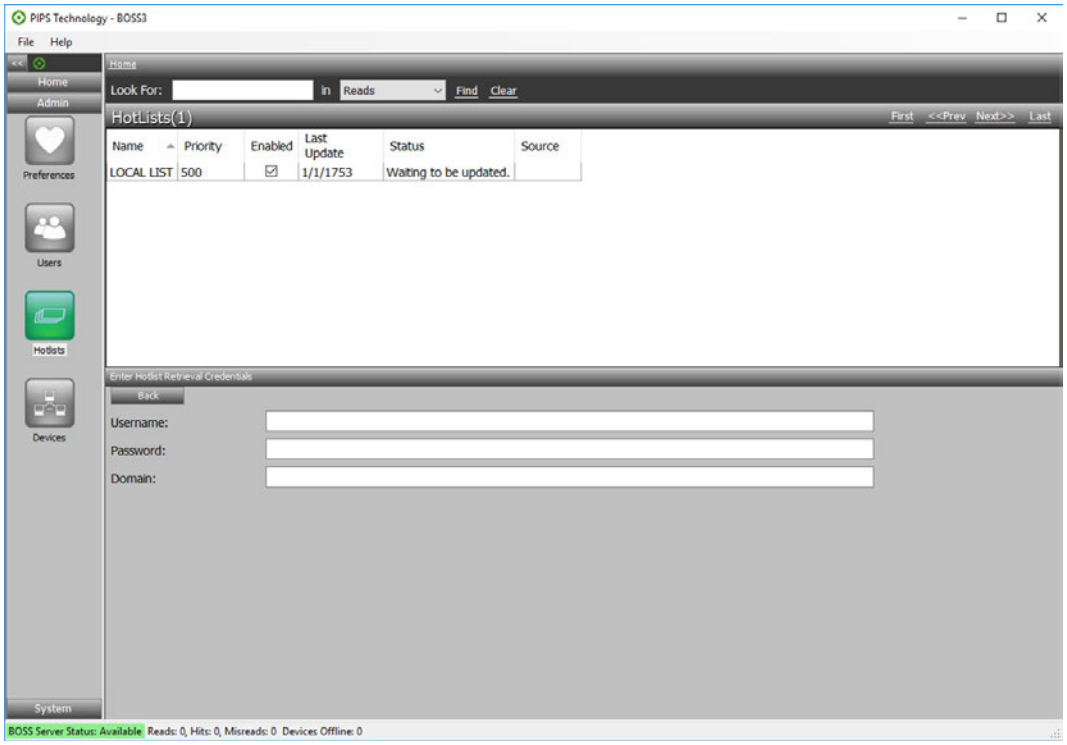
Some sources will require credential settings (e.g., login information) in order to allow BOSS to access that data. To enter the **Credentials** Settings screen from the Hotlist Source screen, click the Credentials button.
The credentials depend on the source type as follows:

Network-HTTP – If the HTTP (website) source defined requires login information, it should be entered in the Credentials Setting screen. This information will include username and password. The domain field may be necessary as well. Consult the Administrator of the HTTP source for required login information.

Network-Remote BOSS system – A username and password valid on the remote BOSS system must be entered (as in remote sites configuration, described in Section 6.0, BOSS Data Sharing). Consult the Administrator of the remote BOSS system for a username and password.

To set credentials for a source:

1. Click the **Credentials** button. The Credential Input screen appears.
2. Enter the username, password, and domain information applicable to the source you are specifying.
3. Click the **Back** button to return to the Source Entry form.
4. Click the **Back** button again to return to the New Hotlist Entry screen.



Advanced Options are values that allow you to further define details of the new Hotlist. To access the Advanced Options, click the **Advanced**... button.

Covert – A covert hotlist is one that contains sensitive information that should only be available to certain user groups. The effects of defining a hotlist as covert are as follows:

- A Hit on covert hotlist will not be alerted to users in mobile vehicle “Pagis”, unless the logged-in user is a Pagis administrator.
- A hit on the covert hotlist will not be alerted in the Boss application, regardless of the user’s alert preference. Hit alerts for covert hotlist can be send via email.
- When reads are queried, git information on covert hotlist will be displayed only to users in the Notification list for the hotlist. Other users will see that the read is a hit, but no information will be shown.
- Hit information for hits from covert hotlist will not be sent to remote Boss servers.

Whitelist – This option, when selected, defines the hotlist to be a whitelist, which works in reverse to a normal hotlist. A whitelist defines a list of plates that are **authorized** and not of concern. When a whitelist is active, license plates read that do **not** match an entry on the list will trigger a hit/alert.

7.1.5 Defining Hotlist Advanced Options (continued)

An example of whitelist use might be a secure parking lot where fixed camera devices are monitoring vehicles entering. Authorized plates will match entries in a whitelist hotlist. If a plate is read that does not match an entry in the whitelist, an alert occurs.

Whitelists and hotlists can be active simultaneously for a device.

Note: Whitelist support in PAGIS requires a separate license. If you do not have the license and wish to use whitelists, please contact your PIPS sales representative for further information.

Ext Trigger – This option, when selected, sets the External Trigger flag on a hotlist when it is passed to PAGIS. It is only supported in PAGIS version 2.6.6 or above and will have no effect on earlier versions of the software.
One Time – This option, when selected, specifies that the hotlist data should only be accessed from its defined source one time; no subsequent updating will occur after the initial import.
Alert Timeout – This setting allows you to define how current a hit (from this hotlist) must be in order to cause an alert. This primarily pertains to information coming in from mobile units, where there may be a large delay. Alert Timeout can be specified in minutes, hours, days, or months.
Delete Inactive – BOSS updates hotlists in an incremental manner, and instead of deleting hotlist entries that no longer exist, non-existent entries are marked as "inactive." If the entry subsequently becomes valid, the entry is marked as active again. The Delete Inactive value determines how long inactive entries are kept in the BOSS hotlist database.
Notify Email – One or multiple email addresses may be defined to receive an alert when there is a hit. Multiple

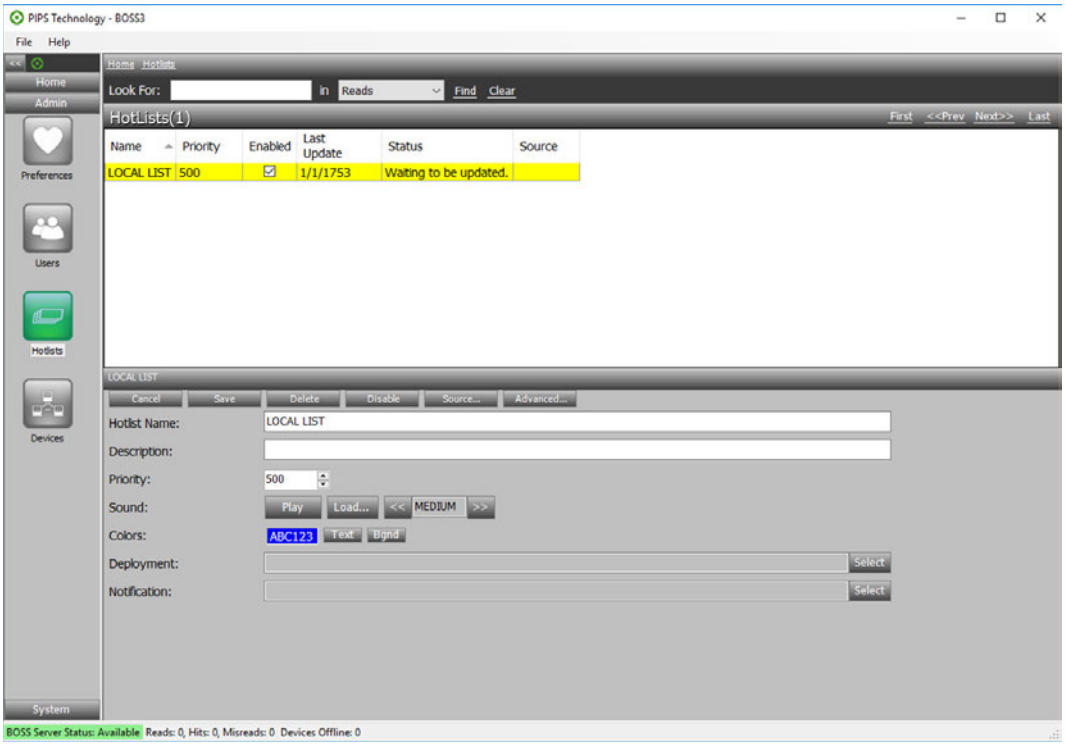
Note: If PAGIS mobile units are used, this value should be set to the longest time between begin shift downloads to PAGIS.

email addresses can be entered in the field, separated by a comma.
Remote Alerts To – Select the remote sites in which to send alerts. When a BOSS system sends an alert to a remote system, it is sent as a read; the remote BOSS system then determines whether to treat the read as a hit.

Note: This setting is only applicable if remote sites are defined.

Expires – Determines the date that the hotlist will stop importing data from its source. For a hotlist that is intended to be permanent, leave the expiration at the default value, 30 years from current date.

7.2 Enabling and Disabling a Hotlist



1. Select the **Admin** category on the Shortcut bar.
2. Click the **Hotlists** shortcut. A list of all hotlists appears in the Browse/Edit area.
3. Click the desired hotlist. Details for the selected hotlist appear in the Browse/Edit area.
4. Click the **Edit** button.
5. The Hotlist Edit screen appears in the lower half of the screen.
6. Click the **Disable** or **Enable** button.

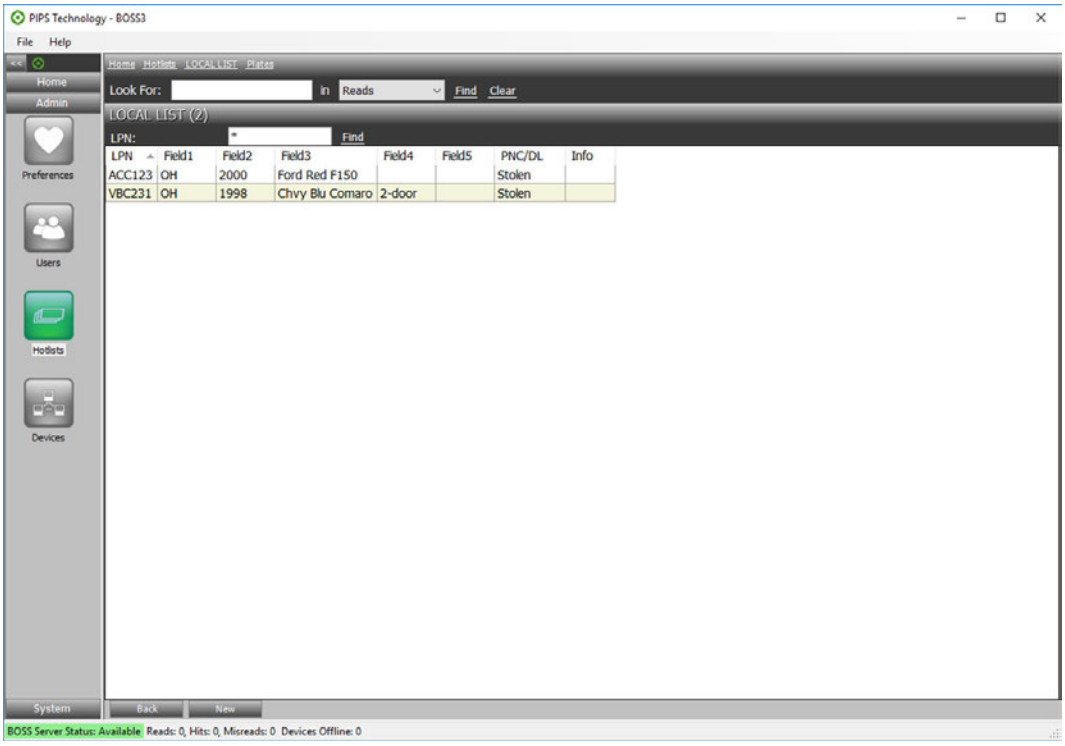
7.3 Modifying Hotlist Entries

BOSS allows viewing, adding, editing, and deleting hotlist entries.

Note: If the hotlist is set to update automatically, any changes to that hotlist made from within the BOSS User Interface application will be lost at the next automatic update.

7.3.1 Querying Hotlist Entries

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Hotlists** shortcut. A listing of all hotlists appears in the Browse/Edit area.
3. Click the desired hotlist. Details for the selected hotlist appear in the Browse/Edit area.
4. Click the **Plates** button.
5. The Hotlist Plates screen will be displayed.

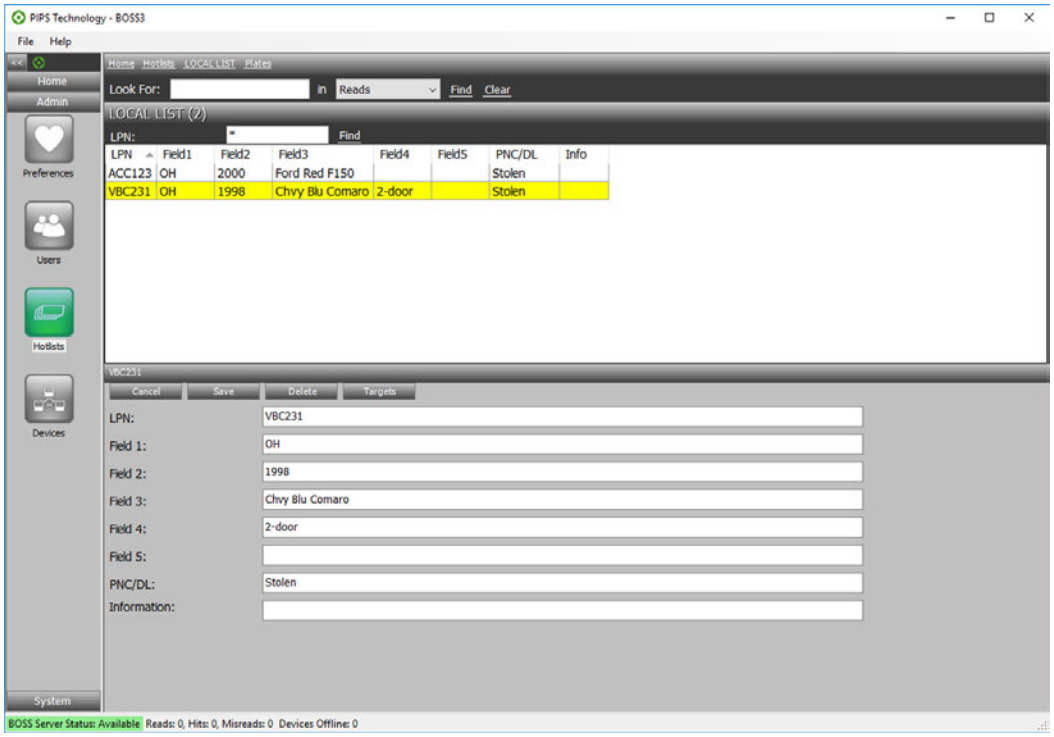


6. Type in the full or partial plate text to search for in the LPN field. (Wildcard searches are supported. See Section 11.1, Wildcards, for more information.)
7. Click on **Find**. License plates that match the criteria will be displayed. Note that only the first 1,000 matching license plates will be shown.

7.3.2 Editing a Hotlist Entry

1. Retrieve hotlist plates as instructed in the previous section.
2. Click on the row showing the desired plate.
3. The Plate Edit form will be displayed at the bottom of the screen.
4. Edit the field values as desired.
5. Click **Save** to save changes.

Note: Manually edited hotlist entries will be lost the next time the hotlist is updated.



7.3.3 Adding a Hotlist Entry Manually

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Hotlists** shortcut. A listing of all hotlists appears in the Browse/Edit area.
3. Click the desired hotlist to select. Details for the selected hotlist appear in the Browse/Edit area.
4. Click the **Plates** button.
5. Click the **New** button. The Plate Edit form will be displayed at the bottom of the screen.
6. Enter the **LPN** (mandatory) and other fields (optional).
7. Click **Save** to save changes.

Note: Manually edited hotlist entries will be lost the next time the hotlist is updated.

7.3.4 Deleting a Hotlist Entry

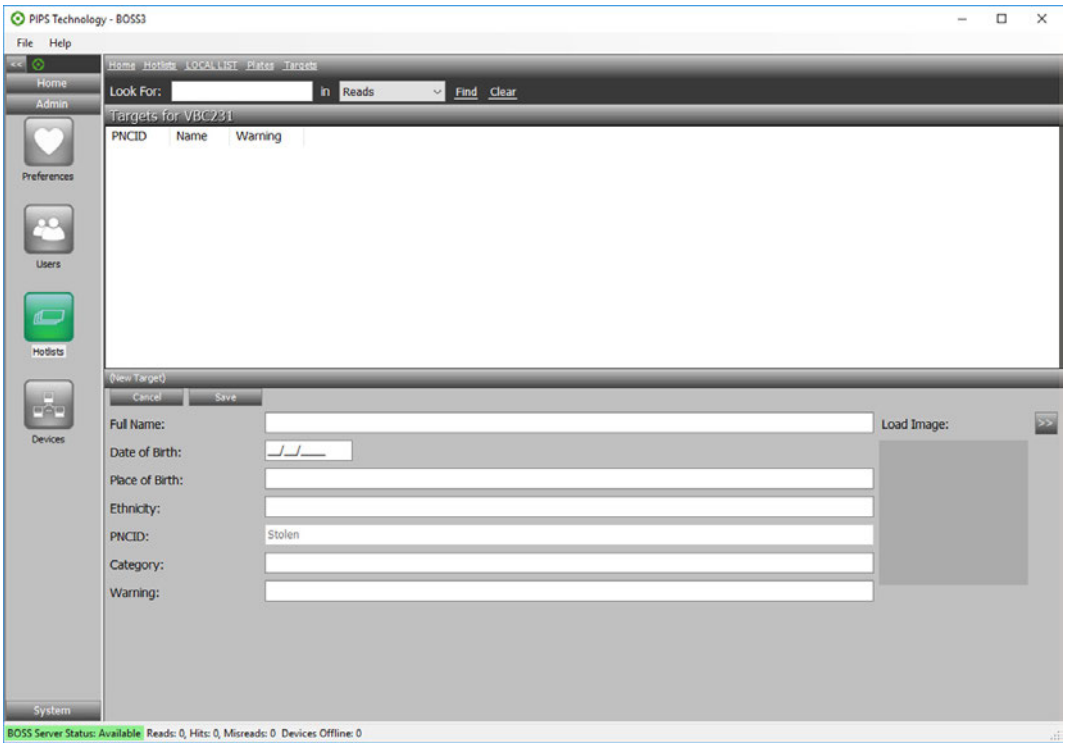
1. Retrieve hotlist plates as instructed in the Querying Hotlists Entries section.
2. Click on the row showing the desired plate. The Plate Edit form will be displayed at the bottom of the screen.
3. Click the **Delete** button.
4. Click **Yes** to confirm the deletion.

Note: Manually deleted hotlist entries may be re-added the next time the hotlist is updated.

7.4 Targets

Targets are individuals of interest associated with a license plate. Target information is downloaded to the PAGIS mobile application from BOSS.

1. Retrieve hotlist plates as instructed in Section 7.3.1, Querying Hotlists Entries.
2. Click on the row showing the desired plate.
3. The Plate Edit form will be displayed at the bottom of the screen.
4. Click the **Targets** button. Information about the target will display.



7.4.1 Creating a New Target

1. Click the **New** button.
2. The Target Edit form will be displayed.
3. Fill in the fields, listed below, with appropriate values.

   Full Name – The first and last name of the target. Date of Birth – The date of birth of the target.

   Place of Birth – The location where the target was born.

   Ethnicity – The ethnicity (race or national origin) of the target.

   PNCID – This field can be used to enter any type of identification number that is available. In the UK this is the Police National Computer identification number of the target. This field is linked to the PNCID field in the hotlist information in the PAGIS application. *See the sample INI configuration file in Section 5 of the Pagis Software User's Manual.*

   Category – The category of the target, such as Felon, Suspect, etc.

   Warning – The warning information to display to the officer.

   Load Image – An image of the target, such as a DMV photo or "mugshot," can also be associated with the Target record. Upload an image by clicking on the Select button and browsing to the image file. Supported formats include JPG, GIF, or BMP.
4. Click the **Save** button.

7.4.2 Deleting a Target

1. Access the Targets screen as described above.
2. Click the row containing the target to be deleted.
3. The Target Edit form will be displayed.
4. Click the **Delete** button.
5. Click **Yes** to confirm deletion.

8 HOTLIST FORMATTERS

Hotlist Formatters define the structure of source data that is imported into BOSS Hotlists. BOSS includes several default formatters when the software is installed. There are three types of formatters:

CSV (comma-separated values) – A flat text file containing one line for every record. Each field in the record is separated by a comma.

Fixed Length – A flat text file containing records that are all the same length. No separator characters are used to determine where each field ends and another begins, but rather, field and record lengths are known up front. In a fixed length file, padding spaces are used where necessary, to accomplish the correct field length.

NCIC (United States National Crime Information Center) – The NCIC database is a computerized index of criminal justice information (i.e., criminal record history information, fugitives, stolen properties, missing persons, etc.), that is available to law enforcement agencies 24 hours a day, 365 days a year. Several NCIC import sources/formats exist within BOSS.

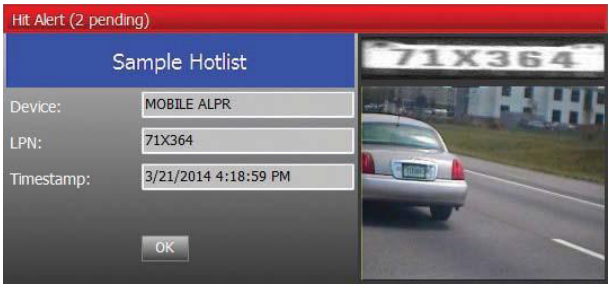
8.1 Creating a New Formatter for Hotlists

Normally, when creating a new hotlist, you will find that one of the default formatters can be used. However, BOSS does give you the flexibility to create new hotlist formatters. Creating a new formatter or modifying an existing formatter should be approached with caution and is beyond the scope of this manual. For more information, please contact PIPS™ Technical Support.

9 ALERTS

BOSS can provide real-time alerts on-screen, via the BOSS User Interface application, or through email. In order to receive alerts through the BOSS application, **the logged-on user must be in a group that is assigned the Dispatch permission**. Email alerts can be sent to any BOSS user or email recipient.

A real-time alert for a hit can pop up on the screen at any time when the BOSS application is running, regardless of which screen the user has active. A sound associated with the hit will be played. Alerts will be queued until the user acknowledges them by clicking **OK**. Real-time alerting in the BOSS application can be turned off by clicking on the **Alerts** toggle button on the BOSS Home screen. The settings for real-time alerts can be modified through the Dispatch screen, (see Section 10, Dispatch).

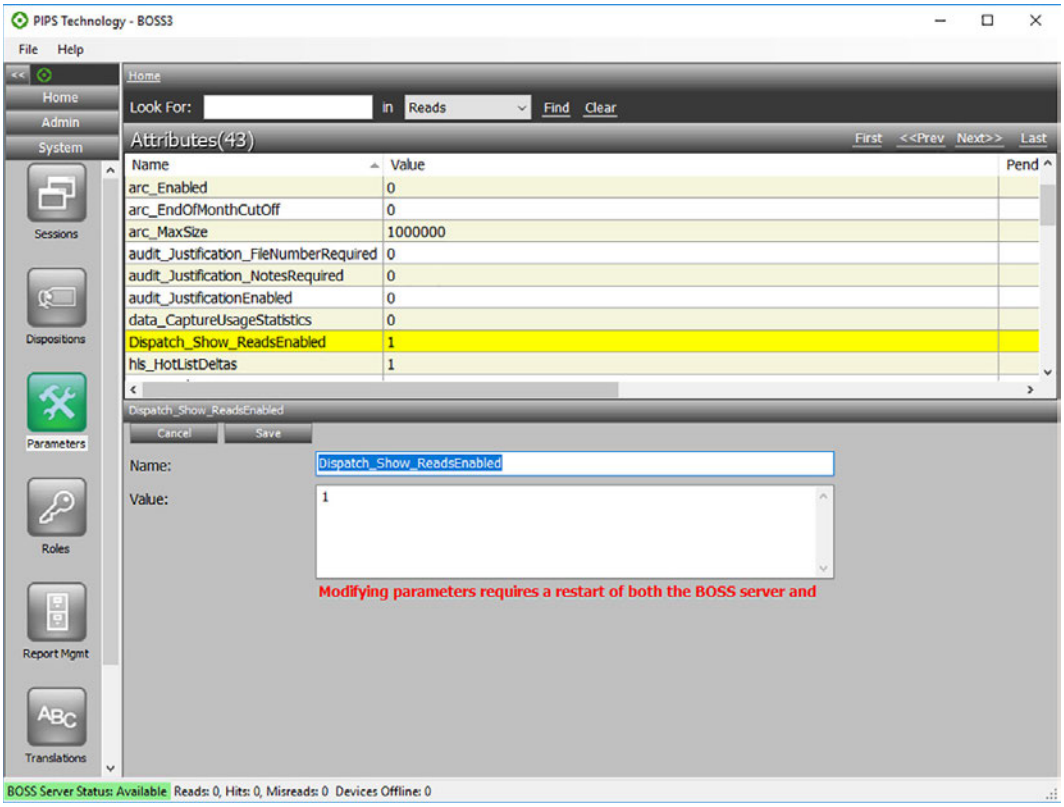


10 DISPATCH

The Dispatch screen is a tool often used by first responder dispatchers. It enables them to easily view hits, monitor reads, and correct license plates as they enter the BOSS system. The information displayed is as near to real time as possible. For ease of viewing, there are three configurations that can be set:

- If only the hits are set to display, they will appear on the whole screen.
- Similarly, if only the reads are set to display, they appear on the whole screen.
- Of the dispatcher is monitoring both hits and reads, then the hits will be displayed on the top half of the screen and the reads will be displayed on bottom half.

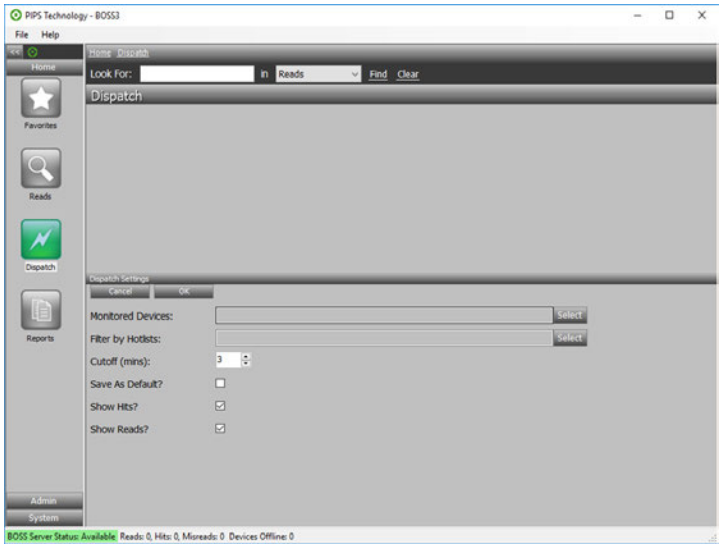
Note: By default, the ability to monitor reads via dispatch is disabled for new Boss installations, this feature can be turned back on by editing the Boss parameter “Dispatch_Show_ReadsEnabled” and setting the value to 1 for on. The Boss service must be restated for this to take effect.



10.1 Dispatch Settings

Dispatch Settings allow you to choose the information shown on the Dispatch screen.

1. Select the **Home** category in the Shortcut bar.
2. Click the **Dispatch** shortcut.
3. Click the **Settings** button in the bottom of the Browse/Edit area.



4. The following settings are available on the Dispatch screen. Change these settings as desired:

   Monitored Devices – Camera sources can be selected or deselected from a pick list to control which ones will supply reads (and resulting hits) to the Dispatch screen. Individual dispatchers can focus on particular camera inputs by selecting/deselecting any combination of sources (one, multiple, or all) for monitoring.

   In large BOSS systems, it may not be practical for a single dispatcher to monitor all sources simultaneously. An organization may choose to assign individual dispatcher personnel to different sources or may select to focus on particular sources during certain time periods or events.

   Filter by Hotlists – Hotlists may be selected to only show hits from designated hotlists. If there are no hotlists selected, hits from the monitored devices will be displayed.

   Cutoff (mins) – The cutoff setting determines how current from the present time a hit or read must be in order to display on the dispatch screen This setting determines the number of minutes before data is discarded from the on-screen display. The maximum time is 10 minutes.

   Save As Default – If checked, the current settings are saved and restored the next time the user logs in. Note that selected devices will always default to the devices where the user is configured to receive notifications in the Hotlist settings. See additional information on notifications in Section 7.1.1, Configuring Basic Hotlist Settings.

   Show Hits? – If checked, hits will display in rows in the top section of the Dispatch screen as they occur. If this option is deselected, rows of hits are not displayed in this section of the Dispatch screen. However, pop-up alerts will still display for hits, regardless of this setting.

Note: If the Alert Toggle button is set to the Off position, hits and reads will not display in the Dispatch screen. See Section 9, Alerts, for additional information.

   Show Reads? – If checked, all reads included in the devices selected in the Monitored Devices field display in the dispatch screen. By default, this option is not selected.

Note: Monitoring reads may slow down the BOSS server. It is recommended that reads are only monitored for diagnostics purposes.

5. Click the **Save** button for the changes to take effect.

10.2 Dispatch Hits

For each row, the columns displayed are:

Device – The device where the read originated.
LPN – The license plate characters read in by a camera or manually entered by a user.
Timestamp – Date and time when the read occurred.
Syntax – The state or region of the plate, if available.
Misread – If checked, indicates that the hit resulted from a read that was marked as a misread. Manual – If checked, indicates that the hit resulted from a manual entry (put in by a BOSS user). Patch – A thumbnail image of the license plate.
Overview – Color overview picture of the vehicle.
Hotlist – The name of the hotlist from which the hit occurred.
Field1 ... Field5 – Fields originating from the hotlist. The content and meaning of these fields vary depending on the composition of the hotlist.
PNC/DL – This field can be used for a driver's license (DL) number in US installations, but primarily used in United Kingdom installations for storing the UK Police National Computer identification number.
Info – Commonly contains additional text associated with the hit record. When the hotlist source contains additional fields, the information from those fields is all stored in this one field.
Priority – Priority assigned to the hotlist, with a lower number being given a higher priority.
Annotation – Notes associated with the read. Annotations are entered by BOSS users.

10.3 Dispatch Reads

For each row, the columns displayed are:

Device – The device where the read originated.
LPN – The license plate characters read in by a camera or manually entered by a user.
Syntax – The state or region of the plate, if available. Timestamp – The date and time when the read occurred. Patch – A thumbnail image of the license plate.
Overview – Color overview image of the vehicle.
Misread – If checked, indicates that this record was marked as a misread.
Hit – If checked, indicates this read resulted in a hit.
Manual – If checked, indicates this read was input manually by a BOSS user, rather than originating from a device.
Annotation – Notes associated with the read. Annotations are entered by BOSS users.

10.4 Manual Entries

There may be times when a read must be manually entered or when a camera does not correctly read a plate. For example, if there was an obstruction between the camera and the plate, then characters may be missed in the read. For this reason, manual entries can be completed by an authorized user via the Dispatch screen.

10.4.1 Adding a Manual Read

1. From the Dispatch screen, click the **Add** button. The Manual Entry screen appears in the lower half of the Browse/Edit area.

Note: The **Add** button will only be present if the logged in user has the Edit Access permission to reads.

2. Enter the plate characters in the LPN field.
3. Click the **Select** button to the right of the disposition field.
4. Select the desired disposition(s) and click the **Save** button to complete the selection.
5. Click the **Save** button to finish saving the manual entry. If the "Manual Entries" device is not being monitored, the manual entry will not appear in the Dispatch screen.

10.4.2 Correcting Reads

1. From the Dispatch screen, click the Add button. The Manual Entry screen appears in the lower half of the Browse/Edit area.
2. Enter the plate characters in the LPN field.
3. Click the **Select** button to the right of the disposition field.
4. Select the desired disposition(s) and click the **Save** button to complete the selection.
5. Click the **Save** button to finish saving the manual entry. If the "Manual Entries" device is not being monitored, the manual entry will not appear in the Dispatch screen.

11 QUERYING STORED DATA

The Reads screen allows for searching and viewing past read records on a local server or on a remote server that has granted access. Reads can be quickly searched by entering a license plate number. This screen also allows for more advanced queries where data can be filtered based on additional fields such as date ranges, location, and radius. Additionally, the Reads screen allows you to perform multiple queries with the use of tabs.

For the queried results returned, there are no limits to the number returned from a local server. To limit the impact on outside systems, there is a limit of 1,000 records returned from a remote server. A maximum of 1000 records will be displayed per page.

Note: Depending on factors such as the size of the BOSS database, the speed of the server, the bandwidth of the connection between client and server, and the parameters of the query, there may be a delay before the results are displayed. A status bar will display that shows that the query progress.

11.1 Wildcards

Wildcards are special characters that represent any alphanumeric character and can be used in searches and queries. Wildcards can make finding a match easier because they can define a portion of the criteria to be ambiguous. Wildcards supported in BOSS are described in the following table.

WILDCARD USED	REPRESENTS
a%	Any values that start with the letter “a”
a	Any values containing “a”
% or *	Any/all values
a_	Any values that are exactly two characters long and start with “a”
_a*b	Any values that have “a” as the second letter and end with “b”
[abc]*	Any values that start with “a”, “b” or “c”

11.2 Quick Search Bar

The Quick Search bar is always visible and available on the top of the BOSS screen regardless of the category or shortcut currently selected. This feature allows for quick, simple searches of various BOSS data.

1. Type the value to search for in the Look For field. This value can include wildcard characters. Multiple values can be entered separated by a comma (e.g., ABC123, XYZ234). However, wildcard values cannot be used when searching for multiple values.
2. In the “In” drop-down box select an area to search. The available options are **Reads**, **Hotlists**, **Users**, **Group Users**, **Groups**, **Devices**, and **Sites**. These areas are described below.
3. Click the Find link to initiate the search. The results will be displayed in the Browse/Edit area of the screen.

11.2.1 Quick Search Fields

When performing a query using the quick search feature, keep in mind that the search is performed in one significant area that can be selected. The search is then run against the significant field in that area, not all fields in that area. For example, when performing a quick search in Users, the text entered is compared against the Username field of all user records.

However, it is not compared to the display names for users. The following is a list of the fields used in the Quick Search:

SEARCH IN AREA	FIELD USED FOR SEARCH
Reads	LPN
Users	Username
Groups	Group Name
Site	Site Name
Hotlists	Hotlist Name
Group Users	Group Name
Devices	Device Name

11.3 Query Result Navigation Icons

Just above the query results are navigation icons that facilitate moving through the data results. These icons can be very useful for larger result sets, providing an easy way to move through records.



Move to the very beginning of the data results, i.e., the first record.



Move forward through the data results.



Move backward through the data results.



Move the very end of the data results, i.e., the last record.

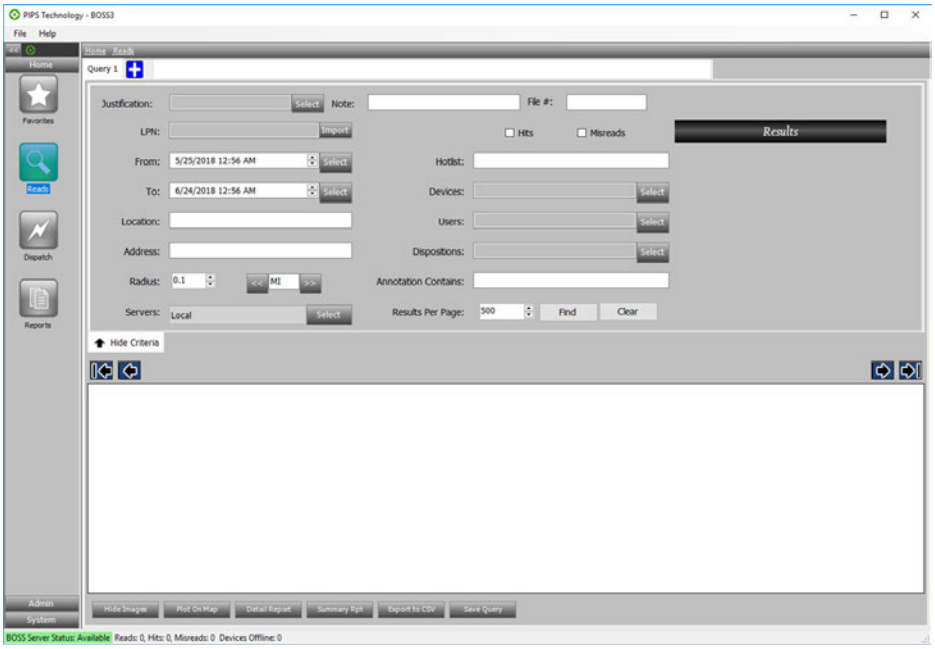
11.4 Advanced Reads Queries

The Reads screen allows for searching and viewing past read records. Reads can be quickly searched by entering a license plate number. The Reads screen also allows for more advanced read queries where data can be filtered based on additional fields such as date ranges, location, or radius. As indicated earlier, a maximum of 1000 records will be displayed.

11.4.1 Performing an Advanced Reads Query

1. Select the **Home** category on the Shortcut bar.
2. Click the **Reads** shortcut.
3. Enter desired query criteria (see the following section, 11.4.2, Entering Advanced Reads Query Criteria). All fields do not have to be filled in. Leaving a query field blank simply means there will be no filtering on that field.
4. Click the **Find** button to run the query.

11.4.2 Entering Advanced Reads Query Criteria



The query criteria fields are:

LPN – Full or partial (using wildcards) license plate number.
From – The start date and time for reads to be retrieved. Either click the **Select** button to display a calendar for quick selection, or type in the date.
To – The end date and time for reads to be retrieved. Either click the **Select** button to display a calendar for quick selection, or type in the date.
Location – The location as entered in the PAGIS application (see the Pagis Software User's Manual for more information).
Near Address – An address to use as the center of a radius search. The address format depends on the mapping system used but typically street name, house number, city and state, or zip code can be entered.
Radius – When a Near Address filter is entered, the search radius from the center point must be entered here.
Servers – Information can be queried from one or more remote BOSS servers. Click the Select button to display a list of authorized BOSS servers.
Justifications – Select the justification that best describes the purpose for the query being performed. This field will only be displayed if Justifications have been enabled in the System Parameters. See Sections 15.3.2, List of BOSS System Parameters, and 15.7, Justifications, for more information.
Justification Note – Enter any additional information necessary to more accurately document the query being performed. This field will only be displayed if Justifications have been enabled in the System Parameters. See Sections 15.3.2, List of BOSS System Parameters, and 15.7, Justifications, for more information.
Hits Only – If checked, only hits are queried.
Misreads Only – If checked, only reads that are marked as misreads are queried.
Hotlist – A search on hits can be limited to a specific hotlist, which can be entered here.
Devices – A query can be narrowed to reads originating from a particular device. Click the Select button to display a list of devices, select one or more.
Users – A query can be narrowed to reads originating by a particular user. Click the Select button to display a list of users and select one or more.

Note: The username can also be typed in.

Dispositions – A query can be narrowed to reads with a particular disposition. Click the **Select** button to display a list of dispositions. Then select one or more dispositions.

Annotation Contains – If text is entered in this field, only reads that contain the text in the annotation field are queried.

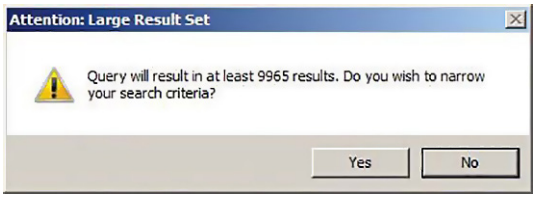
Results Per Page – The maximum number of reads that will be displayed. The default is 500, the maximum is 1,000.

Clear – If clicked, the fields on the current tab will be returned to their default values.

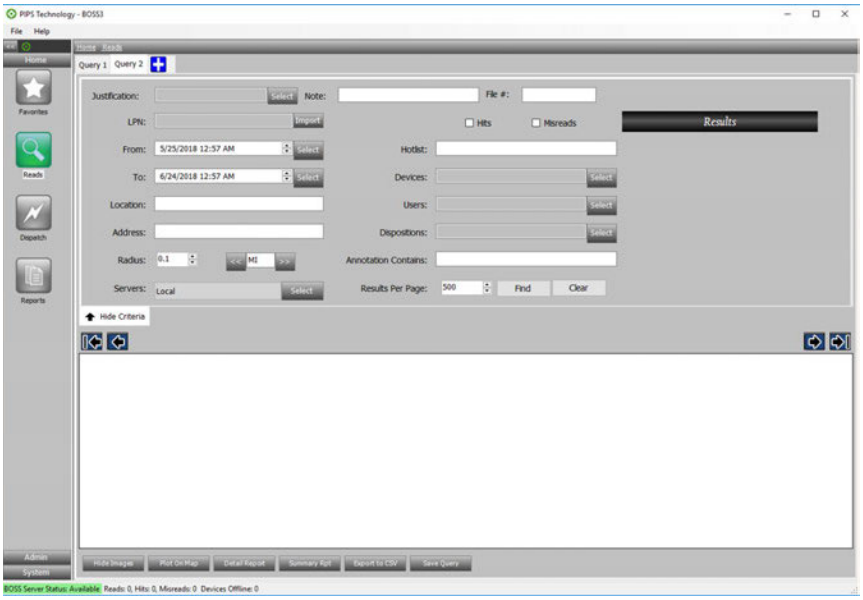
11.4.3 Managing Query Results

With the ability to obtain any number of results from a local server comes the option to narrow the potential results to be returned. If a large number of results will be returned based on the criteria entered, a message is displayed asking if the search criteria should be narrowed. If you select **Yes**, the search criteria is redisplayed offering the chance to make any necessary changes to reduce the results. If you select **No**, the query is performed based on the current criteria selections.

Note: A large number of results can take several minutes to be displayed.



11.5 Multiple Query Tabs



With Query tabs, users can perform multiple queries at a time. By clicking on the last tab, which contains the plus icon, you can access additional Reads Query screens. Enter the desired search criteria on each new screen to obtain additional information through the varying results. Each query can be given a descriptive name by right-clicking on the tab, and obsolete queries can be removed the same way.

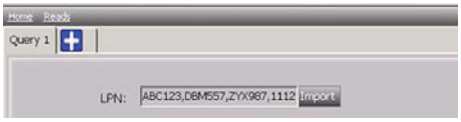
11.6 Cross-Referencing External Data

BOSS allows cross-referencing external data, such as DMV information. To query BOSS based on external information, take the following steps:

1. Create a CSV text file containing the license plate numbers to be cross-referenced. **The license plate number must be in the first field.**
2. Open the Reads Query screen.
3. Click the **Import** button next to the LPN field.



4. Click **Open** to import the plate numbers. A maximum of 50 plate numbers can be referenced at a time. Imported plate numbers will show up in the LPN field:

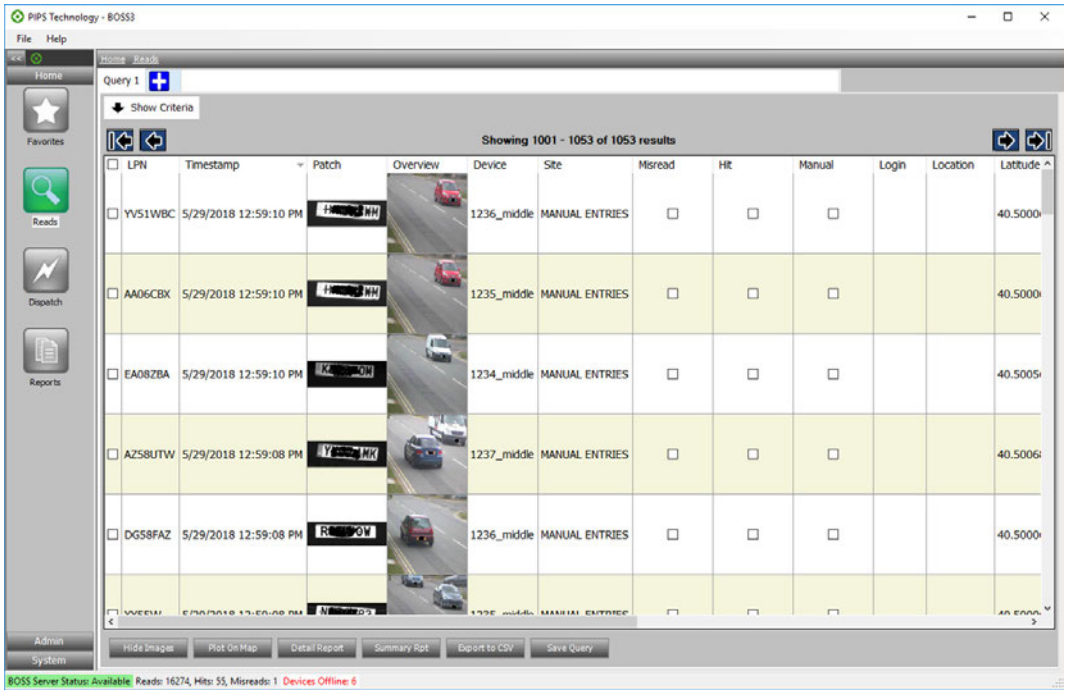


5. Enter other query criteria, as needed, and click **Find** to run the query.

11.7 Working with Queried Reads

11.7.1 Viewing Query Results

The results of both Quick Searches and Advanced Reads Queries are presented in the same manner.



The columns displayed are:

LPN – The plate text (characters) read in by a camera or manually entered by a user.
Timestamp – The date and time when the read occurred.
Patch – A thumbnail image of the license plate. Overview – The color overview picture of the vehicle. Device – The device where the read originated.
Site – The site where the read originated.
Misread – Indicates whether the read was marked as a misread by a user.
Hit – Indicates whether the read is a hit.
Manual – Indicates whether the read was entered manually.
Login – The username logged into the device at the time the read originated.
Location – The location entered in the PAGIS system. See the Pagis Software User's Manual for more information.
Latitude – The latitude coordinates of the device at the time the read originated. Longitude – The longitude coordinates of the device at the time the read was originated. Hotlist – The name of
the hotlist that produced the hit.
Field1 ... Field5, PCNID, Information – Information from the hotlist that produced the hit.
Annotation – Annotations entered for the read.
Server – The name of the server that has provided this information. This can be a local or remote server.

11.7.2 Query Results Actions

There are several button options available at the bottom of the Reads Query Results screen that offers additional uses of the data results.



Hide Images/Show Images – Used to remove the image columns, patch and overview, from the view. This can be done to provide more room for text fields to be displayed. When clicked, the Hide Images button's caption changes to Show Images. When the button is clicked again, images will again be displayed.

Plot On Map – When clicked, any selected records will be plotted on a map. One or multiple records can be selected by clicking the checkbox in the first column of the record. To select all of the records, click the checkbox in the headings column.

Detail Report – Click to generate a detailed report of selected reads. To select one or more records, click the checkbox in the first column of the record. To select all of the records on the current page, click the checkbox in the headings column. Use the navigation buttons to move to additional pages to select additional records.

Summary Rpt – Click to get a summary report of selected reads. To select one or more records, click the checkbox in the first column of the record. To select all of the records on the current page, click the checkbox in the headings column. Use the navigation buttons to move to additional pages to select additional records. To include all results choose the All Results option in the Reads Summary Detail Report option box.

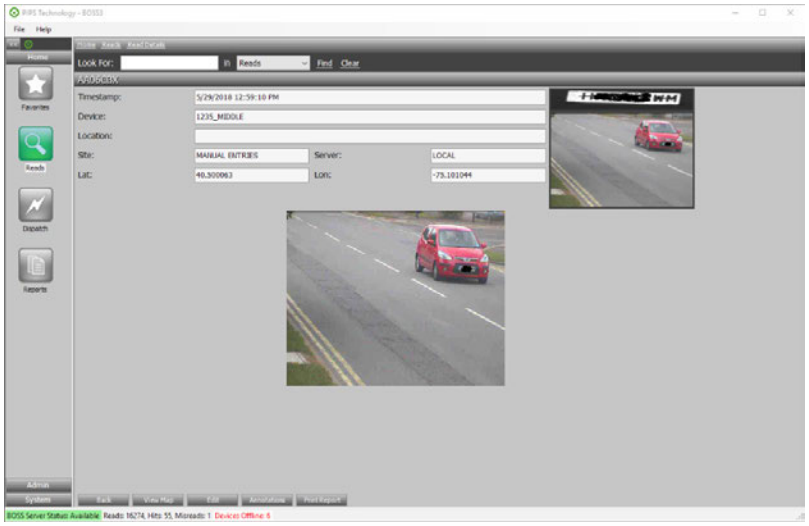
Export to CSV – Click to save the results to a file in a CSV format. Select to save the current page or all results provided. Use the navigation buttons to move to additional pages to select additional records.

Save Query – Click to save the query criteria as a favorite for future use. See Section 11.8, Favorites, for more information.

11.7.3 Viewing Read Details

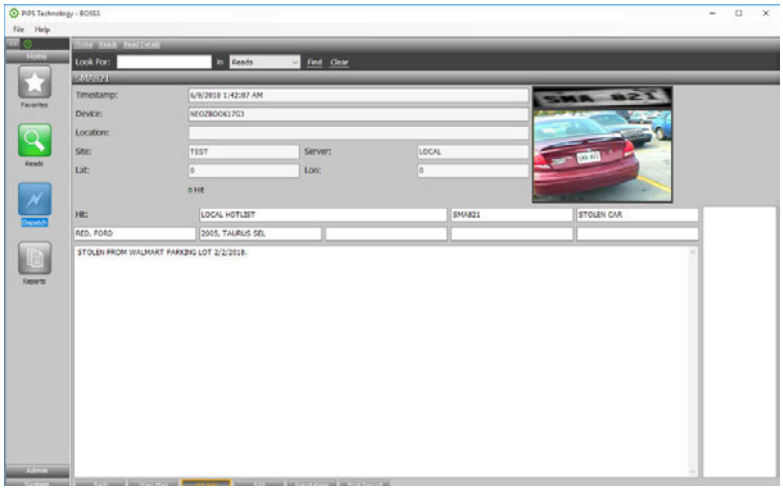
Click a row in the query results to view the details of the record.

The Read Details screen displays the license plate text in the title. The timestamp, originating device, site, and geographical coordinates are displayed below. The plate patch and vehicle color overview images are on the right.

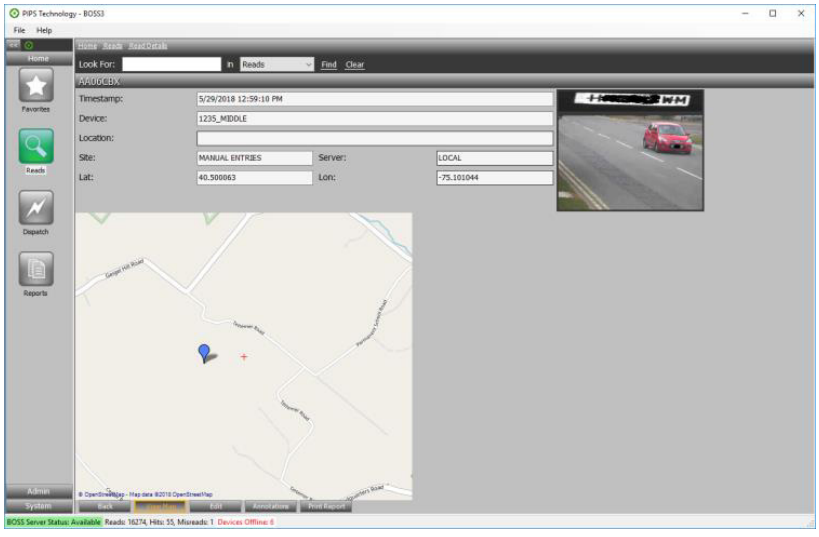


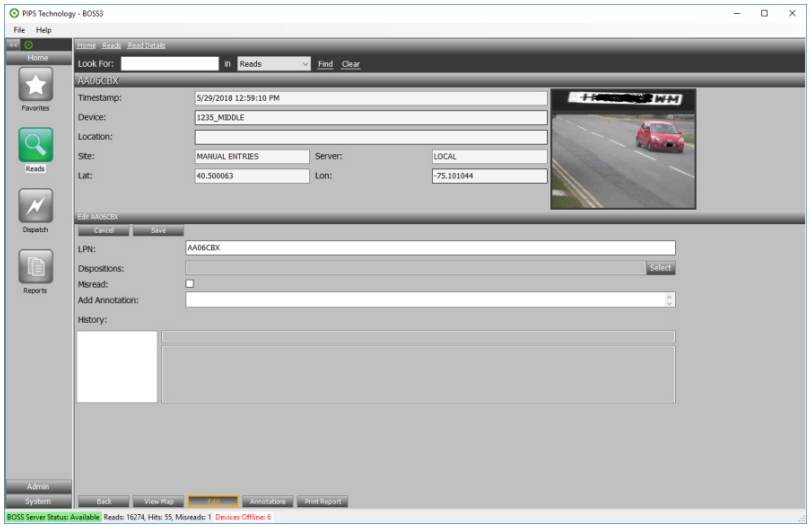
The vehicle color overview picture can be enlarged by clicking on the picture. Use a mouse scroll wheel or the cursor up and down keys to resize the image. Left-click on the enlarged image to close. Right-click on the image to copy the image to the Windows Clipboard.

If the read is a hit, details of the hit can be displayed by clicking on the Hit Info button at the bottom of the screen.

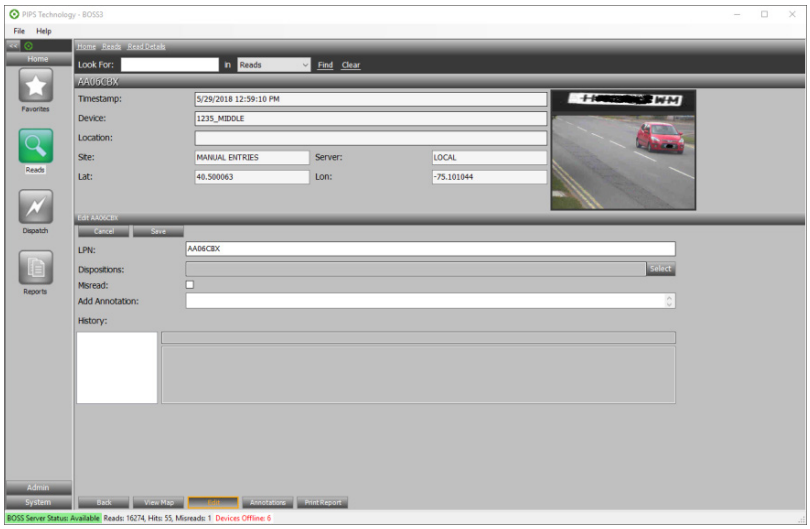


A map plotting the location where the read occurred can be displayed by clicking on the View Map button.

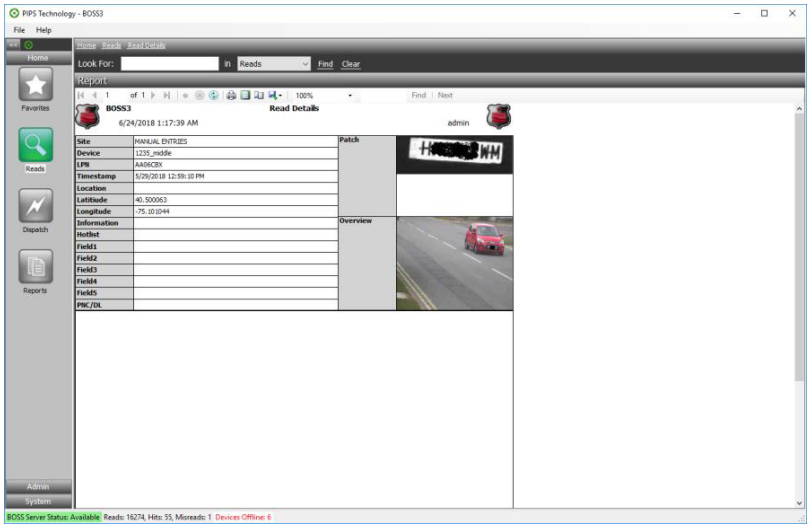




Use the Edit button to correct the plate text and/or assign a disposition and annotation to the read. Click on Save to save the changes. The plate text can also be marked as misread if the read information is found to be incorrect.



Annotations associated with the read can be viewed by clicking on the Annotations button.



A report containing the read's details can be printed by clicking on the Print Report button.

11.8 Favorites

Favorites are read queries that use specified criteria, which have been saved. Favorites can be reused, which allows the user to quickly perform frequently needed queries without having to define the parameters each time. Favorites are specific to each user.

11.8.1 Creating a New Favorite

1. Select **Home** on the Shortcut bar to access its icons.
2. Click on the **Read** shortcut.
3. Enter the desired query parameters in the Browse/Edit area (e.g., data range, location, radius, servers).
4. Click the **Go** button to run the query.
5. When the query results window appears, click the **Save Query** button.
6. A dialog box will appear, prompting for a name. Enter a descriptive name for the new favorite.
7. Select the Use Relative Date Range option if desired.

   Use Relative Date Range Option – If this option is selected when saving a query, and when the resulting favorite query is run in the future, it will use a From and To date and time range relative to the From and To date and time entered for the original query. It will not use the actual range entered in the original query. Also, it is important to remember that the time span between the From and To date and the time range used is relative to the date and time when the original query was run.

   Consider a query that is saved as a favorite and originally defined on 8/9/20xx to search reads between 8/02/20xx and 8/8/20xx (the prior week). If the Relative Date Range option is selected, the query is saved to always run against the prior week rather than those actual dates. If the Favorite option is invoked on 12/3/20xx, it will return results from 11/26/20xx through 12/2/20xx. It is important to note that the results will be relative to the actual time of the original query and when it is rerun. Suppose you run a query at 5 pm today to search for reads occurring between 9 am and 5 pm and save it as a favorite. When you run the query again tomorrow, it will search for reads that occurred eight hours **before** the current time, which may not necessarily fall between 9 am and 5 pm.
8. Click **OK** to complete. The query definition is now saved as a favorite and can be accessed at any time.

11.8.2 Activating a Favorite

1. Select the **Home** category in the Shortcut bar (if not already selected).
2. Click the **Favorites** shortcut.
3. A listing of all favorites is displayed in the Browse/Edit area.
4. Click the desired favorite. (The selected favorite will be highlighted in yellow.)
5. Click the **Go** button in the bottom area of the Browse/Edit area.
6. The query results will appear in the Browse/Edit area.

11.8.3 Deleting a Favorite

1. Select the **Home** category in the Shortcut bar (if not already selected).
2. Click the **Favorites** shortcut.
3. A listing of all favorites is displayed in the Browse/Edit area.
4. Click the desired favorite. The selected favorite will be highlighted in yellow.
5. Click the **Delete** button in the bottom area of the Browse/Edit area.
6. Press **Yes** to confirm deletion.

12 REPORTS

Several reports are included, automatically, with a new BOSS installation. These reports are available for use as soon as a BOSS Administrator assigns role permissions to the reports.

12.1 Running a System Report

1. Select the **Home** category on the Shortcut bar.
2. Click the **Reports** shortcut.
3. The Browse/Edit area will display a list of available reports. (Reports to which the user does not have permissions are not displayed.)
4. Click the desired report. The selected report is highlighted in yellow. Parameters for the report appear in the bottom of the Browse/Edit area.
5. Select **Date Range**. All reports call for From and To dates to define the time range for the report data. By default, the values in these fields define a report for the most recent two weeks. You can change these dates by typing different information into these fields, using the **Up/ Down** arrow keys to the right of the field or by clicking the **Select** button to the right of the field and selecting a date on the calendar and then clicking the **Save** button.
6. Some reports also permit you to filter report results by user(s). For example, the pictures report, which reports pictures taken in PAGIS, allows you to define one or more users to report on.
7. Once desired parameters are selected for the report, click the Go button. The report screen immediately displays, indicating that the server is generating the report until results are displayed.

12.2 Viewing and Printing Reports

The Report screen displays the date and time the report was generated and the title of the report in the heading area. When you place your mouse above a shortcut on the Report Shortcut bar, a label appears indicating what the shortcut button does. Note that some of the buttons on the Shortcut bar are not relevant to BOSS reports and are therefore disabled.
The Report Results Shortcut bar icons are as follows:



First Page – Return to the first page of the report.
Previous Page – Go to the previous page of the report.
Page Input – In this text box, type in a particular page number to bring up on screen.
Next Page – Go to the next page of the report.
Last Page – Go to the last page of the report.
Stop Rendering – This button can be used to cancel the report processing. This can be helpful if a large report was initiated, but is no longer desired.
Refresh – Refresh the report using the most current BOSS data.
Print – Print the report.
Print Layout – Toggle between available print layouts.
Page Setup – Choose among the options for standard page setup, such as page orientation, and paper size.
Save As – Excel/PDF/Word – Save the current results to a Microsoft Excel (.xls), an Adobe Portable Document Format (.pdf) or a Microsoft Word (.doc) document.
Width Zoom Setting – This drop-down list allows you to select a zoom view for the report results on the screen.

12.2.1 Viewing the Login Statistics Report

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Devices** shortcut.
3. Click the **Logs** button at the bottom of the screen.



4. Click **Go** to view the Login Statistics Report.
   Begin Date – Select the start date for the report.
   End Date – Select the end date for the report.
   Selected Users – Select the users to include in the report. Click the **Select** button. Click the checkbox of the desired user. Click on the **Save** button.

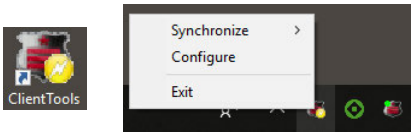
13 CLIENT TOOLS

The Client Tools utility is used to transfer any necessary files needed for a shift from BOSS to an PAGIS system that is being run in the Disk Sync mode. After the completion of a shift, Client Tools can then be used to transfer read data files captured during a shift into BOSS. The utility is configurable and processes files stored on a local, network, or USB flash drive. Like Smart Client, the Client Tools utility does not have to be run on the BOSS server; it can be configured to access the server via an IP Address.

Client Tools does not have a customary interface. Once the utility is started, the Client Tools icon will appear in the Windows System Tray.

Before use, Client Tools must be configured, which is described in Appendix 17. Once the Client Tools has been configured, it can now be used to synchronize information between BOSS and PAGIS:

1. To start, right-click on the **Client Tools** icon.

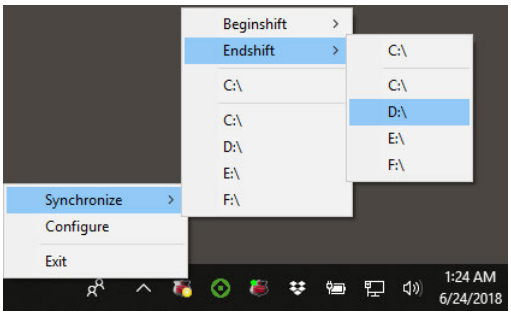


2. Select **Synchronize**. The next menu displayed is divided into three sections.

   a. The first section allows the user to select either **Create Begin Shift Files or Synchronize End Shift Files**. When either option is selected, the next menu is displayed. It is divided into two sections; it is the bottom two sections of the previous menu and functions the same way.

   b. The second section displays the path defined during configuration. This is a shortcut to perform Begin Shift and End Shift at the same time, storing the Begin Shift files in the defined location and processing the End Shift files at the defined location. If there are no End Shift files to process, this feature will be complete after the Begin Shift file is created. No error message will be displayed if the End Shift files are not found.

   c. The last section lists the drive letters currently on the workstation. If one is selected, Client Tools will perform a Begin Shift first and store the files at the root of the drive selected. Then Client Tools will check to see if there are End Shift files at that location. If found, the files will be processed. If not found, the synchronization process is complete. No error message will be displayed. This is an additional option if the configured drive is not currently available.



Note that once End Shift files have been processed, they are deleted.

14 ARCHIVING DATA

It is possible to archive reads that have accumulated in the BOSS database. Based on settings that are configurable in System Parameters, reads that meet the specified criteria are transferred from the main BOSS database to an archived BOSS database. *(See Section 15.3.2, List of BOSS System Parameters, for additional information on configuring this feature.)*

Once enabled, this process is handled by the BOSS server. There should be no noticeable difference to a user logged into a BOSS Smart Client when reviewing or reporting on stored reads. The only indication in the BOSS Smart Client that reads have been archived will be on the BOSS Home screen. The user will be able to see a calculable difference between the reads and hits counts compared to the total reads and total hits counts. The difference between the values will be the number of reads and hits stored in the archived database.

15 SYSTEM SETTINGS

15.1 Sessions

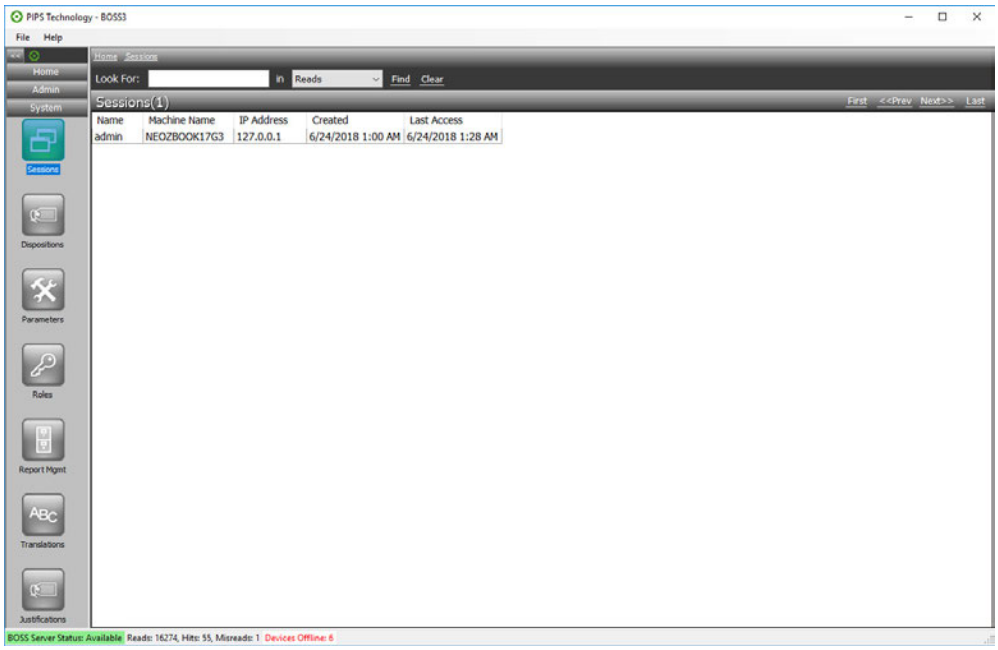
The Sessions screen allows for viewing the current list of logged-on BOSS users. Each login on each computer utilizes a concurrent license of the software. Since BOSS is licensed per concurrent active session, a BOSS Administrator may need to have a session disconnected in order to release a session license. A BOSS Administrator can force a session disconnect in the Sessions screen.

Note: BOSS allows a single "admin" login to access BOSS even if the number of concurrent sessions has been exhausted. Please see Section 2.1, BOSS Administrator Login, for more information about the "admin" username.

15.1.1 Viewing and Disconnecting Sessions

1. Select the **System** category on the Shortcut bar.
2. Click the **Sessions** shortcut. A list of current user sessions appears in the Browse/Edit area.
3. The heading in the Browse/Edit area indicates the total number of current sessions.
4. Click on a session to see details in the bottom half in the Browse/Edit area.
5. To disconnect, click the **Disconnect** button that appears in the detail area, and click **OK**.

Note: You cannot disconnect your own session in this manner. To disconnect your own session, simply log off the BOSS application.



15.1.2 Workstation Power Management and Sessions

Using Windows Power Management to hibernate or suspend a workstation running the BOSS Smart Client will cause the session in BOSS to be terminated after five minutes. When the workstation is resumed from hibernation or a suspended state, the user will have to log in to BOSS again.

15.2 Dispositions

Dispositions are pre-defined classifications that can be assigned to hits. “Arrest Made,” “Vehicle Recovered,” “Surveillance Established” are examples of dispositions. A BOSS Administrator is able to define any number of dispositions for her system. Users can then use those dispositions to specify the action taken or the status of the hit. A new BOSS system will have a Default Disposition category that includes one disposition of “No Action.” Additional categories can be defined as needed.

15.2.1 Defining a New Disposition

1. Select the **System** category on the Shortcut bar.
2. Click the **Dispositions** shortcut. A list of all current dispositions appears in the top of the Browse/Edit area.
3. Click the **New** button in the bottom of the Browse/Edit area.
4. Enter a name for the disposition. If adding it to the default category, simply enter the name of the disposition. If adding it to a new category, the format of the name should be [Category : Disposition Name], i.e., **Auto :Vehicle Recovered**.
5. Enter a **Description** for the new disposition.
6. Specify a **Priorit**y for the disposition. (A lower number means a higher priority.)
7. Select the **Back Office Only** option if the disposition should not be available only in the Correct Reads screen in BOSS, and not exposed in PAGIS.



15.2.2 Deleting a Disposition

1. Select the **System** category in the Shortcut bar (if not already selected).
2. Click the **Dispositions** shortcut.
3. A list of all dispositions is displayed in the Browse/Edit area.
4. Click the desired Disposition. The selected disposition will be highlighted in yellow.
5. Click the **Delete** button in the bottom area of the Browse/Edit area.
6. Press **Yes** to confirm deletion.

15.3 System Parameters

System Parameters allow for configuration parameters for a BOSS system. System parameters only need to be configured during initial system configuration and normally do not need to be modified again after that.

15.3.1 Editing System Parameters

1. Select **System** from the left Shortcut bar.
2. Click on the **Parameters** button in the Shortcut bar.
3. Click on the desired parameter in the right Browse/Edit window. The bottom pane of the Browse/Edit window will display the entry field for the selected parameter.
4. Modify the parameter value as desired and click the **Save** button.

15.3.2 List of BOSS System Parameters

arc_ActiveRetentionDays – This setting dictates how long reads will be maintained in the BOSS database. After reads have been stored for this time, they will be moved to the archived database, creating space for additional reads in the main database. The default setting is 730 days but can be varied based on the size and needs of the system.
arc_ArchiveDBRetentionDays – This setting dictates how many days to retain an archived database. After an archived database has been stored for this time it will be removed, creating space for additional archived databases. The default setting is 0 days, which indicates that the archived databases will never be removed, but the number of days can be modified based on the size and needs of the system.
arc_DatabaseLocation – This setting allows the user to specify where the archived databases should be saved. A blank entry will save them in the SQL default location.
arc_Enabled – To allow the BOSS server to archive aged reads and free up space, enable archiving by setting this to 1. When archiving is not desired, this setting should be 0.
arc_EndOfMonthCutOff – This setting forces a restriction on the size of the archived databases, so that nothing will be added after the end of each month. The default setting is disabled (0). To enable the setting, change the value to 1.
arc_MaxSize – This setting allows the Administrator to determine the number of reads that can be stored in the archived database. The default value is 1 million and can be varied based on the size and needs of the system. Once an archived database has reached this maximum number of records, a new archived reads database will be created.
audit_Justification_FileNumberRequired – When this setting is enabled (1), users performing read queries are required to enter a file number.This information will also be listed in the audit report. The default setting is disabled (0).
audit_Justification_NotesRequired – When this setting is enabled (1), users performing read queries are required to enter a justification note. This information will also be listed in the audit report. The default setting is disabled (0).
audit_JustificationEnabled – When this setting is enabled (1), users performing read queries are required to select a pre-defined justification. This information will also be listed in the audit report. The default setting is disabled (0).
data_CaptureUsageStatistics – When this setting is enabled (1), information sent from a PAGIS device that has been modified due to Privacy settings will still be utilized to generate usage statistic reports. The default setting is disabled (0).
hls_HotListDeltas – When this setting is enabled (1), updated hotlists will be deployed in full. Changing the setting to disabled (0) will cause only the changes made in the updated hotlists to be deployed.
Password_Expiration_Days-Number of days a password is allowed to remain unchanged. Value “1”=enabled, “0”=disabled.

15.3.2 List of BOSS System Parameters (continued)

Proxy_uri/proxy_username /proxy_password/proxy_domain – These settings are only necessary if there is a proxy server involved that requires authentication for connection. Enter a valid Uniform Resource Identifier (URI), username, password, and domain in the associated fields to allow communication through the proxy server. Consult the network Administrator for proxy authentication information

purge_Minutes – This setting is the time, in minutes, between each session of purging or archiving. The default value is 15 minutes and is configurable to any value of 1 minute or greater.

purge_ReadCount – This setting is the number of records to be processed by the purging or archiving process per session. It can be any value, but setting it according to system limitations is recommended because the process can be resource intensive if set too high.

readQuery_fromDate – This setting allows the user to adjust the default From date on the Reads Query screen. Any value can be entered and it is used to decrement from today. Example – a value of 7 would result in a from date seven days earlier than today.

readQuery_toDate – This setting allows the user to adjust the default to date on the Reads Query screen. Any value can be entered and it is used to incremented from today. Example – a value of 7 would result in a to date seven days later than today.

Recent_Read_Time- Time in min. of how long to hold reads in the "Recent reads" table for hit evaluation.

Recent_Reads_Amt- Number of records to delete from "Recent reads" if older then Recent read time.

ResendEmailNotice- Resend Offline notification on Fixed Camera after this amount of time has expired.

rq_ReaperHours – This setting manages how long to retain a temporary database table created when running certain read queries. This allows the user to continue to review the results of those queries for a longer time. The default is a minimum of 48 hours, and there is no maximum value.

smtp_AlertTemplate- Default email template, definitions listed in table below.

smtp_SenderName – In order for the BOSS server to send alerts to email addresses, the SMTP settings must be configured correctly. The SMTP sender field should contain the username that will appear in the from field on an email generated by the BOSS system.

smtp_Server – The name or IP address of the SMTP server should be entered here. The name or address used here must be one by which the SMTP server can be reached from the BOSS server. This field must be populated correctly in order for the BOSS system to send any alerts to email addresses.

smtp_SSL – If Secure Sockets Layer (SSL) is used on your SMTP server, the value of this field should be set to 1. If you do not use SSL, this field should be set to 0.

smtp_SubjectTemplate – This field sets the subject line of alert emails generated by BOSS. The following entry in the field incorporates both static text and a BOSS field variable as well: BOSS alert FROM [SRC].

TOKEN	DESCRIPTION	TOKEN	DESCRIPTION
[LPN]	license plate	[FD1]	field1
[STE]	site	[FD2]	field2
[SRC]	device	[FD3]	field3
[LOC]	location	[FD4]	field4
[LAT]	latitude	[FD5]	field5
[LON]	longitude	[PNC]	PNCID/DL
[HOT]	hotlist name	[INF]	information

smtp_UserName/smtp_password – The SMTP username and password fields should contain a valid SMTP username and associated password for sending alerts through the SMTP (email) server. Normally, a BOSS Administrator coordinates with his SMTP Administrator to create a special SMTP user that will be used exclusively for BOSS alerts.

Soap variables- All are now legacy features not currently used.

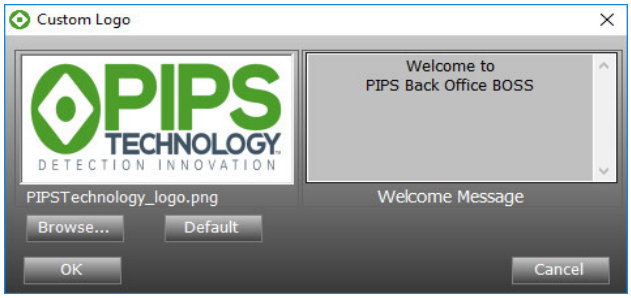
verint_HotlistsMonitored- Enter hotlist by name separated by commas.

verint_NotificationConfigured- Indicates whether the Verint notifier should be used.

15.3.2 Branding

BOSS allows the BOSS Administrator to upload a logo image and a welcome message that is displayed to BOSS users on the Home screen. To define the image and message:

1. Select **System** from the left Shortcut bar.
2. Click on the **Parameters** button in the Shortcut bar.
3. Click on **Branding**.
4. If needed, click **Default** to remove current custom settings.
5. Pick the desired logo image using the **Browse**... button.
6. Type in a message in the Welcome Message box.



Browse – Select an image file (JPEG, GIF, BMP) to be displayed on the home screen. The largest recommended image size is 120 by 380 pixels.

Default – Remove the custom logos and texts.

Welcome Message – A custom welcome message can be typed in here.

7. Click **OK** to save changes, or **Cancel** to discard changes.

15.4 Roles

In addition to the default roles that are automatically created by BOSS, the Administrator can create and configure custom roles as needed. *See Section 4.2, Permissions, for more information.*



15.4.1 Adding New Roles

1. Select the **System** category on the Shortcut bar.
2. 2. Click the **Roles** shortcut. The Browse/Edit area will display a list of existing roles.
3. 3. Click on the **New** button. The New Role entry window will be displayed in the bottom of the window.
4. 4. Enter the name of the new role and assign the desired permissions.
5. 5. Click the **Save** button.

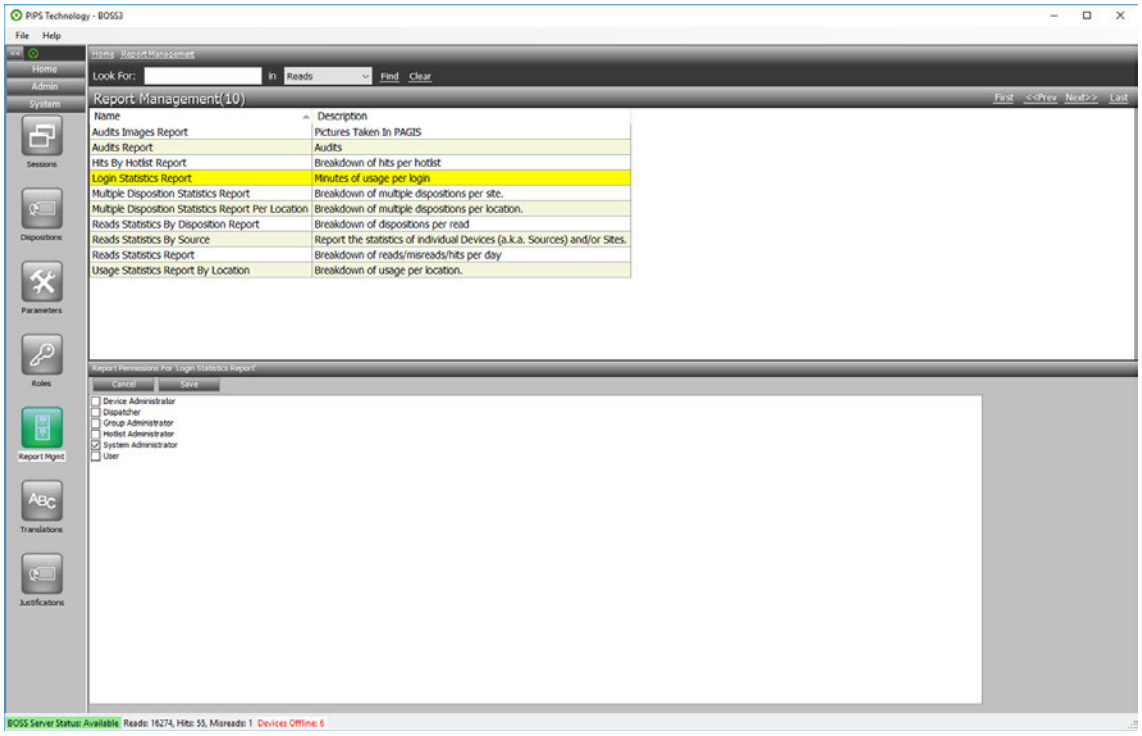
15.4.2 Deleting Roles

1. Select the **System** category on the Shortcut bar.
2. 2. Click the **Roles** shortcut. The Browse/Edit area will display a list of existing roles.
3. 3. Click on an existing role and the edit window will be displayed in the bottom of the window.
4. 4. Click the **Delete** button. Click **Yes** when prompted to complete the operation.

15.5 Report Management

15.5.1 Assigning Permissions to Access Reports

1. Select the **System** category on the shortcut bar.
2. Click the **Reports Mgmt** shortcut. The Browse/Edit area will display a list of available reports.
3. Select a report by clicking the name in the list. The selected report will be highlighted in yellow.
4. Current report permissions for the type of report chosen display in the bottom of the Browse/Edit area. Each BOSS role is listed along with a checkbox. Click a role in the list to select. Click a second time to change an unchecked box to a checked box.
5. After selecting the desired permissions for the report, click the **Save** button.



15.6 Translations

Across various organizations and agencies, terminology related to BOSS can differ significantly. For this reason, a new function added in the BOSS version 3 series gives customers flexibility in naming conventions used in the application. The Translations function provides for changing wording on BOSS screens, which allows a customer to tailor screen labeling to correspond to their own vernacular. Text items in the translations editor correspond to labels on BOSS screens. Authorized users can change these text items as necessary.

Note: This feature is not intended as a replacement for language-specific versions of BOSS. For international versions of BOSS, please contact PIPS™ Technical Support.

15.6.1 Entering a New Translation



1. Select the **System** category on the Shortcut bar.
2. Click the **Translations** shortcut. A list of all current translations appears in the top of the Browse/Edit area.
3. Click the **New** button and the new Translations Entry screen appears in the bottom area.
4. Enter an existing label from the BOSS application in the Caption field, using the exact case and spelling that normally appears on the screen.
5. Enter the desired replacement text in the Translation field.
6. Click the **Save** button to complete the operation.

Note: The user must log off and on again for translation to take effect in the current session.

For Example: A customer preferring to see a label of “Plate” where the software normally uses the term “LPN” would use the translations feature to create the replacement for their installation. The translation Entry Caption field would contain “LPN,” while the Translation field would contain the replacement term “Plate.”

15.7 Justifications

To ensure that sensitive information is being kept secure, systems can be configured to require that users who are performing queries on reads have a valid reason for doing so. Enabling the audit Justification Enabled parameter requires users to justify their reason for querying reads. There are five justifications created by default: Audit, BOLO Post Scan Query, Crime Scene Query, Test and Trend Analysis. These queries will also be documented in audit reports.



15.7.1 Entering a New Justification

1. Select the **System** category on the Shortcut bar.
2. 2. Click the **Justifications** shortcut. A list of all existing justifications appears in the top of the Browse/Edit area.
3. 3. Click on the **New** button. The Justifications Entry screen appears in the bottom area.
4. 4. Enter a justification. There is no validation on the entry for this field.
5. 5. Click the **Save** button to complete the operation.

15.7.2 Deleting Justifications

1. Select the **System** category on the Shortcut bar.
2. 2. Click the **Justifications** shortcut. A list of all existing justifications appears in the top of the Browse/Edit area.
3. 3. Click on the justification to be deleted. The Justifications Edit screen appears in the bottom area.
4. 4. Click the **Delete** button. Click on **Yes** when prompted to complete the operation.

17 APPENDIX: INSTALLATION AND CONFIGURATION

This section is intended for authorized personnel in installation and configuration of a BOSS system. The information in this guide is organized sequentially, in the order that steps would be performed when initially setting up a new BOSS system, with the first section describing the software installation process, and the subsequent sections describing configuration options for a BOSS system.

Upon initial installation of a new BOSS system, the BOSS server application must be configured using the BOSS Controller application. BOSS Administrators may also find the need to modify configuration settings after the system has already been in use. Therefore, the configuration section can be used as an ongoing reference for authorized personnel responsible for maintaining the system.

Note: It is critical that only an IT Administrator or other knowledgeable personnel attempt configuration modifications to a BOSS system. Incorrect configuration settings can cause serious issues with operation and/or adversely affect data integrity. When in doubt, you should consult PIPS Technical Support before making system configuration changes.

OS feature requirements

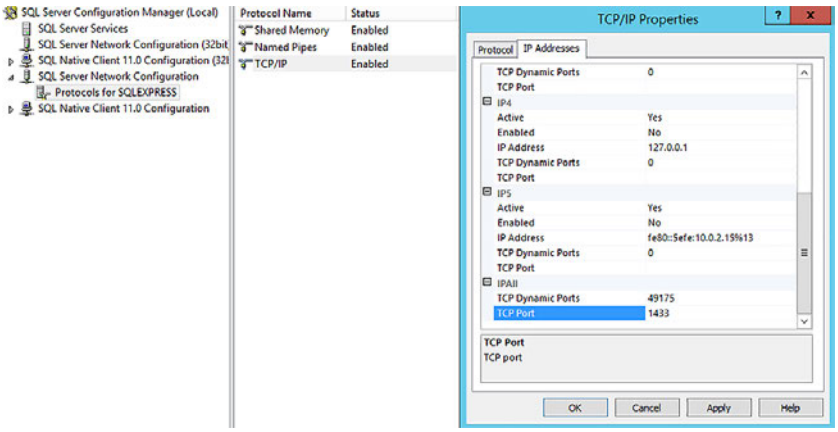
- Windows server 2008 or newer.
- Net. TCP Port Sharing Service must be enabled and running.
- Framework .Net 4.0.

SQL Server Requirements

1. SQL version 2012 or newer required.
2. 2. SQL login account “NT AUTHORITY\SYSTEM” is required to be mapped to Boss3 database as db_owner. For system with existing “Boss3” databases this should be applied prior to Boss software installation. For new installation this can be applied after the Boss service has ran for the first time and created the Boss3 database. See- “Common issues”

Settings under SQL Server Configuration Manger:

3. “SQL Server Network Configurations” Name Pips must be enabled.
4. “SQL Server Network Configurations” TCP/IP must be enabled, with “IP All” set to port 1433.
5. SQL restart required after changes.



17.1 Installing the BOSS Server Application Files

17.1.1 Running the Installer

This guide assumes that the Microsoft SQL Server 2012 or newer instance has already been installed and is available. If the SQL Server is not available, stop now and continue installation after the SQL Server has been installed. To install the Microsoft SQL Server, please follow the instructions provided by Microsoft.

Note: 1. It is recommended that antivirus utilities be disabled during the install.

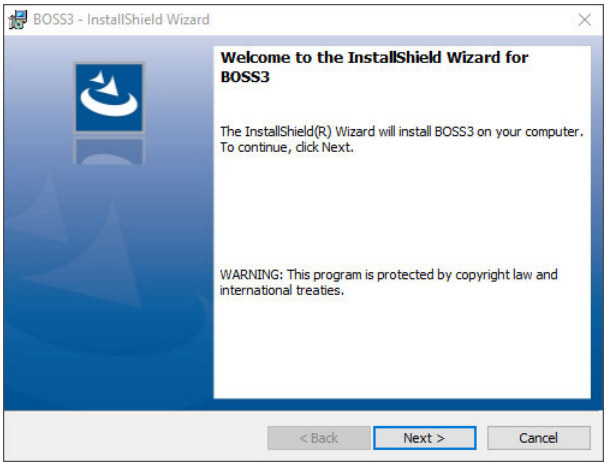
To commence the installation:

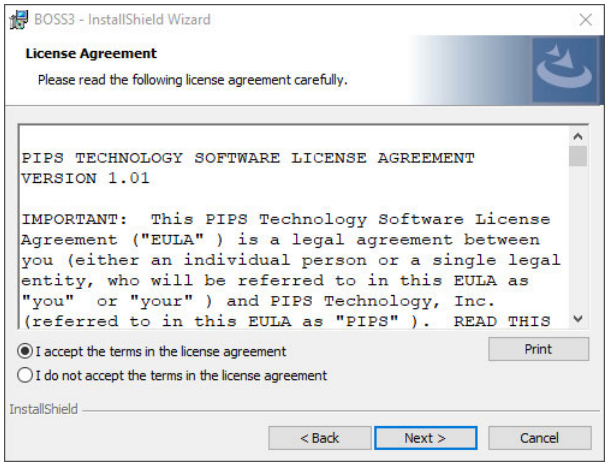
1. Select the link supplied by PIPS to the BOSS installation application.
2. Run the BOSS Setup executable.

Note: Right-click on the installer icon and select Run As Administrator.

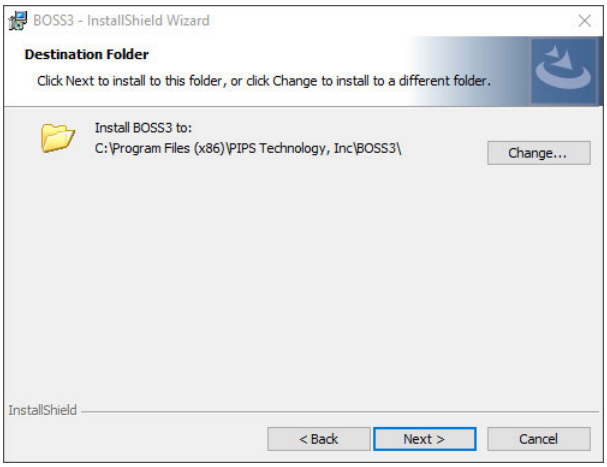
17.1.2 License Agreement

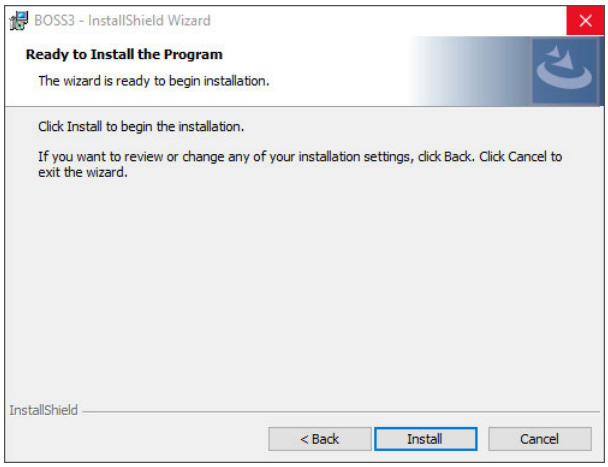
1. Click **Next** then check the license agreement checkbox to acknowledge agreement with the license terms.
2. Click **Next** to continue.



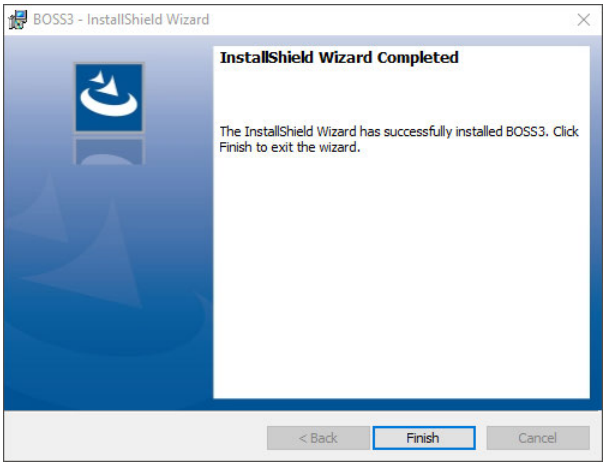


3. Accept the default installation file path or change.
4. Click “Next” to proceed to “Install”





5. When the Installation Complete message is displayed, click **Finish** to proceed to the Licensing.

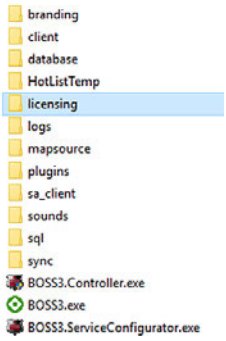


17.2 License Key Management

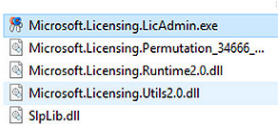
17.2.1 Activating the License Key

Following a new installation, a valid BOSS license key must be entered. There are three options available discussed in the sections below that can be used to activate the license. For upgrades or reinstallation on same server this step is not required as the licensing tool will automagical re-acquire the licensing code.

1. Navigate to the licensing folder in the BOSS3 installation folder.



2. Start Microsoft License Manager (Microsoft.Licensing.LicAdmin.exe). This must be run as an Administrator.



3. In the License Manager User interface, select **File → Activation Wizard** to install the new license
4. When the Activation Wizard dialog opens select one of the following:
   a. I want to activate the software over the Internet. *See Section 17.2.1.1.*

   or

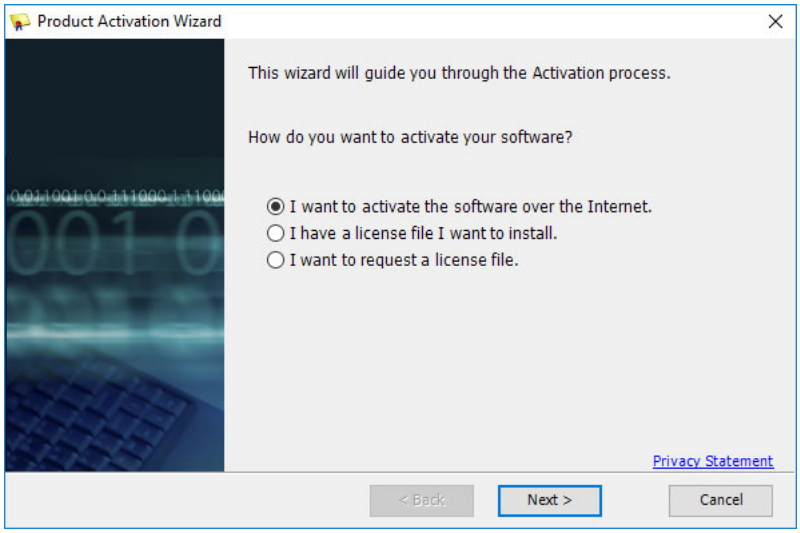
   b. I have a license file I want to install. *See Section 17.2.1.2.*

   or

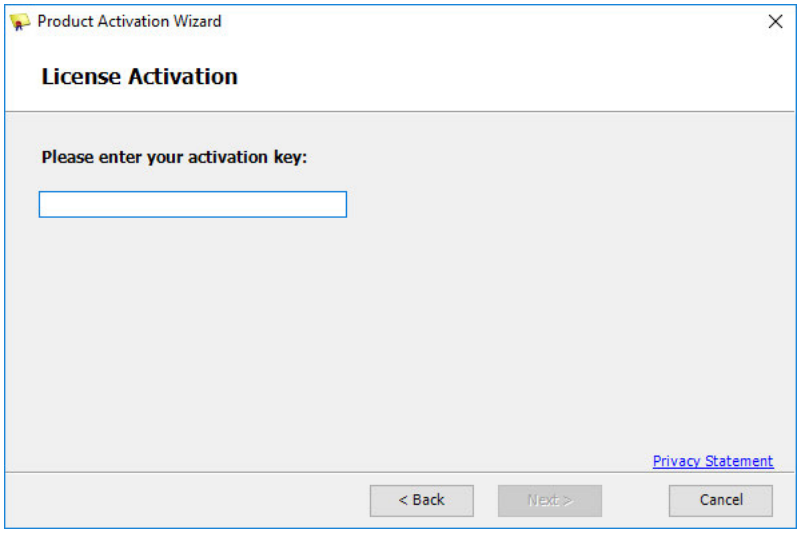
   c. I want to request a license file. *See Section 17.2.1.3.*

17.2.1.1 Activating the License Key over the Internet

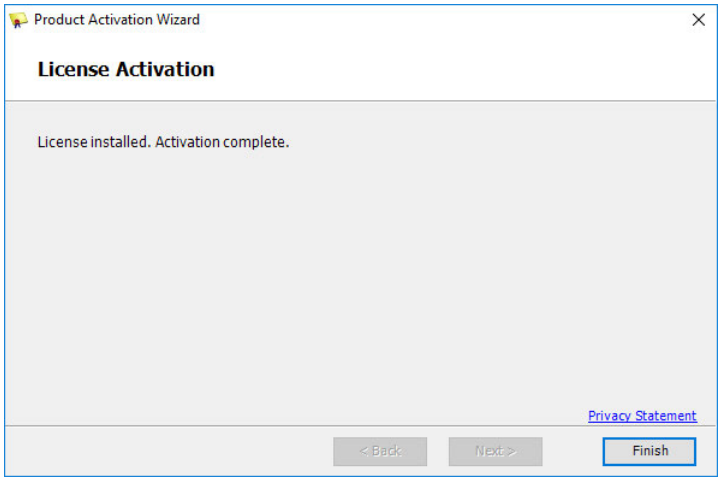
1. Check **I want to activate the software** over the Internet.
2. Click **Next** to continue.



3. Enter the activation key provided by PIPS and click **Next**.



4. The license key will be activated over the Internet. The following screen will display. Click **Finish** to continue.



17.2.1.2 Activating the Software with a License File

1. Check I have a license file I want to install.
2. Click **Next** to continue.
3. Navigate to the location of the license file and select it.
4. Click **Next** to continue.
5. When the activation is completed click **Finish**.

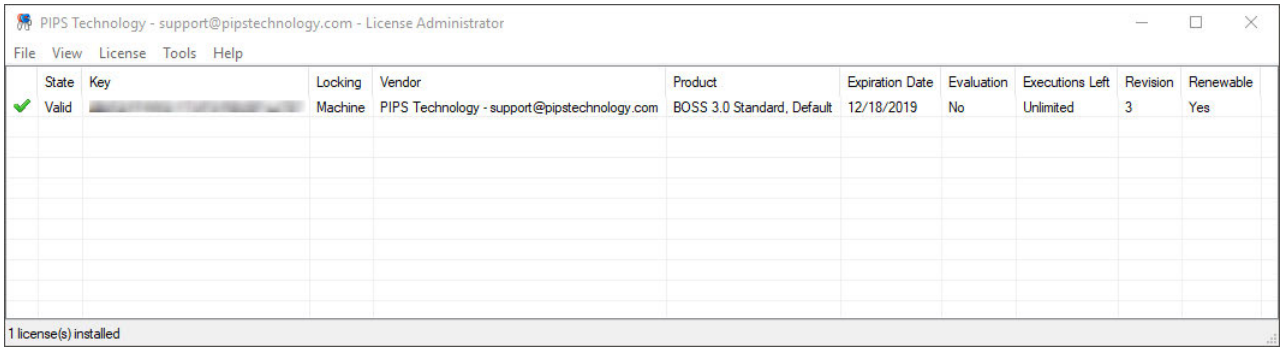
17.2.1.3 Request a License File to Activate the License

1. Click **I want to request a license file**. Press Next.
2. Enter the license key you received previously. Press **Next**.
3. In the screen that displays, copy the text block highlighted (starts with "—BEGIN Request") to the clipboard and paste it into an email. Send the email to PIPS Technical Support (support@pipstechnology.com).
4. Close the Activation Wizard by clicking the **Finish** button.
5. You will be sent an activation file via email. Extract the license file (*.bin) and copy it to a folder on the computer where BOSS is installed. Return to Section 17.2.2 and follow the steps to activate the license.

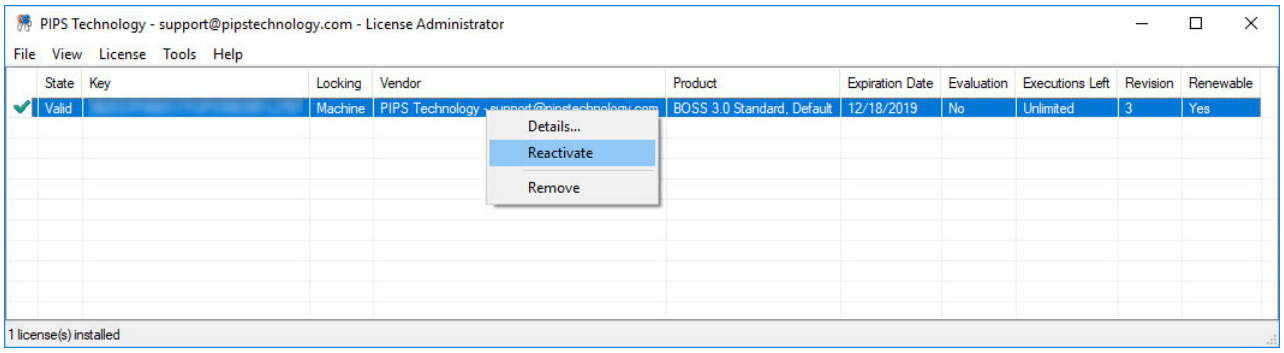
17.2.2 Updating a License Key

If the BOSS license key becomes invalid, or if the license is upgraded, follow these steps to reactivate a BOSS license key:

1. Start Windows Explorer on the BOSS server.
2. Navigate to the folder where the BOSS server application is installed (by default C:\Program Files\PIPS Technology, Inc\BOSS3).
3. Locate the licensing folder as described in Section 17.2.1.
4. Open the folder and right click on the application Microsoft.Licensing.LicAdmin.exe. Select to run as the Administrator. You will see the following screen:



5. Select the license key. Right-click, and from the context menu, select Reactivate.



6. Click Next.
7. When the Installation Complete message is displayed, click Finish.

17.3 Map Display Options with BOSS

BOSS can display collected plate read information plotted on a map. There are two different mechanisms for displaying maps within the BOSS Smart Client application.

17.3.1 U.S. Census Bureau TIGER Maps

U.S Census Bureau TIGER Maps now discontinued.

17.3.2 Advanced Mapping with Internet Maps

PIPS provides an option to purchase an "Advanced Mapping" feature with BOSS. This option enables integration of Maps, an Internet-based service that BOSS can use to display maps in the Smart Client application.

Note: In order to use Advanced Mapping, the BOSS Smart Client will need an unimpeded Internet connection.

17.4 Configuring the BOSS Server Application

After the BOSS installation is completed, the application must be configured using the BOSS Controller program. The following sections explain how to use this program as well as the configuration settings that are available.

17.4.1 The BOSS Controller Application

17.4.1.1 Starting the Boss Controller

BOSS Controller (BOSS3.Controller.exe) is the application used to configure and control the BOSS service. The BOSS Controller is installed on the server computer along with the server application. After the installation is complete the Controller program will start automatically. If this is a new installation the license will need to be activated first. Choose to configure BOSS at a later time by clicking on Cancel.

The shortcut to the BOSS Controller program can be found on the desktop or in the All Programs → PIPS Technology → BOSS3 menu. Right-click on the Controller icon and select Run As Administrator. When the BOSS Controller program is started an icon for the application will appear in the Windows System Tray at the lower right corner of the desktop.

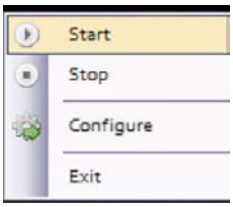


17.4.1.2 Status Colors

The icon for the Controller program includes a "traffic light" that uses a color indicator to show the status of the BOSS service application. When the BOSS service application is running, the indicator is green. When the BOSS service application is not running, the indicator is red. Yellow color indicates that the application is changing state (starting or stopping).

17.4.1.3 Right-Click Menu

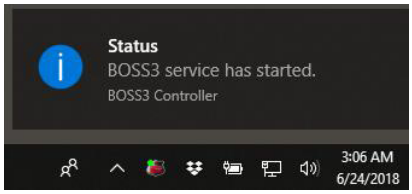
When you right-click the BOSS Controller System Tray icon, a pop-up menu will appear:



Start	Start the BOSS service.
Stop	Stop the BOSS service.
Configure	Present the BOSS Configuration Wizard.
Exit	Close the BOSS Controller application. (Note: This closes the BOSS Controller program, but does not stop the BOSS Service.)

17.4.1.4 Starting the BOSS Service

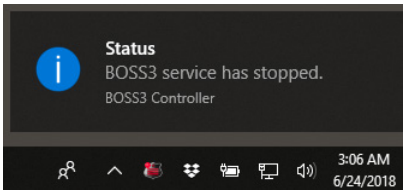
When the **Start** action is selected, and the service starts successfully, a Success message will be displayed:



The traffic light in the BOSS Controller icon will turn green to indicate the status.

17.4.1.5 Stopping the BOSS Service

When the **Stop** action is selected, and the service stops successfully, another Success message will be displayed, and the traffic light changes to red:

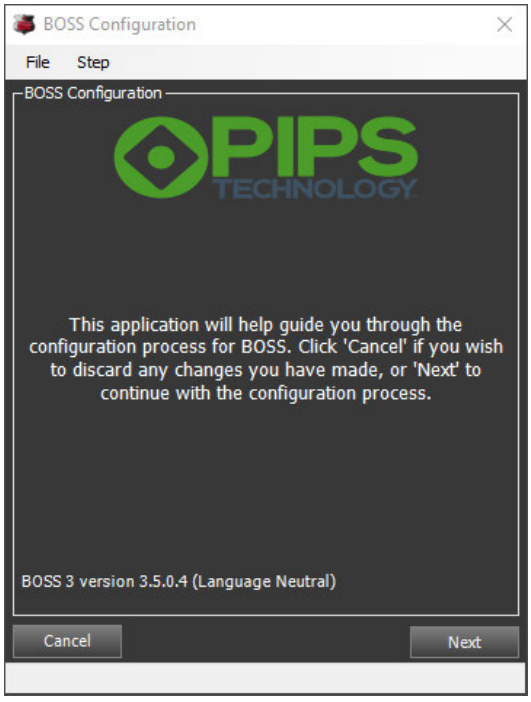


17.4.2 BOSS Configuration

17.4.2.1 Activating the Configuration Wizard

1. Right-click the **Controller System Tray** icon.
2. Select the **Configure** option. The Configuration Wizard options are explained in the following sections.

17.4.2.2 BOSS Configuration Wizard



Step through all configuration screens in the BOSS Configuration Wizard by simply clicking the **Next** button on this first screen. Click **Next** on each subsequent screen after entering in the desired settings. Note: This step-by-step process is recommended when you are configuring the system for the first time.

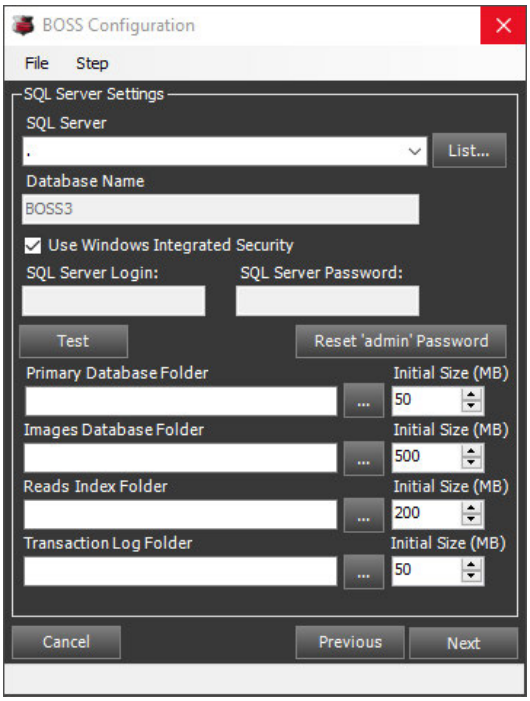
OR

Click the **Step** menu option to access the configuration menu and proceed to the step choice.

For each configuration step (described in Sections 17.4.2.3 – 17.4.2.9), clicking **Next** will take you to the next configuration screen, clicking **Previous** will take you to the previous one, and clicking Cancel will clear any changes you have made on the current screen.

17.4.2.3 SQL Server Configuration

SQL Server configuration is required for a new BOSS system, in order to specify the location and necessary authentication information for the SQL database.

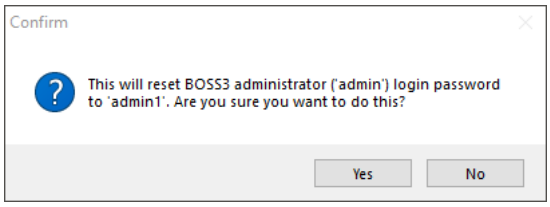


SQL Server – Select the SQL Server instance for BOSS. Press **List** to choose from a list of available SQL Servers. The SQL Server Browser service must be running at this point. You may also type in the server IP address or host name. Enter a dot "." to use a local SQL Server that is running on the same machine as the BOSS service.
Use Windows Integrated Security – If checked, BOSS will use Windows Integrated Security to access the SQL Server database.
SQL Server Login and SQL Server Password – If Windows Integrated Security is not selected, enter the SQL Server username and password provided for BOSS to use to access the database.
Test – The **Test** button can be used to test the SQL Server settings currently in place. The Test button initiates a connection. A message box will appear to indicate whether the test connection fails or succeeds.
Database file locations: BOSS database can be divided among multiple locations as follows if necessary. When selecting a folder path for the database files keep in-mind that the folder path is referenced from the standpoint of the SQL server location.
Primary Database Folder – The drive and folder where the BOSS primary database will reside.
Images Database Folder – The drive and folder where the BOSS will store images.
Reads Index Folder – The drive and folder where BOSS will store database indices for stored plate reads.
Transaction Log Folder – The drive and folder where BOSS will store the database transaction log file.
Initial Database Sizes - By Default Boss will predefines the sizes as indicated in the controller.



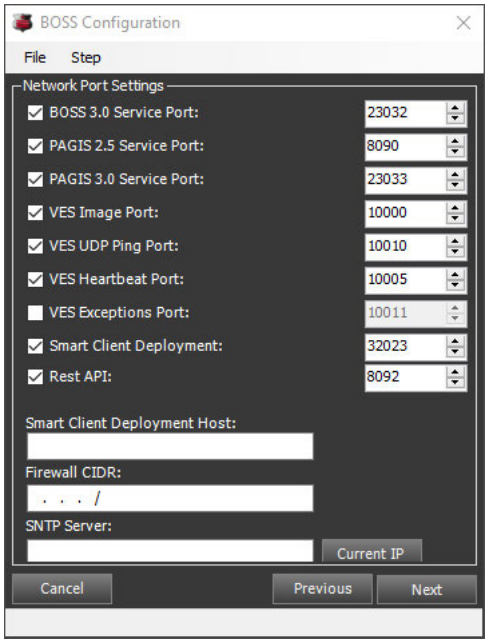
17.4.2.4 Resetting the Administrator Password

If you have forgotten the BOSS administrator (admin) password, you can press the **Reset 'admin' password** button to reset the password to "admin1."



Pressing **Yes** will immediately reset the password.

17.4.2.5 Network Port Settings



BOSS uses a number of TCP/IP and UDP network ports for communication between server and client applications and server and license plate reading devices.

17.4.2.5 Network Port Settings (continued)

FIELD	DESCRIPTION	DEFAULT PORT
BOSS 3.0 Service Port	TCP/IP port used to provide access for BOSS Smart Clients	**23032**
PAGIS 2.5 Service Port	TCP/IP port used to provide access for older mobile client versions older than Pagis 2.6.8	**8090**
PAGIS 3.0 Service Port	TCP/IP port used to provide access to various mobile client versions	**23033**
VES Image Port	TCP/IP port used to receive reads from fixed cameras	**10000**
VES UDP Ping Port	UDP port used to receive keep alive ping messages from fixed cameras	**10010**
VES Heartbeat Port	TCP/IP port used to receive heartbeat status messages from fixed cameras	**10005**
VES Exceptions Port	TCP/IP port used to receive exceptions messages from fixed cameras	**10011**
Smart Client Deployment	TCP/IP port used for BOSS client installations via BOSS server	**32023**
REST API Port	HTML port used for the communication between the BOSS service and newer versions of PAGIS	**8092**

If the checkbox in front of the port name is left unchecked, the corresponding connection will be disabled.

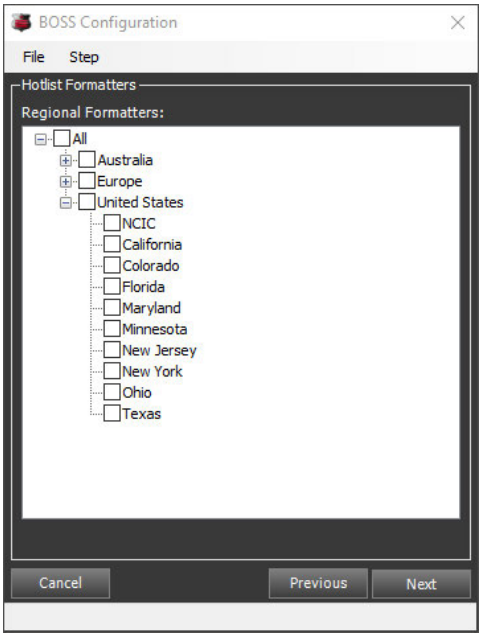
Smart Client Deployment Host – If this information is entered, BOSS Smart Clients will use the given hostname to distribute the smart client application. This can be left blank to use the local host name.

Firewall CIDR – BOSS provides a built-in firewall for incoming fixed camera connections. If a value is entered, only cameras with an IP address matching the CIDR will be allowed to connect. CIDR (Classless Inter-Domain Routing) is a standard industry method for specifying a range of included IP addresses. The format of the CIDR entry is A.B.C.D/N, in which the dotted decimal portion before the "/" is interpreted, like an IPv4 address, as a 32-bit binary number that has been broken into four octets. The value of N indicates the number of shared initial bits, counting from the left-hand side of the address.

For Example: For an entry of 10.200.200.255/24, the CIDR value 24 leaves 8 bits that can be changed. Therefore, addresses 10.200.200.x are permitted addresses.

SNTP Server – BOSS has a built-in time service. The fixed ANPR/ALPR cameras do not support automatic daylight savings time (DST) adjustment. The BOSS time service provides a customized SNTP service for these cameras in order to support DST. To use the built-in time service, Windows Time Service has to be disabled in the Services Control panel, and the BOSS time server IP address entered in this field.

17.4.2.6 Regional Hotlist Formatters

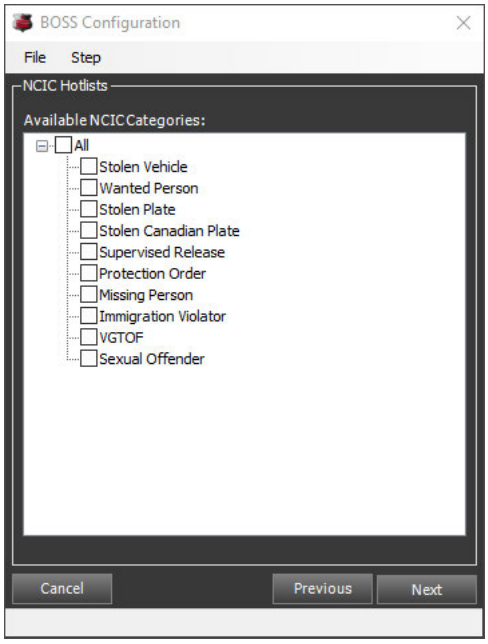


The BOSS allows the selection of predefined hotlist formatters. These formatters define the input format (structure) of hotlist data files. Custom formatters can be defined via the BOSS Smart Client application *(see Section 13 of this manual for more information)*. Also, when installing BOSS in the United States, National Crime Information Center (NCIC) data formatters can be selected for specific states (see section following).

To select or unselect formatters, click on the formatter title to add or remove a check mark. Additional formatters can be added to a system as needed. These will be provided by PIPS Technical Support upon request.

17.4.2.7 NCIC Hotlist Formatters

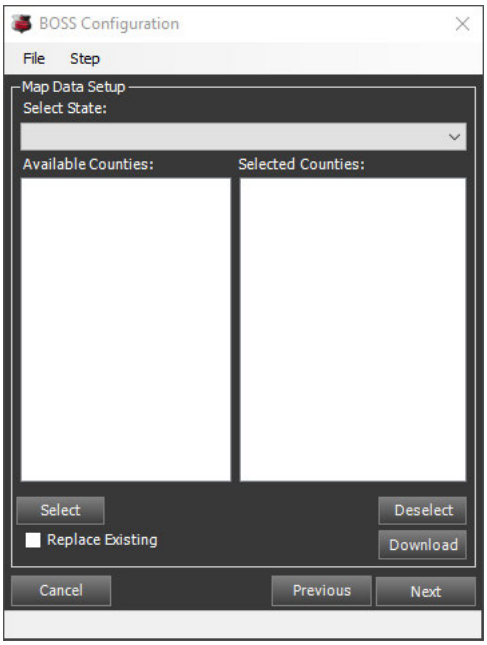
BOSS supports hotlist import in the United States National Crime Information Center data format. This option is available only in the United States.



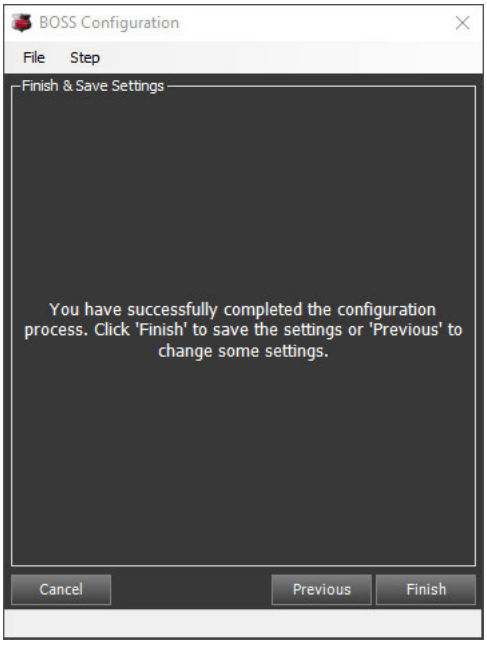
To configure formatters for the desired categories, check those categories. Once the desired categories have been selected, press **Next** to proceed.

17.4.2.8 Map Data Setup

U.S Census Bureau TIGER Maps now discontinued. Do not utilize this section, click “Next”



17.4.2.9 Finishing Configuration



Click **Finish** to complete configuration. BOSS will save the chosen configuration.

17.5 Installing the BOSSUI Smart Client Application

17.5.1 Installation over the Web

To initiate a web installation on a workstation, start up Microsoft Internet Explorer and navigate to this web address: **http://{boss_server_ IP_address}:32023/publish.htm**, where {boss_server_IP_address} is the address of the server running the BOSS server application.

For Example: To install the Smart Client on the BOSS server itself, navigate to http://127.0.0.1:32023/publish.htm. The installation webpage will be presented. The advantage of installing the Smart Client over a web browser is that the application will automatically check for updated versions every time it is started.

17.5.2 Stand-Alone Installation

The BOSS Smart Client is a zero-administration desktop application meant for administration of the BOSS server application and querying data collected in the BOSS database as described in this manual. The BOSS Smart Client is installed as a single executable program. This program can be copied to any Windows workstation, or to a shared network drive.

To install the stand-alone application:

1. Start Windows Explorer on the BOSS server.
2. Navigate to the folder where the BOSS server application is installed (**by default C:\Program Files\PIPS Technology, Inc\BOSS3**)
3. Locate folder **sa_client.**
4. Copy the **sa_client** folder to the workstation or shared network folder of choice.

17.6 Configuring Client Tools

Client Tools is used to transfer any files needed during an Pagis shift from BOSS to an Pagis system that is being run in the Disk Sync mode. *See Section 13, Client Tools, and the Pagis Software User's Manual.*

Client Tools does not have a customary interface. Once the utility is started, the Client Tools icon will appear in the Windows System Tray. Before use, Client Tools must be configured and can be quickly completed with the simple configuration wizard provided:

1. To start the wizard, right-click the icon and select **Configure**. The initial screen provides information about the tool.
2. Click **Next** to continue the configuration, or **Cancel** to exit the wizard.
3. Enter a path so that Client Tools knows where to store the files it creates and where to look for files to process. This path can be a local, network, or external drive. Enter the path or click on the … button and browse to the location.
4. If the Begin Shift files that Client Tools creates need to be encrypted, click **Encrypt Output**. Click **Previous** to return to the previous screen, or click **Next** to continue.
5. The data used to create the Begin Shift files is created and managed in BOSS. Client Tools needs to know where the BOSS Server is located. Enter the server IP and the port to use to connect to it. Click **Previous** to return to the previous screen, or click **Next** to continue.
6. The final screen provides additional information on how to use the wizard. Click **Previous** to return to the previous screen, or click **Finish** to save the changes and exit.

Common Issues

Missing Permissions on the database user

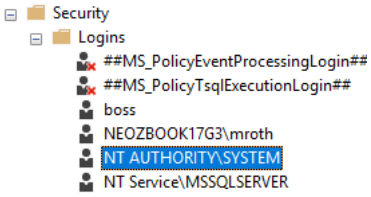
PIPS Boss service does not start: If the service does not start after two tries, go to the logs file located in "C:\Program files(x86)\PIPS Technology, Inc\BOSS3\logs", there look for the following message:

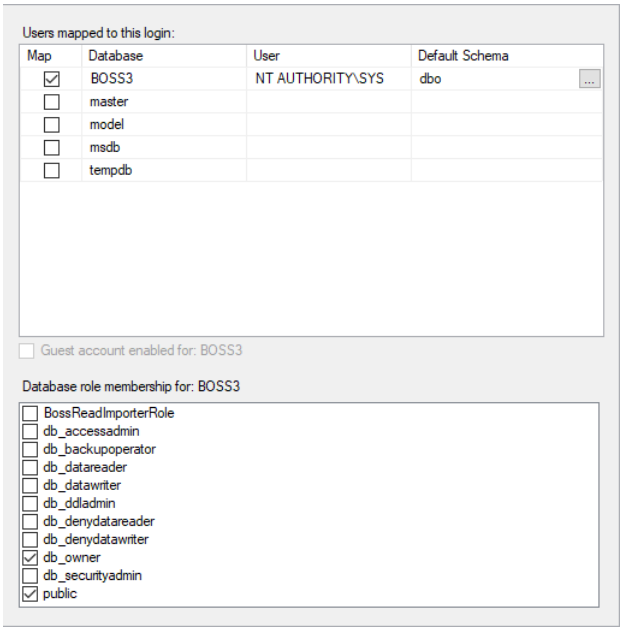
a. The server principal "user" is not able to access the database "BOSS3" under the current security context:
This problem is caused by missing permissions in the database user you are using.
To fix this problem you need to go to the Microsoft SQL Server Management Studio application and connect with a user with sysadmin privileges, inside the object explorer expand the folder Security, within the logins folder identify your user, right click on the user and select Properties. Inside "Server Roles" mark the sysadmin box.
After this restart the BOSS service.

The Underlying Provider failed

When a read query is made, the application shows the message **The Underlying Provider failed**

a. Inside the logs file, look for the line with the message "Login failed for user" identify the user, example- "Login failed for user 'NT AUTHORITY\SYSTEM". If this occurs log into SQL Studio Manager and map the BOSS3 Db to that account, also add the membership role of "db_owner" to the account.





Failed login

Check that the service is running, and the credentials are valid, also, check the server configurations, if you have localhost instead of 127.0.0.1 replace it for 127.0.0.1. If the problem persists go to the logs file and identify the error and contact PIPS customer support support@pipstechnology.com.

Relocating BOSS3 database

- When an upgrade requires you to move your existing BOSS3 database to a new location follow the recommend step in our "PIPS Relocate Boss Data Files" document for step by step instructions.

18 Appendix: Troubleshooting

When troubleshooting an issue, always start by looking for error messages in the Server log file, usually found at ...\PIPS Technology, Inc\ BOSS3\logs\BOSSServerLog.txt. Proceed based on the following information, recognizing that escalation may be necessary. If so, obtain a copy of the complete error message and include it with all escalated documentation.

ISSUE REPORTED	EXPLANATION	STEPS TO CORRECT
Just after an installation/upgrade, the UI won't start.	It takes several moments for the BOSS Server to be completely started and ready for information to be accessed.	After starting the BOSS server, wait for several moments before attempting to start the UI. If this is an upgrade this could be several minutes while the database is being updated.
I start the BOSS Controller, but it stops a moment later. The following error message may display "Error: Error in BOSS3 Controller. Please check the log files." (New installation scenario)	The license was not activated. When checking the BOSS Server Log, there will be two error messages : – 'Licensed for 0 concurrent clients' and – 'Failed to set registry parameter [_tmpbaliked a63] to value System.Byte[].'	Return to the licensing activation and updating checklist. (*See Section 17.2, BOSS Version 3.2 and Above License Key Management.*)
I start the BOSS Controller, but it stops a moment later. The following error message may display "Error: Error in BOSS3 Controller. Please check the log files." (Upgrade scenario)	The Upgrade Tool must be run before starting the Controller.	Run the Upgrade Tool. (*See Section 17.7 The BOSS Upgrade Tool.*)
I start the BOSS Controller, but it stops a moment later. The following error message may display "Error: Error in BOSS3 Controller. Please check the log files." (Other scenario)	If the Upgrade Tool has been run, there may be a problem with the database.	Look for error messages in the BOSS Server Log. Provide this information to Technical Support.
A fixed camera won't connect.	The firewall could be blocking the communications.	Ensure that the firewall is allowing communications through the VES ports, found in the BOSS Configuration Controller on the Ports screen.
PAGIS won't connect.	The firewall could be blocking the communications.	– Ensure that the firewall is allowing communications through the REST API (for PAGIS 2.7.x) and PAGIS 3.0 Service (for versions of PAGIS) ports, found in the BOSS Configuration Controller on the Ports screen. – Ensure that the device has been enabled in the BOSS UI Devices screen.
Hotlist will not update.	There is typically a problem with the source file.	– If it is a network hotlist, ensure that the site can be reached by entering the address in a browser. – If a local hotlist, ensure that the file is on the system and can be opened.
The NCIC Hotlist formatter that I need is not available. (New installation scenario)	The NCIC formatters were not added during the initial installation.	Stop the BOSS Service. Go to the Configure option on the BOSS Controller. Step to the NCIC screen. Select the desired NCIC formatters. Click **Save** and exit. Restart the BOSS Service. The formatters will now be available.

ISSUE REPORTED	EXPLANATION	STEPS TO CORRECT
I am unable to see reads/hits in the Dispatch screen.	The time on the read/hit coming in must be relatively close, within a couple of minutes, to the BOSS server time.	For a mobile ALPR system, correct the time on the laptop or ALPR processor. A fixed camera can be configured to use a time server. If issue persists, the server that BOSS is running on could also be configured to sync with a time server.
An error message, "Compressed method not supported," was found in the BOSS Server Log.	There are various reasons that this message can occur.	Obtain a copy of the complete error message. Provide this information to Technical Support.
An error message, "Transaction has aborted," was found in the BOSS Server Log.	There are various reasons that this message can occur.	Obtain a copy of the complete error message. Provide this information to Technical Support.
An error message. "Error #nn appeared in the db for Stored Procedure xxxx on line nn." was found in the BOSS Server Log.	An error occurred when running the stored procedure listed in the message.	Obtain a copy of the complete error message. Provide this information to Technical Support.
An error message, "Timeout expired. The timeout period elapsed prior to completion of the operation or the server is not responding," was found in the BOSS Server Log.	A SQL timeout error has occurred.	Obtain a copy of the complete error message. Provide this information to Technical Support.
An error message, "SNTP server not started, could not bind to InterNetwork 0.0.0.0:123," was found in the BOSS Server Log.	This is an expected error message that occurs when BOSS has not been configured to access a time server.	If no time server has been configured, this message can be ignored. If one has been configured, this needs to be escalated for further assistance.
After a new installation, the BOSS server stops running with an error message, "Failed in working with the database. Ensure connectivity is properly defined. Try running the BOSS Controller again and checking settings," was found in the BOSS Server Log.	When BOSS was started, there was a connection issue between it and the SQL Server.	Start by checking the information in the Controller. If that is all correct, then check to ensure that the SQL Server is running. If no issues are found there contact Technical Support Obtain a copy of the complete error message.
After a new installation, the BOSS Server stops with no error message in the BOSS Server Log.	The server needs to be run with Administrator privileges.	The server should be restarted in the Console as an Administrator. If running BOSS as a service then the BOSS Controller must be run as Administrator.
Error message in BOSS Server Log says that the file "httpconfig.exe" cannot be found.	This is an error that can occur when the system has not been updated in some time. It has been seen for other uncertain reasons as well.	Obtain a copy of the complete error message. Provide this information to Technical Support.
After a new installation, the BOSS Server starts but stops moments later. The BOSS Server Log contains the error message. "The system cannot find the file specified Additional Exception Message: Unhandled exception from 'Name:BOSS3.exe. There are no context policies." However, no file is listed in the message.	This typically occurs on older systems, especially Windows Server 2003, or systems that have not been updated for a while.	The file httpcfg.exe needs to be copied into the c\Windows\System32 directory.
The BOSS Server won't start, and there is an error message, "Transport Manager failed to listen on the supplied UIR using the NetTcpPortSharing service: failed to start the service because it is disabled," in the BOSS Server Log.	The NetTcpPortSharing Service is not running.	Obtain a copy of the complete error message. Provide this information to Technical Support.
The BOSS server stops running, and there is an error message, "Cannot open database "<Database Name>," in the BOSS Server Log.	There is an issue with the connection between the BOSS server and the SQL Server.	Start by checking the information in the Controller. If correct, then check to ensure that the SQL Server is running. If no issues are found contact Technical Support. Obtain a copy of the complete error message.

ISSUE REPORTED	EXPLANATION	STEPS TO CORRECT
The BOSS Server won't start and there is an error message "A file activation error occurred. The physical file name '<filename>' may be incorrect." in the BOSS Server Log.	There could be multiple reasons, but it is probably due to a database connection issue.	Obtain a copy of the complete error message. Provide this information to Technical Support.
When running the upgrade tool, an error message is displayed. A message is included in the BOSS Server Log: "Current upgrade state: One of the upgrade scripts failed to run as expected. Please contact support for direction."	This most likely occurred due to upgrading from an old version of BOSS.	Obtain a copy of the complete error message. Provide this information to Technical Support.
An unexpected response or behavior occurs in BOSS, and there is an error message, "Object reference not set to an instance of an object," in the BOSS Server Log.	This is a generic error message that can occur for various reasons.	Unless the issue has an obvious cause contact Technical Support. Obtain a copy of the complete error message.
The following error message, "Discarding tmp buffer because it's corrupted," has been found in the BOSS Server Log.	This message is associated with a database issue.	Obtain a copy of the complete error message. Provide the information to Technical Support.
The following error message, "SMTP server is not defined, email alerts disabled," has been found in the BOSS Server Log.	This message is informational indicating, as it states, that an email server has not been configured.	If attempts have been made to configure an email server and this error message occurs, recheck the settings and the server. If the error remains contact Technical Support.
The BOSS Service stops running, and the BOSS UI indicates that the server is not available. The following error message, "Cannot access a disposed object," is found in the BOSS UI Log.	This is an informational message provided by the UI confirming that it is no longer able to communicate with the BOSS server.	Restart the BOSS server and the BOSS UI will reconnect. If this does not correct the issue contact Technical Support.
The following error message, "The socket connection was aborted," is found in the BOSS UI Log.	This is an informational message provided by the UI confirming that it is no longer able to communicate with the BOSS server.	Restart the BOSS server, and the BOSS UI will reconnect. If this does not correct the issue contact Technical Support.
A problem occurs while adding a hotlist and the following error message "Invalid object name '<hotlist name here>'," has been found in the BOSS Server Log.	This indicates that there is an issue with the hotlist formatter being used.	Confirm that the correct formatter is being used. If so, confirm the source file is formatted correctly. If so, contact Technical Support. Provide a copy of the full error message.
While installing BOSS, an error message displays: "Error opening file for writing: <File Name>."	This indicates that the application listed in the error message is still running.	Check the Windows System Tray for any BOSS applications still running on the system. Close the application(s) and continue the installation.
The BOSS applications are installed under one user, but are not found when another user logs in.	The application was not installed using administrative privileges.	The application will need to be uninstalled and reinstalled using administrative privileges.
While using Client Tools to create Begin Shift files, an error message displays: "Client has not been activated on the server."	Mobile devices must be enabled on BOSS to synchronize data to it. This message is displayed the first time that Client Tools is used to create Begin Shift files because it has not been enabled yet.	Configure Client Tools on BOSS (see Section 17.6) so that BOSS adds Client Tools as a device.
When using Client Tools to synchronize End Shift files to BOSS, the following error message displays: "Error: Could not find <file and path name>."	Client Tools was unable to find the End Shift files to be processed at the defined path.	Check that the location assigned for the End Shift file matches the location chosen when Client Tools was configured. If it does not, move the file to the configured location.

19 Appendix: Plug-Ins

BOSS allows the use of third-party code via a plug-in that serves the needs of BOSS customers with specific data requirements. Once a plug- in is created and compiled, a copy of the DLL and any other necessary files can be copied to the plug-ins directory under BOSS. BOSS will automatically detect the existence of the plug-in at that point and permit reads to be passed to the ReceiveData method of your plug-in.

The functions of the currently available BOSS plug-ins are described in Sections 19.1 and 19.2. For more information and guidance on installing a plug-in, contact PIPS Technical Support for guidance.

19.1 The BOSS Truck Drayage Utility

Regulation of diesel-fueled heavy-duty trucks and a Drayage Truck Registry (DTR) were implemented by the California Air Resources Board (ARB) to help reduce both emissions from these vehicles and public exposure to contaminants in those emissions. Drayage trucks subject to regulation (Class 7 and Class 8) are registered and information about them is maintained on an ARB web service.

The Truck Drayage Utility is BOSS plug-in that provides access to the ARB web service. The utility is designed to contact the web service, retrieve data, and add it to a comma-separated values file. In BOSS, the Hotlist Administrator will then create a whitelist that uses this CSV file as the source file.

The connection to the ARB web service (managed by the Windows Task Scheduler) can be made once daily for a full download of the data, with subsequent connections allowed no more frequently then every 30 minutes for updates. This whitelist can then be deployed to a mobile or fixed camera in the monitored area. If a plate is read that is not included on the whitelist, a notification will be displayed in BOSS. Appropriate action can be taken at that time.

If the ARB web service is unavailable and downloads cannot be completed, the BOSS whitelist will not be updated. There will also be warning messages in the BOSS log such as “Could not connect to <web service address>. TCP error code nnnnn: <Error description>.” If this occurs, the utility will try again in 30 minutes. If the errors persist, it may be necessary to seek assistance.

19.2 The BOSS LPRD Plug-in

The BOSS LPRD plug-in relays the reads the BOSS server receives on to the national database at the Automated Regional Justice Information System (ARJIS), a joint powers agency that facilitates information-sharing among more than 70 law enforcement agencies—local, state, and federal—in the two California counties (San Diego and Imperial) that border Mexico. ARJIS operates a secure intranet (ARJISnet) with more than 11,000 users in San Diego County alone.

19.3 The BOSS DEA Plug-in

The BOSS DEA plug-in writes LPR messages to the file system as reads are received by the BOSS server. Those files will then be available for the Drug Enforcement Agency, DEA, File Transporter to act upon.

20 Appendix: BOSS Mantis

The Mantis service adds analytical analyses to new and existing read images within BOSS providing the user the ability to search based on vehicle Type, Brand, Color & Unique markings. BOSS Mantis is an additional PAID service that can be enabled on BOSS versions 3.6.x.x and above, older version of BOSS can support this feature by upgrading, providing they meet the system

20.1 How Dose Mantis Work

The service is hosted in the Amazon Web Services (AWS) Elastic Compute Cloud (EC2) platform, running in instances comprised mainly by Graphics Processing Units (GPUs). The only information sent to the Mantis endpoint is the vehicle image, known as the Overview image by the BOSS. Communication between BOSS and Mantis is performed as a client-server architecture, meaning the Mantis server uses the 443 (https) port to allow clients to reach the Mantis endpoint.

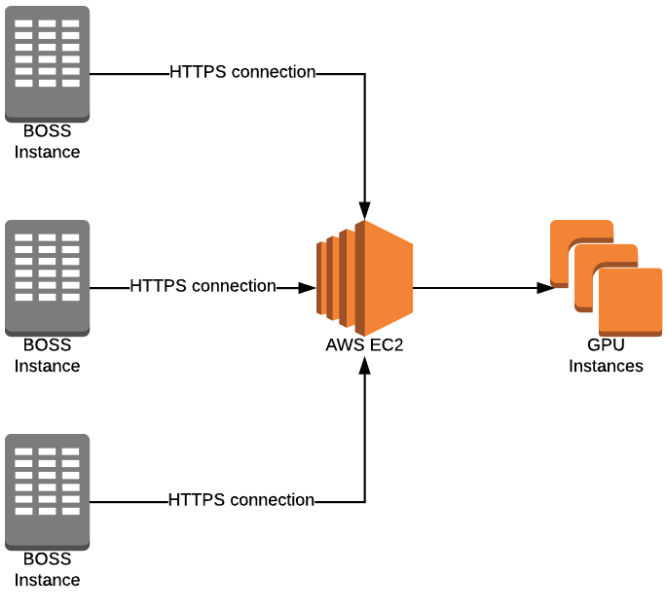


Figure 1 Multiple BOSS instances connected to the Mantis API.:

The information between BOSS and Mantis flows only in one way, this means that only BOSS clients can send data to Mantis, where it will be processed, and a response will be received by the BOSS server. Mantis cannot reach the BOSS Server or perform any kind of operations on the user's behalf over the data stored inside BOSS.

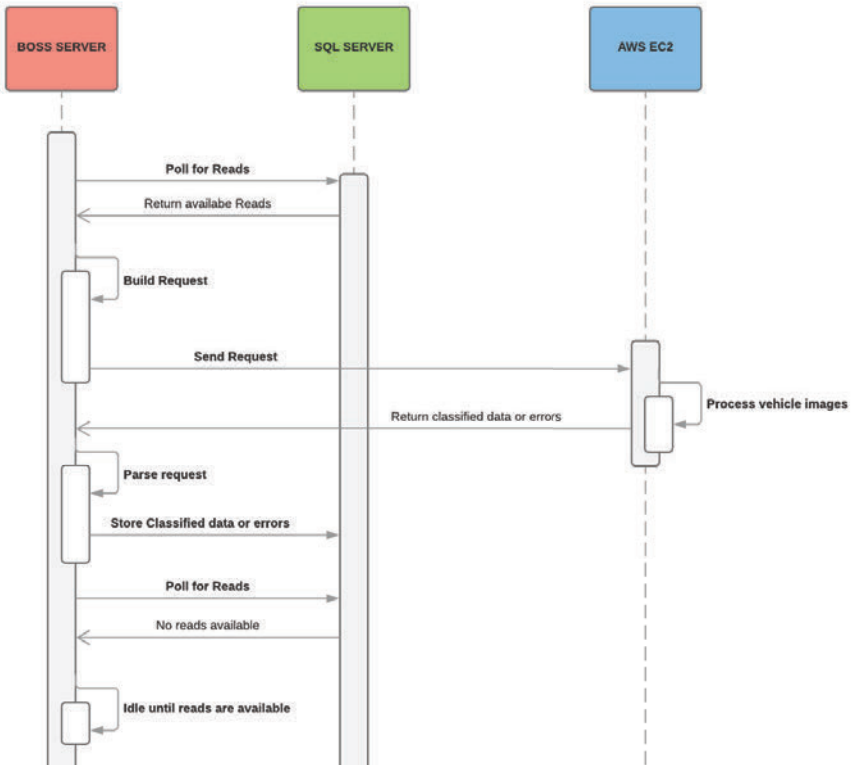


Figure 2 Sequence diagram for the current BOSS-Mantis Integration

20.2 Mantis Security and Encryption

As a summary description for the HTTPS protocol, its security is that of the underlying TLS (Transfer Layer Security) cryptographic protocol, where a certificate is used to authenticate the server, thus, the data flow between the client and the server is encrypted.

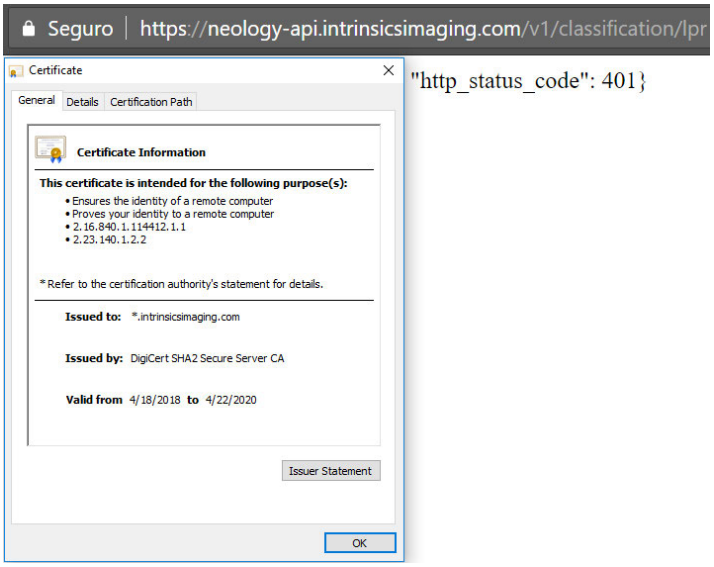


Figure 3 Available details for the certificate on the Mantis-Neology endpoint

20.3 Mantis Requirements

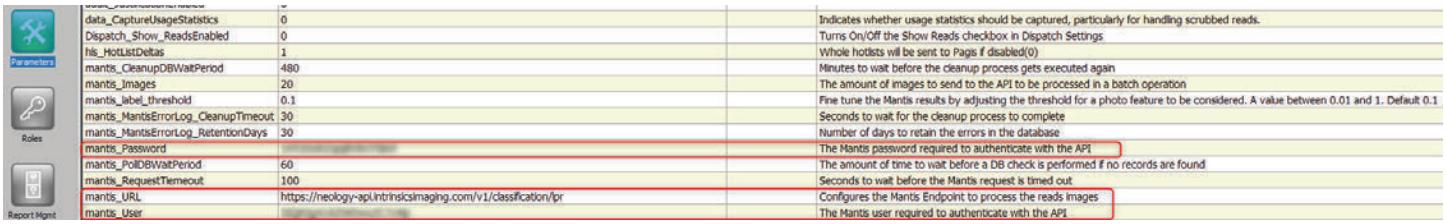
1. BOSS version 3.6 or newer.
2. Open communication to Mantis API URL (https://neology-api.intrinsicsimaging.com/v1/classification/lpr) via port 443.
3. Mantis Licensing feature required.
4. A valid Mantis User name and password. User name and password provided at time of licensing purchase.

20.4 Mantis Installation

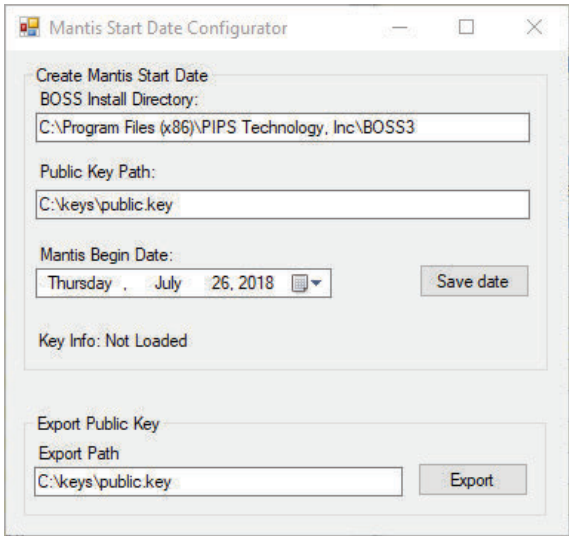
1. To upgrade or install Mantis version of BOSS follow the installation steps provide under Appendix 17. If upgrading from previous BOSS version you will also need to reactive your existing license to reflect the addition of the Mantis feature, see section 17.2.2.
2. Once BOSS is installed or upgraded, start the BOSS service to perform additional Mantis configurations.

20.5 Mantis Configurations

1. Start and login to the BOSS UI, navigate to System > Parameters.
2. In the Attributes table, look for the entries with the following names:
    - **a. mantis_User:** Assign the provided Mantis user name here.
    - **b. mantis_password:** Assign the provided Mantis user password here.
    - **c. mantis_URL:** Set the Mantis URL here. https://neology-api.intrinsicsimaging.com/v1/classification/lpr

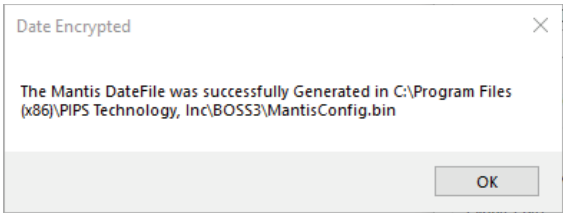


3. Additional parameters can be configured, see Mantis Parameters for details.
4. Once all the entries were assigned their corresponding values, close the BOSS UI and stop the BOSS service.
5. Download and place the “MantisStartDateGenerator.exe” file in the root BOSS3 folder, this executable is sperate from the BOSS installer and will need to be downloaded and placed manually.
6. Start the “MantisStartDateGenerator.exe” utility with administrator permissions.



7. Set the BOSS Install Directory to the Path of the folder where BOSS was installed.:

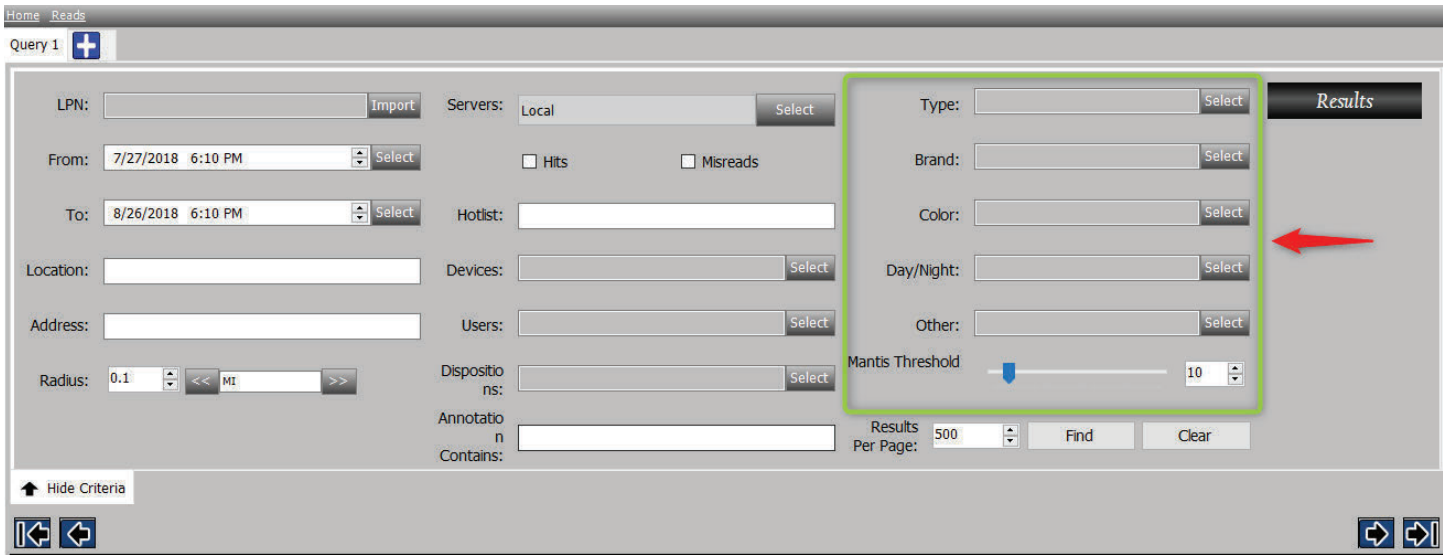
8. Set the Export Public Key path to a folder where you can access the generated public key, then click the Export button, and verify that the key was exported to the path.
9. Select a date that you want Mantis to take as the begin date for reads to be retrieved “Mantis Begin Date”. Reads that entered the system before this date, won’t be processed.
10. Click the Save date button to create the “MantisConfig.bin” file in the installation directory. A message confirming the file creation will appear.



11. Start the BOSS service.
12. When BOSS is started, the existing reads in the BOSS database will be sent to and processed by the Mantis API. The results will be stored on the local database.
13. Start and login to the BOSS UI.

20.6 Mantis Search Features

The Mantis fields should be visible in the right side of the reads panel in the BOSS UI. In case the fields are not available, diagnose the possible problems in the Mantis Configuration Troubleshoot section 20.8.



20.6.1 Mantis Search Definitions

- **Type=** Vehicle configuration style, i.e. Car, Box-Truck, Full-Size-Van, Hatchback, Minivan, Other-Truck, Pickup, Sedan, Suv.
- **Brand=** Vehicle manufacture.
- **Color=** Vehicle primary color.
- **Day/Night=** Vehicle capture in day or night.
- **Other=** Includes additional vehicle identifiers such a roof racks, spare-time, spoiler, ect...
- **Threshold=** Adjust the threshold slide bar to increase or decrease the confidences level of the Mantis search criteria based on selected filters, 1 being the lowest and 100 the highest confidence level available. When threshold is utilized in searches a new “Confidence” column will appear in the results, a user may now use this column to further sort the results by descending or ascending order.

20.7 Additional Mantis Parameters

As a summary description for the HTTPS protocol, its security is that of the underlying TLS (Transfer Layer Security) cryptographic protocol, where a certificate is used to authenticate the server, thus, the data flow between the client and the server is encrypted.

Parameter Name	Description	Default value
mantis_URL	The URL for the Mantis endpoint. The latest value should be available in this document. See Ports configuration for the corresponding value or ask a PIPS Technology representative.	None
mantis_User	Part of the credentials provided, it may be referenced also as the Mantis API key.	None
mantis_Password	Part of the credentials provided, it may be referenced also as the Mantis API password.	None
mantis_Images	The number of images to send to the API to be processed in a batch operation	20 images
mantis_PollDBWaitPeriod	The amount of time to wait before a DB check is performed if no records are found	60 seconds
mantis_RequestTiemeout	Seconds to wait before the Mantis request is timed out	100 seconds
mantis_MantisErrorLog_RetentionDays	Number of days to retain the errors in the database	30 days
mantis_MantisErrorLog_CleanupTimeout	Seconds to wait for the cleanup process to complete	30 seconds
mantis_CleanupDBWaitPeriod	Minutes to wait before the cleanup process gets executed again	480 minutes
mantis_label_threshold	Fine tune the Mantis results by adjusting the threshold for a photo feature to be considered. A value between 0.01 and 1.	10% (0.1)

20.8 Mantis Configuration Troubleshoot

To trouble shoot any Mantis issue, access to the BOSS Server logs is required. The logs are available inside the logs directory, inside the installation folder, e.g. "C:\Program Files (x86)\PIPS Technology, Inc\BOSS3\logs".

Inside this folder, there are two types of outputs:

- **BOSSMantisLog.txt.*:** This files contain Mantis Service specific information.
- **BOSSServerLog.txt.*:** This files contain overall BOSS Server information.

Known errors

L	Level	Error	Description
	INFO	**Mantis Service: Not available**	The Mantis feature was not enabled in the license key with which BOSS was activated
		Solution	Contact a Neology PIPS Technology agent for information on how to request the activation of the feature in your current license key
	INFO	**Mantis configuration not loaded, the service will not be started**	This error signals missing configuration Look for the additional messages described in the following rows.
	ERROR	**Mantis endpoint not configured, shutting down service**	The mantis URL parameter was not set properly, it cannot be a null or empty value.
		Solution	Review the ports configuration and set the mantis URL parameter to the given mantis URL. If you have an outdated version of this document, contact the Neology PIPS Technology support team to get the latest information.

	ERROR	**Mantis credentials are not configured, shutting down service**	Either the mantis_User or the mantis_password parameter was not set.
		Solution	Check that these values do not have a null or empty value. If you were not provided with these credentials, contact the Neology PIPS Technology support team.
	INFO	**Due to a request error, the next Mantis request will be performed in seconds**	There are three known errors related to mantis functionality: • **Mantis Failure**: Mantis failed to process the uploaded information. This error will not be retried because with the same image, Mantis will produce the same output. • **Connection error**: There was a problem establishing a connection with the server. This batch will be retried. • **Mantis Server Error**: An exception was received from the server. This error will be retried.
		Solution	For the above three errors, the possible solutions or actions to take are described below: • **Mantis Failure:** If too many instances of this error appear, contact the support team to diagnose the error. • **Connection error:** Verify that the appropriate rules for the firewall and whitelisting for URL and ports was set. See Mantis requirements for more details. • **Mantis Server Error:** If too many instances of this error appear, contact the support team to diagnose the error.

For a full list of all the messages produced by Mantis and a more detailed explanation about them, see the Mantis Log messages catalog.

20.8.1 Mantis Log Messages Catalog

Below is a description for the messages produced by the Mantis Service. Only applicable messages will have a solution appended to them.

Glossary

Term	Definition
ALPR	Automatic license plate recognition (also called automatic number plate recognition, or ANPR)
Annotation	A note or comment that can be made about and added to a read.
Deployment	The distribution or making available of a hotlist to a device
Device	A source of ALPR data; an PAGIS unit or a fixed or mobile camera
Disposition	The classification of a hit; e.g., a recovered stolen vehicle
Fixed Camera	An ALPR camera permanently mounted above a roadway
Group	A group of BOSS users that belong together administratively
Hit	A match on a plate read against a hotlist
Hotlist	A list or database of license plates of interest, e.g., the NCIC database
Justification	A purpose for running a query on the captured data. There are several justifications included in the system by default. The BOSS Administrator can also create custom justifications to be used.
LPN	License plate number; also known as the Vehicle Plate Number
PAGIS	PIPS™ Mobile Software, the ALPR Mobile application
Local Server	A server running on a local system, in relation to the SQL server or the BOSS UI Misread A read that was marked as a misread by a user
Mobile Unit	An ALPR system with cameras, a mobile processor, and software, such as Pagis Software, installed in a vehicle
Notification	Propagation or delivery of an alert resulting from a hit
Overview	A color image of the vehicle to which the license plate is attached
Patch	A small image of the license plate
Permission	Authorization to access specified functionality in BOSS
Read	A license plate detection event that results in the plate text optical recognition and pictures being taken
Remote Server	A BOSS server that is running in another location
Role	A position, such as Administrator, with the authorization to access specified functionality in BOSS
Site	A group of related devices
Translation	The interpretation from a word in English to a word in a selected language
User	An authorized BOSS user (with a username and password)
Whitelist	In BOSS a whitelist hit is the opposite of a hotlist hit. When a license plate read does not exist in an enabled whitelist database, the same Hits (Alert) screen will be displayed.

For additional information, assistance or maintenance questions please contact Neology ALPR/ANPR Support at:
PHONE: 833-PIPS-LPR (833-747-7577)
• Option 1 for Sales
• Option 2 for Support

For the U.S/Can and all other areas:
Sales Enquiry Email: sales@pipstechnology.com
Support Request Email: support@pipstechnology.com

For Europe, Middle East and Africa:
Sales Enquiry Email: sales@pipstechnology.co.uk
Support Request Email: support@pipstechnology.co.uk

IS A TRADEMARK OF NEOLOGY INC., AND EITHER REGISTERED OR PENDING REGISTRATION IN SEVERAL JURISDICTIONS.

Neology Headquarters San Diego
Address: 12760 Danielson Ct.,
Suite A Poway, CA 92064

Neology UK Ltd
Address:Form 1 Bartley Wood Business Park
Hook, Hampshire
RG27 9UP

Neology México
Plaza Carso II, Lago Zurich No. 219-Piso 10
C.P. 11529 Ciudad de México

	BOSS 4 Annual License Subscription	MANTIS 4-D Vehicle Detection Annual Subscription	Hosted Subscription
BOSS 4 Standard Software Application For either on-premise or Neology Hosted option	x		
Free Periodic SW Enhancements and Maintenance release in line with Neology standard SW release cycle	x		
Unlimited Helpdesk Access for BOSS 4 SW Available from 08:00 to 17:00 Central Standard Time	x		
Vehicle Classification Add-in for all vehicle detections including: - Vehicle Type - Vehicle Brand - Vehicle Feature (Spoiler, roof rails etc) - Vehicle Color -		x	
Enhanced ALPR "Deep Learning" capability enabled on Neology's latest generation Mobile (Golden Eagle) and Fixed (IRIS) Camera		x	
Access to the latest OCR and Vehicle Classification algorithms for all Neology / PIPS legacy devices in line with Neology standard release cycle		x	
Application and Database Server(s) with corresponding network provided on CJIS compliant Infrastructure			x
Elastic Database retention and storage in line with subscription level			x

High Availability and Resilience to ensure 99.999% infrastructure availability with 4 layers of Severity Monitoring (Urgent, High, Medium, Low)			x
Infrastructure Security Monitoring, including annual penetration testing and patching where required			x
Proactive System Health Monitoring (database, application and infrastructure) to pre-empt incidents			x
Service Management reporting on quarterly basis			x
Out of Hours Support for Critical Severity Infrastructure Issues			x

Clear Form

BOSS4 Questionnaire

After completion and submission of this document, the delivery team will review and submit to you the recommended Systems Specifications. Further logistical planning shall proceed after delivery of the initial Systems Specifications.

BOSS4 Server Type		Software Upgrade	
On-Prem: ☐	Hosted (Cloud): ☐	BOSS Upgrade. Yes: ☐ No: ☐	Current BOSS Version:

Customer Information			
Agency Name:		Date:	
Point of Contact Name:			
Email Address:			
Phone Number:			

Items to Migrate When Upgrading					Not Applicable: ☐
Migrate Reads	Yes: ☐	No: ☐	Migrate Hits	Yes: ☐	No: ☐
Migrate Users	Yes: ☐	No: ☐	Migrate Groups	Yes: ☐	No: ☐
Migrate Roles	Yes: ☐	No: ☐	Migrate Devices	Yes: ☐	No: ☐
Migrate Sites	Yes: ☐	No: ☐	Migrate Hotlists	Yes: ☐	No: ☐

Current ALPR Data Statistics			Not Applicable: ☐
Average **Monthly Read** intake.		Average **Yearly Read** intake.	
Current number of **Devices.**		Current number of **Users.**	
Current number of **Hotlists.**		Current Data **Retention Policy.**	

5 Year Projected Growth - ALPR Statistics

Projected read estimates help us ensure the ALPR system specifications are properly configured over time. Example, if the agency currently reads 500,000 plates per month, and growth is expected to double that count in five years, the projected number would be 1,000,000 below.

Projected number of **Reads** per/month.		Projected number of **Devices.**	
Projected number of **Users.**		Projected Data **Retention Policy.**	

Data Integration

Are you planning or are you currently using any kind of third-party application to ingest data from the BOSS database? If so, please provide a detailed explanation of this process.

BOSS4 Cloud
Specifications for Requirements

Cloud Application Servers

Below, there are the minimal recommended configurations for different capacity configurations for BOSS4 hosted on Amazon Web Services infrastructure.

Application Servers Specifications				
Configuration	**Demo**	**Medium**	**Large**	**High Capacity**
ALPR Devices	1 to 3	3 to 50	50 to 150	Beyond 150
Average Daily Intake	Around 30,000 events	Around 500,000 events	Around 1,500,000 events	Beyond 1,500,000 events
Average of users querying data	3 users	15 users	25 users	Beyond 25 users
Alert list averaging	Around 1M records	Around 2M records	Around 2M records	Around 2M records
EC2 AWS Instances for Microservices	t3.small 2.5GHz Intel 2 cores 2 GB RAM Amazon Linux	t3.large 2.5GHz Intel 2 cores 8 GB RAM Amazon Linux	t3.xlarge 2.5GHz Intel 4 cores 16 GB RAM Amazon Linux	t3.2xlarge 2.5GHz Intel 5 cores 32 GB RAM Amazon Linux
EC2 AWS Instance for Controller	t2.small 3.3GHz Intel 1 core 2GB RAM Amazon Linux	t2.large 3.0GHz Intel 2 cores 8GB RAM Amazon Linux	t2.xlarge 3.0GHz Intel 4 cores 16GB RAM Amazon Linux	t2.2xlarge 3.0GHz Intel 8 cores 32GB RAM Amazon Linux
Fargate AWS Instance for Microservices	3.3GHz Intel 5 cores 8GB RAM	3.0GHz Intel 16 cores 32GB RAM	3.0GHz Intel 32 cores 32GB RAM	3.0GHz Intel 48 cores 128 GB RAM
Storage and Application Space	Amazon EBS gp2 SSD 128GB	Amazon EBS io1 SSD 256GB	Amazon EBS io1 SSD 320GB	Amazon EBS io1 SSD 512GB

This document and its contents are intended for the recipient only. Copying, redistributing, or discussing with any other party outside of the intended recipient and Neology is prohibited.

Cloud Database Service

BOSS4 uses the MongoDB engine.

Database Service Specifications				
Configuration	**Demo**	**Medium**	**Large**	**High Capacity**
ALPR Devices	1 to 3	3 to 50	50 to 150	Beyond 150
Average Daily Intake	Around 30,000 events	Around 500,000 events	Around 1,500,000 events	Beyond 1,500,000 events
Average of users querying data	3 users	15 users	25 users	Beyond 25 users
Alert list averaging	Around 1M records	Around 2M records	Around 2M records	Around 2M records
Database Server Engine	MongoDB Atlas	MongoDB Atlas MongoDB Enterprise		
Dedicated Cluster	M20 2 vCPU 4 GB RAM Network Performance 100MB	M50 8 vCPU 16 GB RAM, Network Performance 10Gbps	db.r5.4xlarge 16 vCPU 64 GB RAM Network Performance 10Gbps	db.r5.8xlarge 32 vCPU 131 GB RAM Network Performance 10Gbps
Storage	General	General	General / Local NVMe SSD	General / Local NVMe SSD
Multimedia Storage	AWS EBS General Purpose SSD (gp2)		AWS EBS Provisioned IOPS SSD (io1)	

This document and its contents are intended for the recipient only. Copying, redistributing, or discussing with any other party outside of the intended recipient and Neology is prohibited.

BOSS4 On-Premise Specifications for Requirements

On-Premise Applications Server

Below, there are the minimal recommended configurations for different capacity configurations for BOSS4 On-Premise infrastructure.

Application Servers Specifications				
Configuration	**Demo**	**Medium**	**Large**	**High Capacity**
ALPR Devices	1 to 3	3 to 50	50 to 150	Beyond 150
Average Daily Intake	Around 30,000 events	Around 500,000 events	Around 1,500,000 events	Beyond 1,500,000 events
Average of users querying data	3 users	15 users	25 users	Beyond 25 users
Alert list averaging	Around 1M records	Around 2M records	Around 2M records	Around 2M records
Operating System	Amazon Linux / Amazon Linux 2 x64 Linux x64 (RHEL/CentOS, Ubuntu, Debian, SUSE) macOS x64 Windows 10 Professional x64 Windows Server 2016 x64			
Memory	16GB	32GB	64GB	192GB
Processor	x64 2.0 GHz 8 cores o better	Server Processor x64 (Intel Xeon Gold) 2 GHz 4 cores, 8 threads, 4MB cache	Server Processor x64 (Intel Xeon Platinum) 2.4 GHz 16 cores, 32 threads, 8MB cache	Server Processor x64 (Intel Xeon Platinum) 2.4 GHz 24 cores, 48 threads, 24MB cache
Hard Drive	7200 RPM SATA3	SSD SATA3	SSD SATA3 or NVMe PCI Express	SSD SATA3 or NVMe PCI Express
Application Space	128 GB of available space	256GB of available space	320GB of available space	512GB of available space

This document and its contents are intended for the recipient only. Copying, redistributing, or discussing with any other party outside of the intended recipient and Neology is prohibited.

On-Premise Database Server

BOSS4 uses the MongoDB Database Engine.

Specifications of the Database Server				
Configuration	**Demo**	**Medium**	**Large**	**High Capacity**
ALPR Devices	1 to 3	3 to 50	50 to 150	Beyond 150
Average Daily Intake	Around 30,000 events	Around 500,000 events	Around 1,500,000 events	Beyond 1,500,000 events
Average of users querying data	3 users	15 users	25 users	Beyond 25 users
Alert list averaging	Around 1M records	Around 2M records	Around 2M records	Around 2M records
Database Engine	Mongo DB Community	MongoDB Enterprise		
Operating System	Amazon Linux / Amazon Linux 2 x64 Linux x64 (RHEL/CentOS, Ubuntu, Debian, SUSE) macOS x64 Windows 10 Professional x64 Windows Server 2016 x64			
Processor	x64 2.0 GHz 8 cores o better	Server Processor x64 (Intel Xeon Gold) 2.5 GHz 4 cores, 8 threads, 4MB cache	Server Processor x64 (Intel Xeon Platinum) 2.4 GHz 16 cores, 32 threads, 16MB cache	Server Processor x64 (Intel Xeon Platinum) 2.4 GHz 24 cores, 48 threads, 24MB cache
Memory	N/A	32 GB	128GB	256GB
Hard Drive	7200 RPM SATA3 Not suitable for camera implantation with any kind of data retention expected	SSD SATA3 RAID level redundancy and scheduled DB backups recommended *See sizing chart for storage.*	SSD SATA3 or NVMe PCI Express RAID level redundancy and scheduled DB backups recommended *See sizing chart for storage.*	SSD SATA3 or NVMe PCI Express RAID level redundancy and scheduled DB backups recommended *See sizing chart for storage.*

This document and its contents are intended for the recipient only. Copying, redistributing, or discussing with any other party outside of the intended recipient and Neology is prohibited.

BOSS4 On-Premise & Cloud Storage

The calculation of storage applies to Cloud and On-Premise configurations.

Assumptions for the calculation:

Storage of metadata per read event: 32KB
Storage of imagery per read event: 160KB

Events from Golden Eagle or P500 cameras			
# of records	Database size Metadata and indexes	Repository Size Imagery	Total
1 Million	32GB	153GB	**185GB**
5 Million	64GB	763GB	**827GB**
10 Million	320GB	1.5TB	**1.82TB**
50 Million	1.6TB	7.5TB	**6.1TB**
100 Million	3.2TB	15TB	**18.2TB**

The calculation for the storage is approximated and it can vary depending on the conditions for the processing of the indexes, Mantis Metadata, compression of the images, among others.

It is not considered the storage for the backup of the databases nor the imagery repository.

This document and its contents are intended for the recipient only. Copying, redistributing, or discussing with any other party outside of the intended recipient and Neology is prohibited.

Massachusetts State Police
Policy and Procedure
Index

ADMINISTRATIVE

CODE	TITLE	DATE
ADM-01	Oath of Office	6/25/2008
ADM-02	State Police Mission and Policy	6/25/2008
ADM-04	State Police Authority	6/25/2008
ADM-05	Organizational Structure	6/21/2017
ADM-06	Command Staff Responsibilities	6/25/2008
ADM-07	Written Directives, Schedules and Forms	8/20/2014
ADM-08	Strategic Planning	11/5/2008
ADM-08A	Grant Approval Process	11/5/2008
ADM-09	Line Inspections	4/23/2009
ADM-09A	Staff Inspections	4/23/2009
ADM-10	Awards	4/10/2018
ADM-11	Sick Leave	4/16/2009
ADM-11A	Temporary Modified Duty	3/31/2017
ADM-11B	Injury Reporting and Leave	6/25/2008
ADM-11C	Maternity Leave and Guidelines	6/25/2008
ADM-11E	Leaves of Absence	11/5/2008
ADM-12	Serious Injury/Death of a Member	4/23/2009
ADM-13	Notification of Medical Examiner and/or Next of Kin	4/23/2009
ADM-14	Personnel Investigations	6/14/2018
ADM-15	Internal Affairs	6/25/2008
ADM-16	Notifying Prosecuting Agencies Regarding Evidence	5/4/2018
ADM-17	Employee Evaluation System	6/25/2008
ADM-18	Unlawful Harassment, Sexual Harassment and Discrimination	8/1/2017
ADM-19	Vehicle Management	11/5/2008
ADM-19A	Vehicle Use and Maintenance	12/11/2019
ADM-19B	Automated Vehicle Locator (AVL) Technology	5/2/2018
ADM-20	Weapons Management	8/1/2017
ADM-21	Communications	11/5/2008
ADM-22	Court Attendance and Fees	4/23/2009
ADM-24	Department Radio Call Signs	6/14/2018
ADM-25	Paid Details	6/14/2018
ADM-26	Military Service	6/25/2020
ADM-27	Transfers	5/21/2018
ADM-28	Department Motor Vehicles	3/1/2016
ADM-29	Workplace Violence	4/23/2009
ADM-30	Asset Management	6/14/2018
ADM-34	Information Technology Resources (ITR)	4/23/2009
ADM-34A	Social Media/Networking	6/17/2013
ADM-35	Body-Worn Camera and Cruiser-Mounted Camera Pilot Program	1/31/2019
ADM-36	Diversity and Equal Opportunity	11/5/2008
ADM-41	Telephone Use/Access	11/5/2008
ADM-46	Sexual Activity in Public Places	4/23/2009
ADM-47	Bias-Based Profiling	1/7/2020

GENERAL

CODE	TITLE	DATE
GEN-01	Personal Appearance	9/03/2019
GEN-01A	Tattoos and Body Modifications	6/22/2020
GEN-02	Uniforms	1/25/2018
GEN-04	Military Courtesy	4/23/2009
GEN-04A	Ceremonial Tributes	6/17/2013
GEN-05	Communicable Diseases	11/5/2008
GEN-06	Drug Testing	11/5/2008
GEN-07	Automatic External Defibrillators	4/23/2009
GEN-08	Ride-Along/Observer	11/5/2008

INVESTIGATIVE

CODE	TITLE	DATE
INV-01	Criminal Investigations	5/21/2018
INV-01A	Case Management	5/21/2018
INV-02	Confidential Informants	6/14/2018
INV-02A	Confidential Funds	4/23/2009
INV-03	Prescription Monitoring Program	5/21/2018
INV-05	Special Protections for Juveniles	7/12/2018
INV-07	Non-Published Telephone Numbers	5/21/2018
INV-08	Criminal Intelligence	5/21/2018
INV-09	Polygraph Examinations	4/23/2009
INV-10	Evidence Collection and Preservation	4/23/2009
INV-11	Controlled Substance-Storage & Handling	5/10/2012
INV-11A	Property and Contraband	6/17/2013
INV-13	Asset Forfeiture	4/23/2009
INV-14	Seized Currency	4/23/2009
INV-15	Field Interview and Observation Reports	4/23/2009
INV-16	Electronic Recording of Interrogations	4/23/2009
INV-16A	Eyewitness Identification	9/20/2010
INV-17	Travel/Immigration Status Inquiries & Investigations	8/1/2017

PRISONER

CODE	TITLE	DATE
PRI-01	Warrant Management	4/23/2009
PRI-01A	Warrants, Summons, or Subpoenas	4/23/2009
PRI-02	Custodial Inventory	5/5/2017
PRI-03	Prisoner Transportation	4/23/2009
PRI-04	Holding Facility Design and Inspection	5/20/2016
PRI-05	Identification of Persons in Department Custody	6/14/2018
PRI-06	Prisoner Monitoring	5/5/2017
PRI-07	Detainee Sexual Abuse and Sexual Harassment	5/21/2018
PRI-07A	Detainee Sexual Abuse and Sexual Harassment Investigations, Review and Data Collection	5/5/2017
PRI-08	Gender Identity and Expression	7/5/2017
PRI-09	Juvenile Detention	7/12/2018
PRI-10	Protective Custody	7/12/2018

SPECIAL OCCURRENCES

CODE	TITLE	DATE
SOC-01	Hazardous Materials	6/28/2019
SOC-02	Bomb Threats/Explosive Incidents	6/28/2019
SOC-03	Emergency Planning	3/25/2020
SOC-03A	Emergency Operations Center (EOC)	3/25/2020
SOC-03B	Response to Emergency Situations	3/25/2020
SOC-03C	Response to Civil Disturbances	3/25/2020
SOC-03D	All Hazards Incident Command Framework	3/25/2020
SOC-04	Lost/Missing Person Searches	7/11/2011
SOC-04A	Amber Alert Activation	4/23/2009
SOC-05	Special Considerations	7/22/2014
SOC-06	Administration of Naloxone Hydrochloride (Narcan)	7/29/2014
SOC-07	Domestic Abuse	4/23/2009
SOC-07A	Domestic Abuse Arrest/Investigations	4/23/2009
SOC-07B	Domestic Abuse Involving Members	6/17/2013
SOC-07C	Abuse of Children/Disabled/Elderly	7/22/2014
SOC-09	Terrorism/ WMD Incidents	6/28/2019
SOC-10	Clandestine Drug Laboratory Response	6/28/2019

SUPPORT

CODE	TITLE	DATE
SUP-01	Jurisdiction/Mutual Aid	4/23/2009
SUP-03	Media Relations	4/23/2009
SUP-04	Employee Assistance Unit	7/11/2011
SUP-05	State Police Chaplain Corps	4/10/2019
SUP-06	Binding Written Agreements	4/23/2009
SUP-12	Office of the Ombudsman	7/11/2011

TACTICAL OPERATIONS

CODE	TITLE	DATE
TOP-01	Special Operations Command and Control	6/14/2018
TOP-02	Special Tactical Operations Team	6/17/2013
TOP-03	Crisis Negotiation Team	6/17/2013
TOP-04	Mounted Unit	6/17/2013
TOP-05	Canine Unit	6/17/2013
TOP-06	Underwater Recovery Team	6/17/2013
TOP-07	Air Wing	6/14/2018
TOP-07A	Small Unmanned Aerial System (UAS)	6/28/2019
TOP-08	Marine Unit	6/14/2018
TOP-09	Incident Management Assistance Team	6/28/2019
TOP-10	Special Emergency Response Team	6/17/2013
TOP-11	Emergency Management Unit	6/17/2013
TOP-12	Motorcycle Unit	7/22/2014

TRAFFIC

CODE	TITLE	DATE
TRF-01	Mission, Goals, and Objectives	11/5/2008
TRF-02	Patrol	4/23/2009
TRF-03	Selective Traffic Enforcement	11/5/2008
TRF-04	Motor Vehicle Pursuits	5/10/2012
TRF-04A	Foot Pursuits	4/23/2009
TRF-05	Traffic Incident Management	11/5/2008
TRF-07	Motor Vehicle Stops	11/5/2008
TRF-08	Citations	4/23/2009
TRF-09	Towing	6/14/2018
TRF-10	Vehicle Inventory	4/23/2009
TRF-11	Automatic License Plate Recognition	10/01/2019
TRF-12	Crash Investigations	4/23/2009
TRF-14	Operating Under the Influence-Alcohol	7/22/2014
TRF-14A	Operating Under the Influence-Drugs	7/22/2014
TRF-14B	Preliminary/Portable Breath Test Devices	7/22/2014
TRF-15	Sobriety Checkpoints	4/23/2009
TRF-16	Speed Measuring Devices	4/23/2009
TRF-17	Emergency Roadblocks	4/23/2009
TRF-20	Department Vehicle Crashes	7/08/2009
TRF-21	Tire Deflation Devices	4/23/2009
TRF-22	Escorts and Relays	5/21/2018

TRAINING

CODE	TITLE	DATE
TRN-01	Training Administration	9/18/2018
TRN-02	Recruit Training	4/23/2009
TRN-03	Field Training Program	11/5/2008
TRN-04	Professional Development	5/10/2012

USE OF FORCE

CODE	TITLE	DATE
UOF-01	Use of Force	6/11/2020
UOF-02	Lethal Force-Response	8/1/2017
UOF-03	Reports	7/3/2019
UOF-04	Use of Force-Equipment	7/3/2019
UOF-05	Firearms Qualification	11/5/2008
UOF-06	Electronic Control Weapons (ECW)	7/3/2019

Department of State Police
General Order

Effective Date	Number
June 25, 2008	**ADM-01**

Subject

Oath of Office

Policy

All sworn members of the Department of State Police shall take and affirm an Oath of Office prior to the initial performance of duties.

Oath of Office

I, do solemnly swear, that I will bear true faith and allegiance to the Commonwealth of Massachusetts, and will support the Constitution thereof, so help me God.

I, do solemnly swear and affirm, that I will faithfully and impartially discharge and perform all the duties incumbent on me as a Massachusetts State Police Trooper: according to the best of my abilities and understanding, agreeably, to the rules and regulations of the Constitution, and the laws of this Commonwealth, so help me God.

I, do solemnly swear, that I will support the Constitution of the United States.

References

MGL c.22C, s.15

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 25, 2008	**ADM-02**

Subject

State Police Mission and Policy

Mission

As the principal statewide law enforcement agency in the Commonwealth, the Massachusetts State Police, in partnership with local communities, shall provide for the public safety by providing quality policing directed at achieving safer roadways, and reducing crime through investigations, education and patrol services, and by providing leadership and resources during natural disasters, civil disorders and critical incidents.

Policy

The Department of State Police, in cooperation with the Executive, Legislative, and Judicial branches of government, shall ensure that justice in a free society is perpetually prevalent.

Organizational Values

The value statements of the Massachusetts State Police are:

- Maintenance of the highest standards of integrity and ethics;
- Excellence and teamwork in the performance of duty;
- Protection of Constitutional Rights;
- Problem solving for continuous improvement;
- Continuous planning for the future; and
- Performing public service and law enforcement tasks so as to provide leadership to the police profession.

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 25, 2008	**ADM-04**

Subject

State Police Authority

Policy

Within the Commonwealth, sworn members shall exercise all the powers of police officers as authorized by law and exercise professional discretion when appropriate.

Limits of Authority

No member may be used or called upon for service at any industrial dispute unless actual violence has occurred therein, and then only by written order of the Governor.

Members shall not exercise police powers on a reservation or other property of the United States of America unless requested by the person in charge of the reservation or property.

No member shall serve civil process.

Discretion

When Rules and Regulations, Policy and Procedure, other Orders or Directives, fail to provide specific guidance, members shall exercise professional discretion that may be based upon:

- Training, experience, common sense;
- Principles, values, ethics;
- Advice from supervisors, senior officers; and
- Professionally accepted standards.

Discretionary measures may include:

- Application for complaint;
- Verbal or written warnings;
- Referral to other divisions, departments, or agencies;
- Guidance from the Attorney General/District Attorney; and
- Informal resolution.

References

MGL c.1, s.7, s.22C, s.10, s.50
40 USC s.318

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 21, 2017	**ADM-05**

Subject

Organizational Structure

Policy

The Department's organizational structure is arranged in a manner which simplifies the direction, coordination, and control of personnel.

Organizational Structure

The Superintendent does hereby establish the following operational Divisions for the effective and efficient delivery of services:

- Division of Field Services;
- Division of Investigative Services;
- Division of Administrative Services;
- Division of Standards and Training; and
- Division of Homeland Security and Preparedness.

Organizational Charts

Organizational charts graphically depict organizational entities, levels of command, lines of authority, and positions established for the duties of personnel.

The charts must be:

- Reviewed by each Division Commander prior to the next fiscal year; and
- Revised through the Office of the Superintendent.

Accountability

Each employee is accountable:

- For the use of their authority delegated to others; and
- For the performance of any personnel under their control.

Subject	Number
Organizational Structure	**ADM-05**

Chain of Command

The chain of command is the extension of authority and responsibility from the Colonel/Superintendent down to the level of execution.

Responsibility is accompanied by commensurate authority.

The chain of command for sworn members, in order of descending rank, shall be:

- Colonel/Superintendent;
- Lieutenant Colonel/Deputy Superintendent;
- Lieutenant Colonel;
- Major;
- Detective Captain;
- Captain;
- Detective Lieutenant;
- Lieutenant;
- Sergeant; and
- Trooper - The senior Trooper is in command, when necessary.

Command

Each organizational entity shall be:

- Under the direct command of only one supervisor.

Each employee shall be:

- Accountable to only one supervisor at any given time; and
- Bound by the chain of command that is applicable to their position.

Supervisory ratio must be:

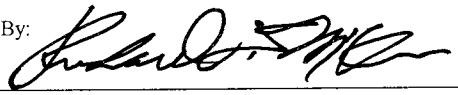
- Adequate to provide guidance and control, as determined by the Colonel/Superintendent.

Ranking personnel shall:

- Assume line control outside their own organizational entity when failure to do so would seriously endanger the Department's:
    1. Ability to maintain law and order; and
    2. Public image.

References

Rules and Regulations Article 3

Promulgated By: 

Department of State Police
General Order

Effective Date	Number
June 25, 2008	**ADM-06**

Subject

Command Staff Responsibilities

Policy

The Command Staff is responsible for the administrative and operational control of the Department. Each member of the Command Staff shall maximize their involvement in the operations of the Department to deliver the highest level of public safety services to the citizens of the Commonwealth.

Definition

The Command Staff shall include the following ranks:

- Colonel/Superintendent;
- Lieutenant Colonel/Deputy Superintendent;
- Lieutenant Colonel;
- Major; and

Civilian Member of the Command Staff:

- Chief Administrative Officer.

Responsibilities

Position	Duties
Superintendent	• Act as the Chief Executive Officer of the Department; • Assume full authority over the organization, administration and discipline of the Department; and • Promulgate all rules, regulations, policies, procedures, orders and directives.
Deputy Superintendent	• Act as the Chief Operating Officer of the Department; and • Assume command of the Department as assigned and during the absence of, or when so designated by the Colonel/Superintendent.
Division Commander	• Act as the Chief Operating Officer of a Division.

Subject	Number
Command Staff Responsibilities	**ADM-06**

Meetings

Staff meetings shall be conducted to encourage and support the exchange of information. This may include a weekly staff meeting between the Colonel and all Divisions. Information from these meetings shall be distributed to all affected personnel as directed by Colonel/Superintendent.

References

MGL c.22C, s.2, s.3
Rules and Regulations 3.1, 3.2, 3.3, 3.6.2

Promulgated By:

Department of State Police
General Order

Effective Date	Number
August 20, 2014	**ADM-07**

Subject

Written Directives, Schedules and Forms

Policy

The Department shall provide administrative direction and operational guidance through an internal written directive process.

Directive Format

Directive	Issued by	Reason
General Order	Superintendent	• To promulgate or rescind Policy & Procedure, Rules & Regulations or written directives.
Personnel Order	Superintendent	• Assignments • Transfers • Appointments • Discharges • Discipline • Commendations
Special Order	Superintendent	• Specific instructions for specific personnel; and/or • Dissemination of information relative to a particular topic or incident.
Superintendent's Memorandum	Superintendent	• Formal or informal clarification or inquiry.
Division Commander's Order	Division Commanders	• Administrative order issued for members under their command.
Administrative Notice	Superintendent/ Deputy Superintendent	• To inform members about general issues (crime, training, law updates, etc); and/or • Address item(s) not covered by the above directives.

Subject	Number
Written Directives, Schedules and Forms	**ADM-07**

Duration

All General Orders, Personnel Orders, and Superintendent's Memorandums shall:

- Remain in effect until rescinded by the Colonel/Superintendent; or
- Remain in effect until superseded by another General Order, Personnel Order, or Superintendent's Memorandum.

Division Commander's Orders shall:

- Remain in effect until rescinded by the Division Commander or Colonel/Superintendent; or
- Remain in effect until superseded by another Division Commander's Order or General Order promulgated by the Colonel/Superintendent.

All other written directives are valid for one (1) year, unless rescinded. New directives may be issued at any time.

Attendance Calendars

Duty Assignment Supervisors shall:

- Maintain **Original** Attendance Calendar(s) for each subordinate (sworn/civilian employee) under their command;
- Submit through channels to their respective Division Commanders by January 20th of each year, the **Original** Attendance Calendar(s) for the previous year for each subordinate under their command sorted alphabetically by last name;
- Provide to the member/civilian employee a copy of their **Original** Attendance Calendar for the previous year; and
- Retain copies of Attendance Calendar(s) at respective Troop/Station/Section/Units for record keeping purpose, but under no circumstances shall a copy be submitted to the respective Division Commander.
  Note: Any **Original** Attendance Calendar that is unable to be located shall be reported immediately to the respective Troop/Station/Section/Unit Commander.

Troop/Stations/Sections/Units or Stations/Sections/Units under the command of a Non-Commissioned Officer, shall have designated Commissioned Officers within the chain of command to:

- Ensure members/civilian employees Attendance Calendars are monitored, reviewed and properly completed on a bimonthly basis on even months; and
- Verify a review was conducted on the reverse side of the subordinate's Original Attendance Calendars beginning January 2015.

Continued next page.

Attendance Calendars (Continued)

Division Commanders shall:

- Forward all Division members/civilian employees Original Attendance Calendars to the Human Resources Section, as soon as practicable.

The Human Resources Section shall;

- Ensure that each Original Attendance Calendar is inserted into the respective members/civilian employees Personnel File; and
- Ensure that the Original Attendance Calendar is kept on file for each year of Department service.

The Master Vacation Schedule

Each Troop/Station/Section/Unit Commanding Officer shall:

- Submit through channels the Master Vacation Schedule for all sworn and civilian employees under their command to their Division Commander on or before February 14th of each year; and
- Ensure that all sworn and civilian employees have selected vacation week(s) according to their collective bargaining agreement.

Division Commanders shall:

- Retain submitted Master Vacation Schedules for the current year for all sworn and civilian employees under their command.

Office of the Superintendent/Strategic Planning Section shall:

- Post a blank copy of the Master Vacation Schedule to DocuShare prior to January 1st.

"SP" Forms

The Office of the Superintendent-Strategic Planning Section shall:

- Review, authorize and post to DocuShare, if applicable, any request received through channels concerning the creation of a new Department "SP" Form;
- Ensure the new form is assigned a number through the "SP" Numbering System and recorded into the "SP" Master Forms List.
  Note: The Forensic Services Group shall be excluded from compliance with this section, however they shall maintain a similar record for internal forms used.

Station/Section/Unit Forms strictly used within their station/section/unit for Department business and not forwarded to any outside entities, shall be excluded from the requirement of obtaining an "SP" number.

Subject	Number
Written Directives, Schedules and Forms	**ADM-07**

Archives

Departmental written directives, excluding Division Commander's Orders and Personnel Orders, shall be maintained by the Office of the Superintendent-Strategic Planning Section, including the signed "master copy" of all written directives.

Division Commanders and the Human Resources Section shall maintain the signed "master copy" of their Division Commander's Orders or Personnel Orders.

Publications

All Department written directives shall be published and archived on DocuShare.

If applicable, Troop/Section Commanders shall ensure that Department bulletin boards are maintained with up-to-date directives and are accessible to all personnel.

Changes

All written directives shall be amended to coincide with the terms of current Collective Bargaining Agreement(s), state and federal laws, and including Executive Orders.

The Strategic Planning Section shall review and post all written directives, except Division Commander's Orders and Personnel Orders.

Members are encouraged to make suggestions and recommendations to change or create written directives. Such suggestions/recommendations shall be written and forwarded, through channels, to the Office of the Superintendent-Strategic Planning Section for review.

Exclusive Directives

Commanding Officers may create written directives for the administration of their respective entities. Directives shall be filed with their appropriate Division Commander and shall remain in effect for one (1) year unless:

- Rescinded; or
- The directive conflicts with a General Order.

Standard Operating Procedures (SOP)

Section/Unit Commanders shall:

- Create and maintain an internal standard operating procedure (SOP) specific to their function; and
- Forward a copy through channels to their Division Commander for approval and filing.

Subject	Number
Written Directives, Schedules and Forms	**ADM-07**

Distribution

The Colonel/Superintendent shall ensure written directives are properly distributed and/or posted to DocuShare.

It is the responsibility of each sworn and civilian employee to read promulgated directives. Sworn and civilian employees shall:

- Read and become familiar with the contents of all posted written directives; and
- Familiarize themselves with Policy & Procedures and Rules & Regulations as issued.

Requesting Written Directives

To obtain a copy of a written directive, members shall access DocuShare. If unable to access DocuShare, members shall consult their commanding officer who shall make the request through channels to the Strategic Planning Section.

Responsibilities for Written Directives

Position	Duties
Division Commanders	• Ensure all Division Commander's Order are posted and archived accordingly; • Assign a member to review all current and proposed written directives; and • When applicable, forward approved proposals/drafts to the Office of the Superintendent-Strategic Planning Section.
Office of the Superintendent-Strategic Planning Section	• Create, edit or review proposed written directives; • Post promulgated written directives on DocuShare; and • Archive all written directives, excluding Division Commander's Orders and Personnel Orders.
Colonel/ Superintendent	• Sign and promulgate written directives.

References

M.G.L. c. 22C, s. 2, s. 3

Promulgated By:

Department of State Police
General Order

Effective Date	Number
November 5, 2008	**ADM-08**

Subject

Strategic Planning

Policy

In order to affectively manage, the Department shall continuously:

- Review written directives;
- Exercise oversight over the grant process; and
- Establish inter-divisional cooperative work groups regarding strategic plans.

Strategic Planning Responsibilities

The Strategic Planning Section shall:

- Prepare and update written directives;
- Instruct and assist members with the grant application process;
- Maintain oversight on grant program operations and reporting;
- Develop strategic plans;
- Conduct reviews and evaluations of programs when requested;
- Research emerging technologies and trends;
- Maintain the forms management process, including design, inventory, and implementation;
- Assist the Command Staff with the Department's administration and control through planning, research and coordination; and
- Report to the Office of the Superintendent.

References

ADM-07 Written Directives

Promulgated By:

Department of State Police
General Order

Effective Date	Number
November 5, 2008	**ADM-08A**

Subject

Grant Approval Process

Policy

Whenever Department employees seek to obtain services and/or funding through private, public, state or federal entities; or to acquire or transfer equipment from an outside entity, the following procedures within this policy shall be adhered to.

Definitions

Grant requests can be any of the following:

1. *Grant*: An award of financial assistance from an external entity where no "substantial involvement" is anticipated between the awarding entity and the Department during performance of the agreed upon activity.
2. *Cooperative Agreement*: An agreement of financial assistance where there is "substantial involvement" anticipated between an external entity and the Department during the performance of an agreed upon activity. Cooperative agreements are often non-cash agreements involving services provided to or by the Department.
3. *Interagency Service Agreement* (ISA): An agreement between the Department and a state entity which is committing funds for a specific program.
4. *Equipment Acquisition Agreement*: Agreements, where upon the Department shall receive equipment to provide services, perform a specific function, or to use within its operations.

Match Money: The portion of funds that the Department shall provide to supplement the funding agency's contribution. The match is usually a percentage of the project's total budget.

Project Administrator: An employee appointed by their Division Commander to oversee a specific request/project and is responsible for the completion of all quarterly and annual reports.

Grants Manager: A manager from the Department's Fiscal Section, who is responsible for the grant fiscal oversight process through the Office of the State Comptroller and who ensures the timely submission of appropriate documentation as necessary to receive funding.

Continued next page.

Subject	Number
Grant Approval Process	**ADM-08A**

Definitions (Continued)

Grants Coordinator: A member from the Strategic Planning Section, who is responsible for monitoring the grants request process or equipment acquisitions and also assists members in the research, application, and reporting process.

Request Review Meeting: The initial meeting between the Project Administrator, the Grants Manager, and the Grants Coordinator to review the application requirements and to ensure the Department is eligible.

Review Committee: A Department committee which reviews existing programs to ensure their stated goals and objectives progress according to the best interest of the Department and forwards program recommendations to the Colonel/Superintendent.

SP 426 Grant/Agreement Approval Request Form: A form to be completed by employees requesting approval to initiate the application process for any services, funding and/or equipment acquisitions.

Process

Unless prior written approval has been granted from the Colonel/Superintendent, employees shall not:

- Enter into any grants, cooperative agreements, or interagency service agreements; or
- Solicit, submit an application, or accept funding and/or equipment from any outside entities.

Equipment

Project Administrators shall comply with ADM-30 Asset Management when receiving equipment through a grant request.

Grants Review Committee

The Grants Review Committee shall review existing funded programs throughout the year. The Review Committee shall consist of the following members:

- Grants Coordinator;
- Grants Manager;
- Deputy Chief Administrative Officer or designee; and
- Strategic Planning Section Commanding Officer or designee.

Subject	Number
Grant Approval Process	**ADM-08A**

Request Process

Position	Process
Employees	• Shall submit all requests through channels to the appropriate Division Commander or designee, **at least fifteen (15) days prior to the filing date deadline**; • Submitted requests shall include the following information: 1. A completed SP 426; 2. A copy of the original solicitation/application that identifies the funding source and requirements i.e. eligibility, application deadline, and matching amount requirements; 3. A program statement narrative that identifies the goals and objectives, as well as the intended outcome to be accomplished, and any supporting documentation; and 4. A budget which includes current information regarding personnel and/or equipment costs and the services to be performed and/or purchased.
Division Commander or Designee	• Shall review all requests; • Ensure adequate time is available to allow for modifications to the application before the filing deadline; • Endorse the SP 426; • Forward the request to the Strategic Planning Section; and • Designate a Project Administrator.
Strategic Planning Section Commander	• Shall immediately review the approved request; • Assign the request to the Grants Coordinator; • Ensure a Request Review Meeting is scheduled; and • Forward completed requests to the Colonel/Superintendent for approval.
Grants Coordinator	• Shall document approved requests; • Immediately schedule a Request Review Meeting with the designated Project Administrator; and • Notify the Grants Manager.
Grants Manager	• Shall record requests received from the Grants Coordinator; • Ensure the request budget is appropriate and accurate; and • Attend Request Review Meeting with the Grants Coordinator and the designated Project Administrator.

Continued next page.

Subject	Number
Grant Approval Process	**ADM-08A**

Request Process (Continued)

Position	Process
Colonel/ Superintendent	• Approve or deny the request; • If approved, sign the original application and the SP 426.

References

ADM-30 Asset Management
SP 426 Grant/Agreement Approval Request Form

Promulgated By:

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**ADM-09**

Subject

Line Inspection

Policy

Line Inspections shall be conducted to improve the operational readiness of the Department by ensuring that all members adhere to all established rules, regulations, policies, procedures, orders, directives, and general laws.

Members shall immediately correct unsatisfactory behavior and conditions in order to avoid the consequences which erode the trust and confidence of the public.

Procedure

Members from the rank of Captain through Trooper shall be inspected.

Members assigned to duties requiring civilian attire are exempt from the uniform/appearance portion of the inspection.

Troop/Section Commanders may require additional line inspection procedures within their respective commands.

Line Inspections

Troop/Section Commanders or designee, shall:

- Oversee the entire line inspection program for their command;
- Ensure that all members are inspected at least quarterly by their first line supervisor; and
- Ensure inspections are properly documented on PayStation.

First Line Supervisors Duties

First Line Supervisors shall:

- Conduct a inspection of all immediate subordinates at least quarterly, including their assigned cruisers and equipment; and
- Submit a report of the inspection, including an explanation of the inadequacies, via PayStation quarterly during the months of January, April, July, and October.

Minor deficiencies, which can be corrected during the course of a first line inspection, may be reported as adequate via PayStation. Repeated minor deficiencies shall be documented on an Employee Evaluation System (EES) form.

Continued next page.

Subject	Number
Line Inspection	**ADM-09**

First Line Supervisors' Duties (Continued)

Line Inspections shall include:

- Personnel: Uniform, equipment, appearance, cleanliness/neatness, jewelry, hygiene, cosmetics, and hair;
- Use of force equipment: All issued use of force equipment;
- Cruiser: General condition, issued equipment, cleanliness, and maintenance;
- Citations and audit sheets: Review citations and audit sheets, ensure documentation for racial profiling requirements are correctly submitted; and
- Licenses and Identification Cards e.g., Massachusetts Drivers License, License to Carry Firearms, and Department Identification Cards.

Reviewing Supervisor Duties

Each submitted inspection report shall be reviewed by a second level supervisor prior to approval via PayStation. The reviewing supervisor shall:

- Discuss any deficiencies noted within the report with the inspecting member prior to approving the report; and
- Take corrective action to ensure that all deficiencies and inadequacies are addressed.

Station/Unit Inspection

Station/Unit inspections shall be performed in conjunction with the Annual Fixed Assets Inventory. Station/Unit Commanders shall examine Department facilities and determine where there are inadequacies, deficiencies or areas not otherwise in compliance with Department rules, regulations, policies, procedures, orders, directives, and general laws.

Any written reports generated shall be forwarded to the Troop Commander through channels.

Annual inspections shall include at a minimum:

- Buildings and grounds of facility: Conduct a general inspection of the facility with attention to the condition of maintenance and safety issues;
- Entrances, exits, and security;
- Public accommodation: Parking, handicap access, toilet facilities/ public restrooms, and lobby area;
- Holding facilities: As required under PRI-04 Holding Facilities; and
- Employee cards/records: Are current and complete for all assigned employees.

References

ADM-30 Asset Management
PRI-04 Holding Facilities

Promulgated By:

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**ADM-09A**

Subject

Staff Inspections

Policy

The Department shall continuously audit and inspect all resources, facilities, equipment, personnel, practices and policies, in order to update the Command Staff on the quality of Department services.

Staff Inspections Protocols

To accomplish the mission of Staff Inspections, Inspectors shall have complete and unrestricted access to all Department records and properties.

Staff Inspections shall:

- Be performed on all resources, entities, and facilities within the Department;
- Be an open inspection conducted with the full knowledge and co-operation of everyone involved;
- Notify the appropriate Commanders of the intended date and scope of inspections, at least seven (7) days in advance of the inspection; and
- Include a list of those materials, files, and subjects to be reviewed or examined by the inspector.

Troop/Section Commanders shall work cooperatively with the Inspector, and shall prepare and provide all materials requested.

Upon request of the appropriate Division Commander, Staff Inspections may conduct unannounced inspections of any Department entity.

Routine Staff Inspections

Routine Staff Inspections may include:

- Narcotics, contraband and physical evidence;
- Seized monies/asset forfeiture;
- PayStation including overtime and details;
- Found/held property;
- Holding facilities;
- Racial Profiling compliance;
- Line inspections;
- Administrative journals and records;
- Issued Department equipment; and
- Other areas as directed by the Division Commander of Standards and Training.

Subject	Number
Staff Inspections	**ADM-09A**

Inspection Finding and Reports

Staff Inspectors shall prepare and submit a detailed report through channels to the Colonel/Superintendent within sixty (60) days of each inspection. This report shall include at a minimum:

- Findings and observations; and
- Opinions, recommendations and conclusions.

Copies of this report shall also be forwarded to the appropriate Division Commander.

Upon receipt of a Staff Inspection report, Troop/Section Commanders shall submit a report outlining the specific actions taken to ensure correction of all deficiencies noted. This report shall be submitted within thirty (30) days to the appropriate Division Commander, with a copy to be forwarded to the Division Commander of Standards and Training.

Promulgated By:

Department of State Police
General Order

Effective Date	Number
April 10, 2018	**ADM-10**

Subject

Awards

Policy

The Department shall make every effort to recognize the people whose actions assist the Department in carrying out its mission and who go beyond normal expectations or requirements.

EES Coordinator

The Employee Evaluation System (EES) Coordinator shall be a Commissioned Officer assigned within the Division of Standards and Training. The EES Coordinator shall be responsible for the Awards Board's administrative duties, preservation of all records, and shall not be a voting member of the Awards Board.

Standard Operating Procedure

The EES Coordinator shall develop a standard operating procedure that details:

- The Board's organization and procedures; and
- Board member duties and responsibilities.

Awards

State Police Members

Medal of Honor Gold Medal Blue/Yellow/Blue Ribbon	Established to honor Department members who have performed acts of extraordinary heroism above and beyond the call of duty. *Elements of consideration are:* • Actions that depict outstanding bravery, courage, and self sacrifice, or overriding concern for others; • Heroic actions taken for the rescue of life or in defense of another life; • Actions taken notwithstanding the potential of being killed; or • Valorous sacrifice (severe injury or loss of life).

Continued next page.

Awards (Continued)

Sworn Police Officers

Medal of Valor Silver Medal White/Red/Blue/Red/White Ribbon	Established to bestow recognition upon police personnel who have performed specific acts of bravery or have exhibited outstanding courage while performing their duties. *Elements of consideration are:* • An act characterized by courage, daring, and bravery; • The officer took immediate and decisive action to avert injury or loss of life to others; • While in a hazardous environment, the officer exhibited outstanding courage while performing their duties; • The officer rescued or defended another; or • Valorous sacrifice (severe injury or loss of life).
Medal of Merit Bronze Medal Blue/White Ribbon	Established to bestow recognition upon police personnel who have performed acts of outstanding achievement, far exceeding normal demands of the Department, which greatly contribute to the operation of the Department. *Elements of consideration are:* • Noteworthy achievements that greatly contributed to a Department operation or a community; • An exemplary act characterized by ingenuity, devotion, creativity, boldness, and outstanding professional conduct; or • Action(s) that reflects great credit to the member and the Department.
Medal of Lifesaving Bronze Medal Red/White Ribbon	Established to bestow recognition upon police personnel who undertake significant actions in the saving of another life. *Elements of consideration are:* • Actions were taken for the preservation of another life; and • The actions actually preserved life. Note: Documentation should be submitted supporting the life threatening nature of the injuries or circumstances.

Continued next page.

Sworn Police Officers and Members of the Public

Awards (Continued)

Superintendent's Commendation Plaque	Established to bestow recognition upon an employee of the Department, or a citizen, who has made an exceptional contribution to the Department. *Elements of consideration are:* • Extraordinary performance that clearly distinguishes the individual; • Performance that significantly contributes to Department operations; • Actions that significantly enhance the positive image of the Department; • Exceptional contribution(s) to the Department; or • Exceptional service to the community.
Division Commander's Commendation Certificate	Established to bestow recognition upon an employee of the Department, or a member of the public, who has made a significant contribution to a Division. *Elements of consideration are:* • Notable performance that clearly distinguishes the individual; • Performance that notably contributes to the Division's operations; • Actions that notably enhance the positive image of a Division; • Exceptional contribution(s) to a Division; or • Exceptional service to the community.
Troop/Section Commander's Commendation Certificate	Established to bestow recognition upon an employee of the Department, or a member of the public, who has made a significant contribution to their Station/Section/Unit. *Elements of consideration are:* • Notable performance that clearly distinguishes the individual, • Exceptional contribution(s) to the Station/Section/Unit; or • Exceptional service to the community.

Continued next page.

Awards (Continued)

Department Entities

Superintendent's Unit Citation Plaque	Established to bestow recognition upon the employees of a particular Station/Section/Unit who have made an exceptional contribution to the Department. *Elements of consideration are:* • Extraordinary performance that clearly distinguishes the Station/Section/Unit; • The successful conclusion or culmination of a significant investigation or achievement of a significant project; • The achievement of outstanding enforcement efforts by a Station/Section/Unit; • Superior support efforts to the Department; or • Actions that significantly increase the positive image of the Department.

Civilians

Distinguished Service Award Gold Medal Red/White/Blue Ribbon	Established as the highest award to bestow recognition upon an employee of the Department, or a member of the public, who has provided extraordinary assistance to the Department. *Elements of consideration are:* • Heroic actions were taken for the rescue of life, or in the defense of an officer or another; • The individual, while assisting the Department, imperiled himself/herself to the risk of great personal injury, or death; • The individual provided assistance to an officer in a critical situation and in need of help; or • The individual's extraordinary actions/achievements greatly contributed to a significant Department operation.
Lifesaving Award Red/White Lapel Pin	Established to bestow recognition upon an employee of the Department, or member of the public, who undertakes significant actions in the saving of another life. *Elements of consideration are:* • Actions were taken for the preservation of another life; and • The actions actually preserved life. Note: Documentation should be submitted supporting the life threatening nature of the injuries or circumstances.

Continued next page.

Awards (Continued)

Public Service Award Certificate	Established to recognize an employee of the Department, or a member of the public, who has provided outstanding assistance to the Department, or has significantly contributed to public safety. *Elements of consideration are:* • Significant actions contributing to Department objectives; • Significant actions contributing to the betterment of policing or public safety; • Noteworthy achievements that greatly contributed to a Department operation; or • Noteworthy achievements that greatly contributed to a community.

Nomination Procedures

Step	Action
1	Supervisors shall make nominations according to the following process: **Department Members** • Consult the list of the Awards Board criteria; • Complete and forward an EES Observation Report through channels to the Division Commander; and • Include any supporting documentation. **Department Civilian Employees or Non-Department Individuals** • Notify the appropriate Division Commander via a To/From letter.
2	Division Commanders shall: • Determine if the act is worthy of recognition; • Forward To/From award recommendations to the EES Coordinator; and • Present the award nominations to the Awards Board with the supporting documentation, if warranted.

Continued next page.

Nomination Procedures (Continued)

Step	Action
3	The Awards Board shall: • Meet monthly to review recommendations from the Division Commanders; • Make recommendations to the Colonel/Superintendent based upon a majority vote; and • Return recommendations, which do not rise to the level of an award, to the Division Commander.
4	The Colonel/Superintendent shall: • Review the monthly recommendations from the Awards Board; and • Notify the Awards Board of any changes to the recommendations.

Non-Department Nominations

Nominations for awards given by organizations outside the Department shall be forwarded to the Awards Board as outlined above.

Ceremony Procedures

Awards shall be presented at least biannually, at ceremonies scheduled during the months of April and October. The Colonel/Superintendent may hold additional ceremonies as deemed necessary.

Position	Duties
Awards Board	• Notify each Division Commander, in writing of all actions taken regarding the awards nominations for that Division; • Notify the Award recipients within thirty (30) days of the Board's decision; and • Notify Media Relations of the nominees at least forty-five (45) days before the next scheduled ceremony.
Media Relations	• Arrange for award ceremonies in April and October of each year; and • Ensure the award recipients have been notified, through the Office of the Superintendent, in writing at least thirty (30) days before the ceremony.
Human Resources	• Maintain a database containing all of the awards recipients' specifics; and • Place supporting award files in recipients' Personnel Files.
Colonel/ Superintendent	• Present the awards.

Continued next page.

Ceremony Procedures (Continued)

Division/Troop/Section Commander's Commendation ceremonies shall be held when necessary.

Position	Duties
Division Commander	• Present Division Commander Commendation Certificates to the recipient in hand; and • Forward a record of the award receipt to the EES Coordinator.
Troop/Section Commander	• Present Troop/Section Commendation Certificates to the recipient in hand; and • Forward a record of the award receipt to the EES Coordinator.

Awards Board Composition

The Awards Board shall be comprised of eight (8) employees with seven (7) voting members. Awards shall be approved based on a majority vote. Employees shall serve for a minimum term of one (1) year.

Representative	Rank/Position	Designated by
President	Major	Superintendent
Department Employee	Civilian	Deputy Superintendent
Field Services	Captain or lower	Division Commander
Investigative Services	Captain or lower	Division Commander
Standards and Training	Captain or lower	Division Commander
Administrative Services	Captain or lower	Division Commander
Homeland Security and Preparedness	Captain or lower	Division Commander
EES Coordinator	Commissioned Officer Non-Voting Member	Division Commander of Standards and Training

Subject	Number
Awards	**ADM-10**

Other Awards

Supervisors may establish:

- Other forms of recognition as necessary and forward documentation to the EES Coordinator for filing purposes.

These recognitions shall not be deemed to be a Department Award within the guidelines of this policy.

Exceptions

In extraordinary circumstances the Awards Board may:

- Vote to make an exception to this policy, providing the vote is unanimous; and
- Forward the exception to the Colonel/Superintendent for approval.

References

Department Employee Evaluation System (EES)

Promulgated By:

Department of State Police
General Order

Effective Date	Number
April 16, 2009	**ADM-11**

Subject

Sick Leave

Policy

The Department recognizes the importance of Sick Leave for its sworn members and their families.

The Department has a responsibility to monitor the use of Sick Leave to prevent abuses.

Sick Leave Credits

Sick Leave credits are granted in accordance with provisions of the applicable Collective Bargaining Agreement (CBA) and the Department's Rules and Regulations. The Collective Bargaining Agreement also provides guidelines for the administration of Sick Leave.

Granting Sick Leave

Sick Leave is granted at the discretion of the Colonel/Superintendent or their designee, to a sworn member when the member cannot perform their duties because they are incapacitated by:

- Personal illness or injury;
- The presence of the member at their work location would jeopardize the health of others, through exposure to a contagious condition; or
- The member's spouse, child, parent, or spouse's parent, or relative living in the member's household, is seriously ill. In this event, a limit to the amount of leave the member can use is set by the CBA and federal and state laws.

Calling On Sick Leave

A member shall notify their duty assignment of their intention to use Sick Leave as early as possible on the first day of absence. This shall be appropriately logged in the Daily Administrative Journal and shall only reflect the member's name, identification number, and type of Sick Leave.

Supervisors shall be informed of:

- The nature of the illness or injury, and anticipated duration of absence, if known;
- The location of their recuperation and a telephone number; and
- Any duties or scheduled court appearances that may require attention.

Subject	Number
Sick Leave	**ADM-11**

Sick Leave

Members who are granted Sick Leave shall not request or work overtime and/or details within twenty-four (24) hours from the start time of their regularly scheduled work shift, unless the members has:

- Worked at least four (4) or more consecutive hours during the first half of their shift for which Sick Leave was granted; or
- Worked at least four (4) or more consecutive hours during the second half of their shift for which Sick Leave was granted.

Members may utilize Sick Leave to attend doctor and dental appointments.

Note: Supervisors shall ensure compliance with ADM-19 Vehicle Management with regards to Department issued vehicles.

Calling Off Sick Leave

Members shall call in at least eight (8) hours before reporting back for their next shift.

If using Sick Leave in excess of five (5) consecutive work days, the member may be required to undergo a medical examination, or provide documentation from a licensed medical practitioner, to determine their fitness for duty.

Location of Recuperation

Members suspected of abusing Sick Leave may be ordered to remain at a reported place of recuperation. A reasonable time period away from this location is allowed to:

- Obtain services or products consistent with medical care;
- Vote or attend religious services;
- Attend to an emergency situation; or
- Attend to other matters with the permission of their supervisor.

Members using Sick Leave may only leave the Commonwealth of Massachusetts:

- With authorization of their Commanding Officer; and
- To obtain medical care as prescribed by their licensed medical practitioner.

Review of Sick Leave

- Supervisors at all levels are responsible for monitoring Sick Leave. Supervisors should review attendance records for signs of Sick Leave abuse, preferably in conjunction with the Employee Evaluation System (EES).

Continued on next page.

Subject	Number
Sick Leave	**ADM-11**

Review of Sick Leave (Continued)

Some potential signs of Sick Leave abuse are:

- Excessive use;
- Patterns of use, such as before or after days off, or on weekends;
- Use on or around a holiday;
- Use after working overtime, details, or extra shifts;
- Use when the member has indicated that they want time off;
- Use when the supervisor believes that the member is not sick; and
- When the Sick Leave repeatedly creates shortages, or overtime.

Review of Sick Leave (Continued)

When a supervisor has *reason to suspect* Sick Leave abuse, the supervisor has the following options:

- Reason to Suspect Abuse in General- Notify the member using SP 382 Abuse of Sick Leave form. This advises the member that future Sick Leave may be subject to extra scrutiny; or
- Reason to Suspect Abuse In a Particular Instance- Notify the member using SP 383 Submission of Medical Evidence form. The member is then required to produce satisfactory medical evidence by submitting SP 384 Request for Certification of Medical Condition form within seven (7) days.

Supervisors should have articulable reasons for suspecting abuse before filing SP 382 Abuse of Sick Leave form. Supervisors may call or visit the member at their place of recuperation to verify the use of Sick Leave. Calls or visits shall not occur between 2200 hours and 0800 hours.

Members who abuse Sick Leave or who are excessively absent from duty may be subject to administrative or disciplinary action and denial of Sick Leave.

Leave Benefits

Leave issues for members are addressed in the Collective Bargaining Agreement.

Commanding Officers shall consult applicable collective bargaining agreements for civilians under their charge.

References

ADM-19 Vehicle Management
ADM-25 Paid Details
SP 382 Abuse of Sick Leave
SP 383 Submission of Medical Evidence
SP 384 Request for Certification of Medical Condition
State Police Association of Massachusetts Collective Bargaining Agreement

Promulgated By:

Department of State Police
General Order

Effective Date	Number
March 31, 2017	**ADM-11A**

Subject

Temporary Modified Duty

Policy

Temporary Modified Duty is designed to provide an alternative work assignment for members who are temporarily unable to meet some of the Department in-service standards. Members failing to meet in-service medical and physical fitness standards due to temporary injury, illness or incapacitation are eligible to undergo reexamination pursuant to M.G.L. c. 22C, §10. Requests for reexaminations shall be made in writing to the Colonel/Superintendent within the period prescribed by M.G.L. c. 22C, §10 or shall be waived.

Temporary Modified Duty

While on Temporary Modified Duty, members shall not:

- Wear a uniform;
- Work overtime;
- Work paid details; and
- Have contact with prisoners, the public in an enforcement capacity, or function as a desk officer in a sub-station.
  Exception: Emergency situations may require the immediate response of the member.

The Colonel/Superintendent may authorize members on Temporary Modified Duty to:

- Operate a Department vehicle; and/or
- Carry a Department issued firearm.

The immediate supervisor of a member on Temporary Modified Duty shall ensure compliance with ADM-19 Vehicle Management.

Eligibility

Eligibility for Temporary Modified Duty status shall:

1. Be recommended by the State Police Surgeon;
2. Require that the member's anticipated period of injury, illness or incapacitation be temporary in nature, meaning less than twelve (12) months in duration; and
3. Be determined by the Colonel/Superintendent.

Members who are not eligible for Temporary Modified Duty may:

- Remain or be placed on Sick Leave, Injured Leave, or other approved duty or leave status as appropriate.

Subject	Number
Temporary Modified Duty	**ADM-11A**

Evaluation By State Police Surgeon

Members who are eligible or assigned to Temporary Modified Duty shall be required to:

- Submit to periodic medical evaluation(s) of their condition as determined by the State Police Surgeon or by order of the Colonel/Superintendent.

Any member who has been assigned to Temporary Modified Duty for a period of twelve (12) months, shall be examined by the State Police Surgeon, who, after reviewing all medical information, shall recommend to the Colonel/Superintendent that the member:

- Remain on Temporary Modified Duty for a period as recommended by the State Police Surgeon and as determined by the Colonel/Superintendent;
- Submit to a medical examination as directed by the Department;
- Be placed on: Full Duty; No Duty; or Temporary Modified Duty; and/or
- Be discharged, separated and/or retired.

Member's Assignment to Temporary Modified Duty

The Colonel/Superintendent may assign a member to Temporary Modified Duty based upon a medical recommendation from the State Police Surgeon. A member may dispute such assignment by:

- Providing a written notification to the Colonel/Superintendent within ten (10) days; and
- Producing a written statement from the member's physician detailing the medical reasons the member cannot perform such assignment.

The Colonel/Superintendent upon receipt of such written notification may:

- Require the member to submit to an examination by a medical physician selected by the Department.

The medical physician selected by the Department shall:

- Examine the member to determine if the member can perform the duties of the proposed assignment; and
- Forward written documentation of the examination with recommendations to the Colonel/Superintendent.

The Colonel/Superintendent shall make all final determinations regarding a member's assignment to Temporary Modified Duty.

Subject	Number
Temporary Modified Duty	**ADM-11A**

Responsibilities

Position	Duties
Colonel/Superintendent	Shall establish and approve Departmental: • Duty Status; • Leave Status; • Medical Standards; and • In-service Standards.
State Police Surgeon	Shall evaluate members and recommend: • Eligibility for Temporary Modified Duty status; and • The frequency of medical evaluation periods.

References

ADM-19 Vehicle Management
MGL c.22C, s.10

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 25, 2008	**ADM-11B**

Subject

Injury Reporting and Leave

Policy

The Department shall investigate and document each on-duty injury to a member. All duty related injury documentation shall be completed and forwarded to the proper authority in a timely manner.

Every injury shall be investigated in accordance with this policy.

Leave Status

Members incapacitated by an injury incurred on-duty shall:

- Be placed on *Injured Leave Pending* (ILP) status by their Commanding Officer or designee until examined by the State Police Surgeon; and
- Officially be placed on *Injured Leave Duty* (ILD) status when so determined and approved by the Board on Claims.

Payroll Information

A member who:

1. Remains on approved ILD into the next calendar year, or
2. Returns from approved ILD in the last quarter of the current calendar year may request:
    - The Colonel/Superintendent to convert excess vacation time credits to Sick Leave.

Members on approved ILD may request a tax exempt status letter through the Payroll Section.

Reporting

If injured while on-duty:

- Division of Field Services members shall immediately advise the Desk Officer who shall notify the Troop Duty Officer; or
- Non-Field Services members shall notify their Commanding Officer.

The nature and cause(s) of a member's injury shall be noted in the Daily Administrative Journal.

Supervisors shall ensure the procedures outlined in TRF-20 Department Vehicle Crashes are followed, if an injury is the result of a cruiser crash.

Subject	Number
Injury Reporting and Leave	**ADM-11B**

Investigation/ Documentation Protocols

The **Troop Duty Officer** (for DFS members) or the **Commanding Officer** (for non-DFS member) shall :

- Assign an investigating officer;
- Ensure that form SP 624 Initial Injury Report is completed; and
- Ensure that prior to the end of the shift, the SP 624 is sent via FAX to General Headquarters Division Commander and the Occupational Health Unit/Human Resources Section.

Injured members should, if necessary, seek emergency medical care or seek treatment from their own personal physician. All bills shall be:

- Made out in the injured member's name and home address;
- Itemized and initialed by the member; and
- Submitted to the investigating officer within seven (7) days.

Injured members (unless physically incapable) shall, within seven (7) days, complete and sign the following forms and submit to the investigating officer:

- Sections 1 through 7 of SP 37 Statement in Support of Claim;
- Commonwealth's Form 1 Notice of Injury;
- To/From Letter (including how the injury occurred and names of any witnesses and statements); and
- SP 625 Authorization for Release of Medical Records.

Investigating officers shall:
When the injured members are physically incapable:

- Prepare the appropriate forms (e.g. SP 37); and
- Forward same on the injured member's behalf.

Within seven (7) days of receipt of claim, submit to the Troop/Section/Unit Commander:

- Statement in Support of Claim, after completing Section 8;
- Notice of Injury;
- Injured member's To-From along with all supporting documentation;
- Any witness statements; and
- Medical records and medical bills, as available.

Troop/Section/Unit Commander shall:

- Complete Section 9 of the Statement in Support of Claim;
- Prepare a To/From letter to the President of the Board on Claims, which shall include a brief account of the facts concerning the injury and conclusions regarding the cause of the injury and forward:
  1. Investigating Officer's Report and documentation; and
  2. The Statement in Support of Claims.
- Forward a copy of the Board on Claims decision letter to the injured member.

Continued on next page.

Subject	Number
Injury Reporting and Leave	**ADM-11B**

Investigation/ Documentation Protocols (Continued)

Troop/Section/Unit Commanding Officer shall, if the injured member is unable to return to duty:

- Place the member on ILP (members who have a recurrence of a previous injury should be placed on Sick Leave); and
- Notify the Occupational Health Unit of the status and request an appointment with the State Police Surgeon.

The **State Police Surgeon** shall:

- Conduct an initial evaluation of the injured member to determine the member's duty status;
- Schedule periodical examinations as deemed necessary to determine the member's duty status;
- Determine and recommend a member's eligibility for Modified Duty; and
- Report to the Department when a member is medically able to return to full duty status.

Recurrent Injuries

All recurrent injuries shall be reported using the same process as new injuries.

Members with any recurrent injuries shall be placed on Sick Leave until officially approved and placed on ILD status.

While on Injured Leave

Members on Injured Leave may only leave the Commonwealth:

- With authorization of their Commanding Officer.

Supervisors shall ensure compliance with:

- ADM-19 Vehicle Management with regards to Department issued vehicles; and
- ADM-20 Weapons Management with regards to Department issued weapons.

References

Commonwealth's Form 1 Notice of Injury
TRF-20 Department Vehicle Crashes
ADM-19 Vehicle Management
ADM-20 Weapons Management
Rules and Regulations Article 8

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 25, 2008	**ADM-11C**

Subject

Maternity Leave and Guidelines

Policy

The maternity policy is designed to provide notification and employment guidelines in order to prevent workplace discrimination on the basis of pregnancy.

Members shall:
- Not be required to disclose her pregnancy except in accordance with this policy.

The Department shall only take action when;
- Requested by the member; or
- The member's physician or obstetrician recommends work limitations.

Notification Requirements

A member shall notify her commanding officer that she is pregnant, when she has:
- Reached her third trimester of pregnancy;
- Requests modification, exemption, or leave from her assigned duties; or
- Been given physical restrictions or limitations by her physician or obstetrician that prohibits her from performing all aspects of her current assignment.

All notifications shall be made:
- In writing, and include the anticipated due date as well as the anticipated date of return to work (if known).

Subject	Number
Maternity Leave and Guidelines	**ADM-11C**

Notification Process

The member shall submit to her commanding officer:

- Within seven (7) days of the initial notification, a letter from her physician or obstetrician regarding her pregnancy; and
- Every thirty (30) days thereafter, a written update from her attending physician or obstetrician.

Each letter shall contain:

- Name, address and contact information for the attending physician or obstetrician;
- Any restriction or limitation on her current work assignment, if none, the letter shall explicitly state so;
- Anticipated due date;
- Anticipated date for return to work (if known); and
- Any other information the member or physician or obstetrician believes would be of assistance to the Department.

Duty Status

A member not placed on alternative duty shall:

- Perform all duties required of her in her current position until such time as other duties are assigned consistent with this policy.

If the member has not notified the Department of her pregnancy and sought alternative duty status under this policy, then her pregnancy:

- Cannot be a defense to any disciplinary action taken against her for failure to perform her duties.

A member may request in writing, at any time during her pregnancy, to be assigned to alternative duty. Alternative duty shall:

- Not affect the member's existing benefits;
- Be consistent with restrictions or limitations identified by her attending physician or obstetrician regarding:
  1. Overtime and paid details;
  2. Interaction with prisoners;
  3. Interactions with the public in an enforcement capacity; and
  4. Dangerous duty such as riots.

  Exception: Any emergency situation that may require the immediate response of the member.

Subject	Number
Maternity Leave and Guidelines	**ADM-11C**

Voluntary Alternative Duty

The Colonel/Superintendent or designee shall:

- Approve and determine a member's request for alternative duty assignment taking into consideration the pregnant member's current assignment and duties.

Eligibility for an alternative duty assignment:

- Does not entitle the member to be transferred to a different position or unit within the Department.

Alternative duty may be:

- A form of modified duties and/or an altered work shift at the request of the member; and
- Consistent with any restrictions or limitations set forth by her attending physician or obstetrician.

Eligible Members:

- Shall not be transferred or have their shift changed involuntarily as the result of seeking alternative duty; however
- A reasonable accommodation may require the member to accept temporary assignment in the geographic area of her current assignment or residence.

Involuntary Alternative Duty

The Department may involuntarily reassign a member to alternative duty based upon medical evidence that the member cannot safely perform her current duties.

A member may challenge such reassignment by:

- Providing a statement from her physician or obstetrician that she can perform such duties;
- Submit to an examination by a neutral obstetrician selected by the member from a list agreed upon by the Department and the representatives of the member's collective bargaining unit;
- Remain in her current duty assignment pending receipt of the opinion of the neutral obstetrician; and
- Be bound by the opinion of the neutral obstetrician.

The neutral obstetrician shall:

- Examine the member and determine whether she can perform the duties of her assigned position; and
- Render an opinion which shall be binding upon the Department and the member.

Subject	Number
Maternity Leave and Guidelines	**ADM-11C**

Duty Assignment

When an alternative duty assignment is unavailable within a member's current assignment, the Colonel/Superintendent or designee shall:

- Find appropriate alternative assignment within the member's immediate geographic area as defined by the Troop Area of her current assignment or her residence; and
- Ensure no member be denied such an assignment within her current assignment, or immediate geographic area.

If a member believes that she has been unreasonably denied such an assignment in violation of this policy, the member shall:

- Submit a To-From outlining the objections to the Colonel/Superintendent or designee.

The Colonel/Superintendent or designee shall:

- Endeavor to remedy the member's concerns within seventy-two (72) hours of receipt of the notice; or
- Respond, in writing, stating the position of the Department with respect to the request.

Department Standards

A member who has notified the Department of her pregnancy in accordance with this policy shall:

- Be exempt from weapons qualification requirements during the course of her pregnancy; and
- Be required, upon return to full duty status, to meet the Department's medical and in-service standards.

Department Issued Vehicles

A member who is placed on alternative duty shall be:

- Issued an unmarked vehicle while on an alternative duty status.

If the Department is unable to provide the member with an unmarked vehicle, the member shall be:

- Provided with a per diem rate in accordance with the same terms and conditions as apply to members of equal rank assigned to the Massachusetts Port Authority.

Members who are currently assigned an unmarked vehicle shall be allowed to continue to operate the vehicle.

Supervisors shall ensure compliance with:

- ADM-19 Vehicle Management with regards to Department issued vehicles.

Subject	Number
Maternity Leave and Guidelines	**ADM-11C**

Members Rights

The member retains all such rights available to her under the collective bargaining agreement, state and federal law to challenge the decision of the Colonel/Superintendent or designee with respect to such a determination by the Colonel/Superintendent or designee as to the implementation of this policy.

References

ADM-19 Vehicle Management

Promulgated By:

Department of State Police
General Order

Effective Date	Number
November 5, 2008	**ADM-11E**

Subject

Leaves of Absence

Policy

The Department may grant sworn and civilian employees leaves of absence, with or without pay, as allowed by:

- Federal and state law;
- Commonwealth's Human Resources Division (HRD);
- Collective Bargaining Agreements (CBA), Personnel Administration Rules (PAR), HRD Red Book; or
- The Colonel/Superintendent.

Leave Coordinator

The Division of Administrative Services (DAS) Commander shall appoint a Leave Coordinator who shall be responsible for:

- Receiving and processing specified requests for leave;
- Assisting employees with paperwork requirements;
- Assisting and coordinating with commanding officers and the Colonel/Superintendent to evaluate requests for leave;
- Coordinating the requirements for employees returning from leave;
- Ensuring personnel records, payroll history, health insurance and other benefits are updated or administered as necessary; and
- Consulting with Office of Employee Relations and Legal Section regarding leave requests.

Approval of Leave

The Leave Coordinator shall forward all requests for leave to the Colonel/Superintendent. The Colonel/Superintendent may approve or deny leave based upon:

- Applicable federal and state laws, and collective bargaining agreements;
- Operational needs of the Department;
- The purpose of the leave; and
- Other factors that may exist.

The Leave Coordinator shall notify an employee, in writing, of the decision of the Colonel/Superintendent.

Conduct on Leave

An employee on a leave of absence for any duration shall:

- Adhere to and abide by all State Police Rules & Regulations, Policies & Procedures, applicable written directives, and collective bargaining agreements; and
- Not work any overtime, details or appear in court on behalf of the Department.

An employee who is on any form of leave in excess of thirty (30) days shall return the following issued equipment to their Troop/Section/Unit Commander:

- All issued Department firearms and ammunition;
- Assigned vehicle along with vehicle issued equipment;
- Department issued fuel card, transponder and snow gate access cards; and
- All issued electronic devices (e.g. cell phone, laptop).

Troop/Section/Unit Commanders shall contact the issuing section regarding storage.

Bereavement Leave

Employees are entitled to leave, without loss of pay or benefits, in recognition of the death of family members, or persons living in the household of the employee, in accordance with their respective collective bargaining agreements.

Blood Donation Leave

Employees

Are permitted a maximum of four (4) hours leave of absence with pay, subject to operational needs and the approval of their supervisor, specifically to enable the employee to donate blood. The decision of their supervisor cannot be appealed.

- Leave time is for:
  1. Travel from work to the donation site;
  2. Actual donation time;
  3. Recovery from donation; and
  4. Travel time back to work.

Leave Time

- Shall be taken on the day the donation occurs;
- Employees shall not accrue compensatory time in lieu of such leave;
- Blood Donation Leave is permitted for a maximum of five (5) times per federal fiscal year, the period of October 1 though September 30 each year.

Employees Blood Bank Form

In order to qualify for the Blood Donation Leave, an SP 635 Employees Blood Bank form shall:

- Be completed certifying the date, location, times and type of blood donation.

Education Leave

Purpose
Employees may be granted a paid leave of absence for educational purposes to attend conferences, seminars, briefing sessions, or other functions of a similar nature that are intended to improve or upgrade the individual's skills or professional ability.

Request Procedure
Shall be made in writing to the Leave Coordinator and at least thirty (30) days in advance of the desired leave, or if unforeseen, as soon as possible.

- Requests shall include:
  1. The anticipated start and end dates of training;
  2. A thorough description of the training accompanied by documentation from the institute hosting the training; and
  3. Rationale for the relationship of the training to the employee's work unit, and/or the Department as a whole.

Approval
Approval is entirely at the discretion of the Colonel/Superintendent, and is not subject to appeal.

- Considerations may include, but not be limited to:
  1. Costs and benefit of the training to the Department as a whole;
  2. Benefit of the training to the individual employee and their work unit; and
  3. The reasonable relationship of the training to the individual employee's work assignment.

Extended Illness Leave Bank (EILB)

Description
A voluntary program to assist employees who have expended their accrued paid leave due to an extended personal illness or injury, thereby enabling the employee to remain on paid leave within the limits of the program.

Program
1. To be eligible for membership, employees shall annually donate an amount of sick, vacation or personal leave credits to the EILB; and
2. Apply to withdraw from the EILB, up to one-hundred and twenty (120) days within a two (2) year period, when extended illness or injury have exhausted all their paid leave time.

Note: Employees seeking further information should contact the Leave Coordinator.

Family and Medical Leave (FMLA)

The Colonel/Superintendent shall grant employees who have completed their probationary period the following:

Family Leave-A leave of absence:

- For the birth, adoption, or placement of a child.

Medical Leave-A leave of absence:

- If an existing serious health condition prevents the employee from being able to perform the functions of their position; or
- To care for family members who have a serious health condition.

Intermittent Leave/Modified Work Schedules

- May be available to employees based on the operational needs of the work station/section/unit/.

Note: Employees shall consult their applicable collective bargaining agreements for specific benefits, durations, definitions, and other information for cited leave.

Request Procedure

Requests shall be made in writing to the Leave Coordinator at least thirty (30) days in advance of the desired leave, or if unforeseen, as soon as possible.

- The request shall contain the following:
    1. Anticipated start and end dates of leave, proposed intermittent usage of the leave or proposed modified work schedule;
    2. Specific reason for taking the leave (family or medical); and
    3. Appropriate documentation.
        i. For the birth, adoption, or placement of the child, a birth certificate or adoption/placement papers may be required.
        ii. For leave due to a serious health condition of the employee or other, a medical certification form provided by the Department in support of the request is required.

Note: Requests for Family and Medical Leave may be denied if the above requirements are not met.

Non-FMLA Family Leave

The Colonel/Superintendent may grant employees who have completed their probationary period, Non-FMLA Family Leave in accordance with the appropriate collective bargaining agreement.

Request Procedure
Requests shall be made in writing to the Leave Coordinator at least fourteen (14) days in advance of the desired leave, or if unforeseen, as soon as possible.

- The request shall contain the following:
  1. The anticipated start and end dates of leave, or the intended days for incremental use; and
  2. The specific reason for the requested leave and any documentation the employee may have in support of the leave request.

Note: Employees shall consult their applicable collective bargaining agreements for specific benefits, durations, definitions, and other information for cited leave.

Leave of Absence Without Pay

Authorization
The Colonel/Superintendent may grant employees authorized leave of absence for up to ninety (90) days and/or grant an extension of leave of absence upon written request filed by the employee.

Request Procedure
Requests for Leave of Absence Without Pay shall be made in writing to the Leave Coordinator at least thirty (30) days in advance of the desired leave, or if unforeseen, as soon as possible.

- The written request shall contain the following:
  1. Anticipated start and end dates of said leave;
  2. A detailed statement of the reason for the leave;
  3. In the event that the absence is illness/injury related, written requests shall be accompanied by substantiating proof of such illness.

Sworn Members – Return to Service Requirements

The Leave Coordinator shall inform sworn members of any requirements necessary for return to service from leave.

Returning to Service – FMLA-Medical Leave or Authorized Leave of Absence Without Pay

- Members returning to service due to their own illness/injury that exceeds ten (10) days shall:
  1. Notify their Commanding Officer to contact the Occupational Health Unit to schedule an appointment with the State Police Surgeon prior to returning to work; and
  2. Have a recommendation from the State Police Surgeon for return to service.

Continued next page.

Sworn Members – Return to Service Requirements (Continued)

Leaves or Break-In-Service

- Members returning from a leave or break in service that exceeds ninety (90) days shall be required to successfully complete:
  1. On-Line Academy; and
  2. An evaluation by the Division of Standards and Training Commander or designee regarding any additional training required.

- Members returning from a leave or break in service that exceeds one (1) year shall be required to successfully complete:
  1. A background investigation;
  2. A medical examination by the State Police Surgeon to include drug testing;
  3. Psychological testing; and
  4. An evaluation by the Division of Standards and Training Commander or designee regarding any additional training required.

- Former members wishing to return from a separation from service that exceeds three (3) years shall:
  1. Meet all requirements for reentry to the Department; and
  2. Successfully complete the Recruit Training for appointment to the position of Trooper.

Note: Failure to successfully complete the Recruit Training may affect pension benefits, if applicable.

Returning From Leave: Civilians

Return From Leave

- Employees returning from a leave that exceeds one (1) year shall be required to successfully complete:
  1. A background investigation;
  2. A drug test;
  3. A medical examination by the State Police Surgeon, as applicable, if returning from medical leave where the employee was the one that was ill; and
  4. Retraining, as determined by the employee's supervisor or the Human Resources Director.

Sworn Members Returning From Disability

In addition to the previously listed requirements, sworn members returning from disability retirement shall have a medical evaluation conducted in conformance with MGL c.32, and the standards of the Commonwealth of Massachusetts Public Employee Retirement Administration Commission.

Subject	Number
Leaves of Absence	**ADM-11E**

Benefits

Employees may be required to pay premiums for certain benefits while on Leave.

Military Leave

Refer to Policy and Procedure ADM-11D Military Leave.

References

MGL c.31, s.37
MGL c.32
NAGE Units 1, 3 and 6-Commonwealth CBA, Article 8
AFSCME Unit 2-Commonwealth CBA, Article 8
SPAM Unit 5A-Commonwealth CBA, Articles 8 and 38
MOSES Unit 9-Commonwealth CBA, Article 8
Personnel Administrator Rules, PAR 13 Leaves of Absence
Red Book §§5.00, 6.00, and 8.00
Mass State Employees Blood Program

Promulgated By:

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**ADM-12**

Subject

Serious Injury/Death of a Member

Policy

The Department recognizes that the death or serious injury of a member is traumatic and shall provide assistance to the member's family, recognizing that the needs of the family generally take precedence over the wishes of the Department.

Department members shall:
- Ensure that whenever a member's next of kin calls, their questions are answered honestly and openly.

OFF-DUTY Death Notification Procedure

When any member becomes aware of the death of a current or retired member of the Department of State Police, or an immediate member of their family, they shall immediately:
- Notify the Office of the Superintendent through channels.

Information for notification shall include:
- Personal information on the deceased person;
- The circumstances of the death;
- Any funeral arrangements; and
- A family contact person.

The Office of the Superintendent shall notify:
- Members of the Department; and
- Special effort shall be made to contact the member's graduating class.

ON-DUTY Death Notification Procedure

If the death or life threatening injury occurs on-duty, the member's Commanding Officer or designee shall immediately notify:
- The Office of the Superintendent.

The Colonel/Superintendent shall immediately:
- Assign a ranking member to personally contact the member's immediate family; however
- Every effort shall be made to use a member of the Department who is a personal friend, along with the ranking member.

Subject	Number
Serious Injury/Death of a Member	**ADM-12**

Liaison Member

If the family chooses, the Colonel/Superintendent shall:

- Appoint a Department member as a liaison, to provide additional assistance to the immediate family of the deceased/injured member or retiree.

As a guide, the liaison member should:

- Assist the family in contacting clergy, friends, and relatives;
- Assist the family with funeral arrangements;
- Provide transportation assistance for the immediate family;
- Arrange for security needs of the home and screening of phone calls prior to and on the day of the funeral;
- Coordinate the family's efforts to determine the status and amounts of compensation to which the deceased member may be entitled; and
- Keep the Colonel/Superintendent informed of all arrangements and developments.

Honor Guard

The Colonel/Superintendent shall:

- Designate a member to be the Officer-in-Charge (OIC) of the funeral detail.

The OIC shall:

- Coordinate with the liaison member; and
- Adhere to GEN-04A Ceremonial Tributes regarding funeral details.

References

GEN-04A Ceremonial Tributes
SUP-04 Employee Assistance Unit

Promulgated By:

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**ADM-13**

Subject

Notification of Medical Examiner and/or Next of Kin

Policy

The Department shall promptly and compassionately notify the nearest relative of victims who have sustained life threatening injuries, or passed away.

Notification of Medical Examiner

The Medical Examiner of jurisdiction shall be notified whenever a member of the Department becomes aware of a death (Specific circumstances appear in MGL c.38, s.4, 6.).

Responsibilities

Note: The District Attorney's Office or State Police Detective Unit of jurisdiction shall direct the investigation of all homicides, suicides, and unattended deaths (including traffic fatalities, as requested by the Office of the District Attorney of jurisdiction).

Position	Duties
First member at the scene	• Notify the Station Desk Officer. • For all homicides, suicides, and unattended deaths, secure the scene, pending arrival of the State Police Detective Unit (SPDU) of jurisdiction.
Station Desk Officer	• Immediately notify the Troop Duty Officer.
Troop Duty Officer	Immediately notify the appropriate: • SPDU of jurisdiction of all homicides, suicides, and unattended deaths, and take any action requested; and • Local Medical Examiner's (ME) Office, as requested by SPDU. If the ME declines to respond to the scene, request authority from the ME to remove the body. If the ME is unavailable, contact the Office of the Chief Medical Examiner at (617) 267-6767 and request authority to remove the body.

Continued next page.

Subject	Number
Notification of ME and/or Next of Kin	**ADM-13**

Responsibilities (Continued)

Position	Duties
Troop Commanders	Ensure that their Troop Duty Office has an updated list of Medical Examiners' phone numbers and addresses.

Next of Kin

Every effort should be made to locate the next of kin in the order of:

- Live-in spouse;
- Parents or legal guardian;
- Adult children;
- Brother or sister; or
- Other relatives.

Request for Notification

Members may be called upon to notify the next of kin that a family member or friend has been seriously injured or is deceased. Except under unusual circumstances, **this notification should be made in person.** No identifying information of the victim or their family shall be transmitted via radio.

Position	Responsibility
Members receiving request to notify the next of kin	1. Request as much information as possible, to include: • Cause of death and/or injuries; • Location of deceased or injured person; and • Contact person and telephone number. 2. If the member is unfamiliar with the caller, seek to confirm the information. 3. Notify Troop Duty Officer.
Troop Duty Officer	1. Notify the appropriate Detective Unit of all homicides, suicides, and unattended deaths (including traffic fatalities if so requested by the DA's Office of jurisdiction). 2. Determine who shall make the notification to the next of kin. 3. If the notification is not to be made in person, determine what means shall be used.

Subject	Number
Notification of ME and/or Next of Kin	**ADM-13**

District Attorney Offices

Whenever there is a homicide, suicide, or unattended death, the Division of Investigative Services shall determine the notification process. Members assigned to an Office of a District Attorney shall follow the protocols promulgated for their particular office.

All other notifications shall be made by the Division of Field Services.

Field Services Procedure

Whenever possible, two (2) members shall be sent to make a notification of serious injury, illness, or death.

The member who is making the notification should carefully prepare their message before speaking with the next of kin. When possible, members shall:

- Seek assistance from clergy, relative, or close friend of the family;
- Make the notification in a private setting, and ask the recipient to sit down;
- Deliver the information to the recipient in a gradual manner;
- Observe the recipient carefully as the information is given;
- If possible, do not leave the recipient alone. Members should attempt to contact a relative, friend, or neighbor to stay with the recipient; and
- When the recipient is operating a motor vehicle, the member shall ascertain if they are able to continue driving. If not, members may transport or make transportation arrangements for the recipient.

References

MGL c.38, s.4, 6

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 14, 2018	**ADM-14**

Subject

Personnel Investigations

Policy

To protect the integrity of the Department and to ensure continued public support:

- All Department employees shall adhere to the Department's Policy and Procedure regarding external complaints (including anonymous ones) against any employee, policy, procedure, or operation of the Department;
- All complaints shall be documented and investigated according to complaint intake procedures; and
- Complaints, when assigned, shall be investigated at the lowest appropriate organizational level, unless determined otherwise by the Division of Standards and Training Commander or designee.

Definition

Personnel Investigation: An investigation or an inquiry into the actions of an employee that may result in charges of misconduct.

Rights of the Accused Employee

An accused employee shall:

- Receive a copy of the complaint, including the name of the complainant, if known, prior to any employee interrogation;
- Be afforded full Constitutional and other legal protections; and
- Be afforded the protections applicable under the Collective Bargaining Agreements.

Rights of the Complainant

The Complainant shall:

- Be notified of the receipt of the complaint, and the steps to be taken;
- Be given a status report when requested; and
- Be notified of the final disposition classification.

Use of Examinations

If during an investigation it becomes necessary to request an employee to submit to an examination or required test(s), the Troop/Section/Unit Commander shall contact the Division of Standards and Training for approval.

The results of medical tests shall be afforded appropriate privacy rights according to applicable laws.

Complaint Intake Procedures

A complaint that requires <u>immediate attention</u> shall:

- Be immediately referred to the Troop/Section/Unit Commander, Duty Officer or Shift Supervisor.

External Complaints

External complaints are to be completed by the Complainant on a SP 340 Citizens Response Form. The Complainant may obtain a SP 340 in the following manner:

- Contacting a State Police facility for instructions;
- Arriving in person to a State Police facility and securing a copy of a SP 340;
- Downloading the SP 340 form from the State Police external website www.mass.gov/msp ; or
- Calling the Citizen Response Intake Line (508) 988-7003 and following the prompts.

When a Complainant calls or arrives at a State Police facility the following shall occur:

- The Desk Officer or employee who attends to a Complainant, either by telephone or in person, shall:
    1. If applicable to their work assignment, log only the name and address of the Complainant into the Daily Administrative Journal (DAJ), the Complainant should <u>not be asked</u> to identify the employee(s) named in the complaint, nor should any employee information pertaining to this complaint be included within the DAJ entry. <u>Note:</u> DAJ information would also include anonymous complaints or when the Complainant refuses to give their name;
    2. Give the Complainant a copy of the SP 340 form; or
    3. Instruct the Complainant on how to obtain a SP 340 form from the above options;
    4. Ensure the Complainant understands all options and the submission procedure; and
    5. Assure the Complainant that all complaints shall be addressed by the Department.

In instances where the Complainant demands to <u>immediately speak to a supervisor</u> the following shall occur:

- Division of Field Services employees shall notify the Troop Duty Officer of jurisdiction and then refer or forward the Complainant to the same Troop Duty Officer; or
- Division of Investigative Services, Division of Administrative Services, Division of Standards and Training, and Division of Homeland Security and Preparedness employees shall notify a Commissioned Officer from within their Division and then refer or forward the Complainant to the same Commissioned Officer.

Continued next page.

Complaint Intake Procedures (Continued)

The Troop Duty Officer or the Division Commissioned Officer shall:

- Record the Complainant within the DAJ, if applicable to their work assignment. Note: DAJ information would also include anonymous complaints or when the Complainant refuses to give their name;
- Explain the complaint intake procedure;
- Instruct the Complainant on how to obtain a SP 340 form from the above options; and
- Assure the Complainant that all complaints shall be addressed by the Department.

Employees who receive complaints about their own conduct shall immediately:

- Notify their Troop Duty Officer or a Commissioned Officer from within their Division; and
- Transfer or refer the Complainant to the same Troop Duty Officer or Commissioned Officer from within their Division.

Internal Complaints

Internal personnel complaints originating within the Department by any employee, shall be documented in a To/From format. The To/From shall be submitted in the following manner:

- Copy faxed to the Division of Standards and Training within twenty-four (24) hours from the date of the To/From;
- Copy submitted through channels to the appropriate Troop/Section/Unit Commander; and
- Original forwarded the to the Division of Standards and Training.

SP340 Citizens Response Form Submission

SP 340 Citizens Response Form shall be submitted in the following manner:

- Delivered in person to the Massachusetts State Police General Headquarters 470 Worcester Road Framingham, MA 01702 / Citizen Response Reports; or
- Faxed to: The Division of Standards and Training/ Citizen Response Reports 508-820-2149; or
- Emailed to: The Division of Standards and Training/ Citizen Response Reports at Citizensresponsereports@pol.state.ma.us ; or
- Mailed to: The Massachusetts State Police Division of Standards and Training/ Citizen Response Reports 470 Worcester Road Framingham, MA 01702.

Interviews

Reasonable arrangements shall be made to accommodate the schedules of the parties involved.

Interviews may be recorded mechanically or by a Department stenographer. The accused employee may independently record their own interview.

Subject	Number
Personnel Investigations	**ADM-14**

Investigation

Step	Action
1	Supervisors shall conduct assigned investigations within thirty (30) days.
2	The complaint shall be categorized as: • Employee's conduct; • Validity of the enforcement action taken; • Department policy, procedure, or operations; or • Other.
3	The investigating member shall make a conclusion of fact for each complaint, which shall be reviewed by the appropriate Troop/Section/Unit Commander. Dispositions shall be classified as: • **Unfounded**- Complaint or incident is false and not factual. • **Exonerated**- Incident occurred, but employee's action was lawful and proper. • **Not Sustained**- Insufficient evidence to prove or disprove the complaint. • **Sustained**- The complaint or incident is supported by sufficient evidence to prove employee misconduct.
4	Complaints classified as **EXONERATED, NOT SUSTAINED, or UNFOUNDED,** and not alleging serious misconduct, shall be filed within the Internal Affairs database. For **SUSTAINED** investigations the Troop/Section/Unit Commander shall: • Prepare a memorandum indicating the category of the complaint, and recommendations; then • Forward the memorandum, with all completed reports and correspondence, through channels to the Division of Standards and Training.
5	The affected employee and Complainant shall be notified of the final disposition classification by the Troop/Section/Unit Commander or the Division of Standards and Training Commander.
	<u>Note</u>: Nothing in this policy should prevent members from taking appropriate and timely action for any allegations of criminal activity or criminal acts.

Subject	Number
Personnel Investigations	**ADM-14**

Responsibilities

Position	Duties
All Employees	• Follow the complaint intake procedures; and • Ensure the Complainant understands: 1. All options for acquiring a SP 340; 2. The SP 340 submission procedure; and 3. That all complaints shall be addressed by the Department.
Supervisor	• Follow the complaint intake procedures; and • Review complaints and conduct investigations when assigned.
Troop Duty Officer or Division Commissioned Officer	• Follow the complaint intake procedures; and • Ensure the Complainant understands: 1. All options for acquiring a SP 340; 2. The SP 340 submission procedure; and 3. That all complaints shall be addressed by the Department.
Troop/Section/Unit Commander	• Initiate investigations on complaints about employees under their supervision or command as assigned by the Division of Standards and Training; and • Forward completed reports and recommendations to the Division Commander within thirty (30) days of assigned date. Note**:** The Division of Standards and Training may authorize a time extension upon a written request.
Complaint Intake Officer	• Process SP 340 received according to standards established by the Division of Standards and Training.

Continued next page.

Subject	Number
Personnel Investigations	**ADM-14**

Responsibilities (Continued)

Position	Duties
Internal Affairs	• Provide oversight of all personnel investigations in accordance with the Section's Standard Operating Procedure (SOP).
Division Commander	• Review investigative reports; • Forward recommendations and requests for disciplinary action to the Division of Standards and Training; and • Issue letters of counseling as appropriate.
Division of Standards and Training	• Review complaints in accordance with the Division's SOP; • Notify the Division Commanders of any personnel investigations conducted by Internal Affairs; and • Review recommendations for disciplinary action with the Deputy Superintendent.
Deputy Superintendent	• Review recommendations for disciplinary action with the Division of Standards and Training; and • Administer disciplinary action as appropriate.
Colonel/Superintendent	• Refer personnel investigations to entities outside the Department, as necessary; and • Prescribe and impose discipline.

References

ADM-15 Internal Affairs
SP 340 Citizens Response Form
MGL c. 4, s.7 and c. 66A, s.2
Carney v. Springfield, 404 Mass 604 (1988)
Kastigar v. U.S., 406 US 441 (1972)
Garrity v. NJ, 385 US 493 (1967)
Collective Bargaining Agreement(s)

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 25, 2008	**ADM-15**

Subject

Internal Affairs

Policy

The Internal Affairs Section investigates allegations of serious misconduct by employees of the Department or as ordered by the Office of the Superintendent or the Division of Standards and Training.

Organization

The Internal Affairs Section has the authority to report directly to the Office of the Superintendent.

Serious Misconduct Defined

Some examples of serious misconduct include:

- Corruption;
- Criminal conduct;
- Use of excessive force; and
- Civil rights violations.

Jurisdiction

Complaints are investigated at the lowest appropriate organizational level in accordance with ADM-14 Personnel Investigations. Internal Affairs may investigate any complaint when:

- Requested by the Troop/Section/Unit Commander, with approval from the Division of Standards and Training;
- Directed by the Office of the Superintendent or the Division of Standards and Training; or
- The complaint alleges serious misconduct.

Use of Examinations

Upon the approval of the Division of Standards and Training Commander or designee, any employee subject to an internal investigation may be asked to submit to tests, examinations, and/or disclosures. These procedures may include, but are not limited to, the following:

- Ballistics and Chemical Tests;
- Forensic and Polygraph Examinations;
- A Photograph Array or Line-Up; and
- Financial Disclosure Statements.

Continued on next page.

Subject	Number
Internal Affairs	**ADM-15**

Use of Examinations (Continued)

Examinations and/or tests shall be:

- Relevant and material to the matter at hand;
- Specifically directed and narrowly related to such investigation; and
- Completed within a reasonable time and according to professionally accepted standards.

A polygraph examination may be used in investigations of criminal conduct.

The results of medical tests shall be afforded appropriate privacy rights according to applicable laws.

Procedure for Internal Affairs Cases

Step	Action
1	Open an Internal Affairs case file.
2	Notify the affected employee regarding; • The nature of the investigation; • The employee's rights as legally required; and • The employee's responsibilities relative to the investigation. NOTE: Internal Affairs can request written authorization from the Division of Standards and Training not to notify the employee, if the notification could hinder the investigation. However, the employee must be informed of the nature of the investigation before any interrogation takes place with the employee.
3	Provide a notification to the employee's Commanding Officer, unless it would hinder the investigation.
4	Conduct the investigation in a timely manner.
5	Prepare a report on the investigation for the Division of Standards and Training, with supporting facts for each allegation and a classification of the complaint: • Unfounded; • Exonerated; • Not Sustained; or • Sustained.
6	The Division of Standards and Training Commander shall notify the affected employee in writing, through channels, of the decision(s).
7	All case files shall be permanently retained.

Subject	Number
Internal Affairs	**ADM-15**

References

ADM-14 Personnel Investigations
MGL c. 4, s.7 and c. 66A, s.2
Furtado vs. Town of Plymouth No. 06-P-892, 69 Mass. App. Ct. 10049

Promulgated By:

Department of State Police
General Order

Effective Date	Number
May 4, 2018	**ADM-16**

Subject

Notifying Prosecuting Agencies Regarding Evidence

Policy

Prosecuting agencies shall be notified of any and all Departmental investigations, to include personnel and/or internal affairs investigations, that are associated with an open criminal prosecution or investigation. Department employees who generate records, percipient witness statements, and/or evidence that relate to a criminal prosecution shall and must notify the appropriate agency prosecuting the case. The assigned lead Departmental investigator in any criminal or administrative investigation is responsible for ensuring such notification is made.

Definitions

Personnel Investigation: Pursuant to ADM-14 Personnel Investigations, any investigation or inquiry into the actions of an employee that may result in charges of misconduct.

Internal Affairs Investigation: Any investigation conducted pursuant to ADM-15 Internal Affairs.

Reporting

A Department investigator assigned to an investigation, to include personnel and/or internal affairs investigations, shall:

- Determine whether the investigation to which he or she is assigned relates to the same facts and circumstances of an open criminal prosecution or investigation;
- Notify the agency prosecuting the open criminal matter of the related Departmental investigation; and document the same in official Department records;
- Upon request of the prosecuting agency, provide any related Departmental records, percipient witness statements and/or evidence to said prosecuting agency, and advise their supervisor and the State Police Legal Section of documents/evidence being provided. The Legal Section will document and maintain a record of the documents or evidence that were provided.
- If the lead investigator believes such notification may adversely affect the investigation to which they are assigned, they shall immediately address the same in writing through their chain of command with a final determination documented in official Department records.

Subject	Number
Notifying Prosecuting Agencies Regarding Evidence	**ADM-16**

References

Brady v. Maryland, 373 U.S. 83
Commonwealth v. Tucceri, 412 Mass. 401
Commonwealth v. Wanis, 426Mass. 639
ADM-14 Personnel Investigations
ADM-15 Internal Affairs

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 25, 2008	**ADM-17**

Subject

Employee Evaluation System

Policy

The Department shall continuously maintain an Employee Evaluation System (EES) to establish and measure performance expectations for sworn members.

The EES shall be conducted in accordance with the Department's EES Manual.

EES Coordinator

The Division of Standards and Training Commander or designee, shall designate a commissioned officer as the EES Coordinator.

EES Purpose

EES is a proven tool for continuous individual and organizational improvement. Some primary purposes of EES are to:

- Maintain continuous supervisor/employee communication and feedback;
- Motivate employees to improve by understanding their needs;
- Establish goals and objectives at all organizational levels;
- Evaluate the quality of performance; and
- Evaluate the readiness to handle greater responsibilities.

References

MGL c.22C, s.22
Department of State Police Employee Evaluation System Manual

Promulgated By:

Department of State Police
General Order

Effective Date:	Number:
August 1, 2017	**ADM-18**

Subject:

Unlawful Harassment, Sexual Harassment and Discrimination

Policy

The Department shall promote and maintain a working environment free from unlawful harassment, sexual harassment and discrimination.

Purpose

This policy addresses all forms of sexual harassment and addresses discrimination and unlawful harassment based on race, color, religious creed, national origin, age (40 or older), sex (including pregnancy), gender identity or expression, sexual orientation, genetic information, ancestry, handicap (disability), active military or veteran status, participation in discrimination complaint-related activities or other protected class under law.
Note: The definitions found in 804 CMR 3.00, et seq., as amended (the MCAD's *Employment Discrimination Guidelines*), shall be applicable to, and are hereby incorporated into, this policy.

This policy does not address conduct, conflicts, or disagreements otherwise addressed through the chain of command or within Department Policy and Procedures. Internal complaints or concerns, which do not relate to an identified protected class or sexual harassment, will not be addressed under this policy. Such complaints may have another course of action such as in ADM-14 Personnel Investigations or SUP-12 Office of the Ombudsman.

Harassment Investigation Unit (HIU)

The Sexual Harassment Officer for the Department is the Division Commander of Standards and Training.

Harassment Investigation Officer(s) shall be Commissioned Officer(s) assigned by the Colonel/Superintendent and shall report to the Division of Standards and Training.

All reports of unlawful harassment, sexual harassment or discrimination shall be forwarded to the Harassment Investigation Unit (HIU). Upon receipt of such a report, the HIU will commence an investigation or recommend an alternative avenue for resolution. All HIU investigations shall remain confidential to the extent practicable.

All Supervisors (except for Supervisors assigned to the Office of the Ombudsman and/or Employee Assistance Unit) shall immediately report incidents of unlawful harassment, sexual harassment or discrimination to the Harassment Investigation Unit.

Subject	Number
Unlawful Harassment, Sexual Harassment and Discrimination	**ADM-18**

Discrimination Defined

Discrimination is the unequal and unlawful treatment of persons ***in employment related decisions*** because of race, color, religious creed, national origin, age (40 or older), sex (including pregnancy), gender identity or expression, sexual orientation, genetic information, ancestry, handicap (disability), active military or veteran status, participation in discrimination complaint-related activities and/or other protected class under law.

Discrimination Examples

Conduct may include, but is not limited to, when the Department:

- Bases employment decisions solely on the race of an applicant; or
- Makes assignments solely on the age of an employee.

Unlawful Harassment Defined

Unlawful harassment is unwelcome conduct that is based on race, color, religious creed, national origin, age (40 or older), sex (including pregnancy), gender identity or expression, sexual orientation, genetic information, ancestry, handicap (disability), active military or veteran status, participation in discrimination complaint-related activities and/or other protected class under law.

Harassment becomes unlawful when:

- Enduring the offensive conduct becomes a condition of continued employment; or
- The conduct is severe or pervasive enough to create a work environment that a reasonable person would consider intimidating, hostile, or abusive.

Unlawful Harassment Examples

Unlawful harassment may include, but is not limited to, conduct, based on race, color, religious creed, national origin, age (40 or older), sex (including pregnancy), gender identity or expression, sexual orientation, genetic information, ancestry, handicap (disability), active military or veteran status, participation in discrimination complaint-related activities and/or other protected class under law, that involves:

- Offensive jokes, slurs, epithets or name calling, or other derogatory comments;
- Physical assaults or threats, intimidation, ridicule or mockery, insults or put-downs, or other verbal or physical conduct that denigrates or shows hostility or aversion; or
- Objects, photographs, images, or demeaning gestures connected to an individual's membership in a protected class.

Subject	Number
Unlawful Harassment, Sexual Harassment and Discrimination	**ADM-18**

Sexual Harassment Defined

Sexual harassment is unwelcome sexual conduct such as: sexual advances, requests for sexual favors, and/or other verbal or physical conduct of a sexual nature, when:

- Submission to or rejection of such advances, requests or conduct is explicitly or implicitly made a term or condition of employment or as a basis for employment decisions;
- Such advances, requests or conduct have the purpose or effect of unreasonably interfering with an individual's work performance; or
- Such advances, requests or conduct have the purpose or effect of creating an intimidating, hostile, humiliating, or sexually offensive work environment.

It is not necessary to meet the threshold of sexual harassment as defined by law to be considered a violation of this policy.

Sexual Harassment Examples

Examples of sexual harassment, may include but are not limited to:

- Direct sexual advances or assaults;
- Sexual inquiries, jokes, and epithets;
- Derogatory comments about a person's sex, sexual orientation or gender identity or expression;
- Other forms of verbal abuse of a sexual nature, such as whistling or catcalling;
- Offensive or unnecessary touching, pinching, patting, etc.;
- The display of sexually suggestive posters, photographs, or objects; or
- An employee receiving job benefits contingent on sexual favors (quid pro quo).

Sexual Harassment Victims

Victims of sexual harassment <u>may</u> be…	**The harasser <u>may</u> be…**
Of the same or different gender as the harasser.	Of either gender.
A third person who is not the intended target of the sexual harassment or conduct.	Any employee or in certain circumstances someone who is not an employee (vendors, contractors).

Liability and Sanctions

Employees may be personally liable if they engage in unlawful harassment, sexual harassment or discrimination.

Any employee found to have engaged in unlawful harassment, sexual harassment, or discrimination in violation of this policy is subject to disciplinary action up to and including termination.

Supervisors may potentially be personally liable if they knew or should have known about incidents of sexual harassment, and did not take appropriate corrective action.

The Department may not be held responsible in cases of unlawful harassment, sexual harassment, and/or discrimination, if it can show that it took prompt and appropriate corrective action.

Subject	Number
Unlawful Harassment, Sexual Harassment and Discrimination	**ADM-18**

Complaint Procedure

Step	Action
1	Process for reporting incidents of unlawful harassment, sexual harassment discrimination, and/or retaliation: • Notify a supervisor, who shall assist in reporting the complaint to the Harassment Investigation Unit (HIU); • Fax a copy of the SP 387 *Unlawful Harassment, Sexual Harassment and Discrimination Complaint* form directly to the HIU at (508) 820-2149, or email to MSPHIU@MASSMAIL.STATE.MA.US; • Forward the original SP 387 to the HIU 470 Worcester Road, Framingham, MA 01702; and/or • Report Complaint to the Director of the Human Resources Section at GHQ.
2	The HIU shall promptly: • Respond to the complainant; • Review all available information pertaining to the complaint; • Determine if the aggrieved individual(s) is/are a member of a class protected under the law and this policy; • Determine if the alleged conduct meets the definition of unlawful harassment, sexual harassment or discrimination as defined in this policy; • Determine an appropriate course of action, including, but not limited to, alternative resolutions; • Conduct an investigation if warranted, to include, but not limited to, an interview with person(s) filing the complaint, any witnesses, and the person(s) alleged to have engaged in unlawful harassment, sexual harassment and/or discrimination; • To the extent practicable, ensure that all interviews are digitally recorded; • Consult procedures included within the Department's Resolution Process as outlined within the Affirmative Action Plan; and • Make a report of findings and forward report to the Commander of the Division of Standards and Training. Consistent with Commonwealth and Department Policy/Rules and Regulations, and in a manner determined by the Division Commander of Standards and Training, completed confidential reports will be made available for inspection to complainants and persons alleged to have committed unlawful harassment, sexual harassment, discrimination and/or retaliation upon request.

Continued next page.

Complaint Procedure (Continued)

Step	Action
3	An employee may also file a complaint with: **Massachusetts Commission Against Discrimination (MCAD)** www.mass.gov/mcad Main Office: One Ashburton Place, Room 601, Boston, MA 02108 Phone 617-994-6000 TTY: 617-994-6196 Regional Offices New Bedford Office: 800 Purchase Street, Room 501, New Bedford, MA 02740 Phone: 508-990-2390 Springfield Office: 424 Dwight Street, Rm. 220, Springfield , MA 01103 Phone 413-739-2145 Worcester Office: 484 Main Street, Room 320 Worcester, MA 01608 Phone 508-453-9630 **Office of Diversity and Equal Opportunity** One Ashburton Place, Room 213 Boston, MA 02108-1516 Telephone 617-727-7441 (Note: this office takes only **Discrimination** complaints.) **US Equal Employment Opportunity Commission (EEOC)** www.eeoc.gov John F. Kennedy Federal Building 475 Government Center, Boston, MA 02203 Phone: 1-800-669-4000 TTY: 1-800-669-6820
4	The Harassment Investigation Unit shall notify the Department's Office of Diversity and Equal Opportunity of complaints of unlawful harassment or discrimination.

Subject	Number
Unlawful Harassment, Sexual Harassment and Discrimination	**ADM-18**

Responsibilities

Position	Duties
Supervisors	• Aggressively monitor the workplace to prevent and detect unlawful harassment, sexual harassment, and discrimination; • Take appropriate corrective action to stop all types of unlawful harassment, sexual harassment, and discrimination; • Immediately report incidents of unlawful harassment, sexual harassment, or discrimination to the Harassment Investigation Unit; • Assist any employee in filing a complaint, or obtaining information on the Commonwealth's Sexual Harassment Policy; and • Contact the HIU for information and guidance pertaining to unlawful harassment, sexual harassment and/or discrimination.
All Employees	• Shall not engage in any harassment, sexual harassment, or discrimination; • Shall cooperate in investigations of any harassment, sexual harassment, and discrimination; • Shall actively participate in the Department's efforts to prevent and eliminate any harassment, sexual harassment, and discrimination; and • May contact the HIU for information and guidance pertaining to any harassment, sexual harassment and/or discrimination.

Office of the Ombudsman/ Employee Assistance Unit

All employees should be aware that conversations with the Office of the Ombudsman and/or Employee Assistance Unit are considered confidential and are not the proper venue to notify the Department of unlawful harassment, sexual harassment and/or discrimination complaints. Supervisors assigned to the Office of the Ombudsman or the Employee Assistance Unit are not required to report such complaints through the official chain of command.

Retaliation

Any retaliation against an individual who has complained about unlawful harassment, sexual harassment, discrimination or for cooperating with a complaint and/or investigation of harassment, sexual harassment, or discrimination is unlawful and shall not be tolerated. Any such retaliation shall be a violation of this policy. Incidents of such retaliation shall be reported to the HIU in To/From format.

Distribution of Policy

This policy shall be issued to each employee upon hiring and to all employees annually thereafter. This policy shall be continuously posted and available on DocuShare.

Statewide Policy

The Department shall adhere to the Commonwealth of Massachusetts Human Resources Division Sexual Harassment Policy.

Subject	Number
Unlawful Harassment, Sexual Harassment and Discrimination	**ADM-18**

Findings

In the event that an investigation is conducted regarding unlawful harassment, sexual harassment, discrimination, and/or retaliation, the findings shall be classified as one of the following:

- ***Unfounded*** - Complaint or incident is false and not factual;
- ***Exonerated*** - Incident occurred, but employee's action was lawful and proper;
- ***Not Sustained*** - Insufficient evidence to prove or disprove the complaint; or
- ***Sustained*** - Complaint or incident is supported by sufficient evidence to prove employee misconduct.

Cases in which the complainant has withdrawn the complaint shall be classified as withdrawn. Cases that are approved for an alternate resolution shall be classified as referred. In all cases, a record shall be made in the case file. All findings, withdrawals and referrals shall be reviewed and approved by the Division Commander of Standards and Training.

Any complaint which is sustained shall be deemed a violation of ADM-18 and/or the Rules and Regulations of this Department and shall be handled in accordance with Rules and Regulations of the Department, as applicable. Whether found to be a violation of ADM-18 or not, any inappropriate employee conduct, including but not limited to making or providing false claims, reports, information, statements and/or testimony, may be deemed a violation of Department Policy/Rules and Regulations and is subject to investigation under ADM-14 Personnel Investigations.

NOTE: Nothing in this policy should prevent members from taking appropriate and timely action for any allegations of criminal activity or criminal acts.

References

ADM-14 *Personnel Investigations*
ADM-36 *Diversity and Equal Opportunity*
SUP-04 *Employee Assistance Unit*
SUP-12 *Office of the Ombudsman*
MGL c.151B, s.3, 3a, and 4
MGL c.214, s. 1c
804 CMR 3.00 Employment Discrimination Guidelines
MCAD Model Sexual Harassment Policy
US Equal Employment Opportunity Commission Regulations and Guidance
Department Rules and Regulations
Department of State Police Affirmative Action Plan
Executive Order 526- Order Regarding Non-Discrimination, Diversity, Equal Opportunity, and Affirmative Action
Commonwealth of Massachusetts HRD Sexual Harassment Policy
Title VII of the Civil Rights Act of 1964
SPAM Collective Bargaining Agreement Article 27
SP 387 *Unlawful Harassment, Sexual Harassment and Discrimination Complaint* form

Promulgated By:

Department of State Police
General Order

Effective Date	Number
November 5, 2008	**ADM-19**

Subject

Vehicle Management

Policy

To establish a central management system for all vehicles owned or controlled by the Department in order to maintain a state of operational readiness.

Procurement

The Fleet Administrator shall authorize and be responsible for the procurement of all Department vehicles including:

- Vehicle specifications;
- Bidding process; and
- Equipment, parts and materials necessary for vehicle maintenance.

Fleet Administrator

The Fleet Administrator shall:

- Maintain a master vehicle inventory for computer/cruiser number, operator, operator assignment, vehicle model year, mileage, registration number, and condition;
- Ensure the annual reconciliation of the master inventory during the month of June;
- Maintain a sufficient inventory of parts, materials, and equipment at Fleet and the Troop/Section garages, subject to available funding;
- Issue parts and materials to Troop/Section garages according to need and availability;
- Maintain detailed vehicle maintenance records; and
- Notify Department personnel of manufacturer vehicle recalls.

Fleet Coordinator

Troop/Section Commander or designee shall act as the Fleet Coordinator:

- Ensure that monthly mileage and state inspection are submitted through established Departmental procedures.

Specialty Vehicles

Requests for specialized vehicles shall be forwarded through the respective Division Commander to the Fleet Administrator.

Specialty vehicles shall:

- Be purchased based on needs of the Department;
- Be assigned to personnel within the specialized sections/units; and
- Remain within the assigned section/unit unless otherwise authorized by the Fleet Administrator.

Subject	Number
Vehicle Management	**ADM-19**

Vehicle Status

Designation	Meaning
Active	Assigned and in-use.
Down*	Inoperable, requires repairs.
Out of Service*	Permanently disabled.
Spare	Unassigned and available for use.
* Vehicles designated "Down or Out of Service" **shall not be operated.**	

Vehicle Assignment

The Fleet Administrator or designee shall:

- Maintain control over vehicle assignment and re-assignment;
- Assign vehicles based on the year, condition, and mileage;
- Assign vehicles to individual personnel based upon availability and particular assignment; and
- Prior to the assignment or replacement of a vehicle:
  1. Analyze inventory reports of affected vehicle(s);
  2. Notify member(s) of scheduled vehicle assignment or appointment; and
  3. Inspect and verify vehicle being turned in for mileage, damage, operational status, cleanliness, and issued equipment.

Note: Personnel failing to report with their assigned vehicle and/or issued vehicle equipment shall not be issued a new or replacement vehicle.

Transfers

If members are…	Then members shall…
Transferred or promoted to a function requiring the same vehicle.	Retain currently assigned vehicle.
Transferred or promoted to a function requiring an alternate vehicle, i.e. marked, unmarked or specialty vehicle.	Contact the Fleet Section for vehicle re-assignment.

Vehicle Disposal

The Fleet Administrator shall:

- Maintain standards and criteria for determining when a vehicle is suitable for disposal;
- Ensure all usable equipment and parts are removed and the vehicle is appropriately prepared for disposal; and
- Provide the Commonwealth of Massachusetts Operational Services Division with the vehicle identification number of disposed vehicles.

Subject	Number
Vehicle Management	**ADM-19**

Extended Leave

Position	Responsibilities
Member	Shall return the following issued equipment to their Troop/Section/Unit Commander when on extended leave in excess of thirty (30) days: • Assigned vehicle along with issued vehicle equipment; and • Department issued fuel card, transponder and snow gate access cards.
Troop/Section Commander	• Shall notify the Fleet Administrator when issued vehicles and equipment are returned due to extended leaves; and • Advise the location of the vehicle and equipment.
Fleet Administrator	• Re-assign vehicle based upon the needs of the Department; and • If practicable, members returning to full duty should be re-assigned the same vehicle.

Forfeited/ Donated Vehicles

The Fleet Administrator has the authority to accept or reject vehicles on behalf of the Department.

Any vehicle accepted by the Department, shall be:

- Delivered to the Fleet Section with appropriate documentation, e.g. order of forfeiture, certificate of title;
- Inspected for mechanical and/or physical safety defects prior to acceptance and registration;
- Assigned a Fleet vehicle computer number; and
- Assigned by the Fleet Administrator based on the needs of the Department.

References

ADM-19A Vehicle Use and Maintenance

Promulgated By:

Department of State Police
General Order

Effective Date	Number
December 11, 2019	**ADM-19A**

Subject

Vehicle Use and Maintenance

Policy

Department vehicles shall be maintained in a safe, clean and serviceable condition at all times for reasons of safety and operational readiness, as well as to enhance the Department's public image.

Members assigned a vehicle belonging to various authorities or other governmental agencies, shall ensure they adhere to the vehicle use and maintenance policies of those authorities/agencies.

Required Equipment

Vehicles used for enforcement purposes shall be equipped with, at a minimum:

- Emergency lights and siren;
- Medical kit;
- Fire extinguisher;
- Radios;
- Prisoner safety barrier (marked, semi marked, low profile vehicles);
- Reflective chevrons displayed to the rear, and reflective pinstripe to both the front and rear, configured as determined by the Fleet Administrator (marked, semi marked, low profile vehicles);
- Conspicuous markings (marked, semi marked vehicles); and
- All other equipment issued with, or made part of the vehicle according to Department specifications.

Note: Cruiser equipment shall not be altered without prior approval of the Fleet Administrator.

Vehicle Inspection

Vehicles and equipment shall be inspected:

- Prior to the beginning of each shift by the vehicle operator;
- Before and after transporting prisoners for contraband and evidence;
- Quarterly by Station/Unit Commanders and documented according to Department procedures;
- For line or staff inspections; and
- When requested by the Fleet Administrator.

Employees shall immediately report, in writing, to their immediate supervisor and the Fleet Administrator, any damage or vandalism to Department vehicles.

Any damage to a Department vehicle caused by a person arrested or summonsed to court shall be immediately reported to the Fleet Section, in order to collect restitution. The Fleet Coordinator shall make arrangements for repairs through the Fleet Section.

Installation of Non-Issued Equipment, Adding or Removing Window Tint or Vehicle Alteration

Employees shall not install non-issued equipment and/or add or remove window tint in any Department vehicle without prior written authorization from the Fleet Administrator.

Employees requesting to install non-issued equipment and/or add or remove window tint in Department vehicles shall:

- Make written requests through the appropriate channels to the Troop/Section/Unit Commander;
- Agree in writing to assume all responsibility for the loss or theft of the equipment, and any damage caused to the vehicle associated with the installation or removal of the equipment;
- Assume all costs associated with the purchase, installation, and service and/or maintenance fees associated with the installed equipment;
- Notify the Fleet Administrator of the location where the professional installation of the equipment shall occur; and
- Immediately remove any equipment as directed by the Fleet Administrator or proper authority.

The Troop/Section/Unit Commander shall review all requests and forward approved requests to the Fleet Administrator or the proper authority.

The Fleet Administrator shall:

- Approve or deny all written requests; and
- Forward the written approval or denial to the appropriate Troop/Section Commander.

Vehicle Ornamentation

Employees shall not affix/install vehicle ornamentation on or in any Department vehicle, including vehicles assigned to various authorities or other governmental agencies, unless approved in advance, and in writing, by the Deputy Superintendent and the Fleet Administrator.

Vehicle Alteration

Employees shall not:

- Remove, cover, or obscure the display of the issued registration plates; or
- Remove cruiser markings from Department vehicles without prior authorization from the Fleet Administrator or proper authority.

Recalls

Recalls issued by the Department or the manufacturer regarding Department vehicles shall be posted by the Fleet Administrator, according to Department procedures. Employees who are assigned Department vehicles are responsible for checking recalls at least monthly. In the event a recall exists, the employee shall:

- Contact an authorized service center to schedule an appointment for service;
- Ensure the recall work is completed as ordered;
- Forward the repair order to the Fleet Section; and
- Retain a copy of the repair order.

Subject	Number
Vehicle Use and Maintenance	**ADM-19A**

Vehicle Use

Members shall operate Department vehicles in a cautious manner, and in conformance with Department Policy and Procedure, Rules and Regulations, and applicable Massachusetts General Laws.

Department vehicles shall be used for:

- Official use only;
- Commuting to and from home to assigned work location;
- Scheduled work assignments, callouts, or training; and
- Paid Details (undercover vehicles shall not be used at road construction sites.)

Employees (sworn and civilian) who use a Department vehicle shall:

- Notify their supervisor and receive authorization prior to using the vehicle outside of normal scheduled work hours, scheduled work assignments, callouts, training, details, or when on any type of time off or days off.

Supervisors shall:

- Only authorize an employee or member the use of a Department vehicle when the employee or member is on time off or days off for activities that are clearly indicative of official Department business; and
- Be responsible for documenting each request and authorization.

Maintenance

The operators of Department vehicles shall be responsible for:

- Maintaining a clean exterior and interior;
- Scheduling routine service and repairs with Fleet Section personnel, or at authorized service locations;
- Reporting all malfunctions to Department vehicles to the Fleet Administrator;
- Ensuring the vehicle registration is current;
- Ensuring the State Safety and Emission Inspection is current;
- Submitting monthly cruiser information according to Department procedures;
- Daily inspection checks; and
- The removal of snow and ice.

Daily Inspection Checks

The daily inspection check shall include, but not be limited to, the following checks:

- Fluid levels (oil, coolant, transmission, brake, steering and washer);
- Tires (pressure, wear and condition);
- Belts and hoses;
- Inspection and registration stickers; and
- Emergency equipment.

Scheduled Maintenance

All Department employees are required:

- To have their currently assigned Department vehicle routinely serviced; and
- To have an oil change at a Department Fleet Facility every 9,000 miles or six (6) months, whichever occurs first.

Appointments shall be made with each individual Fleet Facility prior to mileage/month deadline. No employee shall:

- Have their cruiser serviced at a third party commercial service center, unless the service is specifically pre-approved by the Fleet Administrator.

Troop/Station/Section/Unit Commanders that have specialty, spare, and/or pool vehicles assigned under their command shall ensure compliance.

Fuel Cards

Fuel cards issued to Department employees are restricted to the purchase of fuel for assigned Department vehicles. All purchases for items, other than fuel, shall result in the payment of restitution and/or disciplinary action. Employees utilizing fuel cards shall:

- Sign a receipt when issued fuel card;
- Enter Fleet vehicle computer number for PIN and current mileage when fueling;
- Immediately report lost or stolen cards in writing to the Fleet Section, through channels;
- Fuel vehicles at authorized facilities;
- Purchase regular unleaded fuel only, unless otherwise authorized;
- Use self-service facilities, whenever possible, to assist in controlling Department fuel expenditures;
- Ensure vehicle fuel tanks remain at least half full at all times; and
- Turn in fuel cards through channels to the Fleet Administrator upon any leave in excess of thirty (30) or more days.

Note: Employees shall comply with Massachusetts General Law c. 90 s. 13 by not leaving their vehicle-running while unattended, unless within the scope of their duties e.g. motor vehicle stops.

Transponders and Snow Gate Access Cards

Non-revenue Fast Lane Transponders and Snow Gate Access Cards shall only:

- Be utilized for official business in Department assigned vehicles within the Commonwealth of Massachusetts.

Employees traveling outside of the Commonwealth shall:

- Disable their transponders;
- Pay tolls with cash; and
- File for reimbursement through the standard employee expense reimbursement process.

Continued next page.

Transponders and Snow Gate Access Cards (Continued)

Electronic data associated with the use of these items shall be monitored to ensure compliance. Use of non-revenue Fast Lane Transponders and Snow Gate Access Cards constitutes express consent for the Department to monitor and/or inspect any data created in the course of such use.

Employees assigned non-revenue Fast Lane Transponders and Snow Gate Access Cards shall:

- Use the Fast Lane;
- Disable their transponders when traveling out of state;
- Immediately report lost or stolen transponders or Snow Gate Access Cards in writing to the Fleet Administrator, through channels; and
- Turn in non-revenue transponders and Snow Gate Access Cards through channels to the Fleet Administrator upon any leave in excess of thirty (30) or more days.

Emergency Operation and Response

Members responding in emergency vehicles shall operate vehicles with due care and regard for the safety of all persons and property.

Members, in an emergency and while in the performance of duty:

- May drive in excess of the applicable speed limit, if exercising caution and due regard under the circumstances; and
- May drive through an intersection, contrary to traffic signs or signals, **after coming to a full stop**, and then proceeding with caution; and
- **Shall never pass** a school bus that has stopped to allow pupils to alight or board and has its red lamps flashing.

Response	Action
Non-emergency/non-life threatening.	• Emergency lights and/or siren need not be used; and • Observe all traffic laws and regulations.
Emergency, but non-life threatening.	• Emergency lights and sirens may be utilized; and • May use discretion in approach.
Actual or potential life-threatening injuries or violent situations.	• Utilize emergency lights and sirens; • Expeditious response with due care and regard for public safety; and • May use discretion in approach.

Subject	Number
Vehicle Use and Maintenance	**ADM-19A**

Seatbelts

All occupants shall properly wear seatbelts while traveling in any state owned vehicles as mandated by Executive Order No. 241.

Airbags

No object shall be placed on or in the path of airbags for safety reasons. Airbag switches shall not be installed in any Department vehicle without the prior written approval of the Fleet Administrator.

References

ADM-19 Vehicle Management
TRF-20 Department Vehicle Crashes
Executive Order No. 241 Use Of Seat Belts By State Employees
MGL c. 90 s.13 Safety Precautions for Proper Operation and Parking of Vehicle and Buses
MGL c.89, s.7B
MGL c.90, s.14

Promulgated By:
Colonel Christopher S Mason

Department of State Police
General Order

Effective Date	Number
May 2, 2018	**ADM-19B**

Subject

Automated Vehicle Locator (AVL) Technology

Policy

The purpose of this policy is to establish guidelines and procedures for the use of the Department's Automated Vehicle Locator (AVL) Technology. AVL is designed to increase officer accountability and safety by enhancing the ability to rapidly locate and deploy Department personnel and resources. AVL technology also improves coordination and resource management during tactical situations, assists in improving response times to radio calls and increases situational awareness for all employees.

The Department's AVL utilizes global positioning system (GPS) to determine the location of Department personnel and resources.

AVL technology allows for real-time command and control of Department resources. Knowledge of resources that are in the vicinity of an incident improves officer safety, increases operational efficiency, and provides the Department with a more efficient and dependable means of enforcing work rules. Accordingly, it is the Department's goal and policy to utilize AVL in all marked Department cruisers and as many additional vehicles and resources, subject to operational demands and funding, as determined by the Colonel.

Accountability and safety are the primary focuses of the AVL system; however, AVL data shall be used for all relevant purposes including but not limited to the deployment of personnel, operational efficiency, patrol strategy, personnel and other investigations, the enforcement of work rules, regulations, policies, customs, practices, procedures, orders, commands, and/or directives.

Department employees are reminded that, in relation to the Department's receipt and use of AVL data, they have no expectation of personal privacy.

Subject	Number
Automated Vehicle Locator (AVL) Technology	**ADM-19B**

Definitions

On Duty – for the purposes of this General Order shall refer to any period of time that an employee of the Department is performing any Department function or using a Department vehicle or resource, to include, but not be limited to: the performance of duties, whether assigned or self-initiated or uniformed or plain clothed, patrol, investigative and administrative functions, reporting to and traveling to and from work assignment, court, paid detail or training, and/or commuting to and from home.

Automated Vehicle Locator Technology (AVL) – an electronic means for automatically determining and transmitting the geographic location of Department resources to include: personnel, vehicles and crafts. Examples of AVLs include, but are not limited to: GPS equipped radios, cellular devices, MDTs, and stand-alone hardware devices.

Global Positioning System (GPS) – a satellite system that provides geo-coordinates and time information to a GPS receiver.

Administration

All on duty Department personnel issued AVL Technology or a vehicle or resource equipped with AVL shall use AVL in accordance with all of the following:

- Unless expressly exempted by the Colonel or his/her designee, all on duty members equipped with AVL Technology shall, except where AVL is not self-activated, activate AVL systems or devices at the beginning of being on duty and shall keep it activated until off duty. This requirement includes activating GPS equipped portable radios, logging on to GPS equipped MDT, and activating assigned cellular devices and/or modems.

- A member shall report technical problems and or malfunctions relating to the operation of the AVL system immediately to his or her supervisor and to the Communications Section. The malfunction shall be recorded in the Daily Administrative Journal.

- Any member operating a Department vehicle or resource with a malfunctioning AVL system shall comply with the Officer/Vehicle Status notifications required by ADM-21 Communications.

- Supervisors and the Communications Section shall immediately report any malfunction of the AVL system to the Office of Technology and Information Services (OTIS).

- At least once during a shift, Troop/Section/Unit Commanders, or designees, shall determine the AVL systems of each on duty member, under their command, are working properly.

Subject	Number
Automated Vehicle Locator (AVL) Technology	**ADM-19B**

Equipment

- No member shall use or install any equipment or items that may interfere with Department authorized AVL equipment.
- Members shall not tamper with the AVL/GPS receiver, antenna, wiring, and/or software or attempt to hinder the systems designed performance. Any misuse, abuse, alteration or modification of the AVL software, hardware or any associated components or any violation of this General Order may result in disciplinary action.

Exemptions

The Colonel shall determine which vehicles and resources shall be equipped with AVL technology. A Division Commander, or designee, may authorize the temporary disabling of AVL equipment for members or resources under their command, and shall, when authorized, document the reasons for same in writing.

- Any member whose assignment would be adversely affected by having location information recorded/published may request authorization from the member's Division Commander, or designee, to temporarily disable the AVL system for as long as necessary to complete the assignment.

AVL Records

AVL data:

- Shall be the property of the Department of State Police;
- Shall not be disseminated without authorization from the Department;
- Shall not be accessed, copied, or released for non-law enforcement purposes;
- Shall be preserved and/or made available in compliance with all legal obligations and orders, for investigative and training purposes and other needs of the Department;
- Shall be securely stored and disposed of in accordance with state records retention laws; and
- May be preserved at the request of a Division Commander or designee or for any lawful reason.

Accessing AVL Data

Members and employees may only access Department AVL data when they are expressly authorized to access such data in the course of their assigned duties. Other requests for access to AVL data, live or stored, shall be made in writing and forwarded through channels to the member's Division Commander or designee.

Subject	Number
Automated Vehicle Locator (AVL) Technology	**ADM-19B**

Audits

The Colonel/Superintendent or designee may authorize audits of any AVL device to ensure system integrity and functionality.

The Colonel, Deputy Superintendent, Division Commanders and/or their designee(s) shall have access to AVL data for any lawful, relevant purpose, including but not limited to situational awareness, response times, analysis and improvement of patrol tactics, improvement of officer safety, criminal or personnel investigations, and the enforcement of existing work rules, regulations, policies, customs, practices, procedures, orders, commands, and/or directives.

References

ADM-21 Communications

Promulgated By:

Department of State Police
General Order

Effective Date	Number
August 1, 2017	**ADM-20**

Subject

Weapons Management

Policy

The Armorer shall provide oversight for the control and operational readiness of all Department weapons and ammunition, from acquisition to final disposition.

Members shall continually inspect all weapons and ammunition issued to them or under their control, to ensure cleanliness and operational readiness.

Definition

Firearms: All firearms, rifles, shotguns, and machine guns issued by the Department.

Armorer: A member designated by the Colonel/Superintendent, responsible for all weapons and ammunition under their control or in storage at the Armory.

Armorer

The Armorer shall:

- Maintain an accurate inventory of all weapons;
- Maintain all SP 9 Record of Issue and SP 255 Equipment Transfer/Disposition forms;
- Update the Department Soft Body Armor/Weapons Inspection database;
- Maintain an inventory of ammunition and firearms related supplies;
- Ensure that sufficient quantities of ammunition, parts, and supplies remain at the Armory for Department use;
- Coordinate all firearms repairs;
- Conduct training for all members;
- Ensure each Station/Section/Unit has a suitable bullet trap or body armor for use in unloading firearms; and
- Be available to provide temporary replacement firearms.

Firearms Issue or Transfer

Each firearm issuance and transfer shall be recorded on the SP 9. The Armorer shall ensure the correct information is updated on PayStation.

Continued next page.

Firearms Issue or Transfer (Continued)

Commanding Officers that have firearms assigned to the Station/Section/Unit shall complete a SP 255 form indicating:

- Description of firearms including serial number; and
- Date and location of assignment.

Commanding Officers shall forward one (1) copy to the Armorer and retain a copy for the Station/Section/Unit records.

Storage of Firearms and Ammunition

Commanding Officers that have firearms assigned to their Station/Section/Unit shall:

- Provide a secure, locked, and alarmed storage area;
- Keep all stored items in a state of operational readiness and available for emergency use at any time; and
- Permit immediate accessibility only to authorized members.

Seizure of Firearms

Upon seizure of a duty firearm, the supervisor shall contact the Armorer to:

- Determine if the member has additional issued firearms; and
- Coordinate storage of the seized duty firearms(s).

Disposal of Weapons

Upon determination that Department firearms or ammunition have become obsolete or inoperable, the Armorer shall complete a SP 255 indicating:

- Description of item;
- Reason and method of disposal (sale, trade-in, destruction); and
- Name of receiving agency/company and signature of receiving party.

The Armorer shall dispose of the item in accordance with the guidelines established by the Commonwealth of Massachusetts.

Inspections

During range qualification all firearms shall be inspected for condition and operational readiness by the Armorer or designee.

Supervisors shall ensure:

- A firearms inspection has been completed quarterly for all subordinates during the months of January, April, July, and October;
- A report of the inspection is documented on PayStation; and
- Members on leave during the quarterly period have their firearms inspected on the first day that the member returns to duty.

Only members trained in the inspection of specific firearms shall inspect that particular type of firearm.

Continued next page.

Subject	Number
Weapons Management	**ADM-20**

Inspections (Continued)

Members submitting a firearm for inspection shall:

- Ensure that the firearm is in a safe and unloaded condition with the magazine removed;
- Present the firearm with the slide locked in the open position;
- Shotguns shall be presented for inspection with the action in the open position; and
- Rifles, machine guns and submachine guns shall be presented for inspection in a safe manner as directed by the Inspector.

Weapons shall be unloaded in a safe manner consistent with training, using a suitable bullet trap or ballistic vest as a backdrop in a safe area approved by the Armorer.

Inspectors Duties

Only members trained in the inspection of specific firearms shall inspect that particular type of firearm. Inspectors may use a SP 608 Weapons Inspection form as a guideline during the inspection process.

Firearms Inspectors shall:

- Inspect all Department firearms as assigned and document on the Department database during the months of January, April, July, and October;
- Detail all inadequacies on the database; and
- Remove any weapon or ammunition found to be defective and forward to the Armorer for repair or replacement.

Temporary Firearms

Commanding Officers shall:

- Ensure that the member with the defective firearm is issued a temporary replacement firearm by the Armorer; and
- Document the issue of the temporary firearm on a SP 9.

The Armorer or designee shall issue temporary firearms. The Armorer may be contacted through the GHQ Communications Section.

Leave

Commanding Officers of a member who is on any leave in excess of thirty (30) days shall contact the Armorer for storage of Department issued firearms and ammunition.

References

SP 9 Record of Issue Form
SP 255 Equipment Transfer/Disposition Form
SP 608 Weapons Inspection Form

Promulgated By:

Department of State Police
General Order

Effective Date	Number
November 5, 2008	**ADM-21**

Subject

Communications

Policy

The Department shall maintain an effective and efficient communications system to aid in the performance of its public safety mission.

The Department shall ensure continuous communication accessibility through a twenty-four (24) hour multi-channel radio system capable of two-way operation on joint public safety frequencies.

The Department shall comply with all Federal Communications Commission (FCC) procedures and requirements.

Positions and Responsibilities

Position	Duties
Colonel/Superintendent or designee	• Designate personnel to the Communications Staff positions.
Director of Communications	• Supervise all personnel assigned to the Communications Section.
Communications Officer (commissioned officer)	• Supervise members assigned to the Communications Section; • Oversee the administration of the audio recordings of Department radio frequencies; • Serve as "Keeper of the Records" for the Communications Section; and • Record and preserve E 911 Emergency Lines in accordance to general laws and codes for a period of one (1) year.
Director of Dispatch Services	• Supervise all personnel in the Dispatch Services Unit.
Communications Coordinator	• Provide technical expertise in the operation and implementation of Department radio systems.

Subject	Number
Communications	**ADM-21**

Audio Recordings

Requests for Audio Recordings

Audio recordings are available to comply with all legal requirements, for investigative and training purposes, or for other needs of the Department. Requests for audio recordings shall be:

- Forwarded through channels to the Communications Officer using SP 623 Cellular 911 & Radio Transmission Recording Request form.

Note: The indiscriminate or inappropriate play-back of the Department's recorded messages is strictly prohibited.

Communication Center GHQ

The Communications Officer shall:

- Assign a commissioned or non-commissioned officer as the General Headquarters (GHQ) Communications Desk Officer for each duty shift.

Communications Desk Officer shall:

- During emergencies and/or unusual occurrences that may affect the Department, immediately notify the Command Staff and properly implement on-call procedures and ensure requests for specialized services are processed;
- Physically secure the dispatch area; and
- Monitor GHQ complex.

Communication Facilities and Equipment

Access to the Department Communications Centers and equipment shall be:

- Restricted to authorized personnel.

Each Department facility is equipped with an alternative power source, sufficient enough to operate the radio systems and other vital equipment, in the event of a primary power source failure.

The alternative power source shall be:

- Accessible only to authorized personnel; and
- Inspected and tested weekly by the Troop/Station/Section Commander or designee, and documented.

Emergency Service Numbers

The Troop/Station/Section/Unit Commanders shall ensure:

- The telephone numbers and addresses of available emergency service agencies are up to date and readily available to dispatchers, desk officers, as well as other communications personnel; and
- That the tactical dispatching plans or emergency operational plans that may affect facilities within their specific jurisdiction, e.g., prisons, nuclear plants, sports facilities, are up to date and readily available.

Officer/Vehicle Status

Station Desk Officers and Dispatchers shall know which members are immediately available for service, therefore:

- Whenever a member engages in self-initiated patrol activities, they shall notify the desk officer or dispatcher of the exact location and purpose;
- Whenever a member is not available for normal patrol function, they shall notify the desk officer or dispatcher, and the appropriate status code shall be entered into the "officer assignment" section of the Daily Administrative Journal (DAJ); and
- Whenever a back-up officer is assigned to a call, an appropriate entry shall be made into the DAJ.

Radio Decorum

Department member(s) shall ensure:

- Department radio communications/messages have first priority;
- They properly identify themselves and use clear diction when communicating on the Department network; and
- When making requests for law enforcement information, the member shall do so via their assigned radio frequency, unless doing so would compromise an investigation or the member's safety.

Incident Command

The National Incident Management System (NIMS) has integrated existing best practices into a consistent, nationwide approach to domestic incident management at all jurisdictional levels and across functional disciplines.

Department member(s) involved at a complex critical incident shall:

- Use a clear spoken message-based on common terminology; and
- Refrain from using codes for radio communications.

Subject	Number
Communications	**ADM-21**

Radio Codes

To eliminate lengthy radio transmissions and maintain confidentiality, the following codes shall be used for all radio broadcasts, whenever practicable:

CODE 1	STANDBY FOR AN EMERGENCY - Cease and desist all unnecessary radio traffic. Only primary dispatchers and officers engaged in the emergency shall transmit messages.
CODE 2	TELEPHONE YOUR STATION
CODE 3	TELEPHONE (person) AT (number).
CODE 4	CRUISER OUT OF SERVICE Specify location and/or telephone number.
CODE 5	CRUISER NOW IN SERVICE
CODE 6	WHAT IS YOUR LOCATION?
CODE 7	RETURN TO YOUR STATION OR SPECIFIC LOCATION
CODE 8	STOPPING A SUSPICIOUS VEHICLE – Transmit vehicle make, model, color, registration number, number of occupants, and give EXACT LOCATION.
CODE 9	REQUEST LISTING ON-Transmit registration number and/or vehicle identification number of motor vehicle, and give EXACT LOCATION.
CODE 10	REQUEST STOLEN RECORD ON - Transmit registration number and/or vehicle identification number or serial number of suspected stolen property, and give EXACT LOCATION.
CODE 11	REQUEST LICENSE DATA ON - Transmit name, DOB, license number if known, and give EXACT LOCATION.
CODE 12	ANY MESSAGES FOR ME?
CODE 13	RADIO TEST CALL Give signal strengths as follows: R-1 Barely audible; R-7 Moderately strong signal; R-3 Weak signal; R-9 Strong signal loud and clear. R-5 Fairly good signal;
CODE 14	MISSING OR WANTED CHECK - Transmit name, race, sex, DOB, social security number, registration of vehicle if applicable, and give EXACT LOCATION.
CODE 15	OFFICER REQUESTING ASSISTANCE - Transmit EXACT LOCATION and, if able, reason for request.
CODE 16	CRASH INVESTIGATION (state type) AT (location)
CODE 17	CLEAR – From a previous assignment completed and now back on patrol and/or original assignment and available.
CODE 18	PERMISSION TO LEAVE ASSIGNED PATROL - Transmit EXACT LOCATION, reason and estimated time of absence.
CODE 20	INVESTIGATION (state type) AT (location)
CODE 22	CELLULAR CALLER ADVISEMENT/NOTIFICATION
CODE 30	**OFFICER IN TROUBLE/ TRANSMIT EXACT LOCATION**

Subject	Number
Communications	**ADM-21**

Phonetic Alphabet

Members shall utilize the following phonetic alphabet.

A	Alpha	**N**	November
B	Bravo	**O**	Oscar
C	Charlie	**P**	Papa
D	Delta	**Q**	Quebec
E	Echo	**R**	Romeo
F	Foxtrot	**S**	Sierra
G	Golf	**T**	Tango
H	Hotel	**U**	Uniform
I	India	**V**	Victor
J	Juliet	**W**	Whiskey
K	Kilo	**X**	X-ray
L	Lima	**Y**	Yankee
M	Mike	**Z**	Zulu

References

National Incident Management System (NIMS) March 2004
MGL Chapter 6A
CMR 560 §3

Promulgated By:

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**ADM-22**

Subject

Court Attendance and Fees

Policy

Department employees shall comply with all court orders and summons.

Employees shall be compensated for court attendance according to their applicable collective bargaining agreements.

Definitions

Day Off: Any regularly scheduled day off, including a holiday or an administrative day off.

Vacation Day: A paid vacation day within an approved scheduled vacation week.

Nighttime Shift: A regular duty assignment to the evening or midnight shift.

Court Officers: Shall be designated by a Troop Commander as the Officer-in-Charge of Instruments for Breath Alcohol Testing and be the Keeper of Records for their jurisdiction's Breath Alcohol Testing Devices.

Documentation

All court appearances, depositions, or consultations shall be accurately documented by appropriate log entries in the Daily Administrative Journal (DAJ) including the following:

- Case name;
- Type of appearance;
- Time in/out; and
- Court location.

All court entries within the DAJ shall be reviewed daily by the Station/Unit Commander or designee.

Payment for Court Appearances

Members may be entitled to payment of a court fee for attendance at a state or federal court if the member is on duty at night, on vacation or furlough, or on a regularly scheduled day off and is a:

- Witness testifying in court on behalf of the Commonwealth or United States;
- Subpoenaed witness in criminal court testifying in an official capacity; or
- Defendant in court in a civil rights case in which the member was acting in an official capacity within the scope of employment.

Continued next page.

Payment for Court Appearances (Continued)

Members may not receive a court fee or additional pay when:

- They are not a witness for the Commonwealth;
- They are the plaintiff in a case; or
- They are a witness, on behalf of another Department member, not acting in an official capacity.

Note: Except when on an approved scheduled vacation week, no member shall be granted paid time off which conflicts with a scheduled court appearance, or would result in overtime being generated for the court appearance.

Witness Fees

Any member entitled to a court witness fee may receive and accept such fee, in lieu of but not in addition to, any other type of compensation (MGL c.262, s.50.)

Members shall not receive a court witness fee when:

- Any other type of compensation is received during the period of time of court appearance;
- Appearing at a second court during a time for which the member is still receiving compensation for their appearance at the first court attended;
- Working a day shift;
- On sick, injured, or extended leaves; or
- They are not a witness for the Commonwealth.

Travel Fees

Members may be entitled to a travel allowance from the court when:

- A private vehicle is used to travel to and from court held in a city or town other than a city or town in which the member resides.

Note: Travel allowance is only authorized from the actual point of origin and actual point of return from court attendance.

Members are not entitled to any travel allowance if:

- A state-owned vehicle is used;
- Receiving mileage allowance from any other government or private source; or
- Duplication of mileage occurs from more than one (1) court within one (1) day.

Court Fees

Court appearance fees shall:

- Be computed from the start of the appearance, or the member's actual arrival time, whichever is later, until the end of the appearance;
- Be consistent with Massachusetts General Laws and collective bargaining agreements, unless it overlaps with a member's other duties; and
- Not be paid for member's travel time to or from court.

Injured Leave Status

Members on injured leave subpoenaed to appear in court shall:

- Notify their immediate supervisor and the Court Officer who issued the SP 189 Court Appearance Notification;
- Request a continuance or reschedule the appearance through the court officer of jurisdiction; or
- If a continuance is not granted, request authorization to appear from the Troop/Section Commander or designee.

Temporary Modified Duty Status

Members on Temporary Modified Duty notified to appear in court shall:

- Notify their immediate supervisor and the Court Officer who issued the SP 189;
- Request a continuance or reschedule the appearance; or
- If a continuance is not granted, request authorization to appear from the Troop/Section Commander or designee.

Extended Leave Status

Members on extended leave subpoenaed to appear in court shall:

- Notify their immediate supervisor and the Court Officer who issued the SP 189;
- Request a continuance or reschedule the appearance through the court officer of jurisdiction; and
- Not appear in court on behalf of the Department.

Court Responsibilities

Position	Responsibilities
Employees	• Check the Department email system every work shift, to remain apprised of newly assigned court cases or status changes to pending cases; • Print any emailed SP 189 Court Card Notifications; • Submit complaint applications to the Court Officer of jurisdiction; • If a summons is received directly from an authorized agent of the court, immediately submit the hard copy to the Court Officer of jurisdiction and request a SP 189; • Have any SP 189's signed by the required parties, if any overtime hours are generated by a court appearance; • The SP 189 shall be date/time stamped by the Clerk's Office at the conclusion of the case, if more than four (4) hours of overtime are generated by any court appearance on any single calendar day; • Have the Assistant District Attorney sign the SP 189, including the actual time of the member's appearance, if a date/time stamp is not available;

Continued next page

Court Responsibilities (Continued)

Position	Responsibilities
Employees	• Notify the Court Officer of jurisdiction of any continuances and the parties who requested the continuance; and • Enter information on the case disposition, sign, and submit the SP 189 to their assigned Station/Section /Unit.
Court Officer	• Schedule employee's court appearances in an effort to minimize overtime; • Immediately enter information from summonses, continuances, or cancellations into the Department court database; • Issue the SP 189 for proceedings not scheduled by other Court Officers (e.g., Grand Jury, Superior Court, Federal Court, depositions); • Immediately advise affected employees of court case assignment and status changes to pending cases using all available methods; • Advise the Station/Unit Commander of any court case requiring the appearance of three (3) or more members; • Enter all disposition information into the Department court database; • Shall be the Officer-in-Charge of Instruments for Breath Testing Devices according to TRF-14 Operating Under the Influence of Alcohol, and function as the Keeper of the Records; • Provide the Commanding Officer with a weekly list of court notifications; and • Immediately notify their Commanding Officer if a member: 1. Fails to appear for a scheduled court date; or 2. Appears at court without prior notification by a Court Officer; or 3. Is notified to return to court for additional information required by the court during an arraignment.
Commanding Officers	• Review and reconcile all submitted SP 189's prior to approving PayStation court overtime submissions; • Deny any court overtime submitted on PayStation without a proper and signed SP 189; • Retain all submitted Station/Unit court appearance notification forms for inspection for three (3) years;

Continued next page

Subject	Number
Court Attendance and Fees	**ADM-22**

Court Responsibilities (Continued)

Position	Responsibilities
Commanding Officers	• Review requests for court appearances involving three (3) or more members as notified by the Court Officer and consult with the appropriate court authority to determine if any members appearance is not critical to the case; and • Notify the Troop/Section Commander or designee immediately if a member: 1. Fails to appear for a scheduled court date; or 2. Appears at court without prior notification by a Court Officer; or 3. Is notified to return to court for additional information required by the court during an arraignment.
Troop Cases and Report Officers	• Conduct examinations of submitted PayStation and SP 189's for signs of inefficiency or abuse; • Maintain staff supervision of the Court Officers and conduct semi-annual staff inspections of Court Officer's files; • Report inspection findings and analysis to the Troop Commander; and • Assist Court Officers in addressing problems at their assigned courts, or with conflicts between the courts and the Department.
Troop/ Section Commanders or Designee	• Contact the appropriate court authority to confirm the necessity of the appearance of three (3) or more members on the same day; and • Conduct examinations of submitted PayStation and SP 189's for signs of inefficiency or abuse.

Non-Field Sections/Units

Commanding Officers shall create court appearance guidelines appropriate for their Section/Unit and file a copy with the appropriate Division Commander.

References

ADM-11E Extended Leaves
SP 189 Court Appearance Notification
MGL c.262, s. 53B, 53C
SPAM Collective Bargaining Agreement Article 27

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 14, 2018	**ADM-24**

Subject

Department Radio Call Signs

Policy

The Department shall promote officer safety and efficiency using a standardized Radio Call Sign procedure.

Standardized Radio Call Signs, as referenced within this General Order, shall be used by all employees for all radio transmissions.

Protocol

Whenever a member requests information over the radio, such requests shall be preceded by or ended with the member's exact location.

All transmissions shall be conducted in a concise manner and in accordance with the formats indicated in this General Order. At the end of all transmissions, the receiving party shall acknowledge receipt of the transmission by saying "Received."

Call Sign Structure

The Department shall use the following categories for Radio Call Signs:

- The Executive Branch;
- The Executive Office of Public Safety and Security (EOPSS);
- The State Police Command Staff;
- Division Call Signs;
- Station Identifiers; and
- Specialty Vehicles.

Radio Call Sign Database

The Fleet Administrator shall:

- Maintain a database of assigned cruiser numbers, matching each cruiser number to a vehicle and employee; and
- Ensure Radio Call Signs assigned to Executive Branch, EOPSS, and Department Command Staff are included within the database.

Subject	Number
Department Radio Call Signs	**ADM-24**

Department Radio Call Signs

Department employees (sworn and civilian personnel), unless specifically identified within this General Order, shall:

- Use the Fleet Designated Cruiser Number assigned by the Fleet Administrator as their Radio Call Sign.

Employees assigned spare cruisers or pool vehicles shall:

- Use the assigned spare cruiser/pool vehicle's designated cruiser number as their Radio Call Sign; and
- Provide their name, Department ID number, and rank (if applicable).

Call Signs for the Executive Branch, EOPSS and Command Staff

The Department shall assign Radio Call Signs for the Executive Branch, EOPSS and Department Command Staff. The following Radio Call Signs shall be assigned:

Entity	Call Sign	Assignment
Executive Branch	S-1	Governor
	S-2	Lt. Governor
EOPSS	S-3	Secretary of Public Safety and Security
	S4-10	Available to EOPSS
Department Command Staff	1	Colonel/ Superintendent
	2	Lt. Colonel/ Deputy Superintendent
	3	Lt. Colonel/ Field Services
	4	Lt. Colonel/ Investigative Services
	5	Lt. Colonel/ Standards and Training
	6	Lt. Colonel/ Homeland Security and Preparedness
	7	Chief Administrative Officer
	10	Chief of Staff
	11-19	Majors -Division of Field Services (DFS), Non-Troop
	20-29	Majors and Detective Captains - Division of Investigative Services (DIS)
	30-39	Majors -Division of Standards and Training (DST)
	40-49	Majors and Detective Captains– Division of Homeland Security and Preparedness (DHS)
	50-59	Majors – Division of Administrative Services (DAS)

Division of Field Services

The Division of Field Services (DFS) shall adhere to the following protocol:

Troop Headquarters shall use the appropriate troop phonetic identifier preceded by the word "Station" as the radio call sign e.g., "Station H to 756." Sub-Stations shall use the appropriate phonetic identifier followed by the assigned numerical designation e.g., "B-1", "D-2" (Troops and Sub-Stations along with their corresponding phonetic identifiers are listed below in the "**Troop and Sub-Station Call-Sign**" table.)

Specialty vehicles shall be identified through Radio Call Signs as the name of the unit followed by the assigned number of the vehicle e.g., "Cycle 5."

All DFS personnel shall utilize their Fleet Designated Cruiser Number as their Radio Call Sign, except as follows:

Troop Commander:
- Number one (1) attached to the phonetic troop identifier e.g., "1A;"

Troop Executive Officer:
- Number two (2) attached to the phonetic troop identifier e.g., "2A;"

Troop Captains:
- Numbers three (3) through five (5) attached to the phonetic troop identifier, e.g., "3A," "4A," or "5A;"

Operations Officers:
- Numbers six (6) through eight (8) attached to the phonetic troop identifier, e.g., "6A," "7A," or "8A;"

Station Commanders:
- In numeric sequential order, beginning with the number 11 attached to the phonetic troop identifier e.g., "11A" for the Station Commander of A-1 and "15A" for the Station Commander of A-5; and

Special Operations Troop "S" Commanders shall be identified as:
- Special Operations Captains (2-4) e.g., "2S," or "3S," etc.;
- STOP Team Commander- "5S;"
- SERT Commander- "6S;"
- CVES Commander- "1T;" and
- Canine Unit Commander- "1K."

Personnel assigned to Troop F, the Commercial Vehicle Enforcement Section, and the Canine Unit, shall use:
- Their assigned Authority cruiser number or their Fleet Designated Cruiser Number as their Radio Call Sign, followed by the phonetic identifier "F," "T," or "K" respectively, e.g., "121F," "221T," or "437K."

The Division of Field Services Commander or designee shall ensure that the Radio Call Sign Database is updated accordingly for changes made to personnel within the Division.

Subject	Number
Department Radio Call Signs	**ADM-24**

Troop and Sub-Station Call Signs

A	**Danvers HQ**
A-1	Andover
A-2	Newbury
A-3	Concord
A-4	Medford
A-5	Revere
A-6	Danvers (sub-station)

B	**Northampton HQ**
B-1	Lee
B-2	Shelburne Falls
B-3	Springfield
B-4	Cheshire
B-5	Russell
B-6	Northampton (sub-station)
B-7	Shelburne Falls (dispatch)
B-8	SP Westfield

C	**Holden HQ**
C-1	Athol
C-2	Millbury
C-3	Brookfield
C-4	Leominster
C-5	Sturbridge
C-6	Holden (sub-station)
C-7	Belchertown
C-8	New Braintree (dispatch)
C-9	Devens
C-10	SP Charlton

D	**Middleboro HQ**
D-1	Norwell
D-2	Yarmouth
D-3	Dartmouth
D-4	Middleboro (sub-station)
D-5	Oak Bluffs
D-6	Nantucket
D-7	Bourne

F	**Logan Airport HQ**

G	**General Headquarters, Framingham**

H	**South Boston HQ**
H-1	Government Center
H-2	Framingham
H-3	Foxboro
H-4	Boston
H-5	Brighton
H-6	South Boston (sub-station)
H-7	Milton
H-8	SP Weston
H-9	SP Tunnels

Subject	Number
Department Radio Call Signs	**ADM-24**

Division of Investigative Services

Radio Call Signs for Section/Units Members within the Division of Investigative Services (DIS), who make radio transmissions over the Troop Radio System, shall:

- Use plain language one word unit name followed by their assigned Fleet Designated Cruiser Number e.g., "Middlesex 1234 to Station A" or "VFAS 4321 to Station H".

Section/Unit Commanders/Executive Officers within DIS shall:

- Be assigned specific Radio Call Signs for their sections and units;
- Use the number "1" for the Commanding Officer preceded by the section/unit name e.g., "Middlesex 1 to Station A";
- Use the number "2" for the Executive Officer preceded by the section/unit name e.g., "VFAS 2 to Station H".

The Division Commander, the Division Majors, and Detective Captains are designated call signs in accordance with the "Department Command Staff" table on page 2 of this General Order.

The DIS Commander or designee shall ensure that the Radio Call Sign Database is updated accordingly for changes made to personnel within the Division.

Division of Standards and Training

The Division of Standards and Training personnel shall utilize:

- Their Fleet Designated Cruiser Number as their Radio Call Sign.

The Division Commander and the Division Major(s) are designated call signs in accordance with the "Department Command Staff" table on page 2 of this General Order.

Division of Administrative Services

The Division of Administrative Services personnel shall utilize

- Their Fleet Designated Cruiser Number as their Radio Call Sign.

The Division Commander and the Division Major(s) are designated call signs in accordance with the "Department Command Staff" table on page 2 of this General Order.

Division of Homeland Security and Preparedness

Radio Call Signs for Section/Units Members within the Division of Homeland Security and Preparedness (DHS), who make radio transmissions over the Troop Radio System, shall:

- Use plain language one word unit name followed by their assigned Fleet Designated Cruiser Number e.g., “Compliance 1234 to Station A”.

Section/Unit Commanders/Executive Officers within DHS shall:

- Be assigned specific Radio Call Signs for their sections and units;
- Use the number “1” for the Commanding Officer preceded by the section/unit name e.g., “Compliance 1 to Station A”;
- Use the number “2” for the Executive Officer preceded by the section/unit name e.g., “Compliance 2 to Station H”.

The only two exceptions to this are as follows:

- The Air Wing Commanding Officer will utilize “Whiskey 1” and the Marine Unit Commanding Officer will utilize “Mike 1”; and
- The Air Wing Executive Officer will utilize “Whiskey 2” and the Marine Unit Executive Officer will utilize “Mike 2”.

The Division Commander, the Division Majors, and Detective Captains are designated call signs in accordance with the “Department Command Staff” table on page 2 of this General Order.

The DHS Commander or designee shall ensure that the Radio Call Sign Database is updated accordingly for changes made to personnel within the Division.

GHQ/ COMSEC

The General Headquarters / Communications Section shall be identified with the phonetic letter “G.”

Specialty Vehicles

Specialty vehicles shall be identified through Radio Call Signs as:

- Name of the unit followed by the assigned number of the vehicle e.g., Marine 1, Air 3, and/or Cycle 5.

Portable Radio Call Signs

Members with a Fleet Designated Cruiser Number shall use that number when transmitting on the portable radio.

Members without a Fleet Designated Cruiser Number shall announce their name, rank, and ID number, if needed, while transmitting on the portable radio e.g., members who are assigned to Troop "F".

Subject	Number
Department Radio Call Signs	**ADM-24**

Incident Command

The National Incident Management System (NIMS) has integrated existing best practices into a consistent, nationwide approach to domestic incident management at all jurisdictional levels and across functional disciplines.

Department member(s) involved at a critical incident with multiple agencies shall use a clear spoken message, based on common terminology.

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 14, 2018	**ADM-25**

Subject

Paid Details

Policy

The Department may allow personnel, on full duty status or alternative duty status (as specified in ADM-11C Maternity Leave and Guidelines), to work paid details.

The Department recognizes the importance of maintaining safe and efficient traffic flow at roadway work sites and special events. The Department also recognizes that at major sporting, civic, special events, and other times, members may be required to provide crowd control and/or security.

Paid details may be worked by members:

- From the rank of Trooper through Detective Lieutenant inclusive; and/or
- From the rank of Captain/Detective Captain with approval of the Deputy Superintendent when:

1. The type of detail is "non-construction" i.e., stadium events, security details, in a supervisory capacity where they must supervise at least ten (10) officers; or
2. A vacancy exist on any type of detail after the primary and secondary detail lists of the respective troop have been completely exhausted of eligible members.
   Note: Once assigned to a detail, Captains/Detective Captains shall not be bumped by:
   - another commissioned officer; or
   - a non-commissioned officer or trooper within twenty-four (24) hours of the start time of the assigned detail.

Definitions

Paid Detail (detail): A voluntary assignment paid for by an outside entity, which has been authorized by the Colonel/Superintendent.

Scheduled Work Hours: A regular shift or tour of duty consisting of eight and one-half (8.5) hours.

Work: Shall be defined to include hours actually worked during regularly scheduled duty, overtime, court time and paid details.

Hours of Work

Members shall not schedule or work combinations of assignments and/or details which they know or should know will result in a direct violation of the "sixteen and one-half (16.5) hour rule" as contained within the Collective Bargaining Agreement (CBA) and this General Order (as further clarified in Superintendent's Memo *13-SM-10 Extension to the 16.5 Hour Rule Limitation*.)

Members shall not accept a detail if doing so would require the member not to work a regularly scheduled shift or attend other work obligations of which the member is aware.

Members shall not cancel a detail in order to accept another detail or overtime assignment.

In the event the detail hours exceed the hours of work allowed in any twenty-four (24) hour period, the member shall not be allowed to alter the starting time of their next assigned work shift, but shall use accrued personal leave or vacation leave credits to offset any conflicts with their scheduled work hours.

Members shall be paid for details in conformance with their applicable collective bargaining agreement.

A member shall receive time and one-half Detail pay for the actual hours worked on the calendar day of Thursday, Thanksgiving Day or December 25, Christmas Day.

Overlapping Time

Overlapping detail hours of any kind is strictly prohibited.

In order to prevent any overlapping of scheduled work hours, members shall utilize accrued personal or vacation leave to offset any overlap in conformance with the member's collective bargaining agreement.

Travel Time

Members are required to use at a minimum, one-half (1/2) hour of accrued personal or vacation leave as travel time to or from a detail when one of the following occurs:

1. The travel time overlaps with their scheduled work hours; or
2. The travel time from the duty assignment to the paid detail location, or the paid detail to a duty assignment location, is **greater** than one-half (1/2) hour.

   Note: Members not assigned to a specific sub-station, the geographical boundary for a section/unit is defined as the station of jurisdiction where their **regular reporting** location is sited. Temporary Duty Assignments (TDY) work locations shall be considered as the member's regular reporting location for administration of this General Order.

Continued next page.

Travel Time (Continued)

When a member is assigned to a paid detail they shall:

- Determine the need to use accrued personal or vacation leave to ensure prompt arrival to a detail or when reporting for their tour of duty assignment; or
- Decline the detail if they chose **not to use** the appropriate accrued personal or vacation leave.

Supervisors shall be held responsible:

- To ensure members are held accountable for taking appropriate accrued personal or vacation leave when reporting to or from a paid detail, if it effects their regular tour of duty assignment; and
- To ensure members accurately document and record accrued personal or vacation leave used for travel time to or from a paid detail when **greater** than one-half (1/2) hour.

Requests

Members shall not:

- Make duplicate/same day requests for details in different Troops; or
- Request or work overtime or details within twenty-four (24) hours from the start time of their regularly scheduled work shift when sick leave was taken for:
  1. Personal illness or injury;
  2. The presence of the member at their work location would jeopardize the health of others, through exposure to a contagious condition; or
  3. The member's spouse, child, parent, or spouse's parent, or relative living in the member's household, is seriously ill. In this event, a limit to the amount of leave the member can use is set by the CBA and federal and state laws.

Exception: A member who works at least four (4) or more consecutive hours of their regularly scheduled work shift, in which Sick Leave was granted as outlined in ADM-11 Sick Leave, shall remain eligible to work paid details and overtime.

Members may request only one troop as a primary choice on a SPD-3 Request for Paid Detail form. The primary choice for:

- Members assigned to Field Operations within the Division of Field Services shall be limited to the troop to which they are assigned, or to the troop where they reside;
- Members assigned to the Division of Field Services, but not assigned to a troop within Field Operations, may request any troop as their primary choice; and
- Troop F is reserved for members assigned to: Troop F, Office of the Superintendent, Division of Field Services (see above), Division of Administrative Services, Division of Investigative Services, Division of Standards and Training, and the Division of Homeland Security and Preparedness.

The SPD-3 shall be forwarded to the Paid Detail Officer of jurisdiction prior to the first of March each year or upon transfer.

Continued next page.

Requests (Continued)

Weekly requests for assignments shall be made according to a procedure approved by the Troop Commander. When requesting a detail, a member shall report all out-of-troop details worked for the previous five (5) weeks to the Paid Detail Officer of Jurisdiction.

Member Responsibilities

Members assigned to a road construction type detail shall maintain a professional presence and shall perform the following duties:

- Provide public and site safety;
- Be aware of, and visible to, oncoming traffic;
- Maintain uniform traffic flow through manual direction or other devices as necessary;
- Stand, facing traffic, unless otherwise directed or authorized;
- Wear proper field uniform and assigned traffic vest or raincoat with high visibility side out;
- Remain on the work site, except to perform enforcement duties, or at the direction of the state engineer, site foreman, appropriate authority, or in case of personal necessity; and
- Maintain radio contact with Troop of jurisdiction.

If radio contact is not possible with the Troop of jurisdiction then contact the nearest troop or station.

If more than one member is assigned to a detail then the members shall:

- Position themselves uniformly throughout the site or as directed by the state engineer, site foreman, or appropriate authority; and
- Dress alike, in the duty uniform of the day, or as prescribed by the officer-in-charge (OIC).

Members shall:

- Arrive and depart at the times posted and/or prescribed by the Paid Detail Officer, state engineer, site foreman, or appropriate authority;
- Reflect on the SPD-2 Paid Detail form:
    1. Detail's assigned hours;
    2. The actual hours worked while on the detail;
    3. The scheduled work shift for the day, if applicable; or
    4. The scheduled day-off for the day, if applicable; or
    5. The accrued time-off credits used to work the detail, if applicable.
- Enter into PayStation the detail information including the total amount of hours to be paid; and
- Enter into the Paystation "Comments" field the detail start and end time and the actual hours worked.

Continued next page.

Member Responsibilities (Continued)

Members assigned to a detail shall complete and submit a copy of the SPD-2 to both:

- The Paid Detail Officer of jurisdiction; and
- The supervisor authorizing the member's PayStation entries.

When a member is assigned a detail outside of that member's primary troop choice, the member shall make a photo copy of the SPD-2 and forward the copy to the member's primary Troop Detail Officer.

Failure to adhere to the requirements outlined in this General Order shall constitute unsatisfactory performance and the member may be disciplined under the Department Rules and Regulations. In such instances, the member may be removed from all detail lists until final disposition of the formal disciplinary process.

Supervisory Responsibilities

All supervisory personnel shall:

- Monitor all members assigned to details;
- Immediately address and remedy all observed violations of this General Order; and
- Document all violations on the SP 381 Paid Detail Inspection form, prior to the end of that shift.

The supervisor approving a member's weekly PayStation entry shall:

- Review the member's submitted SPD-2;
- Review the weekly entries made by the member in PayStation;
- Ensure that the submitted SPD-2 corresponds correctly to the PayStation weekly entries;
- Require the member to use accrued personal or vacation leave in order to ensure compliance with this General Order; and
- Report all violations of hours to their Commanding Officer.

Troop Commanders

Troop Commanders are directly responsible for the administration and supervision of this General Order and shall assign a supervisor to:

- Conduct inspections of detail sites within the Troop jurisdiction; and
- Submit SP 381 forms with all applicable findings.

Troop Commanders/Duty Officers of jurisdiction over the detail shall only authorize members to work in excess of 16.5 hours when:

- An emergency situation has arisen that requires the members' presence; or
- The member is on their last scheduled work day; or
- The member is on a day off and has no scheduling conflict.

Extension to the 16.5 Hour Rule

The Troop Commander or Troop Duty Officer of jurisdiction over the detail may grant an extension in order to allow member(s) to extend beyond the sixteen and one-half (16.5) hour limit under the following conditions:

- Member(s) shall not be granted more than one extension to the 16.5 hour rule in any forty-eight (48) hour period; and
- No more than a two (2) hour extension shall be granted without the member being required to take paid leave time, (vacation, personal), to ensure adequate rest before the start of their next assignment.

In no event shall the maximum number of weekly work hours as allowed by the Collective Bargaining Agreement be exceeded. Please refer to Superintendent's Memo *13-SM-10 Extension to the 16.5 Hour Rule Limitation* for further clarification.

Troop Inspections

The Troop Executive Officer shall maintain all SP 381 forms and ensure that those forms indicating unsatisfactory performance are brought to the attention of the Troop Commander.

Troop Inspections shall include:

- Site, time, members present, overall appearance, adherence to General Order;
- Verification of assigned members arrival and departure times with both SPD-2 and state engineer and/or site foreman; and
- Detail violation(s), if any.

Staff Inspections

Staff Inspectors shall conduct random inspections of detail sites and submit written reports to the appropriate Troop Commander of findings and recommendations to include:

- Site, time, members present, overall appearance, adherence to General Order;
- Verification of assigned members arrival and departure times with both SPD-2 and state engineer and/or site foreman;
- Detail violation(s), if any;
- Audit of actual and overall hours worked by assigned members; and
- Audit of Paid Detail Office.

Administration

Troop Commanders shall assign a supervisor as the Paid Detail Officer.

The Paid Detail Officer shall:

- Work an administrative day shift;
- Process requests for details;
- Determine and/or verify personnel assignments, arrival, and departure times;
- Maintain a primary list of eligible members updated according to personnel transfers, requests, and so forth;

Continued next page.

Administration (Continued)

- Establish and post, in the Troop Duty Office, an availability list according to details accrued and seniority for filling cancellations/vacancies;
- Establish a secondary list to fill overages;
- Post all detail assignments within jurisdiction not less than thirty-six (36) hours prior to the commencement of that week's details, except in the event of late scheduled details;
- Be responsible for all billing, payroll, and accounts receivable activities as they pertain to details; and
- Immediately notify the Legal Section if informed that a contractor has filed for bankruptcy protection or is going out of business.

Member assignments shall be made:

- From the primary list;
- According to the number of detail hours accrued within the previous five (5) weeks, and then by seniority;
- From the availability list if a cancellation occurs; and
- As close to the member's residence as reasonably possible.

Cancellations shall be made by assigned members:

- To the Paid Detail Officer, or the Troop Duty Officer of jurisdiction if the Paid Detail Officer is unavailable; and
- At least, twenty-four (24) hours in advance of assignment.

Cancellations and/or refusals by members, for reasons other than personal illness or official duties, shall count as a detail worked. In cases where details are cancelled because of court, the member shall provide a copy of a signed SP 189 Court Card to the respective Paid Detail Officer.

Cruisers

The Paid Detail Officer with the approval of the Troop Commander shall determine the number of vehicles at details.

Marked and unmarked vehicles shall:

- Have working emergency lighting activated, when appropriate;
- Be conspicuously and strategically placed between oncoming traffic and the work site; and
- Be properly fueled prior to the detail.

Undercover vehicles shall not be used at road construction sites.

Subject	Number
Paid Details	**ADM-25**

Commercial Motor Vehicle Escort Details

Prior to an escort detail, a member assigned to the Commercial Vehicle Enforcement Section, or the member assigned to the detail, shall inspect all oversized or overweight loads for:

- Permits;
- Load security;
- Vehicle condition; and
- Operator qualifications.

Breaks

To minimize impact on the work site, breaks shall be taken:

- At scheduled times in conjunction with vendor's/contractor's scheduled breaks; and
- Out of public view whenever possible.

References

ADM-11 Sick Leave
ADM-11C Maternity Leave and Guidelines
10-SM-04 Rank of Captain and Detective Captain Working Paid Details
13-SM-10 Extension to the 16.5 Hour Rule Limitation
SPD-2 Paid Detail Form
SPD-3 Request for Paid Detail Form
SP 189 Court Card
SP 381 Paid Detail Inspection Form

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 25, 2020	**ADM-26**

Subject

Military Service

Purpose

To establish and define military service protocols for Department of State Police personnel.

Policy

The Department shall allow sworn and civilian employees who are members of a Reserve Component of the United States Armed Forces (i.e. the Army National Guard of the United States, the Air National Guard of the United States, the Army Reserve, the Navy Reserve, the Marine Corps Reserve, the Air Force Reserve, and the Coast Guard Reserve) to attend drills and other training as required.

The Department shall allow employees who are members of the Massachusetts Army and Air National Guard, called to emergency/contingency duty in the service of the Commonwealth, to perform their required duties in accordance with the provisions of M.G.L. c.33, Sections 38, 40, 41, 59, 59A, 60 and 61, and perform duties under Title 10 and 32 of the United State Code.

The Department shall allow employees who are members of the Army and Air National Guard of other states or U.S. territories, to perform active duty as required by the proper authority of the other state or territory.

The Department shall support and facilitate the transition of employees who are called to active service under Title 10 and Title 32 of the United States Code (USC) upon their activation/mobilization as well as their return from active duty. This will ensure that the employee is treated fairly and equitably in accordance with all applicable federal and Massachusetts state law pertaining to their service and employment rights.

Notifications

Employees shall notify Station, Section and/or Unit Commanders of Inactive Duty Training Drill (IDT Drill), Annual Training, emergency/contingency activation/mobilization, as well as any other service obligations that conflict with regular work schedules with as much advance notice as possible.

Notifications Procedure

1. All military orders, yearly drill schedules and military leave earning statements (LES) shall be submitted via email to polmilitaryleave@massmail.state.ma.us immediately upon your notification of military activation if eligible for pay difference during any portion of that military service.

Continued next page.

Notifications Procedure (Continued)

2. All military service orders and drill schedules will be reviewed by the Department's Human Resources Military Service Coordinator. Based on the military orders submitted, instructions will be provided to the employee and supervisor to ensure the proper weekly time reporting codes are utilized during the employee's military service. Payroll will not process any paid Military Service selections in the time reporting system without having received current military orders or drill schedules.
3. Until documentation is received and reviewed by the Human Resources Military Service Coordinator, the employee's payroll status will be "Military Leave/No Pay." Additionally, timely notice of pending military service shall be made through the chain of command via a "To/From." The notice shall include:
    - The timing and purpose of said service;
    - Reference of any applicable law; and
    - A copy of official orders or correspondence on official letterhead.
4. In the event the employee has not received written orders in hand, he/she shall submit their notification through the chain of command to the Office of the Superintendent/Deputy Superintendent and polmilitaryleave@massmail.state.ma.us with the following additional information:
    - The name and rank of the military commanding officer;
    - A contact phone number for such commanding officer; and
    - Notice that written orders will be forthcoming.

Time Reporting

Employees on Military Leave With or Without Pay shall be placed on an administrative schedule (i.e. a 5 & 2 schedule) for the duration of any individual or consecutive leaves in excess of thirty (30) consecutive/calendar days. All pertinent station, section and/or unit records must reflect such schedule. Please note that employees who are performing annual training, drill or related assemblies do not require this schedule change.

Station, Section and /or Unit Commanders shall ensure that the appropriate notations are entered into the time reporting system to reflect the employee's military leave/work status if the employee is unavailable to do so.

Authorized Leave

Refer to the accompanying <u>ADM-26 Military Leave – Matrix</u> that is incorporated into this policy.

Department Work While on Military Leave

While an employee is on a military leave of any duration, he/she:

- Is deemed to be separated from service with the Department; and
- Shall not work any overtime assignments, detail assignments, or be compelled by the Department to perform any other function on behalf of the Department or in the capacity of a Department employee.

Subject	Number
Military Leave	**ADM-26**

Leave Accrual, Seniority, and Other Pay Considerations for Employees on Military Leave

Employees who are called to military service that qualifies them for Military Leave With Pay (pursuant to M.G.L. c. 33, Sections 38,40 or 41) or Without Pay (under Title 10 or 32 USC or for service with the National Guard of another state or U.S. territory pursuant to M.G.L. c. 33, Section 13), shall:

- Retain all employment rights as stipulated in federal and Massachusetts state law;
- Suffer no loss of Department seniority or for retirement purposes;
- Continue to accrue all regularly accrued paid leave time (sick, vacation, and personal leave) as though still present for duty;
- Leave accrued while on active military leave status cannot be applied to that same unpaid military leave;
- Leave accrued while on active military leave status cannot, upon the employee's return to work, be applied retroactively to result in compensation for previously unpaid leave time;
- Employees on military leave without pay may request to use compensatory time and paid leave time accrued prior to the onset of the military leave without pay as a substitute for unpaid leave, provided that the employee does not qualify to receive pay difference. Such use of compensatory time earned and accrued leave shall be in accordance with regularly applied rules for use as set forth in the applicable CBA and Policies & Procedures;
- Personal leave accrued while on military leave remains use/lose time for that calendar year. There is no carry-over of personal leave;
- Vacation leave accrued while on military leave remains subject to annual carryover rules per the applicable CBA and state policies; and
- Employees on military leave with pay are only entitled to pay for benefits that are seniority based, not performance based, unless otherwise specified in the applicable CBA. (ex: shift differential, weekend differential, commuting differential, on-call or stand-by pay, clothing allowance, etc.).

Holidays and Administrative Days Off for Employees on Military Leave

Employees in the armed forces of the Commonwealth on Military Leave With Pay due to activation under M.G.L. c. 33, s. 38, 40 and/or 41 shall receive holiday pay as regularly compensated per the applicable CBA and state policies, however they shall not be eligible to accrue compensatory time or "holidays owed". On the Commonwealth's day of observance, the payroll code for Holiday – Did Not Work shall be entered into the time reporting system and recorded accordingly in station, section and unit records for the employee.

In accordance with the applicable CBA and state policies, employees who are on Military Leave Without Pay shall not receive holiday pay and are therefore are not eligible for accrual of compensatory time or "holidays owed" for legal holidays that occur while the employee is in leave of absence without pay status. Please be advised that the military pay difference for an employee in Military Leave Without Pay status does include compensation for holidays that occur during the leave period.

Administrative Days Off (ADOs) are equivalent to Days Off Regular and shall not be accrued.

Subject	Number
Military Leave	**ADM-26**

Time Limit for Return to Work

Time limits for returning to work from military service depend on the duration of the orders. The rules are:

Service of 1 – 30 days: the beginning of the next regularly scheduled work period on the first full day following completion of service and expiration of an eight-hour rest period.

Service of 31 – 180 days: application for reinstatement to duty through chain of command in To/From format to the Office of the Superintendent/Deputy Superintendent shall be submitted not later than 14 days after completion of military duty.

Service of 181 or more days: application for reinstatement to duty through chain of command in To/From format to the Office of the Superintendent/Deputy Superintendent shall be submitted not later than 90 days after completion of military duty.

In the event an employee does not return to work in a timely manner, he/she is subject to the Department's Rules and Regulations, Policies and Procedures, and applicable provisions of CBA for unauthorized absences.

Requirements for Return to Department Service

Sworn members returning from any military leave that exceeds one year shall be required to successfully complete:

- A background investigation;
- A medical examination, to include drug testing, by the State Police Surgeon;
- Psychological testing; and
- A training evaluation by the Commandant of the Academy and any training required by him/her.

Civilian employees returning from any military leave that exceeds one year shall be required to successfully complete:

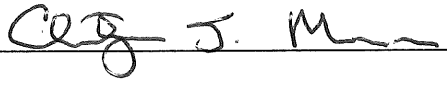
- A background investigation;
- A medical examination, to include drug testing, by the State Police Surgeon;
- Psychological testing; and
- Retraining, as determined by the employee's supervisor or the Human Resources Director.

References

MGL c.33, Sections 38, 40, 41, 59, 59A, 60, and 61
Title 10 USC, c. 11, §270 Title 32 USC (National Guard)
Title 38 USC, c. 43, §§4301-4333 (USERRA)
National Defense Act of 1933
NAGE Units 1, 3 and 6-Commonwealth CBA, Article 8, §6 AFSCME Unit 2-Commonwealth CBA, Article 8, §7 MCOFU Unit 4-Commonwealth CBA, Article 8, §6 SPAM Unit 5A-Commonwealth CBA, Article 8, §2.c., Article 38, §§3 and 4 MOSES Unit 9-Commonwealth CBA, Article 8, §6
Rules Governing Paid Leave for Managers and Confidential Employees (HRD Red Book)

[1] Pursuant to MGL c. 33, s.59 (a) employees of the Commonwealth "shall be entitled to receive pay without loss of ordinary remuneration as a public employee during service in the uniformed services, annual training under section 60 or drills and parades under section 61, not exceeding 40 days in any federal fiscal year, and shall not lose any seniority or any accrued vacation leave, sick leave, personal leave, compensation time or earned overtime." The proviso of 40 days is the maximum amount of paid military days that may be used by a Commonwealth employee in the service of a reserve component of the armed forces of the Unites States – to include the Army or Air National Guard of any state or territory under the jurisdiction of the United States – to cover absences due to military service for the period of October 1 to September 30 of any given year.

Promulgated By:



Massachusetts State Police
ADM-26 Military Leave – Matrix

Reserve Component and Duty Status	Entitled to Pay Difference Per M.G.L. c. 33, §59?	Entitled to Accrue VAC/SIC/PER & Holiday Pay?	How Is The Employee Paid While On Military Leave?	SHORTCUT
MA NATIONAL GUARD Activation under Title 10 or 32 USC Includes Annual Training – AT,[1] Drills, IDT[2], military schooling, and other calls to active duty for members of a reserve component of the armed forces of the United States	YES	VAC/SIC/PER YES Holiday Pay NO[3] (See footnote on pay difference)	Per M.G.L c. 33, §59 (a), employees may use Military Leave with Pay for up to 40 paid days per federal fiscal year (i.e. 10/1 - 09/30) to cover time off from work for duty under Title 10 or Title 32. Per M.G.L c. 33, §59 (c), employees who are called to active duty under Title 10 or 32 are eligible for the pay difference from Day 1 of active duty. They may opt to defer receipt of the pay difference in order to use some or all of their 40 paid days first.	Up to 40 paid WORK days only for AT, Drills, IDT, military schooling and related activities, *and/or* paid leave accrued prior to the active duty orders per the cba; *then* pay difference
MA NATIONAL GUARD State Active Duty under MGL c. 33, §§38, 40 or 41	YES	VAC/SIC/PER YES Holiday Pay YES for holidays in the first 30 consecutive/ calendar days or pay difference	Per M.G.L. c. 33, §59 (b), employees may use Military Leave with Pay for the first 30 consecutive/calendar days of leave (*not DOR/ADOs in those 30 calendar days*). They are eligible for the pay difference after the first 30 consecutive/calendar days. The 40 days under Section 59(a) and (c) for activation under Title 10 or 32 USC are *not* eligible to be used for this military status.	Pay for WORK days only in the first 30 consecutive/ calendar days; *then* paid leave accrued prior to the active duty orders per the cba *or* pay difference
NATIONAL GUARD **Other U.S. States & Territories** State Active Duty by other U.S. State/ Territory	NO	VAC/SIC/PER NO Holiday Pay NO	Employees in this status cannot receive military pay from this Department nor can they use any Military Leave With Pay (to include the 40 paid days) to cover their absence from work. Employees receive pay from the National Guard of the U.S. state or territory for which they have been activated. They may use other paid leave credits per the cba (e.g. VAC, PER) acquired prior to the start of the military leave to cover time off payroll.	Unpaid Military Leave only. No paid military time permitted. May use paid leave accrued prior to the active duty orders per the cba

[1] 32 U.S. Code §503(a)(2) and §503c provides further clarification for training and duty.

[2] 32 U.S. Code §502b-502e provides definitions for assemblies and drills.

[3] Please be advised that the military pay difference for an employee in Military Leave Without Pay status does include compensation for holidays that occur during the leave period.

Massachusetts State Police
ADM-26 Military Leave – Matrix

Reserve Component and Duty Status	Entitled to Pay Difference Per M.G.L. c. 33, §59?	Entitled to Accrue VAC/SIC/PER & Holiday Pay?	How Is The Employee Paid While On Military Leave?	SHORTCUT
NATIONAL GUARD & U.S. Reserve Units **Other U.S. States & Territories** Activation under Title 10 or 32 USC Includes Annual Training – AT, Drills, IDT, military schooling, and other calls to active duty for members of a reserve component of the armed forces of the United States	YES	VAC/SIC/PER YES Holiday Pay NO (See footnote 3 on pay difference)	Per M.G.L c. 33, §59 (a), employees may use Military Leave with Pay for up to 40 paid days per federal fiscal year (i.e. 10/1 - 09/30) to cover time off from work for duty under Title 10 or 32. Per M.G.L c. 33, §59 (d), **employees in this status are eligible for the pay difference only if on orders to duty for 31 or more consecutive days**. Before receiving the pay difference they may opt to use some or all of their 40 paid days - or other leave credits per the cba (e.g. VAC, PER) acquired prior to the start of the military leave - to cover time off payroll.	Up to 40 paid WORK days only for AT, Drills, IDT, military schooling and related activities; *and/or* paid leave accrued prior to the active duty orders per the cba; *then* pay difference
	NO		• Employees whose orders to active duty for **30 consecutive days or less** may opt to use their 40 paid days, or other leave credits (ex: VAC,PER) per the cba acquired prior to the start of the military leave to cover time off the payroll. Otherwise, they shall be Military Leave Without Pay. (Employees are not eligible for pay difference with orders of this duration.)	***30 consecutive days or less*** Up to 40 paid WORK days if employee chooses, *and/or* paid leave accrued prior to the active duty orders per the cba; *then* Military Leave Without Pay.
	YES		• Employees whose orders to duty for **31 consecutive days or more** may opt to use their 40 paid days, other leave credits (ex: VAC, PER) per to cba acquired prior to the start of the military leave, or pay difference from day 1 of the military leave.	***31 consecutive days or more*** Up to 40 paid WORK days if employee chooses, *and/or* paid leave accrued prior to the active duty orders per the cba; *or* pay difference anytime from day 1 on.

Department of State Police
General Order

Effective Date	Number
May 21, 2018	**ADM-27**

Subject

Transfers

Policy

In order to maintain and enhance the operational functions of the Department, transfers may be made to:

- Ensure adequate staffing levels;
- Provide efficient public safety services; and
- Meet other goals and objectives of the Department.

Transfer Restrictions

Troopers assigned to the Division of Field Services, who have three (3) or fewer years of creditable service shall not be considered for any job posting or positions outside of the Division of Field Services.

This restriction does not preclude the Colonel/Superintendent from assigning troopers with three (3) or fewer years of creditable service to positions outside of the Division of Field Services based upon specific expertise (e.g. language skills, etc.) which a trooper may possess.

Troopers with five (5) or more years of creditable service may bid on positions within the Division of Field Services-Field Operations pursuant to the Collective Bargaining Agreement.

Biddable Assignments

Biddable Assignments: All assignments established as a biddable assignment pursuant to the Collective Bargaining Agreement.

Non-Biddable Assignments

Non-biddable Assignments: All assignments not otherwise established as a biddable assignment pursuant to the Collective Bargaining Agreement.

Department non-biddable assignments include, but are not limited to:

- Division of Investigative Services;
- Division of Administrative Services;
- Division of Standards and Training;
- Division of Homeland Security and Preparedness;
- Division of Field Services pursuant to the Collective Bargaining Agreement, and
- Office of the Superintendent.

Due to the specialized nature of these assignments, and the knowledge and skills required, these positions require a selection process.

Request for Transfer: Biddable Assignments

Members who request a transfer to a biddable assignment within the Division of Field Services shall:

- Submit an electronic transfer request.

Only those requests received at least twenty-one (21) days prior to the end of a fifty-six (56) day bid cycle shall be considered for the next fifty-six (56) day bid cycle.

Members are allowed to have only one (1) transfer request for a biddable assignment at any time.

The Human Resources Section shall publish a list of transfer requests for the Division of Field Services on Docushare containing the requesting member's name, current assignment, request, and seniority. Two (2) lists shall be maintained: one (1) list for troopers and one (1) list for supervisors.

Note: Requests for transfers to a biddable assignment within the Division of Field Services shall remain on file until honored or withdrawn.

Request for Transfer: Non-Biddable Assignments

Members who request a transfer to a non-biddable assignment within the Department shall submit the following to Human Resources Section:

- A To/From;
- A resume; and
- Any other materials required within the posting.

The member shall forward a copy of the above items to:

- Their current Commanding Officer; and
- The Commanding Officer of the requested section/unit.

Requests for transfer to a non-biddable assignment shall not be kept on file at the Human Resources Section. All requests shall be submitted within the specified time periods of the posting.

Members who request a transfer to a non-biddable assignment within their respective troop or station shall submit the following to the Troop Commander:

- To-From;
- Resume; and
- Any other materials required within the posting.

Posting and Selection Process: Non-biddable Assignments

Vacancies for non-biddable assignments for members shall be posted for at least ten (10) calendar days on Docushare.

Providing that the minimum qualifications are met, members may apply to:

- Department non-biddable assignments;
- Troop non-biddable assignments when the member is assigned to the troop; and
- Station non-biddable assignments when the member is assigned to the station.

Each posting shall include:

- Assignment, location, and work schedule;
- Name of the current Commanding Officer;
- Rank requirements, if any;
- Minimum commitment and retention requirements, if any (e.g., completion of specialized training or the ability to develop a specialized skill); and
- Other requirements or information as appropriate.

Note: All qualified applicants shall be considered. Members who are on leave are responsible for keeping themselves informed of such postings.

Department Procedure: Non-biddable Posting and Selection

Step	Action
1	The Commanding Officer of the section/unit shall seek approval to fill the vacancy from their Division Commander.
2	The Division Commander shall seek approval to fill the vacancy from the Deputy Superintendent.
3	The Division Commander shall submit a SP 389 Posting Request form to the Human Resources Section for any anticipated openings.
4	The Human Resources Section shall post the anticipated openings for non-biddable assignments for ten (10) calendar days.
5	The Human Resources Section shall forward all timely non-biddable transfer requests to the Section/Unit Commander for review.
6	The Commanding Officer of the section/unit shall schedule interviews, conduct the selection process, and select the candidate(s).

Continued next page.

Department Procedure: Non-biddable Posting and Selection (Continued)

Step	Action
7	The Commanding Officer of the section/unit shall submit a To/From to the Division Commander detailing: • The names of all applicants; • The names of the qualified applicants interviewed, the members of the interview panel, questions asked, and the evaluation instrument; and • The candidate chosen. The chosen candidate's resume and other applicable documentation shall be attached to the To/From.
8	If the Commanding Officer of the section/unit does not find an acceptable candidate, the position may be posted again using the process identified above.
9	The transfer order shall serve as official notice to the candidate(s).

Department Procedure: Troop and Station Non-biddable Posting and Selection

Step	Action
1	The Troop Commander shall post within the troop for ten (10) calendar days for anticipated openings for troop/station non-biddable assignments.
2	The Troop Commander, along with the Commanding Officer of the section/unit where applicable, shall review submissions, schedule interviews, conduct the selection process, and select the candidate(s).
3	If the Troop Commander does not find an acceptable candidate, the position may be posted again using the process identified above.
4	The transfer order shall serve as official notice to the candidate(s).

Interview Process: Non-biddable Assignments

Commanding Officers shall:

- Create an interview panel with a minimum of two (2) people;
- Create a list of standard questions using guidelines from the Human Resources Section; and
- Ensure that a minimum of three (3) qualified applicants are interviewed using the standard questions referenced above. (Follow-up questions may be asked, as necessary.)

If there are less than three (3) qualified applicants, all qualified applicants shall be interviewed.

If the section/unit works in conjunction with another agency (e.g., District Attorney's Office), a representative of the other agency may be one of the interview panel members.

Responsibilities

Position	Duties
Deputy Superintendent	• Schedule transfer meetings as needed; • Obtain the transfer request list from the Human Resources Section and conduct inter-divisional transfer meetings; • Review candidates and the operational needs of the Department; • Make written recommendations for transfers to the Colonel/Superintendent; and • Notify Commanding Officers of pending transfers.
Colonel / Superintendent	• Review and approve or deny the recommendations for transfer; and • Forward the approved transfers to the Human Resources Section.
Human Resources Section	• Issue transfer orders through the Office of the Colonel/Superintendent; and • At least five (5) days before the transfers become effective, notify all members affected by the transfers, through transfer orders.

Transfer Process

Transfer meetings shall take place in conjunction with the fifty-six (56) day bid cycle.

Commanding Officers shall be immediately notified of the finalized transfers.

Transfers shall be effective seven (7) days prior to the end of the current 56-day bid cycle.

Commanding Officers may make transfers outside of the fifty-six (56) bid cycle based on operational needs of the Department.

Bidding and Bid Cycle

All bidding shall conform to the Collective Bargaining Agreement. Once in effect, the fifty-six (56) day bid cycle shall not be violated.

Exceptions are as follows:

- Promotions;
- Training activities, with five (5) days notice given to the affected member;
- Vacancies created as a result of retirement, illness, or leave;
- Emergencies; or
- With the mutual consent of all parties.

Subject	Number
Transfers	**ADM-27**

Intra-Troop/Division Transfers

Troop and Division Commanders may make transfers within their Troop or Division at any time within the guidelines of this policy. Troop and Division Commanders shall notify their respective commanders and the Human Resources Section of the pending transfers.

Temporary Duty (TDY) Assignments

TDY assignments may be made by the Colonel/Superintendent at any time.

TDY assignments:

- Need not be posted; and
- Shall not exceed ninety (90) days without a review and written extension by the Colonel/Superintendent.

Members shall maintain only one (1) TDY status at any given time.

Troop Commanders may make TDY assignments within their troop and shall forward a copy of the order to the Human Resources Section.

Deployment

Each Division Commander shall conduct a needs assessment in order to deploy personnel in the best interests of the Department.

The Human Resources Section shall maintain a Position Management System that contains:

- A table of organizational entities, as approved by the Colonel/Superintendent;
- A position description, classification, and task analysis;
- The number, type, and location of each position; and
- A monthly report indicating whether each position is filled or vacant.

Supervisory Members

Supervisory members do not have bidding rights but may be considered for posted positions in accordance with the process identified in this policy.

Equal Opportunity

The Diversity Officer shall obtain and review transfer request lists from the Human Resources Section. The Diversity Officer may make recommendations in writing to the Colonel/Superintendent.

References

MGL Ch. 22C
Collective Bargaining Agreement Article 28
SP 389 Posting Request Form
SP 389A Troop Posting Request Form

Promulgated By:

Department of State Police
General Order

Effective Date	Number
March 1, 2016	**ADM-28**

Subject

Department Motor Vehicles

Policy

State owned vehicles shall be operated for official use only and in accordance with Policy and Procedure ADM-19 *Vehicle Management* and ADM-19A *Vehicle Use and Maintenance*.

Commuting in Cruisers

Members with cruisers who are traveling to and from home to their duty stations or assignments shall undertake all necessary activities ordinarily performed during motor patrol.

While commuting in a cruiser, all members are to be attired in the required duty uniform unless their usual duties require otherwise.

While commuting with a cruiser, discretion in choosing routes of travel should be used in order to promote the visibility concept on roadways which receive little or no coverage.

A member coming upon an accident scene while in commuting capacity shall immediately notify the substation or police agency of jurisdiction. The member shall then assist at the scene until relieved by an officer from the substation or police agency with primary jurisdiction, or receives instructions to take appropriate action. If the accident occurs on a roadway where the State Police has primary jurisdiction and a State Police patrol is not available, he/she shall investigate the accident, advise the substation having jurisdiction of the pertinent details, and make a report of same upon returning to duty.

A commuting member arriving at his/her residence shall ensure that the cruiser is properly secured in a safe place and that all equipment is secured in a locked compartment within the cruiser. Firearms shall not be left in an unattended cruiser unless secured in accordance with UOF-04 *Use of Force Equipment*. The vehicle, whenever possible, shall not be parked on a public way. A member may garage a cruiser, at no expense to the Commonwealth, away from his/her residence if the Troop or Section Commander approves the location.

Members shall be required to commute in cruisers, when available, to and from their duty stations and/or assignments and homes, between shifts, unless otherwise authorized by the Troop or Section Commanding Officer.

An asterisk (*) will be marked on the officer's audit sheet to show a violation notice while in commuting capacity.

Subject	Number
Department Motor Vehicles	**ADM-28**

Vehicle Maintenance

Members shall ensure that cruisers assigned to them are given proper maintenance and care. Members shall also ensure that expended or faulty emergency and safety equipment is promptly replaced. Before returning from days off and starting a tour of duty each member shall inspect the cruiser assigned to them in order to determine if the vehicle is in good condition and undamaged and that all equipment prescribed for the vehicle is present and operable. Any deficiencies shall be recorded in the Station Daily Administrative Journal/Department Records Management System and corrective action shall be initiated.

Vandalism to an unattended cruiser shall be reported to the member's duty station or assignment as soon as possible after discovery. Any damage to a cruiser or its equipment, sustained while commuting, responding, or on recall, shall be reported as prescribed for regular on-duty status.

References

ADM-19 *Vehicle Management*
ADM-19A *Vehicle Use and Maintenance*
UOF-04 *Use of Force Equipment*

Promulgated By:

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**ADM-29**

Subject

Workplace Violence

Policy

The Department shall maintain zero tolerance for workplace violence and ensure the workplace environment remains free from any form of violence.

This policy does not apply to situations where members are exposed to threats or violent acts from persons in their care or custody, or the public at large, as an unavoidable component of the lawful performance of their law enforcement duties.

Workplace Violence Defined

Workplace shall be defined as:

- Any Commonwealth owned or leased property;
- Any location where Commonwealth business is conducted;
- Any site where an employee is considered on duty;
- Commonwealth vehicles or private vehicles being used for Commonwealth business; or
- Any location if the violence has resulted from an act or decision made during the course of conducting Commonwealth business.

Workplace violence shall include, but is not limited to:

- Intimidation or threats communicated by any means;
- Physical assault and/or battery;
- Threats and/or acts of intimidation communicated by any means that cause an employee to be in fear of their own safety;
- Disruptive or aggressive behavior that causes a reasonable person to be in fear of their own safety or that of a colleague or that causes the disruption of workplace productivity; or
- Property damage.

Incidents of workplace violence may be individual acts or may take place between an employee(s) and:

- Other employee(s);
- Clients/customers/vendors;
- Acquaintances/partners; and
- The general public.

Subject	Number
Workplace Violence	**ADM-29**

Workplace Violence Coordinator

The Workplace Violence Coordinator shall be a Commissioned Officer assigned by the Colonel/Superintendent. The Workplace Violence Coordinator shall report directly to the Commanding Officer of the Division of Standards and Training.

Workplace Violence Safety Incident Team

The Deputy Superintendent shall designate employees to the Workplace Violence Safety Incidence Team and provide such names to the Commonwealth's Human Resource Division. The established team shall consist of:

- A commissioned officer or senior manager from each division; and
- Representation from the Department's Human Resources Section, the Office of Employee Relations, Division of Standards and Training, and the Legal Section.

Disciplinary Action

Any employee found to have engaged in any act of workplace violence, in violation of this policy, is subject to disciplinary action up to and including termination.

Disciplinary action may also require the employee to participate and to successfully complete counseling, anger management education, or other appropriate programs.

The Department may consider acts of workplace violence, along with an employee's success in completing recommended programs, within the promotional process and other work related determinations (where not prohibited by statute, regulation or collective bargaining agreement).

Investigations

The Workplace Violence Coordinator does not conduct investigations into workplace violence. All investigations shall be conducted in accordance with ADM-14 Personnel Investigations.

Responsibilities

Position	Duties
Department Employees	• Not engage in workplace violence behavior; • Immediately report any incident, threat of incident, or potential incident of workplace violence to their immediate supervisor; • Cooperate in investigations of workplace violence; and • Actively participate in the Department's efforts to prevent and eliminate workplace violence.

Continued next page.

Responsibilities (Continued)

Position	Duties
Sworn Members	• Promptly respond to reports of workplace violence; • Take appropriate and immediate enforcement action in response to an incident to ensure the safety of those involved; • Follow proper reporting and investigating procedures as prescribed by this policy; and • Make notification to the Workplace Violence Coordinator, **within seventy-two (72) hours of the incident** utilizing a SP 390 Workplace Violence Incident Report.
Supervisors	• Aggressively monitor the workplace to prevent and detect workplace violence; • Take appropriate corrective action to stop workplace violence; • Immediately report any incident of workplace violence to the Troop/Section Duty Officer and the Workplace Violence Safety Incidence Team Member designated for their Division; • Conduct investigations in a manner that is sensitive to the safety concerns and privacy of the victim(s), the perpetrator, and all witnesses; • Assist the employee/victim of a workplace violence incident by providing any additional support or services necessary to ensure their protection and safety; • Forward a copy of the final report for all workplace violence incidents, through channels, to the Workplace Violence Coordinator; • Make appropriate referrals to the Employee Assistance Unit, the Office of the Ombudsman, or Human Resources Section as needed; and • Ensure notification is made to the Workplace Violence Coordinator, **within seventy-two (72) hours of the incident** utilizing a SP 390.
Station/Section/ Unit Commanders	• Ensure, if necessary, written workplace protection plans are devised for employee(s) who are victims of workplace violence; and • File a copy of the workplace protection plan with the Workplace Violence Coordinator.

Continued next page.

Responsibilities (Continued)

Position	Duties
Workplace Violence Safety Incident Team	• Meet as needed, to devise, review policies, procedures and safety protocols for workplace violence; • Ensure, when necessary, written workplace protection plans for employees who are victims of workplace violence are operative; • Ensure consistent and coordinated responses to acts of workplace violence; • Evaluate and/or make additional notification, recommendations as required when notified of an incident of workplace violence by a supervisor; and • Review and evaluate any serious or critical incidents of workplace violence and make any appropriate recommendations to the Workplace Violence Coordinator necessary to enhance safety considerations.
Workplace Violence Coordinator	• Review and file all final reports of workplace violence incidents and make recommendations to the Division Commander of Standards and Training and the Workplace Violence Safety Incident Team; • Coordinate and schedule meetings as needed with the Workplace Violence Safety Incident Team; and • Annually report statistical data relative to workplace violence incidents within the Department to the Division Commander of Standards and Training.
Human Resources Section	• Coordinate with Workplace Violence Coordinator and the Commonwealth's Human Resources Division regarding Workplace Violence Training; and • Maintain all records of civilian employees trained in workplace violence.

Exceptions

All employees should be aware that conversations with the Office of the Ombudsman and/or Employee Assistance Unit are considered confidential and that these entities are not the proper venue for notification to the Department for workplace violence complaints or incidents.

Retaliation

Any retaliation against an individual who has complained about workplace violence and any retaliation against individuals for cooperating with an investigation of workplace violence are prohibited and shall not be tolerated.

Subject	Number
Workplace Violence	**ADM-29**

Distribution of Policy

This policy shall be shall be issued to each employee upon hiring, and shall be continuously posted and available on DocuShare.

References

Executive Order No. 442
SP 390 Workplace Violence Incident Report
ADM-14 Personnel Investigations
SUP-04 Employee Assistance Unit
SUP-12 Office of the Ombudsman
SPAM Collective Bargaining Agreement Article 27

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 14, 2018	**ADM-30**

Subject

Asset Management

Policy

The Department shall conduct an Annual Fixed Asset Inventory.

The Department shall:
- Record and report Governmental Generally Accepted Accounting Principles (GAAP) Fixed Assets of $50,000 or more within the Massachusetts Management Accounting and Reporting System (MMARS) twice per year pursuant to State Comptroller policy;
- Maintain an automated Asset Management System that reflects all Non-GAAP Fixed Assets with a useful life of one (1) year or more and a cost between $1,000 -$49,999; and
- Maintain inventories of other assets in accordance with State Comptroller policy and as determined by the Division of Administrative Services.

Definitions

Fixed Assets: Tangible property with a cost of $1,000 or more and a useful life of one (1) year or more.

Asset Forfeiture or Federal Grant Fixed Asset: Tangible property funded with asset forfeiture or federal grant funds with a useful life of (1) one year or more, regardless of original cost.

Technology Asset: Tangible asset determined to have the capability of storing data, regardless of original cost (excludes USB flash drives, digital versatile disks, or other consumable technology).

Asset Management

The Asset Management Unit shall manage fixed asset transactions and conduct an annual inventory.

The Division of Administrative Services Chief Administrative Officer or designee shall:
- Designate the Asset Manager for the Department; and
- Ensure the Asset Management Unit reports to the Division of Administrative Services Chief Administrative Officer or designee.

When Commanding Officers acquire, transfer, lose, or dispose of fixed assets, they shall:
- Notify the Asset Management Unit by forwarding a copy of the SP 255 Equipment Transfer Form to the Asset Management Unit.

Annual Fixed Assets, Biannual Capital Assets Inventories, Asset Forfeiture, Technology, and Federal Grant Inventories

Step	Action
1	The Asset Management Unit shall distribute two (2) copies of the inventory to the Commanding Officer of each reporting entity.
2	Commanding Officers shall: • Reconcile the inventory with their previous inventory by physically accounting for each item listed; • Complete and return the SP 255 form for fixed assets that have been acquired, transferred, lost, or disposed of; • Complete and return the SP 255A form for all disposals; this form is in addition to the SP 255 form; • Tag newly acquired items with an inventory control identification number; • Rectify discrepancies; • Retain copies of the inventory printout and SP 255 and SP 255A forms; • Sign-off on Capital (Fixed) Asset Inventory confirmation sheet for biannual review of GAAP Fixed Assets; • Complete, sign, and return Compliance letter for annual inventory reviews; and • Continue to monitor and update the Fixed Asset inventory on a perpetual basis throughout the year. Assets should be added when acquired, and updated at all times to reflect their current location and disposition.

The Asset Management Unit shall:

- Coordinate the Annual Fixed Assets Inventory Review; and ensure:
    1. All sections/units receive reports of their fixed asset inventory as of June 30th of each year. All sections/units must complete this inventory annually;
    2. The Biannual Capital (GAAP/Fixed) Asset Report shall be completed as of December 31st and June 30th of each year; and
    3. All sections/units receive reports of their Annual Asset Forfeiture, Technology, and Federal Grant Inventory as of January 31st of each year. All sections/units must complete this inventory annually. Assets associated with each of these funding sources shall be accounted for regardless of value.

Whenever there is a change of command at a reporting entity, or a change in the personnel assigned to manage specified fixed assets, an asset inventory shall be completed.

Note: The Asset Management Unit shall be notified before fixed assets are disposed of, so that surplus procedures can be followed.

Subject	Number
Asset Management	**ADM-30**

Exceptions

The following Sections/Units are responsible for the management of their assigned inventory:

- Fleet Section;
- Armorer;
- Traffic Programs (radars, lidars and portable breath test devices);
- Communications Section;
- Special Operations Section/Units; and
- Other Department Section/Units as determined by the Chief Administrative Officer or designee.

Commanding Officers shall maintain a master inventory of their assigned fixed assets that:

- Is accurate and reflects changes as they occur; and
- Includes the valuation of the assets.

These Sections/Units shall also conduct an annual inventory, reconcile their databases, and forward the updated inventory report to the Asset Management Unit by June 30th of each year.

References

MGL c.7, s.4A
802 CMR 3.00
Chapter 647 of the Acts of 1989

Promulgated By:

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**ADM-34**

Subject

Information Technology Resources (ITR)

Policy

The Department shall regulate the use of Information Technology Resources (ITR), including computers, printers and other peripherals, programs, data, local and wide area networks, and use of the internet.

ITR communications including email messages are considered public records, copies of which may be requested by the public.

Definitions

Department Information Technology Resources: Include computers, printers and other peripherals, programs, data, local and wide area networks, and use of the internet.

User: Any employee and/or contractors of the Department that utilizes any of the above resources.

User Responsibilities

Failure to adhere to this policy may subject employees to disciplinary action, up to and including termination.

Employees assigned to a Department entity where they may have occasion to access another system not owned or supplied by the Department shall comply with the terms and provisions of this policy for all such usage.

Acceptable Uses

All employees are allowed to use ITR to the fullest extent possible for any legitimate law enforcement function.

Unacceptable Uses of Agency ITR

Unless conducting a legitimate law enforcement function, it shall be unacceptable for any employee to use ITR:

- In furtherance of any illegal act, including violation of any criminal or civil laws or regulations;
- For any political or commercial purpose;
- To send threatening, sexual, or harassing messages;
- To access or share obscene, or otherwise inappropriate materials;
- To infringe any intellectual property rights;

Continued next page.

Unacceptable Uses of Agency ITRs (Continued)

- To gain, or attempt to gain, unauthorized access to any computer or network;
- For any use that causes interference with or disruption of network users and resources, including distribution of computer viruses or other harmful programs;
- To intercept communications intended for other persons;
- To misrepresent either the Department or a person's role at the Department; or
- To libel or otherwise defame any person.

Supervisor Responsibilities

Supervisors are responsible for ensuring that employees under their command comply with the provisions of this policy, and shall monitor use in order to ensure compliance.

Data Confidentiality

Under no circumstances is it permissible for employees or contractors to acquire access to confidential data, unless such access is required to perform their job or task.

Under no circumstances may employees or contractors disseminate any confidential information that they have rightful access to, unless such dissemination is authorized by proper supervisory authority.

Copyright Protection

Employees shall exercise care and judgment when copying or distributing computer programs or information that could reasonably be expected to be copyrighted.

Hardware or Software Installation

Employees shall not install hardware and/or software on any Department ITR without express written authorization from the Division of Administrative Services.

Computer Viruses

Employees shall exercise reasonable precautions in order to prevent the introduction of a computer virus into the local area or wide area networks. Many viruses are spread using email attachments.

Virus scanning software shall be used to check any software downloaded from the internet or obtained from any questionable source. All disks or software shall be inspected for virus infection prior to introduction into the Department system or stand-alone computers or laptops.

Security

Employees shall:

- Change passwords at least every ninety (90) days;
- Never share their passwords with anyone else, unless ordered by proper authority;
- Promptly notify the Division of Administrative Services if they suspect their passwords have been compromised;
- Log off the network or have password-protected screen savers in operation if leaving their ITR unattended for extended periods;
- Not access the internet or other external networks via modem unless they have received prior written permission from the Division of Administrative Services;
- Not move desktop computers, terminals, and printers from their assigned location without written notification and the consent of the Division of Administrative Services; and
- Not transfer to another employee any mobile equipment assigned to the individual such as laptop computers, mobile data terminals, and portable printers without prior written notification from the Division of Administrative Services.

Email

Employees are reminded that email messages are considered public records, copies of which may be requested by any member of the public.

Employees shall:

- Consider email messages to be the equivalent of letters sent on official letterhead and be written in a professional and courteous tone;
- Be aware that emails can be stored, copied, printed, or forwarded by recipients; and
- Not subscribe to email mailing lists, unless related to their job function.

Email shall only be used to communicate official business documents to official recipients. The forwarding of non-business related information is prohibited. Employees who are the recipients of non-business related email are required to discard them and shall not forward them to anyone.

Email attachments that are received from an unknown party should be considered suspicious, and shall not be opened until the sender's identity can be confirmed.

Emails which represent privileged correspondence between Department attorneys and other Department employees shall be clearly marked within the message as "Attorney Client Privilege". In addition, documents that are sent as attachments to an email shall also be clearly marked with "Attorney Client Privilege."

Subject	Number
Information Technology Resources	**ADM-34**

No Expectation of Privacy

The Department retains the right to inspect any employee's computer at any time.

Use of Department ITR constitutes express consent for the Department to monitor and/or inspect any data that employees create or receive, any messages they send or receive, and any web sites that they have accessed.

Employees shall be aware that network administrators routinely monitor network traffic.

Compliance

Staff Inspections shall conduct periodic inspections of all ITR to ensure compliance with all provisions of this policy.

References

Rules and Regulations
SPAM Collective Bargaining Agreement Article 27
Executive Order 504 Order Regarding the Security and Confidentiality of Personal Information

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 17, 2013	**ADM-34A**

Subject

Social Media/Networking

Policy

The personal use of social media can have bearing on departmental personnel in their official capacity. As such, this policy provides information of a precautionary nature as well as prohibitions on the use of social media by Department of State Police Employees.

When using social media/networking, Department Employees (sworn and civilian) should be mindful that their speech becomes part of the worldwide electronic domain.

Department Employees should also be mindful to treat Department of State Police business as confidential per Rules and Regulations Article 5.

Definitions

These definitions are evolving as social media, networking, and internet usage and capabilities evolve as well.

Social Media and Networking: Are categories of internet-based resources that integrate user-generated content and user participation. They are online platforms where users can create profiles, share information, and socialize with others professionally, personally, or informally. The interface is conducted through posts or speech via a range of technologies such as computers, cellular phones, and tablets to name a few.

Social Media: A form of electronic communication through which users create online communicated to share information that may include, but are not limited to: personal messages, videos, photo and video sharing sites, blogs, micro blogging sites, Facebook, MySpace, Twitter, You Tube, Pinterest, Instagram, and Snapchat.

Networking: An exchange of information or services among individuals, groups, or institutions that may include, but are not limited to: the cultivation of productive relationships for employment or business, networking sites, podcasts, as well as comments posted on a site, message or discussion boards, LinkedIn, Plaxo, Jobster, Craigslist, and MyWorkster.

Post: Contents an individual shares on a social media/network site or the act of publishing the contents on a site.

Speech: Expression or communication of thoughts or opinions in spoken words, in writing, by expressive conduct, symbolism, photographs, videotape, or related forms of communication.

Subject	Number
Social Media/Networking	**ADM-34A**

Supervisor Responsibilities

Supervisors are responsible for ensuring that employees under their command comply with the provisions of this policy and address violations as soon as possible.

Responsibilities of Employees

In accordance with Department Rules and Regulations and Policy and Procedures, Department Employees using social media/networking applications shall:

- Use appropriate discretion in their reference to the Department and not discredit themselves or the Department;
- Be aware that speech and/or related activities on social media/networking sites may reflect upon them in their official capacities and/or upon the Department, and act accordingly;
- Be cautioned that speech, on or off-duty, may form the basis for disciplinary action under current law;
- Be aware that privacy settings and social media/networking sites are constantly in flux, and they should never assume that personal information posted on such sites is protected;
- Expect that any information created, transmitted, downloaded, exchanged, or discussed in a public online forum may be accessed by the Department at any time without prior notice;
- Not divulge information gained due to their authority; and
- Not make any statements, speeches, appearances, and endorsements or publish materials that could reasonably be considered to represent the views or positions of this Department without express authorization.

Department Employees should use common sense in all communications, particularly on any social media/networking site. An examination of the facts could potentially result in an internal personnel investigation. Employees are responsible for anything you write or present online. Some examples of prohibited action may include, but not be limited to:

- Speech containing obscene or sexually explicit language, images, or acts and statements or other forms of speech that ridicule regardless of the intent to malign, disparage, threaten harm or otherwise express bias against any race, any religion, or any protected class of individuals; and
- Speech involving themselves or other Department personnel reflecting behavior that would reasonably be considered reckless, irresponsible or unprofessional.

Continued next page.

Responsibilities of Employees (Continued)

Department Employees should exercise care if they choose to post personal information on the internet. Some activities in an employees' personal life may impact job performance, the performance of other employees, and/or interests of the Department. Once information is posted, it is accessible by anyone, indefinitely, and such information may result in unintended consequences, such as:

- Limiting future career opportunities e.g., undercover, covert operations, or attainment of a security clearance;
- Manipulation by defense counsel to undermine or impeach an employee's credibility or integrity, hindering a successful prosecution; and
- Being viewed, altered, printed and redistributed by other internet users including criminal organizations.

Department Employees, who choose to identify themselves as an employee of the Massachusetts State Police whether explicitly, implicitly, or visually, shall:

- Be considered to be publicly representing the agency in a professional manner from that period forward while still employed by the agency; and
- Be responsible for all content published on their individual social media site(s).

Creation of Media Application

Colonel/Superintendent shall approve in writing before the creation of any:

- Website, page, fan group or other application of social media using the Department as the basis of such application. Examples may include, but are not be limited to:
  1. Creating a website or fan group dedicated to Massachusetts State Police;
  2. Creating an identity using a username such as Massachusetts State Police, MSP or any term associated with the Department.

Department Employees shall

- Not publish Commonwealth or Department images of intellectual property using social media without prior approval from the Colonel/Superintendent, e.g., photos of sworn personnel in uniform, marked agency vehicles, videos of training or operations exercises, compilation videos of personnel, vehicles, or equipment, electronic artwork of the State Police patch or seal; and
- Not create an identity, website, page, fan group or other application of social media using the Massachusetts State Police as the basis of such a creation without prior approval from the Colonel/Superintendent, e.g., creating a website or fan group dedicated to Massachusetts State Police, using "Massachusetts State Police" or "MSP" in a username.

Subject	Number
Social Media/Networking	**ADM-34A**

Violations

Department Employees shall notify their immediate supervisor when they become aware of:

1. Any personal identifying information of themselves on the internet in violation of this policy; or
2. Have knowledge of a posting and/or website in violation of the provisions of this policy.

.

Any sites deemed inappropriate, bringing discredit to the Department and or employees, and promoting misconduct whether on or off duty shall be:

- Investigated either through a criminal or administrative investigation.

Investigative Activities

Department Employees shall:

- Not conduct any activity related to ongoing investigations through their personal social networking accounts.

References

Department Rules and Regulations
Department Policy and Procedures

Promulgated By:

Department of State Police
General Order

Effective Date:	Number:
January 31, 2019	**ADM-35**

Subject:

BODY-WORN CAMERA AND CRUISER-MOUNTED CAMERA PILOT PROGRAM

Sec. 1. GENERAL CONSIDERATIONS:

The Massachusetts State Police (MSP) will conduct a six (6) month pilot program of the use of Body-Worn Cameras and Cruiser-Mounted Cameras (collectively, "BWCs") by members to determine their effectiveness in enhancing policing transparency and increasing public trust and police-community relations. BWCs are an effective tool to preserve factual representations of member-civilian interactions. BWCs are effective in capturing video and audio evidence for use in criminal and internal investigations and member training.

The purpose of this policy is to establish guidelines for the proper use, management, storage, and retrieval of video and audio data recorded by BWCs during the MSP Pilot Program.

It is the policy of the Department to respect the legitimate privacy interests of all persons in the Commonwealth, while ensuring professionalism in its workforce. The recording of a civilian based solely upon the civilian's political or religious beliefs or upon the exercise of the civilian's constitutional rights to freedom of speech and religious expression, constitutional petition and assembly is prohibited. BWC footage shall not be reviewed to identify the presence of individual participants at such events who have not engaged in unlawful conduct.

Sec. 2. PROCEDURES:

Sec. 2.1. Training:
All BWC members and all supervisors who may supervise BWC members shall complete Department-approved training on the operation of the system and this policy.

Sec. 2.2. BWC Activation and Incidents of Use:

Members will activate the BWC only in conjunction with official law enforcement duties, where such use is appropriate to the proper performance of duties, and where the recordings are consistent with this policy and the law. If there is an immediate threat to a member's life or safety, making BWC activation impossible or dangerous, the member shall activate the BWC at the first reasonable opportunity to do so. The BWC shall not be deactivated until the occurrence has fully concluded and/or the member leaves the scene (See Section 2.8, BWC Deactivation). Members shall individually be required to record all contact with civilians in the following occurrences:

1. Vehicle Stops;
2. Investigative person stops: consensual, or articulable reasonable suspicion stops, or stops supported by probable cause;
3. All dispatched calls for service involving contact with civilians;
4. Initial responses by members, including on-site detentions, investigations pursuant to an arrest, arrests, and initial suspect interviews on-scene;
5. Pat-frisks and searches of persons incident to arrest (if not already activated);
6. K-9 searches;
7. Incidents of Emergency Driving (primary and secondary responding members);
8. Incidents of Pursuit Driving (primary and secondary responding members);
9. When a member reasonably believes a crowd control incident may result in unlawful activity;
10. Any contact that becomes adversarial, including a Use of Force incident, when the BWC had not been activated; or
11. Any other civilian contact or official duty circumstance that the member reasonably believes should be recorded in order to enhance policing transparency, increase public trust and police-community relations, or preserve factual representations of member-civilian interactions.

In addition, some triggering events may automatically activate the BWC (e.g., activation of blue lights), depending on the technology employed. Members using event-triggered BWCs will receive specific written explanations of these features prior to deployment.

Sec. 2.3. Recording within a Residence:
Members recording in a residence shall be mindful not to record beyond what is necessary to the civilian contact, and not to use the BWC with exploratory intent in an effort to create an inventory of items in the residence.

Sec. 2.4. Recording in Areas Where There May be a Reasonable Expectation of Privacy:
BWC members should be mindful of locations where recording may be considered insensitive, inappropriate, or may be prohibited by privacy policies. Such locations may include locker rooms, places of worship, religious ceremonies, certain locations in hospitals or clinics, law offices, day care facilities, etc. At such locations, at the member's discretion and based on the circumstances, BWCs may be turned off. The member may consider the option to divert the

BWC away from any subjects and record only audio, if appropriate. When exercising discretion in such situations, the decision whether to stop recording, divert the BWC, or record only audio should generally be based on the following BWC Discretionary Recording Considerations:

- the extent to which the member observes activities or circumstances of a sensitive or private nature;
- the presence of individuals who are not the subject of the member-civilian interaction;
- the presence of people who appear to be minors;
- a request by a civilian to stop recording; and
- the extent to which absence of BWC recording will affect the investigation.

Sec. 2.5. Notice of Recording:
Unless there is an immediate threat to the member's life or safety, making BWC notification impossible or dangerous, BWC members shall inform civilians that they are being recorded at the earliest opportunity. BWC members shall notify civilians with language such as "Ma'am/Sir, I am advising you that our interaction is being recorded by my Body Worn Camera." BWC members shall not record civilians surreptitiously. For custodial interrogations, BWC members are reminded to comply with the requirements of INV-16 Electronic Recording of Interrogations. Use of a BWC is one acceptable method of conducting a recording under such circumstances.

Sec. 2.6. Consent to Record:
Aside from the restriction in Section 2.3 (Recording within a Residence), BWC members are not required to obtain consent to record. If a civilian has requested the BWC member to stop recording, members have no obligation to stop recording if the recording is initiated under any of the circumstances identified in Section 2.2 (BWC Activation and Incidents of Use). When evaluating whether or not to continue recording as an interaction develops, BWC members should weigh the BWC Discretionary Recording Considerations specified in Section 2.4 (Recording in Areas Where There May be a Reasonable Expectation of Privacy). A civilian's request to turn the BWC off should be recorded, as well as the member's response.

Sec. 2.7. Recording of Victims / Witnesses:
If a BWC member is in visual- or audio-recording range of a victim or witness who is giving their first account of a crime, the member may record the encounter but should weigh the BWC Discretionary Recording Considerations specified in Section 2.4 (Recording in Areas Where There May be a Reasonable Expectation of Privacy) in determining whether to activate or discontinue recording. If the BWC member decides to activate and/or continue recording the member shall notify the victim or witness as specified in Section 2.5 (Notice of Recording). If the victim or witness is in anyway unsure of the need for the recording to be made or is uncomfortable with the thought of being recorded, the member shall inform the civilian that they can request to have the BWC turned off. If the camera is already activated, the request to turn the BWC off should be recorded, as well as the member's response.

Sec. 2.8. BWC Deactivation:
To the extent possible, prior to deactivating a BWC, the member shall state the reason for doing

so. Generally, once the BWC is activated, recording should continue uninterrupted until or unless the event has concluded. Below are examples of when an event shall be considered concluded:

1. Victim and/or witness contact has concluded;
2. All persons stopped have been released or left the scene or an arrestee has arrived at the barracks for booking. If a transporting member has a BWC, recording shall continue until the transporting member arrives inside the station at the booking desk;
3. The event is of a sensitive nature and the BWC member has weighed the BWC Discretionary Recording Considerations specified in Section 2.4 (Recording in Areas Where There May be a Reasonable Expectation of Privacy) and decided to deactivate the BWC;
4. The incident has concluded prior to the arrival of the member;
5. The incident or event is of such duration that deactivating the BWC is necessary to conserve available recording time; or
6. The member is ordered to turn the BWC off by a supervisor.

Sec. 3. BWC DEPLOYMENT:

Sec. 3.1. Member Responsibilities:

1. At the beginning of each shift, the BWC member will:
   a. Ensure that the issued equipment has a fully charged battery and is functioning properly;
   b. Notify a Supervisor whenever there is a malfunction or damage to the BWC;
   c. Shall use only MSP issued and approved BWC technologies; and
   d. Wear BWC in a manner that does not obstruct or intentionally defeat the purpose of the BWC Policy.

2. While on duty, the BWC member shall:
   a. Activate the BWC and record as outlined in Section 2 above;
   b. Document the existence of a BWC recording in all of the appropriate documents, i.e. Incident Report, Citation, FIO, Administrative Reports, etc.;
   c. To the extent practicable, notify individuals present, including, but not limited to, law enforcement agency personnel, of the existence of the BWC recording;
   d. If a member fails to activate the BWC, fails to record the entire contact, interrupts the recording, or the BWC malfunctions, the member shall document the circumstances and reason in the incident report or any other applicable report; and
   e. Comply with additional responsibilities that are contingent upon the use of a specific BWC technology that have been conveyed to BWC members through written instructions during the pilot deployment.

Sec. 3.2. Supervisor Responsibilities:

The Supervisor of any BWC members will:

1. Ensure all members assigned a BWC utilize the BWC in accordance with this policy;
2. Upon notification of a malfunction, Supervisors will remove the BWC from service, report the malfunction or damage to the Management Information Section at 508-820-2690 and issue a spare unit, where available ; and
3. Access BWC recordings during the course of duties in accordance with this policy's Section 4 Internal Access/Review.

Sec. 4. INTERNAL ACCESS/REVIEW:

Sec. 4.1. BWC Member Access to Footage:

BWC members may review BWC recordings as they relate to:

1. Their involvement in an incident for the purposes of completing an investigation and preparing official reports. To help ensure accuracy, members are encouraged to review the BWC recording(s) prior to preparing reports;
2. Providing testimony in court to refresh recollection. Members will ensure that the prosecuting attorney is aware that the member has reviewed the BWC recording(s) prior to a court appearance; and
3. Providing a statement pursuant to an internal investigation, including member-involved shooting investigations and other critical incidents as outlined in Section 4.2. BWC Member Access to Footage Following a Member-Involved Shooting.

Sec. 4.2. BWC Member Access to Footage Following an Officer-Involved Shooting:
Following an officer-involved shooting, or other use of deadly force, members, including supervisors, shall not view the BWC recording prior to the Force Investigation Response and Support Team ("FIRST") and/or the State Police Detective Unit (SPDU) of jurisdiction investigating officer(s) viewing the footage and uploading it into the system. This prohibition shall not apply where exigent circumstances exist, such as a member being injured, or where the BWC recording may reasonably provide identifying suspect information or other pertinent, time-sensitive information that may be valuable in addressing the exigent circumstances in a timely manner. BWC members involved in an officer-involved shooting and BWC members who witness an officer-involved shooting or other use of deadly force shall be authorized, upon receiving written permission from their supervisor, to view BWC recording(s) prior to a walkthrough and/or statement.

4.3. Collecting and Securing BWC Footage following an Officer-Involved Shooting or Other Use of Deadly Force:
In the event of an officer-involved shooting or other use of deadly force, FIRST Team personnel and/or SPDU of jurisdiction investigating officer(s) will be responsible for collecting and securing the BWCs from all involved members and witness members at the earliest opportunity. FIRST Team personnel and/or the SPDU of jurisdiction investigating officer(s) will ensure that all involved BWCs are uploaded into the system. Consistent with evidence collection and preservation protocols, BWC(s) will be returned to member(s) once the BWC digital files have been uploaded into the system.

Sec. 4.4. Non-BWC Member Access to Footage:
Non-BWC members who are not supervisors, as defined in Section 4.5 (Supervisor Access to Footage), shall only access footage with the written permission of a supervisor.

Sec. 4.5. Supervisor Access to Footage:
Any supervisor within the recording member's chain of command, any Division Commander, or the Colonel or his or her designee, may review the footage. If a supervisor outside of the chain of command requests to see footage, it shall only be allowed with the written permission of the recording member's commanding officer.

Sec. 4.6. Staff Inspections Access to Footage:
Staff Inspections shall conduct periodic checks to ensure BWCs are being used appropriately.

Sec. 4.7. Use of Footage for Training:
Any member can forward a request to the Division of Standards and Training to use a BWC recording for training purposes.

Sec. 5. EXTERNAL ACCESS:

BWC recordings related to an ongoing investigation or in support of a prosecution shall be provided by the recording member to the applicable law enforcement entity in accordance with ADM-16 Notifying Prosecuting Agencies Regarding Evidence. Should a member receive a subpoena for BWC footage, the member shall direct the subpoena as soon as practicable to the State Police Legal Section. BWC recordings are presumptively subject to a public records request (M.G.L. c. 66, § 10). If a member receives a request for BWC footage from members of the media, the request shall be directed to the Legal Section, with a copy to the Director of the Office of Media Relations. All other requests for BWC recordings, including victim or witness requests, shall be directed to the Legal Section. Members are reminded of the requirements of Rules and Regulations Article 5.23 Dissemination of Information.

Sec. 6. RETENTION:

During the BWC pilot program, no recording or footage shall be deleted. Footage recorded during the pilot program will be retained for no longer than one year after the pilot program concludes; provided, however, that BWC footage recorded during the pilot program that relates to any criminal or civil proceeding, any criminal or administrative investigation, or any use of force will be retained during the pendency of any relevant proceeding (including appeals), investigation, or statute of limitations period, and preserved in accordance with any litigation hold requests issued by appropriate Commonwealth or Department personnel, whichever is longest. The retention period for footage recorded pursuant to the pilot program may be superseded by any future BWC policy implemented, or by specific order of the Colonel or his or her designee.

Sec. 7. RESTRICTIONS:

Sec. 7.1. Improper Recording:

BWCs shall not be used to record:

1. During breaks, lunch periods, or time periods when a member is not responding to a call, or when not in service;
2. Any personal conversation of or between other department employees without the recorded employee's knowledge;
3. Non work-related personal activity, especially in places where a reasonable expectation of privacy exists, such as locker rooms, dressing rooms, or restrooms;
4. Investigative briefings;
5. Encounters with undercover members or confidential informants;
6. Departmental meetings, workgroups, in-service training, or assignments of an operational or administrative nature. Using BWCs for training purposes is not a violation of this restriction;
7. Communication with other law enforcement agency personnel;
8. A telephonic conversation, except in accordance with the provisions of State and Federal Law while in the performance of official duties; or
9. Strip searches (refer to PRI-02 Custodial Inventory).

Sec. 7.2. Improper Use of BWC Footage:

BWC recording/footage shall not be:

1. Used for the purposes of ridiculing or embarrassing any employee or person depicted on the recording;
2. Randomly reviewed by the Internal Affairs Division for disciplinary purposes;
3. Disseminated by any employee unless approved by the Colonel or his/her designee, or disseminated in the course of their official duties; or
4. Copied by any employee (e.g., using their personal electronic device to copy).

Sec. 8. PROSECUTORIAL & COURT ORDERED RESTRICTIONS

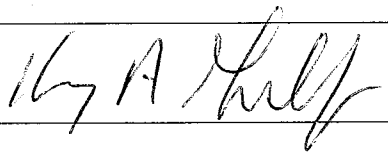
Access to BWC recordings/footage pursuant to Section 4 Internal Access/Review and/or Section 5 External Access, above, may, at the request, direction or order of appropriate prosecutorial and/or judicial authorities be limited, restricted and/or denied.

BWC recordings/footage shall, when subject to the same, be preserved, stored, and retained in accordance with the requests, directions, and orders of appropriate prosecutorial and/or judicial authorities.

References

M.G.L. c. 66, § 10
Rules and Regulations Article 5.23 Dissemination of Information
ADM-16 Notifying Prosecuting Agencies Regarding Evidence
INV-16 Electronic Recording of Interrogations
PRI-02 Custodial Inventory

Promulgated By:



Department of State Police
General Order

Effective Date	Number
November 5, 2008	**ADM-36**

Subject

Diversity and Equal Opportunity

Purpose

The Department prohibits discrimination in employment on the basis of race, color, religious creed, national origin, ancestry, gender, sexual orientation, Vietnam Era Veteran status, age, and disability.

Policy

The Department recognizes that when the effects of employment practices, regardless of their intent, discriminate and create adverse impact against any group of people, affirmative action shall be taken to ensure diversity and equal opportunity and provide equitable remedies for the consequences of present and/or past discriminatory practices. This provides a positive benefit by expanding opportunities to society, the public and all current and future employees.

Strategy for Implementation

The Department shall develop a strategy, which includes plans to address:

- Affirmative Action; and
- Diversity and Equal Opportunity.

The Department, as required and limited by state and federal law, remains committed:

- To ensure equitable participation of minorities, women, Vietnam Era Veterans and persons with disabilities, in all of its operations.

Scope

This policy applies to all employment practices and programs including, but not limited to:

- Recruitment, selection, promotions, termination, transfers, layoffs, compensation, training, and benefits as well as terms and conditions of employment.

The Department shall review, investigate, and when necessary change:

- The policies relative to facilities and programs accessible to the public; and
- Provisions of reasonable accommodation for persons with disabilities.

Subject	Number
Diversity and Equal Opportunity	**ADM-36**

Diversity Officer

The Colonel/Superintendent shall appoint a Diversity Officer who shall:

- Develop and implement:
  1. An Affirmative Action Plan; and
  2. A Diversity Plan.
- Report to the Colonel/Superintendent:
  1. Specific goals and timetables for achievement of each plan;
  2. The Department's compliance with reporting guidelines and requirements; and
  3. Any recommendations regarding equal opportunity.

Responsibilities

The Colonel/Superintendent has the overall responsibility for ensuring equal opportunity and affirmative action in the Department. Supervisors at all levels have the responsibility for the successful implementation of the affirmative action and equal opportunity plans.

References

ADM-18 Anti-Harassment/Sexual Harassment and Discrimination;
Department of State Police Affirmative Action Plan;
Department of State Police Diversity Plan;
Massachusetts General Laws Chapter 151B;
Executive Orders 237, 240, 390 and 478;
The Equal Pay Act of 1963;
Title VI and Title VII of the Civil Rights Act of 1964;
The Age Discrimination in Employment Act of 1967;
The Equal Employment Opportunity Act of 1972;
The Civil Rights Act of 1991;
Section 504 of the Rehabilitation Act of 1973;
The Americans With Disabilities Act of 1990;
The Family and Medical Leave Act of 1993,

Promulgated By:

Department of State Police
General Order

Effective Date	Number
November 5, 2008	**ADM-41**

Subject

Telephone Use/Access

Policy

The use of Department telephones is limited to conducting official business.

Equipment and Access

Any equipment not issued by the Department is restricted from being connected to any Department telephone jack or telephone line.

Telephone Lines

If…	Then…
Additional line is needed or no longer needed	The commanding officer shall contact the Telecommunications Section at GHQ through channels.

Telephone Bills

Commanding Officers shall:

- Review all telephone bills to ensure compliance with this policy;
- Sign the lower right-hand corner of the front page of the bill to indicate that it was reviewed; and
- Employees shall reimburse the Commonwealth for non-business related calls.

Division Commanders shall:

- Ensure commanding officers and all personnel under their command are in compliance with this policy.

Cellular Phones

Department issued cellular phones are restricted to employees whose duties require them in order to effectively perform their duties.

Continued next page.

Subject	Number
Telephone Use/Access	**ADM-41**

Cellular Phones (Continued)

Cellular phones are maintained and controlled by the Fiscal Section.

Requests for cellular phones shall be:

- Submitted through channels, in writing, to the Chief Administrative Officer.

Cellular phones usage is limited to time critical communications. The restrictions on Department telephone use shall also apply to issued cellular phones.

Employees issued a cellular phone shall:

- Sign for the issued equipment;
- Notify through channels their Division Commander and the Fiscal Section if the cellular phone is lost or stolen; and
- Return the cellular phone to the Fiscal Section when leaving their current assignment.

Promulgated By:

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**ADM-46**

Subject

Sexual Activity in Public Places

Policy

The Commonwealth of Massachusetts has a legitimate enforcement interest in ensuring that sexual activity and/or genital exposures do not occur in public places, where the likelihood of being observed by a casual passerby is reasonably foreseeable.

Disparate enforcement of applicable statutes against any particular group and/or disparate treatment of any group is unacceptable.

Definitions

Sexual Conduct: The exposure or touching of the genitals, buttocks, or female breasts for purposes of sexual arousal, gratification or offense, or public solicitation to engage in such conduct in a public place. Sexual conduct does not include socializing and expressions of affection absent the particularized conduct described in this subsection.

Public Place: A place where the person engaging in sexual conduct knows or reasonably should know that there is a substantial risk that his or her sexual conduct will be observed by a casual passerby. Sexual conduct does not occur in a public place simply because it is observed by another. An area may be open to the public and not be considered a public place if a reasonable person would not foresee such a substantial risk.

Subject	Number
Sexual Activity in Public Places	**ADM-46**

Criminal Laws

Members shall pay particular attention to the elements of the various offenses when making a determination to arrest possible offenders for engaging in sexual conduct on public property (e.g. rest areas, parks).

All of the elements of a particular offense shall be met in order to charge an individual with an offense.

Most criminal complaints involving consensual sexual conduct on Commonwealth lands generally allege violations of the following Massachusetts General Laws (MGL):

MGL c. 272, s. 16 Open and Gross Lewdness
To sustain a conviction for open and gross lewdness, the Commonwealth must prove five (5) elements:

- That the defendant exposed their genitals, buttocks, or female breasts to one or more persons;
- That they did so intentionally;
- That they did so openly, i.e., with the intent of exposing themselves, or in reckless disregard or substantial risk of public exposure, to others who might be offended by such conduct;
- That defendant's act was done in such a way as to produce alarm or shock; and
- That one or more persons were in fact alarmed or shocked by defendant's exposing their self. Members should identify at least one witness, who is not a police officer, to satisfy this requirement.

MGL c. 272, s. 35 Unnatural Acts
The conduct must:

- Occur in a public place;
- Involve oral contact with the genital or anal area, anal intercourse or masturbation of another person; and
- Be done intentionally or with reckless disregard that others may observe the conduct and be offended.

MGL c. 272, s. 53 Indecent Exposure and Lewd and Lascivious Behavior
A charge of lewd and lascivious behavior requires both:

- The sexual conduct must occur in a public place; and
- That it be by a person who knows or should know of the presence of another person or persons who may be offended by the conduct.

This section also prohibits the:

- Public solicitation of conduct to be performed in a public place; when
- The conduct committed or solicited involves touching of the genitals, buttocks, or female breasts for the purpose of sexual arousal, gratification, or offense.

Subject	Number
Sexual Activity in Public Places	**ADM-46**

Procedure

Members are free to approach and make inquiries to persons in public areas. The approach or inquiry, however, shall neither explicitly nor implicitly assert that persons must respond to their inquiries.

Persons cannot be arrested:

- For failing to respond;
- On mere suspicion;
- For failing to give an account which satisfies the member; or
- Because of a past offense.

Members shall not order someone to leave a public area in the absence of unlawful conduct.

An investigatory stop or brief detention shall be based on reasonable suspicion.

An arrest shall be based on probable cause.

References

MGL c. 272, s. 16
MGL c. 272, s. 53
MGL c. 272, s. 35

Promulgated By:

Department of State Police
General Order

Policy Date:	Number:
January 7, 2020	**ADM-47**

Subject:

Bias-Based Profiling

Purpose

Except in "suspect specific incidents", members are prohibited from considering the race, national origin, ethnicity, sexual orientation/identity, socio-economic status, religion, immigration status, and/or age, gender identity or expression, cultural group, or disability, of members of the public in deciding to detain a person or stop a motor vehicle and in deciding upon the scope or substance of any law enforcement action. Bias practices are unfair, ineffective, promote mistrust, and perpetuate negative and harmful stereotypes. The Department is committed to bias-free policing.

Introduction

The Department of State Police is committed to protecting the constitutional and civil rights of all citizens. Allegations of bias-based profiling or any other type of discriminatory practice, real or perceived, are detrimental to the relationship between the police and the communities they protect and serve, because they strike at the basic foundation of public trust. This trust is essential to effective community based policing.

Bias-based profiling is illegal and an ineffective method of law enforcement. Bias-based profiling results in increased safety risks to members and citizens and is a misuse of valuable police resources. More importantly, such improper methods violate the civil rights of members of the public and may lead to increased exposure to liability. The Department is committed to an ongoing and open dialogue with community leaders to ensure that it is engaging in bias-free policing. The Department is committed to community policing in all of the commonwealth's cities and towns, and specifically proactively engaging with youth, families and community members to build relationships, solve problems, and prevent crime.

In conducting law enforcement activities such as criminal investigations, personnel shall not consider personal characteristics such as race, ethnicity, national origin, gender, gender identity/expression, cultural group, sexual orientation/identity, socio-economic status, religion, immigration status, and/or age, except when credible intelligence relevant to the location and time frame links a person or people of a specific race, ethnicity, cultural group, national origin, gender, gender identity/expression, sexual orientation/identity, socio-economic status, religion, immigration status, and/or age to a specific unlawful incident, incidents, criminal patterns or schemes.

Continued next page.

Subject	Number
Bias-Based Profiling	**ADM-47**

Introduction (continued)

The Department does not endorse, train, teach, support, or condone any type of stereotyping, or bias-based profiling by its members. While recognizing that most members perform their duties in a professional, ethical and impartial manner, the Department is committed to identifying, investigating, and eliminating any instances of bias-based profiling.

Definitions

Bias Based Profiling: Any prohibited pattern or practice, including but not limited to stopping, detaining, questioning, frisking, and searching by police officers, that is based upon a generalized belief that a person of a particular race, ethnicity, national origin, gender, or other characteristic, status or trait, is more likely to commit certain types of crimes. This type of inappropriate reliance on certain characteristics such as race, ethnicity, national origin, religion, sex, sexual orientation, immigration status, gender identity or expression, economic status, age, cultural group, or disability as the basis for providing differing law enforcement services or enforcement activity as outlined is strictly prohibited.

Suspect Specific Incident: An incident in which a member is lawfully attempting to detain, apprehend, or otherwise be on the lookout for one or more specific suspects who have been identified or described in part by national or ethnic origin, gender, race, religion, sex, sexual orientation, immigration status, gender identity or expression, economic status, age, cultural group, or disability or any other protected characteristic.

Bias-Based Profiling Prevention

To prevent bias-based profiling, the Department shall:

- Provide training programs to ensure that appropriate employees receive training on bias-based profiling practices, implicit bias, and the standards established by this policy;
- Ensure that this policy is disseminated to all members, dispatchers and appropriate civilian employees;
- Continuously review and, where appropriate, revise all procedures that involve the stop, detention, apprehension, or search of individuals to ensure that procedures are in compliance with the provisions of the law and this policy;
- Continuously review performance recognition and evaluation systems, training curricula, policies, and customs of the Department to determine if any practice encourages conduct that may support or lead to; and
- Work with the Executive Office of Public Safety and Security (EOPSS) and the Registry of Motor Vehicles to educate the public on what to expect when either stopped or detained by the State Police, as well as what the officer's expectations are during motor vehicle stops or detainment, to ensure both officer and citizen safety.

Subject	Number
Bias-Based Profiling	**ADM-47**

Enforcement of Profiling Policy

To enforce the provisions of this policy, the Department shall:

- Take appropriate and timely action to investigate allegations of bias-based profiling; and
- Take appropriate and timely measures to correct any institutional practice or policy that may support or lead to the use of bias-based profiling.

Responsibilities

Division of Standards and Training shall:

- Promote professionalism throughout the Department;
- Ensure that all employees receive training on the prevention and elimination of bias-based profiling;
- Assist supervisors in identifying and modifying potentially problematic behavior;
- Utilize appropriate citizen complaint procedures to document and investigate allegations of bias-based profiling; and
- Investigate referrals from the EOPSS.

Position	Duties
Colonel/ Superintendent	Shall: • Promote the Department's commitment to prevent and eliminate bias-based profiling; • Ensure all employees receive a copy of this policy; • Ensure all employees comply with this policy; and • Ensure the continuing analysis and public release of analysis related to documented police interactions with community members.
Supervisors	Shall: • Monitor members conduct to ensure that the standards of this policy are being carried out; • Ensure that members collect data on race, gender, and searches in accordance with laws, and TRF-08 Citations; and • Take positive steps to identify, prevent, and eliminate any instances of bias-based profiling by members of the Department.

Continued on next page

Subject	Number
Bias-Based Profiling	**ADM-47**

Responsibilities (continued)

Members	Shall: • Provide everyone with fair and impartial police services consistent with constitutional and statutory mandates; • Respect the diversity and the cultural differences of all people; • Uphold the Department's commitment to lawful and nondiscriminatory enforcement that promotes public safety and strengthens the public's trust and confidence; • Promptly reporting any instances of bias-based policing to a supervisor; and • Take affirmative and positive steps to identify, prevent, and eliminate any instances of bias-based profiling by other members.

References

TRF-08 Citations

Promulgated By:

Col. Chris S. Mc

Department of State Police
General Order

Effective Date	Number
September 3, 2019	**GEN-01**

Subject

Personal Appearance

Policy

As the principal law enforcement agency within the Commonwealth of Massachusetts, members shall present an image of the highest standard, order, and professionalism to the public.

Members shall correct any deficiencies in their personal appearance, uniform, or equipment as soon as practicable, unless otherwise specified in this Order.

Jewelry

No jewelry, pins, necklaces, or bracelets of any kind shall be worn with the uniform. Exceptions, if conservative, are:

- Wristwatch;
- Medic Alert bracelet;
- Rings; and
- Necklaces worn discreetly beneath the shirt.

Note: Earrings shall not be worn while in uniform; however, conservative earrings may be worn by members in plainclothes assignments.

Members shall not display implants or facial/body piercing, while on duty or representing the Department. Note: In some instances, implants may be acceptable if a licensed medical practitioner requires the medical procedure and the procedure is performed under their supervision.

Facial/body piercings include, but are not limited to:

- Piercing of the face, tongue, nasal septum, lips or lip plate; or
- The deliberate expansion of a healed fistula (hole in the skin) for wearing body-piercing jewelry; or
- The transdermal or microdermal implants.

Exception:
Members who are on undercover assignment may display facial or body piercings, when authorized by their Division Commander.

Subject	Number
Personal Appearance	**GEN-01**

Hygiene and Oral Hygiene

Members' personal care shall conform to the highest personal hygiene standards.

Members, when in any uniform or representing the Department, shall ensure:
- Teeth will be clean and free of foreign debris;
- There is an appearance of a full set of teeth; and
- Missing or broken teeth and/or loose orthodontics shall be replaced or repaired as soon as possible.

Members shall not display dental/oral modifications to their teeth or mouth area while on duty or representing the Department. Note: In some instances, dental/oral modifications or procedures may be acceptable if a licensed dental or medical practitioner requires the medical procedure and the procedure is performed under their supervision.

Dental/oral modifications include, but are not limited to:
- Tongue splitting or bifurcation;
- Abnormal filing of the teeth; and
- Dental veneers or laminates ornamented with designs, jewels, initials, or any other decoration.

Cosmetics

Cosmetics, if worn, shall be:
- Subdued and blended to match the natural skin color; and
- Conservative.

No false eyelashes or unnaturally colored contact lenses shall be worn.

No fingernail polish of any color shall be used when in uniform.

Tattoos and Body Modifications

Members shall comply with General Order GEN-01A Tattoos and Body Modifications.

Hair

Hair shall:
- Be clean, neat, and well groomed;
- Not touch the top of the uniform shirt collar, at the back, when standing with the head in a normal posture;
- Not interfere with the wearing of any issued headgear; or
- Not be dyed or tinted in an exaggerated or unnatural color.

Note: Wigs or hairpieces may be worn if they conform to the above standards.

Continued next page.

Subject	Number
Personal Appearance	**GEN-01**

Hair (Continued)

Males in Uniform:
Hair shall be:
- Either tapered or blocked at the back of the neck; and
- Tapered or blocked at the sides but may not touch the ears.

Sideburns shall be:
- Neatly trimmed and rectangular;
- Trimmed horizontally, at a right angle;
- Of even width; and
- No longer than the midpoint of the tragus of the ear.

Faces shall be clean shaven except:
- Members assigned undercover, and with the approval of the Unit/Section Commander; or
- Members with a temporary medical condition, verified by the State Police Surgeon.
  Note: Members with mustaches, beards, or goatees shall not appear in uniform.

Females in Uniform:
- Hair may extend over, but not below, the bottom of the ear, nor more than two inches forward of the ear;
- Conservative ponytails, braids, hair buns, etc., may be used if secured to the head; and
- Inconspicuous hair aids that blend in with the hair may be used.

References

MGL c. 22C, s.19
GEN-01A Tattoos and Body Modifications
Inturri v. City of Hartford, 2006 WL 231671 (2nd Cir. 2006)
Department Rules and Regulations Article 10-Regulations Establishing Recruit Minimum Entrance Requirement

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 22, 2020	**GEN-01A**

Subject

Tattoos and Body Modifications

Policy

Pursuant to GEN-01 Personal Appearance, members shall present an image of the highest standard, order, and professionalism to the public.

Members of the Department shall maintain their personal appearance to the highest standards possible and in conformance with GEN-01 Personal Appearance.

All Sworn Members

No sworn member of the Department shall have ANY tattoo, scarification or brand that is considered extremist.

Extremist tattoos, scarifications or brands are those affiliated with, depicting, and/or symbolizing extremist philosophies, organizations, or activities. Extremist philosophies, organizations, and activities are those which advocate racial, gender and/or ethnic hatred or intolerance; advocate, create, or engage in illegal discrimination based on race, color, gender, gender identity, sexual orientation, ethnicity, religion, or national origin; and/or advocate violence or other unlawful means of depriving individual rights under the U.S. Constitution, Federal, or State law.

For purposes of this policy, the above prohibition on *extremist* tattoos, scarifications or brands shall also include indecent, sexist and racist tattoos, scarifications or brands:

1. *Indecent* tattoos, scarifications or brands are those that are grossly offensive to modesty, decency, or propriety; shock the moral sense because of their vulgar, filthy, or disgusting nature or tendency to incite lustful thought; or tend reasonably to corrupt morals or incite libidinous thoughts.
2. *Sexist* tattoos, scarifications or brands are those that advocate a philosophy that degrades or demeans a person based on gender or gender identity, but that may not meet the same definition of "indecent."
3. *Racist* tattoos, scarifications or brands are those that advocate a philosophy that degrades or demeans a person based on race, ethnicity, or national origin.

Continued next page.

Subject	Number
Tattoos and Body Modifications	**GEN-01A**

All Sworn Members (Continued)

No sworn member shall have a tattoo, scarification or brand on his or her face, neck or hands (wrist to fingertips).

NOTE: This prohibition pertaining to face and hands does not apply to members who have:

- Permanent commitment band(s) on the hand(s); and/or
- Permanent eyeliner, eyebrows or lipstick, as long as the permanent color is conservative and compliments the complexion and uniform.

However, under no circumstances shall any sworn member be allowed to add ANY additional permanent markings to his or her face.

Effective June 22, 2020, no sworn member shall add any additional tattoo, scarification or brand, regardless of size, normally visible while on-duty in ANY authorized uniform or attire.

Applicants

All applicants seeking sworn appointment to the Department shall be screened during applicant processing to assess whether they are in compliance with this General Order.

If an applicant is found to be in violation of this General Order, then the applicant may, at his or her sole discretion, have the non-compliant tattoo, branding, or body art, or visible portion thereof, removed at his or her own expense. If an applicant expresses a willingness to remove a non-compliant tattoo, branding, or body art, his or her application for appointment will be suspended until the removal process is completed and re-evaluated for compliance. Removal of any markings will not per se absolve the applicant of being deemed as having such affiliation or adherence to said philosophies, organizations or activities that may be apparent in any phase of the selection process.

No applicant shall add any additional tattoo, scarification or brand, regardless of size, normally visible while on-duty in ANY authorized uniform or attire**.**

Prior to appointment to the Massachusetts State Police Training Academy, any applicant who has tattoos/body art/brands/scarifications, normally visible while on-duty in **ANY** authorized uniform or attire, shall submit to the Division of Administrative Services / Human Resources Section for inclusion in the applicant's personnel file:

- An SP 802A Applicant Identification and Reporting of Tattoos/Body Art/Brands/Scarifications

The SP 802A must contain the following information:

1. The date the tattoo/body art/brand/scarification was received;
2. A description and photograph(s) of the respective tattoo/body art/brand/scarification; and
3. The size and location of the tattoo/body art/brand/scarification on the member's body that is visible while wearing the Department uniform.

Subject	Number
Tattoos and Body Modifications	**GEN-01A**

Body Modifications

Body modification to any area of the body that is visible while on-duty in ANY authorized uniform or attire is prohibited.

The use of gold, platinum or other dental veneers or caps for the purpose of ornamentation while on-duty is prohibited. Teeth, whether natural, capped, or veneer shall not be ornamented with designs, jewels, initials, etc.

Body piercing jewelry not concealed by any authorized uniform or approved attire while on-duty is prohibited with the exception of earrings worn in compliance with GEN-01 Personal Appearance.

- The wearing of any facial jewelry to include, but not limited to tongue piercings, lip piercings, nose piercings, brow piercings by any sworn member of the Department while on-duty is prohibited.
  Exception: Members who are on undercover assignment may display facial or body piercings when authorized by their Division Commander.

References

Department Rules and Regulations Article 10-Regulations Establishing Recruit Minimum Entrance Requirement
GEN-01 Personal Appearance
SP802 Sworn Member Identification and Reporting of Not Previously Documented Tattoos/Body Art/Brands/Scarifications
SP 802A Applicant Identification and Reporting of Tattoos/Body Art/Brands/Scarifications

Promulgated By:

Department of State Police
General Order

Effective Date	Number
January 25, 2018	**GEN-02**

Subject

Uniforms

Policy

Members of the Department shall maintain their personal appearance and uniforms to the highest standards possible.

Cruiser Operation

While operating Department vehicles, all members are required to wear the authorized uniform or appropriate business attire.

Members shall display their badge of office while operating a Department vehicle; exceptions may be allowed for:

- Members assigned to the Division of Investigative Services or to other assignments where the member's identity should not be revealed.

General

Supervisors are responsible for continuous line inspections in order to ensure that members under their control maintain a professional appearance and correctly wear the uniform.

Whenever two (2) or more members are gathered in the same location, the members shall dress the same as the Officer in Charge (OIC) or Senior Trooper, or as otherwise ordered.

Members while in uniform shall not:

- Participate in social functions, unless authorized to do so by their Division Commander;
- Wear unauthorized or non-issued clothing, parts, medallions, ornaments, or other appurtenances;
- Wear personal headphone devices or cellular phone headsets;
- Consume alcoholic beverages;
- Use tobacco, chew gum, or have any foreign object protruding from the mouth when they are:
  - (1) in view of the public; and/or
  - (2) in formation.

Members shall not permit any non-member to wear any part(s) of any issued Massachusetts State Police uniform assigned to them.

Members shall not wear any part of the uniform while off-duty, unless authorized to do so.

Replacement of Uniforms or Equipment

When items are worn out, damaged, destroyed through normal use, or do not fit, members may turn in items to the Troop Clerk and requisition a replacement.

When items are damaged or destroyed through negligence or misuse, the member shall replace the item(s) at their own expense.

Cleaning and Maintenance

- Boots, shoes, and leather shall be highly polished.
- Brass shall be clean and highly shined.
- Clothing items shall be clean, stain free, and pressed.
- Necessary alterations or repairs may be done through the Troop Clerk.
- Whenever an occasion causes deficiencies in personal appearance, uniform, or equipment, members shall avail themselves of the first opportunity to correct the condition.

Riot Gear

All members, unless undercover, shall carry all issued riot gear in the trunk of their cruiser.

The OIC at a riot or disturbance may designate the following items as optional:

- Necktie and tie clasp, cross-strap, name tag, badge of office, whistle and chain, and gas mask; and/or
- Use of force equipment as defined in *UOF-04 Use of Force Equipment*

Summer and Winter Uniform Dates

The Summer Uniform shall be worn from:

- April 15th through October 14th.

The Winter Uniform shall be worn from:

- October 15th through April 14th.
  Note: The Winter shirt is optional for thirty (30) days before and after this period.

Note: Staff Officers while in any uniform shall wear the garrison cap at all times.

Full Dress (Class "A") Uniform

The Class "A" Uniform is for ceremonial or dress occasions. It consists of:

- Long sleeve shirt;
- Necktie and tie clasp;
- Blouse;
- Breeches;
- Field boots; and
- Duty belt with only the holster and firearm, ammunition case, handcuff case, club ring, and the cross-strap;

Continued next page.

Full Dress (Class "A") Uniform (Continued)

- Appropriate cover (the garrison cap during Winter for all members; the straw campaign cover during Summer for all members, except Staff Officers who shall wear the garrison cap);
- Black or white gloves, when authorized; and
- Authorized ribbons and medals.

Sunglasses, keepers, and extra handcuffs shall not be worn with the Class "A" uniform.

For designated periods of mourning, a black badge shroud shall be worn around the badge of office.

Summer Field Service (Class "B") Uniform

- Straw campaign cover shall be worn with cord trimmed to an appropriate length (not knotted) and as follows:
  - *Troopers* – silver hat badge and silver acorns;
  - *Non-Commissioned Officers* – silver hat badge and silver acorns;
  - *Commissioned Officers* – gold hat badge and gold acorns;
- Short sleeve shirt, top button unbuttoned, no undergarments or jewelry visible;
- Slacks;
- Jump boots;
- Garrison belt;
- Duty belt with keepers, holster and firearm, handcuff case, club ring, ammunition case, and other authorized equipment;
- Sweater (optional) tucked into slacks with badge on left chest, name tag on right chest;
- Issued outerwear (optional); and
- No ribbons or medals, except service ribbon.

If the long sleeve shirt or issued sweater is worn, a necktie and tie clasp shall be worn without the cross-strap.

Winter Field Service (Class "B") Uniform

- Garrison cap shall be worn with:
  - *Troopers* – silver hat badge and black leather strap on front and back;
  - *Non-Commissioned Officers* – silver hat badge and silver hat band on front with black leather straps removed;
  - *Commissioned Officers* – gold hat badge and gold hat band on front with black leather straps removed;
  - *Command Staff* – gold hat badge, gold fretting, and glossy gold hat band with black leather straps removed;
- Long sleeve shirt, completely buttoned, with necktie and tie clasp;
- Breeches;
- Field boots;
- Garrison belt;

Continued next page.

Winter Field Service (Class "B") Uniform (Continued)

- Duty belt with cross-strap, keepers, holster and firearm, handcuff case, club ring, ammunition case, and other authorized equipment;
  - Cross-strap shall be worn diagonally across the wearer's front and back, secured directly in front of and behind the holster.
- Sweater (optional), tucked into breeches with cross strap removed and badge on left chest, name tag on right chest;
- Issued outerwear (optional);
- Black gloves and balaclava (optional); and
- No ribbons or medals, except service ribbon.

Knit caps shall not be worn with the Winter Field Service (Class "B") uniform.

Specialty Uniforms

When authorized to do so by their Division Commander, members may wear specialty uniforms. Only members who are performing a specialized function shall wear specialty uniforms.

The Division Commander of Standards and Training, or designee, may revise the duty uniform of personnel assigned to the Academy.

Issued Uniform Parts and Equipment

The **Badge of Office** shall be:

- Prominently displayed by wearing it on the left breast area of the outer uniform garment.

The **Headgear badge** shall be:

- Worn on all campaign covers and garrison caps.

Collar insignias shall be:

- Worn on summer and winter shirts and the dress blouse only;
- Placed with the Commonwealth ornament on the right hand side;
- Placed with the troop designation ornament on the left hand side; and
- Placed one (1) inch back from the leading edge of the collar and centered between top and bottom.

Service chevrons may be:

- Worn, one (1) for every two (2) years of service; and
- Worn on the left sleeve of the blouse, pointing downward with the lowest chevron centered one and one-half (1 ½) inches above the semicircular cuff edging.
  Note: Service chevron shall not be worn by commissioned and non-commissioned officers.

Continued next page.

Issued Uniform Parts and Equipment (Continued)

Non-Commissioned Officer stripes shall be:

- Worn on both sleeves of all shirts, the dress blouse and outer garments except traffic vest and rain jacket;
- Aligned so that the points of the stripes face upward;
- Positioned on the right sleeve so that the point of the highest stripe touches the bottom point of the MSP patch; and
- Positioned on the left sleeve so as to mirror the location of the stripes on the right sleeve.

Commissioned Officers Rank Insignia shall be:

- Worn on both shoulders of all shirts, the blouse, and outer garments, except traffic vest and rain jacket; and
- Centered between the shoulder seam and shoulder strap.

Name tags shall be:

- Prominently displayed on all outer uniform garments, except rain jacket and high visibility safety apparel;
- Affixed to the lower seam edge running horizontally across the right breast and centered over the button of the shirt/blouse pocket; and
- Positioned so as to appear centered between the lapel edge and shoulder seam.

Tie clasps shall be:

- Worn on the tie, clipped to the shirt, and horizontally even with the name tag.

The **chain, key and whistle** shall be:

- Worn suspended from the right epaulet button and attached to the right breast pocket button on the blouse or shirt;
- Worn with the chain under the name tag; and
- Worn in the following order from the right: chain-key-whistle.

The issued **use of force equipment, ammunition, and handcuffs** shall be:

- Carried and secured in appropriate cases on the duty belt.

The **rain jacket** shall be:

- Worn during inclement weather**,** high visibility side out (see *Issued High Visibility Safety Apparel* section of this General Order), except for solemn or ceremonial occasions, where the black side shall be out.
  Note: No rank insignia shall be worn on the rain jacket.

The **traffic vest**:

- See *Issued High Visibility Safety Apparel* section of this General Order.
  Note: No rank insignia shall be worn on the traffic vest.

Promotion Instructions

Prior to the effective date of promotion, all officers shall report to the Supply Section in order to be issued appropriate uniforms and gear. Unless specifically detailed below, uniforms and uniform parts shall remain the same as the next highest rank.

All Ranks

Patrol Jackets
Both reversible patrol jackets should be returned to the Supply Section for an exchange or for application of new rank insignia in the appropriate location(s).

Staff Officers and Commissioned Officers

Rank Insignia
The following ranks will be issued the respective cloth and brass rank insignia**:**

- **Colonel –** Silver Eagle;
- **Lieutenant Colonel –** Silver Oak Leaf;
- **Major –** Gold Oak Leaf;
- **Detective Captain –** Double Silver Bars;
- **Captain –** Double Gold Bars;
- **Detective Lieutenant –** Single Silver Bar;
- **Lieutenant –** Single Gold Bar.

Cloth Rank Insignia shall be

- Sewn onto both shoulders of all uniform shirts; and
- Centered between the shoulder seam and shoulder strap.

Brass Rank Insignia shall be worn on:

- Blue side of patrol jackets;
- Dress blouse; and
- Sweater.

Gold Braiding
Detective Lieutenants/Lieutenants will be issued a dress blouse with the appropriate gold braiding already affixed.

The following ranks will be issued additional gold braiding to be affixed to the sleeve of the lieutenant dress blouse, resulting in:

- **Colonel** – four (4) rows of one-half (1/2) inch braiding affixed one-eight (1/8) inch from each other;
- **Lieutenant Colonel** – three (3) rows of one-half (1/2) inch braiding affixed one-eight (1/8) inch from each other;
- **Major** – One-half (1/2) inch braiding, then one-quarter (1/4) inch braiding, then one-half (1/2) inch braiding affixed one-eight (1/8) inch from each other;
- **Detective Captain/Captain** – two (2) rows of one-half (1/2) inch braiding affixed one-eight (1/8) inch from each other.

Continued next page.

Promotion Instructions (Continued)

Detective Lieutenants/Lieutenants

Detective Lieutenants/Lieutenants will be issued the following:

1. Uniforms
   - Dress Blouse with the appropriate gold braiding already affixed;
   - Slacks and Breeches with two (2), one-half (1/2) inch blue braiding sewn along each pant leg; and
   - Long and short sleeve shirts.

2. Gold Accessories
   - Chain / handcuff key / whistle;
   - Collar ornaments;
   - Duty Belt brass; and
   - Tie clasp.

3. Gold MSP Patches – All blue MSP patches should be removed from the current issue, except rain jacket, and replaced with the gold patches. Troop Clerks may be consulted for alteration locations.

4. Gold Reflective Tape for Riot Helmet:
   - one (1) gold strip of tape is to be placed horizontally on the back of the helmet from rivet to rivet; and
   - one (1) gold strip of tape is to be placed starting on the crown of the helmet downward to the front visor.

Sergeants

Sergeant will be issued the following:

1. Cloth Non-Commissioned Officer Stripes Rank Insignia with dark blue stripes and light blue background which shall be affixed accordingly:
   - Sewn onto the dress blouse and onto all uniform shirts;
   - Worn on both sleeves of dress blouse, and all shirts;
   - Aligned so that the points of the stripes face upward;
   - Positioned on the right sleeve so that the point of the highest stripe touches the bottom point of the MSP patch; and
   - Positioned on the left sleeve so as to mirror the location of the stripes on the right sleeve.

Note: Cloth Non-Commissioned Officer Rank Insignia with light blue stripes and **dark** blue background are for winter sweaters and patrol jackets only.

2. Silver Reflective Tape for Riot Helmet:
   - One (1) silver strip of tape is to be placed horizontally on the back of the helmet from rivet to rivet; and
   - One (1) silver strip of tape is to be placed starting on the crown of the helmet downward to the front visor.

Issued High Visibility Safety Apparel

High Visibility Safety Apparel is comprised of fluorescent colored background material that has retro-reflective applications affixed to it, thus providing the wearer with a high degree of visibility during both daylight and darkness.

The following Department issued apparel shall be considered high visibility safety apparel:

- High visibility yellow traffic test;
- Civilian traffic vest;
- Reversible Rain Jacket with high visibility yellow side out; and
- Reversible Patrol Jackets with high visibility yellow side out.

Department Employees (sworn and civilian) are advised that issued high visibility safety apparel shall be:

- Worn in accordance with current state and federal laws.

Specific clothing worn by certain sections of the Department may be considered high visibility safety apparel, only if the article of clothing has an American National Standards Institute-International Safety Equipment Association (ANSI/ISEA) certified label affixed to it.

The Department realizes that members performing motor vehicle stops have discretion when balancing their need to be visible to approaching traffic and their need to ensure proper patrol procedures/officer safety during the course of the motor vehicle stop.

Employees (sworn and civilian) are <u>not required</u> to wear high visibility safety apparel when:

- A member is performing a motor vehicle stop; or
- A civilian employee is performing functions away from the roadway and traffic areas.

However, members who choose <u>not to wear</u> high visibility safety apparel during motor vehicle stops shall:

- Remain vigilant and understand that they are less likely to be seen by approaching motor vehicle traffic particularly:
    1. In darkness; or
    2. In periods of diminished visibility due to inclement weather.

Employees (sworn and civilian) wearing uniforms or plain clothes <u>shall wear</u> high visibility safety apparel during all hours and lighting conditions when engaged in the following activities:

- Directing traffic;
- At all road and highway motor vehicle crash scenes;
- When working at lane closures and obstructed roadways;
- On all road and highway work zones and construction details including moving details (excluding dignitary protection); and/or
- Special or significant events when ordered by the OIC.

Subject	Number
Uniforms	**GEN-02**

Eye Wear

Members performing a line function and wearing prescription lenses shall have:

- Safety lenses; and
- Conservative and secure frames.

Sunglasses may be worn for outside assignments only, and shall be of a conservative style.

Department Issued Ribbons and Medals

While in Class "B" uniform, Department members who have attained ten (10) years of service shall be allowed to wear over the left breast pocket of the shirt:

- The Department issued Service Ribbon (blue/white/blue); and
- If applicable, one (1) gold star for each additional five (5) years of service to be inserted onto the white section of the ribbon.

Department issued ribbons and medals shall be worn on the Class "A" uniform over the left breast pocket of the blouse. However, if the member has military awards, the Department ribbons and medals shall be worn over the right breast pocket of the blouse.

Memorial pins, medallions, insignias, or other ornaments shall not be worn, unless authorized by the Colonel/Superintendent.

Military Ribbons and Medals

Awarded ribbons and medals issued by the U.S. Armed Forces may:

- Be worn or displayed, in military fashion, while in Class "A" uniform over the left breast pocket of the blouse.

No military ribbons or medals shall be worn or displayed while in Class "B" uniform.

References

MGL c.22C, s.19
MGL c.149 s. 6
Massachusetts State Police Rules and Regulations Article 5
UOF-04 Use of Force Equipment
Commonwealth of Massachusetts Division of Occupational Safety
Department of Transportation Federal Highway Administration Manual on Uniform Traffic Control Devices
American National Standards Institute-International Safety Equipment Association (ANSI/ISEA) 107 & 207 Standards

Promulgated By:

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**GEN-04**

Subject

Military Courtesy

Policy

The Department has been a paramilitary organization since its inception; the application of military courtesies shall continue to maintain this tradition.

Salutes

Salutes shall be given when members are both in uniform and covered, unless it would interfere with the performance of duty.

Salutes shall be given to a Staff Officer or a Commissioned Officer, and be smartly and promptly acknowledged by that member. In the case of Commissioned Officers, this rule shall only apply to members of superior rank.

The salute shall also be given to the Governor, President and Vice President.

This policy shall also apply when meeting uniformed members of other police agencies and the Armed Forces.

Salutes in Formation

Members shall salute upon a command from the Commanding Officer when:

- In formation at a halt, the commands are "Attention", then "Present Arms" and the recovery command is "Order Arms"; and
- In a moving formation, the salute is only executed by the Commanding Officer leading the formation; the command for the formation is "Eyes Right" (or left), and then "Ready Front" as the salute.

Attention

Upon entering the office of the Colonel/Superintendent, a Lieutenant Colonel, or a Major, a member shall remove their cover and stand at attention.

National Anthem

Members in uniform shall stand at attention and salute when the National Anthem is played:

- Facing the music (unless the National Flag is displayed); and
- Starting at the first note of the anthem, continuing to the last note.

If in civilian clothes, the right hand is placed over the heart in lieu of the salute.

Subject	Number
Military Courtesy	**GEN-04**

National Flag

Unless it would interfere with the performance of duty, uniformed members wearing the appropriate cover, shall stand at attention facing the flag and salute when:

- It passes by on all public occasions, ceremonies, parades, etc. (The salute shall be given when the flag has arrived within a distance of six (6) paces and maintained until it has passed six (6) paces beyond); or
- It is carried into any building, room, or other place where members are present; or
- It is formally raised or lowered.

If in civilian clothes, the right hand is placed over the heart in lieu of the salute.

Pledge of Allegiance

Unless it would interfere with the performance of their duty, during the Pledge of Allegiance members shall:

- Stand at attention facing the flag and salute when in uniform wearing the appropriate cover; or
- Stand at attention facing the flag and place their right hand over their heart if in civilian clothes.

Display of Flags

The Flags of the United States and the Commonwealth shall be flown at all Department facilities. The National Colors shall be flown on the flag's own right, (on the right as facing the street), and slightly higher than the Commonwealth Flag.

Flags shall be flown:

- Every day when the weather permits; and
- At night if they are directly illuminated

The National Flag shall be flown at half-staff in honor of a member who dies while in the line of duty, from the notification of death until dusk of the day of interment.

The Flag of the Commonwealth shall be flown at half-staff when:

- The National Flag is at half-staff;
- As ordered by the Governor; or
- As ordered by the Office of the Superintendent.

On Memorial Day, the flags should be flown at half-staff until noon, and then raised.

To display flags at half-staff, the flags should be hoisted to the peak, and then lowered to half-staff.

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 17, 2013	**GEN-04A**

Subject

Ceremonial Tributes

Policy

The protocols identified within this policy shall be adhered to during ceremonial tributes in honoring Department members or when attending tributes with other agencies.

Request Procedure and Authorization

The Colonel/Superintendent shall authorize final approval for all Department tributes and requests from outside agencies. The Division of Field Services shall handle implementation, unless otherwise ordered.

Ceremonial Tributes

The Department may provide the following as determined by the Colonel/Superintendent:

Line of Duty Death

- Wake – Organized police walk-by, honor guard and/or color guard detail;
- Drill and Ceremonial Unit;
- Rifle Salute;
- Mounted Unit;
- Motorcycles;
- Air Wing;
- Vocalist and bugler(s);
- Department Pipes & Drums;
- Classmates of the Deceased;
- Specialty Unit/Team to which the member belonged;
- Minimum of forty (40) members; and
- All available members of the Command Staff.

Off-Duty Death

- Wake – Honor guard at wake consisting of member's troop/section;
- Drill and Ceremonial Unit;
- Motorcycles;
- Classmates of the Deceased;
- Vocalist, bugler and piper;
- Specialty Unit/Team to which the member belonged;
- Minimum of twenty (20) members; and
- Division Commanders or Designees.

Continued next page.

Subject	Number
Ceremonial Tributes	**GEN-04A**

Ceremonial Tribute (Continued)

Death of Immediate Family Member of an Active Member, (spouse, child, brother, sister, parent of member or spouse)

- Four (4) members, provided for by the member's Station/Section/Unit, to cover calling hours, funeral detail, and the procession.

Retired Member(s)

- Two (2) members to be provided by the Division of Field Services to cover calling hours, funeral detail, and procession.

Active Public Safety Officers

The Colonel/Superintendent shall determine any ceremonial tributes provided for active public safety officers killed in the line of duty.

Funeral Attendance

The Department shall attempt to allow as many on-duty members as possible to attend the calling hours and funeral services of an active member.

Members to attend calling hours and funeral services in uniform shall:

- Wear the appropriate uniform-of-the-day as indicated on calling hours and funeral services announcements;
- Be authorized, when attending off-duty, to wear the uniform-of-the-day as indicated on calling hours and funeral services announcements; and
- While inside a funeral home or church carry their headgear under their left upper arm, unless directed otherwise or when participating as a member in the honor guard.

Honor Guard

Details at funeral homes should consist of at least four (4) members. The senior member should coordinate with the family liaison. Members shall wear the class "A" uniform, with a black badge shroud and white gloves, unless otherwise directed.

Funeral Processions

Upon leaving the funeral home or church, members should:

- Cover and form two (2) lines along the path where the casket is to be carried;
- The formation shall start at the funeral home or church and end at the hearse; and
- A proper interval shall be maintained between members.

Subject	Number
Ceremonial Tributes	**GEN-04A**

Badge Shrouds

As designated by the Colonel/Superintendent, black badge shrouds shall be worn for thirty (30) days by all members in honor of an active member who dies in the line of duty.

Black badge shrouds shall be worn by all members in honor of an active member who dies off duty, from the date of the death notification until the interment.

Black badge shrouds shall be worn by uniformed members while appearing at a funeral or memorial service for active or retired members.

Funeral Escorts

Department vehicles escorting or following the funeral procession shall:

- Be operated at a speed consistent with that of the hearse and far enough ahead of the procession to control traffic; and
- Have all the emergency warning lights activated and left on during the entire escort.

Members assigned to traffic control duties where the funeral procession is passing by shall:

- If conditions allow, stand at attention and render the hand salute while the hearse is passing.

If the escort terminates at the entrance to a cemetery, church, or funeral home, the escorting members shall:

- Stand at attention in two (2) lines, face each other; and
- Render the hand salute until the hearse has passed by.

Promulgated By:

Department of State Police
General Order

Effective Date	Number
November 5, 2008	**GEN-05**

Subject

Communicable Diseases

Policy

The Department shall provide its employees with equipment and information on communicable diseases to prevent exposure to dangerous and life-threatening diseases.

Definitions

Communicable Disease: Infectious illnesses and viruses that are transmitted through contact with bodily fluids, tissue, or breath of an infected individual.

Bodily Fluid: Liquid secretions such as blood, semen, vaginal secretions, saliva, vomit, urine, and feces.

Airborne Exposure: Contact with bacteria, virus, chemical, smoke, or any foreign particle suspended in the environment.

Unprotected Exposure: Any bodily fluid or tissue that comes into direct contact with a mucous membrane (e.g., eyes, nose, and mouth) or non-intact skin (e.g., cuts, chapped skin). This includes a bite from a human or animal.

Communicable Disease Prevention

All employees should assume that all persons are potential carriers of communicable disease.

When coming into contact with people or evidence where the transfer of bodily fluids is a possibility, employees should wear protective clothing and equipment to minimize their exposure to disease. This includes:

- No eating, drinking, or smoking at a scene where bodily fluids are present;
- Wear **disposable gloves** when administering first aid or handling anything that has been exposed to bodily fluids (double gloves should be used, if necessary);
- Wear a **protective mask**, eye wear, and coveralls if available, in situations where bodily fluids may come into contact with the employee;
- Use the issued **plastic mouth piece** or other barrier resuscitation device when performing CPR;

Continued next page.

Communicable Disease Prevention (Continued)

- Use extra care when handling contaminated sharp objects (e.g., wear **protective gloves** when conducting a search, or when handling sharp objects);
- Use a **flashlight or baton** to conduct an initial sweep of areas where sharp objects may be hidden;
- Place hypodermic needles in leak proof, rigid, puncture-resistant, shatterproof containers (needles should not be recapped, bent, broken or removed from the syringe); and
- All employees assigned to the Forensic Service Group involved in the collection and handling of evidence shall follow Communicable Disease Prevention procedures identified in the current version of the Laboratory Safety Manual.

Disinfection Guidelines

If…	Then
Any unprotected skin surface comes in contact with bodily fluids	1. Immediately and thoroughly wash the affected area with hot running water and soap for at least fifteen (15) seconds before rinsing and drying. 2. Use alcohol or waterless antiseptic hand cleaning gel when soap and water is unavailable. 3. Hand lotion should be applied after disinfection to prevent chapping and to seal cracks and cuts on the skin. 4. When necessary, report to a medical facility for an examination or treatment.
You are wearing disposable gloves that come in contact with bodily fluids.	1. Thoroughly rinse the glove before removing. 2. Hands and forearms should then be washed as described above.
Uniform or clothing comes in contact with bodily fluid.	1. Remove the uniform/clothing as soon as practical. 2. Place the contaminated uniform/clothing in a paper bag. 3. Any contaminated skin area should be cleaned as described above. 4. Uniforms/clothing should be marked as contaminated and cleaned by: • Laundering in the usual manner; • Turning into the Supply Clerk for an exchange; or • Disposing according to the State Sanitary Code.

Continued next page.

Disinfection Guidelines (Continued)

If…	Then
A Department vehicle becomes contaminated with bodily fluids.	1. The Troop Supply Clerk shall arrange for a complete cleaning and disinfection, as soon as possible.
Non-disposable equipment becomes contaminated with bodily fluids.	1. Wear protective clothing when cleaning. 2. Prepare a cleaning solution containing: • One (1) part bleach to ten (10) parts water; or • A fungicide or a micro bacterial disinfectant. 3. Wipe excess bodily fluids with disposable absorbent material. 4. Clean equipment with the prepared solution or disinfectant. 5. Dispose of the cleaning material according to the State Sanitary Code. 6. Follow manufacturer's guidelines for proper disinfection/cleaning procedures.
Disposable equipment, (such as cleaning materials) contaminated with bodily fluids.	1. Bag and dispose of according to the State Sanitary Code.
Evidence contaminated with bodily fluids is recovered.	1. Place in paper bags and clearly mark as contaminated. 2. Allow items to dry out. 3. Take additional precautions as necessary. 4. Consult with Crime Services Section for proper disinfection/handling procedures.

Transport and Custody

When transporting an individual who has bodily fluids on their person or has stated that they have a communicable disease:

Position	Duties
Members shall:	• Take all precautions to minimize the possibility of exposure to the bodily fluids; • Administer necessary first aid; • Transport this individual in a separate vehicle from other people; and • Notify the Desk Officer.
Desk Officers shall:	• Appropriately isolate the person; • Notify the Troop Duty Officer; and • Document the incident in the Daily Administrative Journal.

Reporting Unprotected Exposures

Members who have had an unprotected exposure while on duty should seek immediate treatment at an emergency room. Larger hospitals and teaching hospitals are often better able to assist with potential exposures.

The exposure shall be treated as an on-duty injury, and documented under the guidelines of ADM-11B Injury Reporting and Leave. In addition, a **Department of Public Health Unprotected Exposure Form** shall be filled out to document the exposure and:

- Taken to the medical facility where the member(s) is being treated, and
- Faxed to the Health Unit.

All employees assigned to the Forensic Service Group involved in the collection and handling of evidence shall follow the exposure procedures identified in the current version of the Laboratory Safety Manual.

Department civilian employees shall seek guidance from their immediate supervisors who shall follow the procedures for sworn members.

Supplies

All Department cruisers and/or installations should be stocked with the following communicable disease control supplies:

- Disposable and protective gloves;
- Puncture resistant containers and plastic evidence bags;
- Barrier resuscitation equipment, goggles, and masks;
- Liquid germicidal cleaner;
- Disposable towelettes with 70% isopropyl alcohol; and
- Waterproof bandages.

Health Unit Responsibilities

The Health Unit shall:

- Advise members about communicable disease and infection control matters;
- Conduct training pertaining to communicable disease and infection control matters;
- Distribute protective clothing and equipment; and
- Develop guidelines for the use of the equipment and providing care to the public.

Responsibilities

Position	Duties
Members	• Ensure that all assigned medical supplies are properly maintained; • Keep disposable and protective gloves readily available and easily accessible; • When an on-duty incident results in an unprotected exposure, notify the Desk Officer and follow the guidelines in this policy to minimize the risk of infection; and • No member shall refuse to handle or arrest any person.
Desk Officers	• Notify the Troop Duty Officer; and • Document the incident in the Daily Administrative Journal.
Troop Duty Officer	• Ensure that any employee who has an unprotected exposure while on-duty receives proper first aid and medical treatment; • Assign a supervisor to investigate the exposure; and • Ensure Notice of Injury Report is submitted forthwith per ADM-11B.
Commanding Officers	• Ensure that communicable disease control supplies are made readily available to all members of their Troop/Section/Unit; • In the case of an on-duty unprotected exposure, ensure that the employee receives: 1. Assistance in reporting the exposure; 2. Continued testing for evidence of infection; and 3. Any emotional assistance or counseling as required. • Contact the District Attorney to ascertain if criminal charges are appropriate for intentional exposures.

References

The Ryan White Comprehensive AIDS Resources Emergency Act (Pub. L. 101-381)
OSHA Final Standard on Bloodborne Diseases 29 CFR 1910.1030
Massachusetts Department of Public Health 105 CMR 170-172
Massachusetts Department of Public Health Unprotected Exposure Form
MGL c.111, s.111C
"State Sanitary Code. Chapter VIII", 105 CMR 480.00
Massachusetts State Police Forensic Services Group Laboratory Safety Manual 4.1 dated October 22, 2007.

Promulgated By:

Department of State Police
General Order

Effective Date	Number
November 5, 2008	**GEN-06**

Subject

Drug Testing

Policy

In order to ensure public safety and promote public trust, it is the policy of the Department to maintain a drug-free work environment.

Justification

These compelling reasons justify the use of drug testing:

- **Public Trust**: Members sworn to enforce the law cannot be above it;
- **Public Safety**: The public expects members to have both the physical stamina and psychological stability to properly assume and perform required duties at all times;
- **Potential for Corruption**: Contact with controlled substances and people associated with them exposes members to increased opportunities for corruption;
- **Presentation of Credible Testimony**: A member who illegally uses or abuses drugs would be subject to impeachment through proof or an admission that they violate the law;
- **Morale and Safety in the Workplace**: Every member has the right to be secure in the knowledge that all members are capable of acting in a safe and effective manner; and
- **Loss of Productivity**: The use of controlled substances, and other forms of drug abuse, seriously impair physical and mental health and result in reduced job performance.

Scope

This Drug Testing policy applies to all sworn members of the Department.

Medication Notification

Members shall notify their immediate supervisor when required to use medication that has the potential to impair their job performance.

- The member shall inform their supervisor of the known side effects of such medication and the prescribed period of use;
- The supervisor shall document this information through the use of an internal memorandum to the appropriate Division Commander and shall send a copy to the Occupational Health Unit for review by the State Police Surgeon; and
- The member may be temporarily reassigned other duties, if appropriate.

Subject	Number
Drug Testing	**GEN-06**

Prohibited Activity

Members are prohibited from:

- Illegally possessing any controlled substance;
- Ingesting any unlawful/dangerous drug; and
- Ingesting any controlled substance, unless prescribed by a licensed medical practitioner.

Sanctions

Discipline for members found to be in violation of this Drug Testing policy shall be in accordance with Article 37 of the State Police Association of Massachusetts (SPAM) Collective Bargaining Agreement, the Rules and Regulations for the governance of the State Police, and MGL c. 22C.

Members who refuse to be tested when so ordered, or refuse to enter an Employee Assistance Program or Rehabilitation Program after a positive test, are subject to termination.

Drug Testing Program

Consistent with this policy, the Department has implemented a drug testing program consisting of:

- Drug testing based on reasonable suspicion;
- Random drug testing;
- Post incident drug testing; and
- Annual/biennial physical drug testing.

Employees on extended leave may be subject to drug testing upon their return to service as determined by the Colonel/Superintendent.

Note: The terms “reasonable,” “random,” and “post incident” are defined consistent with Article 37 of the SPAM Collective Bargaining Agreement and all drug testing procedures shall be conducted in accordance with this article.

All drug testing methodologies shall be performed under the Department of Health and Human Services Mandatory Guidelines for federal workplace testing.

References

MGL c.22C
Article 37 SPAM Collective Bargaining Agreement
Rules & Regulations 5.10.2
ADM-11E Extended Leaves

Promulgated By:

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**GEN-07**

Subject

Automatic External Defibrillators

Policy

The Department maintains Automatic External Defibrillators (AED) to help save lives. Only Department members trained in the use of AED's may operate them.

Definitions

Automatic External Defibrillator (AED): An electronic device that when used may:

- Radically reduce the occurrence of disability and death associated with cardiac emergencies through:
  1. An analysis of a victim for bio-electrical activity; and
  2. If needed, administration of an electrical shock.

The supervisor of the Health Unit shall have oversight of AED training, maintenance, and the creation of a standard operating procedure.

Care and Maintenance

Members shall:

- Follow AED procedures prescribed by the Health Unit; and
- Ensure AEDs are not stored in unattended vehicles for any duration, where extreme temperature fluctuations may damage internal components.

Responsibilities for Stations/ Sections with AED

AEDs are considered permanently assigned equipment to the Station/Section. Commanding Officers shall:

- Ensure annually that each device is accounted for according to ADM-30 Asset Management;
- Assign devices according to the Health Unit's standard operating procedure (SOP); and
- Contact the Health Unit for repairs, parts, batteries, or other AED associated supplies as needed.

AED Utilization

AEDs shall only be utilized by members who are trained. Members who possess AED's shall have a copy of the Health Unit's SOP regarding use, maintenance, and reporting procedures.

Each time an AED is utilized to monitor and/or shock an apparent victim of a cardiac arrest the following procedures shall be adhered to:

Position	Duties
The Utilizing Member	• Advise the Desk Officer of AED utilization; and • Before securing from their shift, complete and forward the SP 600 AED Utilization Reporting Form to the Health Unit.
Station Desk Officer	• Document the AED utilization as a Medical Assist into the Daily Administrative Journal; • Do not include the patient name or other identifiers within the entry; and • Provide the incident number to the member who utilized the AED.
Supervisor of the Health Unit	• Ensure AED protocols were followed; • Ensure information received conforms to the SOP; and • Submit the data to the Medical Control Physician for review.

References

MGL c.111, s.201
MGL c.112, s.12V ½
105 CMR 171.180
105 CMR 171.225
ADM-30 Asset Management

Promulgated By:

Department of State Police
General Order

Effective Date	Number
November 5, 2008	**GEN-08**

Subject

Ride-Along/Observer

Policy

The Department may allow approved ride-along/observers to accompany on-duty members for educational purposes.

Requesting Permission to Observe

Requests for an observer(s) to accompany an on-duty member shall be made in writing to the Troop/Section/Unit Commander and detail each observer's:

- Full name;
- Date of birth;
- Address;
- Social Security Number;
- Organization affiliation (if any);
- Date(s) of observation requested;
- Troop/Section/Unit to be observed; and
- Any special considerations (e.g. request to record, request to carry firearm).

The above information shall be forwarded via a SP 629 Observers Release form to the appropriate Division Commander. All requests for ride-along/observers and accompanying forms shall be maintained by the Division Commander's Office.

Media Requests

Requests for a ride-along for media representatives shall be referred to and approved by Commanding Officer of Media Relations.

Responsibilities

Position	Duties
Troop/Section/Unit Commander	• Ensure a background check (including CORI) is conducted on any observer before approving any ride-along/observation; • Approve or deny the request; • Forward any SP 629 to their Division Commander; • Consult with Media Relations, if appropriate; • If approval has been granted, then assign a member to handle the ride-along/observation duty; • Ensure appropriate safety precautions are taken to minimize risk and to ensure the well being of the observer (e.g. require ballistic vest to be worn); and • Detail any conditions the observer and/or assigned member shall follow.
Supervisor	• Ensure adequate scheduled staffing is available; • Ensure appropriate safety precautions are taken to minimize risk and ensure well being of the observer; • Ensure any directives by the Troop/Section/ Unit Commander are adhered to; • Investigate any issues that may arise from an observation assignment per Department policies; and • Provide a summary of the concluded assignment to the Troop/Section/Unit Commander.
Member	• Shall conduct themselves in a professional manner; • Carefully monitor the assigned observer(s); • Immediately report to their supervisor any injuries or issues regarding the observer(s); • Comply with directives issued by the Troop/ Section/Unit Commander; and • Provide a summary of the concluded assignment to their supervisor.

Continued next page.

Subject	Number
Ride-Along/Observer	**GEN-08**

Responsibilities (Continued)

Position	Duties
Observer	• Sign appropriate forms as required by the Department's Legal Section; • Obey all commands and safety directives issued by the escorting member; • Shall wear seatbelts while traveling in state owned vehicles; and • Agree to not electronically record the observation unless prior written approval is granted by the Troop/Section/Unit Commander and Media Relations. Note: Firearms shall not be carried, unless they are a law enforcement officer and the Troop/Section/Unit Commander has specifically approved this request.

References

Executive Order No. 241 Use Of Seat Belts By State Employees
SP 629 Observers Release Form

Promulgated By:

Department of State Police
General Order

Effective Date	Number
May 21, 2018	**INV-01**

Subject

Criminal Investigations

Policy

Investigations shall be conducted on all matters of a criminal nature that fall within the jurisdiction of the Department.

Criminal Investigation

All members assigned to investigate a crime and/or criminal activity shall:

- Be responsible for the thorough and methodical investigation of assigned cases; and
- Continue the investigation until the case is:
  1. Solved or otherwise closed, or
  2. Until it appears that further investigation would be of no significant value.

Division of Investigative Services / Division of Homeland Security and Preparedness

The Division of Investigative Services (DIS) and the Division of Homeland Security and Preparedness (DHS) shall investigate crime and/or criminal activity as determined by the Colonel/Superintendent, District Attorney or Attorney General and in accordance with their section/unit standard operating procedure (SOP).

Cases Involving Human Death

The District Attorney, upon notification of a death shall:

- Have their law enforcement representative direct and control the criminal investigation, in conjunction with the law enforcement agency of jurisdiction. (Massachusetts General Laws c.38 s.4)

Criminal Investigations Field Services Members

Members assigned to the Division of Field Services may initiate criminal investigations, if warranted, in situations where criminal activity is occurring.

Members or their supervisors shall immediately notify, through channels, the appropriate DIS section/unit or DHS section/unit when:

- Circumstances and demands clearly exceed the scope of their investigative abilities or require specialized investigative techniques.

Subject	Number
Criminal Investigations	**INV-01**

Preliminary Investigations for Field Services

In cases where members encounter a situation that necessitates some form of investigation, members may conduct a preliminary investigation concerning those offenses referred to or within the jurisdiction of the Department.

Preliminary investigations may include:

- Determining if a crime has been committed;
- Interviewing the complainant and witnesses;
- Arresting a suspect;
- Protecting the crime scene; and
- Performing other duties necessary to build a solid foundation for follow-up investigators.

Investigations

The first member arriving at a crime scene shall:

- Make scene safety his or her first priority;
- Initiate medical services if needed;
- Secure and preserve the integrity of the crime scene;
- Conduct a preliminary investigation:
  1. Ensuring that evidence is not lost, destroyed, or altered in such a manner as to eliminate its probative value pending the arrival of crime scene/evidence technicians;
  2. Do not move or touch physical evidence unless absolutely necessary, to ensure its preservation; and
  3. If physical evidence is moved, a notation shall be made of its exact location and position at the scene.
- Relinquish their responsibility only when directed by a supervisor or to the designated DIS/DHS investigator assigned to conduct the criminal investigation.

Every effort shall be made to locate, identify and interview reliable witnesses. Witnesses shall be interviewed:

- As soon as possible and in a quiet environment; and
- Separately to ensure independent statements.

If the perpetrator/suspect(s) has left the scene, pertinent information shall be broadcast, as soon as is practicable, utilizing all means necessary.

The member(s) conducting the preliminary investigation should not rely solely on their memory, but should make field notes of all pertinent information. These notes may be subject to discovery by the defense.

The following shall be recorded:

- Date and time of arrival at scene;
- Weather conditions and visibility;
- Exact location, to include addresses, distance measurements, and/or latitude/longitude when possible;

Continued next page.

Subject	Number
Criminal Investigations	**INV-01**

Investigations (Continued)

- Approximate time of the commission of the crime, when it was discovered, and by whom;
- Identity, if possible, or obtain the best available description of the criminal suspect(s);
- Description of any vehicle(s) used by suspect(s);
- Information concerning any physical evidence discovered;
- Name, address of complainant, victim and/or witnesses;
- Identity of other law enforcement officers or civilians present;
- Results of any interviews conducted and statements taken from complainant, victim and/or witnesses; and
- Any other information which may be useful in the apprehension of the perpetrator(s) and subsequent prosecution.

The member conducting the investigation shall complete a written report of the incident.

Reports and Field Notes

All investigative activities, including actions taken, as well as information obtained as a result of said actions, shall be documented in an investigative report.

Investigating members are strongly encouraged to create field notes during the course of an investigation. All relevant facts and information in an investigator's field notes shall be included in the investigative report.

All field notes shall be preserved by the individual member and shall be made available upon request of a supervisor.

Reference

Massachusetts General Laws c.38 s.4

Promulgated By: Ly A Nelly

Department of State Police
General Order

Effective Date	Number
May 21, 2018	**INV-01A**

Subject

Case Management

Policy

Case management is an ongoing process involving all members of the Department. Proper case management facilitates the scope and direction of the investigation, in addition to providing documentation for court proceedings.

Complaint/ Information

All criminal information that is reported to the Department shall be evaluated for appropriate action. Minimum information required from the original source shall include:

- Name;
- Address;
- Telephone number(s);
- Date of birth; and
- Nature of the complaint.

Criminal Investigations DFS Members

Criminal investigations may be initiated by members assigned to the Division of Field Services pursuant to their inherent authority to take immediate, positive, enforcement action in each situation which comes to their attention where laws relating to criminal activity are being violated.

However, the member or first line supervisor shall immediately notify the appropriate investigative section/unit when:

- Circumstances existing at the scene of the incident/offense require the application of specialized investigative techniques; or
- When the demands placed upon the responding member clearly exceed the scope of their investigative authority or abilities.

Case Management

Case management is an ongoing process involving all members, and is used to determine:

- The direction and depth of the investigative process; and
- The necessary resources allocated to a particular investigation.

Subject	Number
Case Management	**INV-01A**

Minimum Complaint Information

For the Division of Field Services, every case assigned or initiated shall be entered into the Daily Administrative Journal (DAJ) to be maintained by all Stations/Sections/Units. Minimum complaint information to be entered shall include:

- Complaint number;
- Date of entry;
- Case received by;
- Complainant's name and address;
- Nature of complaint;
- Investigating member;
- Date of case assignment;
- Date report forwarded; and
- Report number.

For the Division of Investigative Services and the Division of Homeland Security and Preparedness every case assigned or initiated shall be entered into ACISS Case Management. Minimum complaint information to be entered shall include:

- Date Initiated;
- Case Officer;
- Case Type;
- Case Description; and
- Case Status.

Case Number

For the Division of Field Services, all case numbers shall be generated by RAMS.

For the Division of Investigative Services and the Division of Homeland Security and Preparedness, all case numbers shall be generated by ACISS.

Case Responsibility

Assignment of a case shall be to a single member who shall:

- Be responsible for the reports on the case;
- Account for evidence; and
- Coordinate the investigative activity and information.

This does not preclude the assignment of additional personnel, nor does it impair the ability of the supervisor(s) to direct investigative efforts or reporting.

Case File

Department Stations/Section/Units shall maintain a case file system utilizing the case number as the primary filing method.

Subject	Number
Case Management	**INV-01A**

Review/ Approval Process

Reports shall be:

- Reviewed by the reporting member for completeness and accuracy prior to submission;
- Reviewed by a supervisor after submission for completeness and accuracy; and
- Sent back for further investigation if necessary.

Case Suspension

Station/Section/Unit Commanders shall:

- Approve a request to suspend a case by recommendation of the case member when:
  1. Every reasonable avenue of investigation has been pursued and exhausted;
  2. There is a lack of further leads or solvability factors;
  3. Investigative resources are unavailable due to current workload; and
  4. The seriousness of the crime is insufficient to justify continued investigative efforts.
- Ensure that the suspension does not preclude the case from being reopened for any reason.

Note: Certain cases, due to their serious nature, are not eligible for suspended status (e.g., murder, rape, armed robbery).

Case Termination

Only the Station/Section/Unit Commander shall approve requests to close a case and should consider, at a minimum, the following criteria in determining if a case merits termination:

- Seriousness of criminal offense;
- Availability of investigative resources;
- Unfounded complaint;
- Complainant's refusal to cooperate;
- Referral to another agency;
- Declination by prosecutor;
- Adjudication completed; and
- Administrative closing.

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 14, 2018	**INV-02**

Subject

Confidential Informants

Policy

The Department shall develop and use confidential informants, as well as other sources of information, as a means to detect, investigate, and prosecute violators of state and federal law.

Definition

Confidential Informant (CI): A person who provides information to a Department investigator on a continuing or regular basis, and wishes their identity to remain confidential.

This does not include "concerned citizens" who provide information on an informal or casual basis.

Special Circumstances

Certain persons should not be used as informants, except in special circumstances with the approval of the Unit Commander. Such persons include:

- Juveniles (a child who has not yet attained their eighteenth (18) birthday), without parental, guardian or legal custodian's approval;
- Persons wanted on warrants;
- Persons with a criminal record for perjury; or
- Persons with a history of serious mental disorder or defect.

Precautions shall be taken to protect the reputations and safety of informants and investigators. Some informants may require additional precautions:

- Addicts- should be carefully supervised and controlled;
- Parolees- should be avoided whenever possible. Parolees are prohibited from associating with felons and approval from the informant's parole officer is required.

Note: When meeting with informants of an opposite sex or sexual preference, members shall ensure that at least two (2) members are present.

Registration of Informants

When a person indicates a willingness to cooperate and provide information, the Unit Commander or designee shall:

- Interview the person as soon as practicable;
- Investigate the background and suitability of the potential informant; and
- Forward the name and biographical data to the appropriate Detective Captain or Major for entry into the Confidential Informant Database.

The Detective Captain/Major shall:

- Check the CI's name against the Undesirable Informant List; and
- Notify the Unit Commander if the CI is currently cooperating and/or assigned to another section/unit.

The recruiting investigator shall:

- Prepare an SP 405 Informant Information Report when the person is approved to be a CI;
- Keep a copy of the SP 405 within the Unit; and
- Debrief the CI regarding their knowledge of other crimes.

Protecting Informant's Identity

The law recognizes the government's privilege not to reveal the identity of a confidential informant. Protecting the identity of all informants from disclosure is an important factor for two reasons:

1. The informant's safety from retaliation on the part of the criminals they helped implicate; and
2. Disclosure of their identity would prevent the informant from assisting on future investigations.

However, the privilege is not absolute, and should be respected as far as reasonably possible consistent with fairness to a defendant.

Informant Management

Units using informants shall maintain a file for each CI, in a locked and secure location accessible only to the Unit Commander or designee. This file shall include:

- Code Name and Code Number designations;
- Biographical and background information;
- Criminal history records;
- SP 404 Standard Agreement Statement; and
- Other information deemed necessary by the Unit Commander.

Continued next page.

Informant Management (Continued)

Unit Commanders shall:

- Periodically review and evaluate all informants' work performance, usefulness, reliability, desirability and records of payment;
- Meet on a semi-annual basis with all registered informants, both confidential and named, and their controlling officers;
- Submit a determination of the status of the informant in writing to the Division of Investigative Services (DIS) Commander or Division of Homeland Security and Preparedness (DHS) Commander by January 15th and June 15th of every year; and
- Upon the termination of an informant, submit in writing to the DIS Commander or DHS Commander the reason for such termination.

Expenditures

Unit Commanders shall ensure expenditures related to a CI be recorded:

- On a SP 406 Confidential Expenditure Fund Voucher; and
- On a SP 407 Confidential Expenditure Fund Log as outlined in INV-02A Confidential Funds.

Unit Commanders shall:

- Not be required to maintain a SP 407 Confidential Expenditure Fund Log when assigned to the Office of the Attorney General, a District Attorneys Office, or a federal task force where there is an internal mechanism for tracking such Confidential Funds.

Undesirable Informants

The primary handler shall submit a report detailing the CI's undesirable conduct to their Unit Commander whenever a CI:

- Endangers officer safety;
- Deliberately gives false or misleading information; or
- Is otherwise determined to be undesirable for use as an informant.

The Unit Commander shall submit to the appropriate Detective Captain/Major:

- Documentation when a CI is terminated for being undesirable;
- A copy of the applicable SP 405; and
- A copy of the primary handler's report.

The Detective Captain/Major shall:

- Place the CI on the Undesirable Informant List maintained by DIS and DHS.

Promises to Informants

Members may:

- Inform the District Attorney or other agencies of the information provided by the CI and the investigation results;
- Make recommendations to a District Attorney's Office, probation officer, or other criminal justice agency for a disposition on behalf of the CI; and
- Not make any promises to a CI concerning the outcome of a pending court case.

Note: The disposition of court cases is in the province of the District Attorney's Office and the Judiciary.

Precautions

Interactions with CIs should be kept to the minimum necessary for effective investigation purposes. Whenever possible and practical, meetings with CIs shall be:

- Attended by two (2) members; and
- With prior notification of the Unit Commander or a supervisor, or as soon as practicable after the meet.

A member who interacts with a known informant, when not on duty or not during the course of an investigation shall:

- Notify their supervisor as soon as practicable; and
- Document the reason for such interaction in the CI's file with a written report.

Whenever practicable, a CI should not report to the Unit's office in order to protect their identity and the identity of other undercover members. CIs shall not:

- Be introduced to more than a minimum number of undercover members, to ensure that informants gain as little information as possible concerning undercover operations and unit activity.

Any member who uncovers information that an informant has engaged in unauthorized criminal activity shall immediately notify their Unit Commander or designee.

The Unit Commander or designee shall:

- Conduct an immediate evaluation of the information and take such action as they deem necessary; and
- Make every effort to prosecute the CI involved in any unauthorized criminal activity.

Subject	Number
Confidential Informants	**INV-02**

Search Warrants

Search warrant applications and their accompanying affidavits containing information from a CI shall be reviewed and approved by a supervisor before filing the application with the court of jurisdiction.

Division of Field Services

Members assigned to Field Services who are seeking to use an individual as a CI shall advise their Station Commander.

The Station Commander shall:

- Contact their Division Commander through channels for authorization to manage and register the CI; or
- Contact the appropriate DIS Unit Commander or DHS Unit Commander.

References

Commonwealth v. Douzanis 384 Mass. 434,441 (1981)
Commonwealth v. Nelson, 26 Mass. App. Ct. 794 (1989)
Commonwealth v. Lewin 405 Mass. 566 (1989)
Commonwealth v. Brezinski, 405 Mass. 401 (1990)
MGL c.268, s.32
SP 404 Standard Informant Agreement Statement
SP 405 Informant Information Report
SP 406 Confidential Expenditure Fund Voucher
SP 407 Confidential Expenditure Fund Log
INV-2A Confidential Funds
INV-05 Juvenile Operations
Rules and Regulations

Promulgated By:

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**INV-02A**

Subject

Confidential Funds

Policy

Confidential funds may be used to further investigations, and shall be carefully monitored and supervised.

Expenditure of Confidential Funds

Confidential funds may be derived from the funding mechanisms of the Department, the Office of the Attorney General, and the respective District Attorneys' Offices. Grant monies, forfeiture funds, and funds from state and federal government agencies can be used as payment, if such use is not prohibited by state or federal law.

A Unit Commander may maintain a Confidential Expenditure Fund Account. Access to this account shall be restricted to the Unit Commander and/or supervisors.

The Unit Commander may expend monies from a Confidential Expenditure Fund Account for the following investigative purposes:

- The procurement of evidence;
- Payment to a registered confidential informant;
- Investigative expenses; and,
- The purchase of consumable supplies and other equipment in furtherance of an investigation.

Members shall record expenditures from confidential fund accounts on a SP 406 Confidential Expenditure Fund Voucher and shall include the following information:

- Date of expenditure;
- Amount expended; and
- Supervisor's signature.

Members shall ensure the following information is also recorded on the SP 406 where applicable:

- Signature of the member, a witnessing member and the CI confirming receipt of funds.
  Note: CI may use real or assumed name when signing receipt.

Unit Commanders shall maintain a SP 407 Confidential Expenditure Fund Log reflecting:

- The transaction number (expenditures only, from the SP 406);
- The amount of expenditure or deposit; and
- The balance of the account.

Subject	Number
Confidential Funds	**INV-02A**

Accounting and Audits

Prior to the transfer of a Unit Commander, there shall be reconciliation of the accounting records and of the monies on hand with the incoming Unit Commander.

Each quarter, Unit Commanders shall review, evaluate, and analyze all records of expenditures to ensure funds are being used in a cost-effective manner.

An internal audit of all accounting records and accounting practices shall be conducted annually by the appropriate Division Commander.

An audit of Confidential Funds files may be conducted as directed by the appropriate Division Commander or as directed by the Colonel/ Superintendent.

Exceptions

Unit Commanders shall not be required to maintain a SP 407 Confidential Expenditure Fund Log under the following conditions:

- Members who are assigned to the Office of the Attorney General, a District Attorneys' Office, or a federal task force; and
- An internal mechanism exists for tracking Confidential Funds.

References

SP 406 Confidential Expenditure Fund Voucher
SP 407 Confidential Expenditure Fund Log

Promulgated By:

Department of State Police
General Order

Effective Date	Number
May 21, 2018	**INV-03**

Subject

Prescription Monitoring Program

Purpose

The purpose of the Prescription Monitoring Program is to assist health care providers and investigative agencies in addressing drug diversion and the misuse and abuse of pharmaceutical controlled substances.

The Prescription Monitoring Program is a computer-based system that collects prescription data submitted by pharmacies on most prescriptions for controlled substances in Schedules II through V.

Massachusetts General Laws (MGL) c. 94C s.24A established the Prescription Monitoring Program within the Department of Public Health (DPH) effective January 1, 2011. The Department shall, upon request, provide data from the Prescription Monitoring Program to local, state and federal law enforcement or prosecutorial officials working with the Executive Office of Public Safety and Security engaged in the administration, investigation or enforcement of the laws governing prescription drugs; provided, however, that the data request is in connection with a bona fide, specific controlled substance or additional drug-related investigation.

Policy

Only members designated by the Department may access or use information contained within the Prescription Monitoring Program. Access to the system must be pursuant to a bona fide, specific controlled substance investigation or a related criminal investigation.

Any member, who violates this policy and/or state regulations related to the Prescription Monitoring Program, may face disciplinary action, as well as loss of access to the Prescription Monitoring Program.

Subject	Number
Prescription Monitoring Program	**INV-03**

Access to the Prescription Monitoring Program

The Department shall:

- Authorize sworn members assigned to the Division of Investigative Services and the Division of Homeland Security and Preparedness to access and use information obtained via the Prescription Monitoring Program in accordance with state regulations.

According to state regulations, any member granted access to the Prescription Monitoring Program shall:

- Successfully complete any and all required training; and
- Not share their passwords or codes with any other person.

Use Of Data From The Prescription Monitoring Program

Data ascertained from the Prescription Monitoring Program:

- May only be used in furtherance of the official Department investigation for which it was requested;
- May only be shared with authorized personnel from other law enforcement agencies or with state and federal prosecutors who are working on the matter for which it was requested; and
- Shall not be disseminated to others.

Designated members are:

- Allowed to use the Prescription Monitoring Program and the associated data only in connection with the bona fide specific controlled substance related criminal investigation for which it was requested.

Members shall not use the data or information from the Prescription Monitoring Program:

- For the furtherance of any illegal act, including violation of any criminal or civil laws or regulations;
- For any political or commercial purpose;
- To libel or otherwise defame any person(s); or
- For any matter other than the one for which it was requested.

Prior to accessing the Prescription Monitoring Program, the member shall:

- Notify their supervisor;
- Open an investigation;
- Obtain a Department Case Number; and
- Write a short narrative that includes information leading to the belief that prescription drugs are being diverted for illegal purposes.

Subject	Number
Prescription Monitoring Program	**INV-03**

Supervisor Responsibilities

Responsibilities of the Division of Investigative Services and the Division of Homeland Security and Preparedness Supervisors shall include:

- Ensuring that members under their command comply with the provisions of this policy and MGL c.94C s.24A;
- Monitoring members use in order to ensure compliance; and
- Notifying the Prescription Monitoring Program Administrator when a designated member transfers from the unit.

References

Massachusetts General Laws c. 94C §.24A

Promulgated By:

Department of State Police
General Order

Effective Date	Number
July 12, 2018	**INV-05**

Subject

Special Protections for Juveniles

Policy

Courts recognize the vulnerability of children. The Department shall ensure that juveniles are afforded special protections during interrogations.

Definitions

Juvenile: A child who has not yet attained his or her eighteenth (18) birthday.

Interested Adult: An adult in a position, where he or she is an advocate or has the best interest at heart for the juvenile. The adult shall be eighteen (18) years of age or older and preferably be a parent or legal guardian, or an adult sibling, relative, friend, or attorney.

Juveniles and Miranda

The duration of questioning and the number of members present should be as minimal as possible both to prevent a coercive atmosphere and to protect the juvenile's rights.

Before proceeding with a custodial interrogation of a juvenile, Miranda Warnings shall be given in accordance with the following table, and in the presence of the juvenile, their parent, guardian, or other interested adult. The juvenile shall then be allowed to have a meaningful consultation with the adult. Written waivers are preferred.

If the Juvenile's Age is…	Then…
Under twelve (12) years of age e.g., 1; 2; 3; 4; 5; 6; 7; 8; 9; 10; or 11 years.	No criminal charges can be filed. They shall not be questioned, unless a parent or interested adult is present.

Continued next page.

Subject	Number
Special Protections for Juveniles	**INV-05**

Juveniles and Miranda (Continued)

If the Juvenile's Age is…	Then…
Twelve (12) years of age and not yet attained his or her fourteenth (14) birthday, e.g., 12 or 13 years.	Criminal charges can be filed. The juvenile shall not be questioned, unless a parent or interested adult is present. The interested adult and the juvenile must have an actual opportunity to discuss their rights in private. Moreover, police *must* honor any request by the juvenile or adult to meet privately. Questioning can only commence when the juvenile and the adult indicate that they understand the rights and the consequences of waiving these rights; and when the juvenile expressly waives his or her rights.
Fourteen (14) years of age, but not yet attained his or her eighteenth (18) birthday e.g., 14; 15; 16; or 17 years; and a parent or interested adult is not available after reasonable efforts are made to contact them.	Criminal charges can be filed. The juvenile must be given the opportunity to have a meaningful consultation with an interested adult before he or she can waive Miranda rights. The best practice dictates that the interested adult and the juvenile be given the opportunity to confer in private. Moreover, police *must* honor any request by the juvenile or adult to meet privately. However, a statement *may* be taken if the juvenile demonstrates a high degree of intelligence, experience, knowledge, or sophistication in understanding the Miranda Warnings and the consequences of waiving his or her rights and expressly waives his or her rights.

Special Considerations

Members may have to take extra steps to ensure that juveniles understand their rights. This may include explaining or repeating the Miranda rights, or explaining Department procedures or juvenile court procedures to the juvenile.

Other factors to consider are the juvenile's level of schooling, maturity, history of interaction with the juvenile justice system, and any mental or emotional conditions.

Subject	Number
Special Protections for Juveniles	**INV-05**

References

MGL c.119, § 1, § 21, § 34, § 39, § 39H, § 66, § 67, § 68B
MGL c.111B § 8
MGL c.276, § 57-58
MGL c.138, § 34C
MGL Session Law-Acts of 2012 c.240
MGL Session Law-Acts of 2013 c.3 § 5B
Juvenile Justice & Delinquency Prevention Act of 1974 and 2002 (42 USC 5601)
Criminal Justice Information System (CJIS) Extranet

Promulgated By:

Department of State Police
General Order

Effective Date	Number
May 21, 2018	**INV-07**

Subject

Non-Published Telephone Numbers

Policy

Telephone company records shall only be obtained when necessary for the furtherance of a criminal investigation or in an emergency.

Statutes

Administrative Subpoena: Issued in the form of a demand letter for telephone company records and may only be authorized by the Attorney General or District Attorney of jurisdiction. Massachusetts General Laws (MGL) c.271, s.17B.

Electronics Communications Privacy Act: Limits access to certain records maintained and stored by a common carrier such as a telephone company. The act sets forth the requirements needed to obtain such records. (18 USC, s.2703)

Authority For Obtaining Records

In order to obtain telephone records, authority may only be granted by:

- Administrative subpoena authorized by the Office of the Attorney General or District Attorney of jurisdiction;
- State or federal grand jury or trial subpoena;
- State or federal warrant;
- State or federal court order; or
- Consent of the customer or subscriber to such disclosure.

Records Available

When a member has reasonable suspicion to believe that the service of a common carrier is being or may be used for an unlawful purpose, they may request, through the Office of the Attorney General or the District Attorney's Office of jurisdiction, an administrative subpoena, for release of records from the common carrier to include, but not limited to:

- Listing of a non-published telephone number;
- Listing of all optional services;
- Telephone toll records and optional services;
- Telephone services, including non-published number; and
- A copy of the contract, listing, and monthly bills for cellular phone and electronic paging.

Subject	Number
Non-Published Telephone Numbers	**INV-07**

Procedure

Members shall submit a request through channels to the Attorney General or District Attorney requesting a subpoena for the required information.

The request shall:

- Detail the grounds for the member's belief that the telephone is being used for an unlawful purpose; and
- Include the case number and the signature of the member's Commanding Officer.

Members shall also follow any written directives promulgated by the Office of the Attorney General or the District Attorney's Office of jurisdiction to request telephone records.

Members not assigned to the Office of the Attorney General or a District Attorney's Office shall contact, through channels, the appropriate State Police Detective Unit Commanding Officer for assistance in determining the policy of the respective jurisdiction.

Emergencies

Troop Duty Officers or Unit Commanders may authorize members to contact the Directory Assistance Operator in emergency situations, such as a serious motor vehicle accident or threat of imminent harm. The member shall:

- Request the operator contact the non-published customer; and
- Inform the customer to call back the member.

This alternative shall not be used to facilitate investigative inquiries, such as attempting to locate a witness.

Reports

Non-published numbers obtained pursuant to a criminal investigation shall be properly documented in the record of investigation in order to:

- Provide the information to the Criminal Information and Intelligence Section; and
- Eliminate duplicate requests to the common carrier, when possible.

When a non-published number is included in a report it shall be clearly noted as such, so that it is not released to the public via the record of investigation.

References

MGL c.271, s.17B
18 USC, s.2703

Promulgated By:

Department of State Police
General Order

Effective Date	Number
May 21, 2018	**INV-08**

Subject

Criminal Intelligence

Policy

The Department shall share criminal intelligence among the criminal justice community in an effort to prevent and control crime, while protecting the privacy and constitutional rights of individuals.

Definitions

Criminal Information: Raw data, gathered by law enforcement agencies in the normal course of performing their duties, which is maintained as directed by statute or policy.

Criminal Intelligence Information: Information that has been evaluated and determined to be of value to criminal investigations.

Criminal Intelligence System: The equipment, facilities, and procedures used for the receipt, storage, exchange, dissemination, and analysis of criminal intelligence information.

Content Validity: Refers to the accuracy or truth of the information.

Need-to-Know: The necessity to obtain or receive criminal intelligence information in the performance of official responsibilities as a law enforcement authority.

Right-to-Know: The legal authority to obtain or receive criminal intelligence information pursuant to a court order, statute, or case law.

Reasonable Suspicion: When information exists that provides sufficient facts to believe that there is a reasonable possibility an individual or organization is involved in a definable criminal activity or enterprise.

Source Reliability: Refers to the reliability of the source of the information.

Subject	Number
Criminal Intelligence	**INV-08**

Security

Criminal intelligence information shall be stored in a criminal intelligence database that prevents unauthorized access.

The criminal intelligence database shall provide an audit trail that tracks:
- What intelligence was accessed;
- Who accessed the intelligence; and
- The date and time when the intelligence was accessed.

Collection

Criminal intelligence information shall only be collected and maintained if there is reasonable suspicion to believe that an individual or group is involved in criminal activity and the information is relevant to criminal conduct or activity.

Electronic surveillance shall only be conducted in accordance with all applicable state and federal regulations.

Photographic surveillance shall only be conducted in an effort to identify individuals or groups who are believed:
- To have participated in criminal activity;
- To be planning criminal activity; or
- Are currently engaged in criminal activity.

Each criminal intelligence submission shall be attributable to a credible source. All criminal intelligence information shall be forwarded to the Criminal Information and Intelligence Section (CIIS), as soon as possible, using one of the following methods:
- Direct Entry: Information entered by an authorized member into the criminal intelligence database directly from an authorized Department computer; and
- Indirect Entry: Information entered by CIIS on behalf of a member who does not have authorized access to the criminal intelligence database. Note: CIIS may be contacted for guidance, clarification, and additional support to facilitate criminal intelligence submissions.

Members who submit information for entry into the criminal intelligence database shall classify the source(s) as:
- Completely Reliable: The source is unquestioned or has been tested successfully in the past; or
- Usually Reliable: The source can usually be relied upon. The majority of information provided in the past has proved to be reliable; or
- Unreliable: The source has been determined to be unreliable in the past; or
- Reliability Unknown: The source cannot be judged. Its authenticity or trustworthiness has not yet been determined by either experience or investigative corroboration.

Continued next page.

Subject	Number
Criminal Intelligence	**INV-08**

Collection (Continued)

Members who submit information for entry into the criminal intelligence database shall classify the validity of the information as:

- Confirmed: Has been corroborated by an investigator or another reliable independent source; or
- Probable: Is consistent with past accounts; or
- Doubtful: Is inconsistent with past accounts; or
- Cannot Be Judged: Validity of the information cannot be judged, or its authenticity has not yet been determined.

Note: A source classified as "Reliability Unknown" combined with a content validity rating of "Cannot Be Judged" would not meet the burden of reasonable suspicion for inclusion into the criminal intelligence database.

Information concerning individuals or organizations not reasonably suspected of criminal activity that is entered into the criminal intelligence database, shall be marked as "non-criminal identifying information."

Restrictions

Information and criminal intelligence shall not be collected or developed solely on the basis of an individual or group's:

- Support of a particular cause;
- Race;
- Color;
- Religion;
- Gender;
- National origin or ancestry; or
- Political affiliation.

Information pertaining to the above listed factors shall only be collected and maintained if the information directly relates to criminal conduct, and there is reasonable suspicion that the subject is or may be involved in criminal activity.

Dissemination

Submitting Department entities are responsible for the review and evaluation of data entered into the criminal intelligence database and establishing dissemination levels. Criminal intelligence information shall only be disseminated:

- In the furtherance of an authorized law enforcement activity;
- To authorized law enforcement or criminal justice personnel; and
- On a "need-to-know" and "right-to-know" basis.

Subject	Number
Criminal Intelligence	**INV-08**

Review/Purge

Intelligence information held within the criminal intelligence database shall be:

- Reviewed on a continual basis;
- Purged when found to be obsolete or inaccurate; and
- Purged when information has not been updated or verified for five (5) years from date of entry.

The Commanding Officer of CIIS, when determining whether or not to purge intelligence records contained within the criminal intelligence database shall:

- When feasible, contact the member or agency which contributed the intelligence information to determine if any additional intelligence may be added to update the record;
- Purge the record from the system if there is no additional intelligence;
- Ensure only an administrative record of the purge is maintained; and
- Ensure there is no record of the original criminal intelligence information maintained within the system.

References

MGL c.22C, s.38
28 CFR Part 23
MGL c.272, s.99

Promulgated By:

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**INV-09**

Subject

Polygraph Examinations

Policy

The polygraph is a reliable investigative aid when used by a professional examiner. The Department shall use the polygraph with great selectivity, and then, only as an investigative tool.

Polygraph Examiners

Department Polygraph Examiners shall be designated by the Colonel/ Superintendent.

Restrictions on Polygraphs

In general, an employer cannot request or subject an employee or job applicant to take a polygraph within or outside the Commonwealth. (Massachusetts General Laws (MGL) c.149, s.19B)

Polygraph examinations may not be used for any person applying for employment. Department recruit applications shall contain the following notice:

"It is unlawful in Massachusetts to require or administer a lie detector test as a condition of employment or continued employment." MGL c.149, s.19B(2)(b)."

At present, polygraph evidence is inadmissible in criminal trials and may not be used in a criminal trial for any purpose. (Commonwealth V. Mendes).

Subject	Number
Polygraph Examinations	**INV-09**

Administering an Examination

Under MGL c. 149, s.19B law enforcement agencies are permitted to administer a polygraph examination when the polygraph is requested as part of a criminal investigation.

Submission to the polygraph examination must be a voluntary act on the part of the examinee, and this exemption does not invalidate the constitutional rights of the examinee.

Prior to an examination, the examinee shall sign:

- A statement of voluntariness; and
- A witnessed waiver of any rights against the Polygraph Examiner and the Department.

Requesting an Examination

To request an examination, Department members shall contact the Polygraph Unit through channels.

Any requests from local, state or federal agencies shall be referred to the Polygraph Unit. The Polygraph Unit may decline to conduct an examination.

It is the responsibility of the requesting agency to provide the background of the case and transportation of the examinee to and from the place of examination.

Preparing for an Examination

The member requesting the examination is responsible for providing the Polygraph Examiner with pertinent information concerning the case including:

- Information that supports and justifies the use of the polygraph;
- Investigative reports;
- Evidence available and withheld from the subject;
- Background information on the subject;
- Statements made by the subject, complainants, and witnesses including alibis; and
- Newspaper articles or other general information concerning the case.

Members shall not:

- Interrogate a subject immediately before they are to take a polygraph; or
- Attempt to explain procedures that shall be used in the examination.

Subject	Number
Polygraph Examinations	**INV-09**

Internal Investigations

No member of the Department shall be subjected to a polygraph examination for a violation of written directives, except in cases of alleged criminal conduct.

Department Polygraph Examiners shall not be required to conduct examinations on members of the Department.

The Commander of the Polygraph Unit shall establish reciprocal agreements with other State Police agencies for examinations, when warranted, and as approved by the Colonel/Superintendent.

Department members may assist other state and local law enforcement agencies with internal investigations that involve allegations of criminal wrongdoing. Requests for examinations shall:

- Be in writing; and
- Contain a statement that the polygraph is for a criminal investigation.

References

MGL c.149, s.19B
Furtado v. Plymouth 69 Mass. App. Ct. 319 (2007), and SJC-10049 (2008)
Baglioni v. Chief of Police Of Salem, 421 Mass. 229 (1995)
Commonwealth v. Mendes, 406 Mass.201, 212 (1989)
Patch v. Mayor of Revere, 397 Mass. 454 (1986)
Baker v. Lawrence, 379 Mass. 322 (1979)
International Brotherhood of Police Officers v. Labor Relations Commission 391 Mass. 429 (1984)
Carney v. the City of Springfield 403 Mass. 604 (1988)

Promulgated By:

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**INV-10**

Subject

Evidence Collection and Preservation

Policy

The Department shall ensure that evidence is properly recognized, documented, collected, packaged, and stored; and that a chain-of-custody is established for evidence recovered at every crime scene.

Definitions

Chain-of-Custody: The record documenting the location and person in control of evidence from the time of its collection to final disposition.

Evidence Room: Facilities used by the Department to store evidence.

Forensic Services

The Forensic Services Groups within the Division of Investigative Services are a valuable resource at crime scenes. On-call employees within this group are highly trained and equipped to collect many types of evidence.

Crime Lab Response Team (Chemists): This team assists with the recognition, collection and preservation of biological (DNA) evidence including blood, semen and saliva; and can also assist with the recognition, collection, and preservation of gunshot residue and trace evidence such as hairs and fibers.

Crime Scene Services Section (CSSS): This section assists with the recognition, collection, processing, preservation and documentation of many types of physical evidence. Services also include:

- The documentation of crime scenes through photographs, videos, diagrams and sketches;
- The collection and processing for footwear and tire track impression evidence, latent print evidence, and bloodstain pattern analysis; and
- The collection and preservation of many other types of physical evidence.

Digital Evidence and Multimedia Section (DEMS): This section assists with the recognition, collection, preservation, and examination of computers and other digital evidence devices, (e.g., cell phones, cameras, and digital storage media). This section can provide field assistance with drafting of search warrants for digital evidence crime scenes and digital evidence seizures.

Firearms Identification Section (FIS): This section assists with the collection, preservation and documentation of firearms, firearms related evidence, and tool mark evidence.

Subject	Number
Evidence Collection and Preservation	**INV-10**

Arriving at a Crime Scene

Evidence of a criminal nature may potentially be encountered at any incident or call. When arriving at a scene, members should consider the nature of the incident or crime, the jurisdiction, and their investigative authority in the context of recovering evidence of a crime.

Members arriving at a scene shall:

- Attempt to identify and control any dangerous situations or persons bearing in mind the safety of the public and the officer;
- Ensure that medical attention is provided to injured parties;
- Take care when removing the injured or rendering the scene safe and secure; and
- Be mindful that any action taken may affect or alter a potential crime scene and should be documented.

Crime Scene Evaluation

When a scene requires specialized investigative and forensic units, responding members shall:

- Secure the scene and treat the area as a potential crime scene;
- Evaluate the nature of the event or crime and the resources required to effectively respond to the situation; and
- Preserve the scene with minimal contamination and disturbance of potential evidence.

Members shall:

- Notify the Desk Officer or appropriate supervisor of all actual or potential crime scenes;
- Request assistance from other patrols, supervisor(s), investigative, or forensic units as necessary; and
- Document and relay to appropriate supervisory, investigative, or specialized personnel relevant activities and observations made.

Desk Officers shall:

- Notify the Troop Duty Officer of complex crime scenes that require specialized assistance.

Troop Duty Officers shall:

- Request the assistance of specialized units when the scene requires skills or equipment beyond those of the initial responding member(s).

Crime Scene Command and Control

Responding members shall:

- Remain in charge of the scene until command is transferred to a supervisor or to the responding specialized unit(s);
- Continue to provide assistance until released; and
- Document activities while at the scene.

Subject	Number
Evidence Collection and Preservation	**INV-10**

Crime Scene Perimeter and Control

Members responding to a crime scene shall:

- Establish a crime scene perimeter;
- Establish boundaries beyond the initial scope of the crime scene perimeter with the understanding that boundaries can be reduced, but cannot be easily expanded;
- Control access to the scene to authorized personnel only; and
- Document the names of all persons who accessed the scene.

Recovery of Evidence

Crime scenes shall be documented prior to processing and searching. Documentation may include:

- Written description;
- Photographs and videos; and
- Sketches and diagrams.

Members may collect any evidence that does not require assistance from specialized units. Members shall take steps to minimize the handling of evidence. Members shall:

- Wear gloves during evidence collection;
- Understand that when gloved, the handling of evidence may destroy or damage latent fingerprint and DNA evidence; and
- Package evidence in a manner to preserve and prevent spoilage or contamination.

All evidence shall be uniquely identified. The identifiers shall be recorded on the outside of each packaged item and include:

- The case identifier/number;
- Seizing member's name and identification (ID) number; and
- The date, location of seizure, and description of the item(s).

When multiple items are recovered from a single location, members shall sequentially number items for identification purposes.

When personnel from specialized units collect evidence, they shall adhere to their respective policies and directives.

Members shall take appropriate precautions when collecting or storing biological matter or chemical substances, that may pose serious health risks if handled improperly or unprotected.

The Department's Forensic Services Group provides evidentiary guidelines on the proper methods to collect and package different types of evidence. Members may contact the Forensic Services Group for guidance on proper evidence packaging.

Subject	Number
Evidence Collection and Preservation	**INV-10**

Evidence

Station/Section/Unit Commanders shall be responsible for receiving, storing, maintaining, releasing, and accounting of all evidence. Commanders shall ensure that:

- Evidence is placed into the evidence room or other authorized secure location in accordance with Department policy; or
- If analysis is required, evidence is promptly submitted to the appropriate facility.

Any member who recovers or receives evidence to be placed in the evidence room shall have evidence documented at the appropriate station using appropriate Department forms. The inventory shall be witnessed and shall include the following information for all items of evidence:

- Description of the item (including make, model number, and serial number, if any);
- Source (from whom or location obtained); and
- Name of person primarily responsible for collecting the item or items.

References

INV-11 Controlled Substances – Storage and Handling
INV-11A Contraband – Storage and Handling
INV-14 Seized Currency

Promulgated By:

Department of State Police
General Order

Effective Date	Number
May 10, 2012	**INV-11**

Subject

Controlled Substance -Storage & Handling

Policy

The Department shall establish rigid controls for all controlled substances held within its custody to preserve the integrity of the Department and its personnel.

Through the assignment of responsibilities, processing procedures, storage requirements and continuous inspections, all levels of command shall ensure strict compliance with established controls and this policy.

Definition

Controlled Substances: All narcotics, drugs, and substances listed in Massachusetts General Laws (MGL) Chapter 94C.

Narcotics Inspection Unit (NIU): The unit shall exercise administrative control and supervision of procedures concerning the marking, recording, storage, handling, disposal, and destruction of all controlled substances obtained or seized by members of the Department.

NIU Bunker: Narcotics Locker located at the State Police General Headquarters used to store controlled substances that have been transported from a Station/Section/Unit or Central Evidence Locker and are awaiting trial, destruction, or disposal.

Narcotics Central Evidence Locker (CEL): A secure location located within the State Police Troop of Jurisdiction. Each CEL is staffed by NIU personnel. Each CEL shall have direct control and responsibility for the handling, storage, and security of controlled substances seized by members located within their Troop Jurisdiction.

Department Evidence Officer: A member appointed by the Colonel/Superintendent to act as custodian of all controlled substances seized in the course of any arrest or investigation by the Department.

Subject	Number
Controlled Substance	**INV-11**

Responsibilities

Position	Duties
Narcotics Inspection Unit Commander	• Assume responsibility and duties specified in MGL c.94C, s.47A, as the "Evidence Officer" for the Department; and • Shall have command and control of the Narcotics Locker (NIU Bunker) located at General Headquarters.
Troop/Section Commanders	• Ensure the security and safeguarding of all controlled substances held in all Stations/Sections/Units under their command.
Station/Section/Unit Commander	• Has the responsibility as the "Evidence Officer" of their Station/Section/Unit; • Has direct control and responsibility for the handling, storage, and security of controlled substances seized by members under their command; • Retain responsibility of all controlled substances and ensure adherence to Department Policy and Procedures; and • Ensure that members under their command are trained and familiar with the appropriate handling and storage of controlled substances. In addition, Station/Section/Unit Commander may: • Delegate the duties of the Evidence Officer to any member under their command; and • Designate that member to serve as the "Assistant Evidence Officer" for that Station/Section/Unit.
Investigating Officer of Controlled Substance(s)	Upon arrival at the Station/Section/Unit the Investigating Officer shall: • Log in the controlled substance(s) into the Station/Section/Unit Daily Administrative Journal and in the Temporary Narcotics Evidence Locker Journal;

Continued next page.

Subject	Number
Controlled Substance	**INV-11**

Responsibilities (Continued)

Position	Duties
Investigating Officer of Controlled Substance(s)	• Prior to the end of their shift tag each item or place each item in a Department Evidence bag with the information listed below. 1. Defendant's name(s). 2. Defendant's DOB. 3. Case number. 4. Date seized. 5. Location where seized. 6. A brief description of the item, listing the quantities on the evidence packaging and chain of custody form. • Indicate whether the controlled substance(s) have been transferred: 1. Directly to the Evidence Officer; or 2. The controlled substance(s) have been placed in the Temporary Contraband/Controlled Substance Locker with entries made into the Temporary Narcotics Evidence Locker Journal. • Ensure that the SP 295 Narcotics Custody Form is completed. Note: See Controlled Substance Storage Area within this policy for controlled substances that are too large to fit into the Temporary Contraband/Controlled Substances Locker.

Station/Section/ Unit Evidence Officer

The Station/Section/Unit Commander or Evidence Officer shall:

- Maintain the Temporary Narcotics Evidence Locker Journal issued by the Narcotics Inspection Unit;
- Ensure the Temporary Narcotics Evidence Locker Journal is kept near the Temporary Contraband/Controlled Substance Locker;
- Check the Temporary Narcotics Evidence Locker Journal and Temporary Contraband/Controlled Substance Locker during their shift for items that may have been deposited;
- Contact NIU and/or the CEL when controlled substances have been seized and are in the Temporary Controlled Substance Locker; and
- Ensure that the controlled substances are properly labeled and packaged by the Investigating Officer and that they have completed the SP 295.

Note: Assistant Evidence Officers shall perform duties as directed by the Station/Section/Unit Commander.

Controlled Substance Storage Area

Permanent Storage

Permanent Storage of controlled substances shall:

- Be stored at the CEL of jurisdiction and the NIU Bunker; and
- Not be stored in vehicles or personal storage areas.
  Note: For training purposes, controlled substances may be stored at the Troop Headquarters K-9 Aid Storage Lockers with prior approval from the Troop Commander.

Temporary Storage

Each Station/Section/Unit shall:

- Be provided with a Temporary Contraband/Controlled Substance Locker with twenty-four (24) hour access to all authorized personnel;
- Allow for the temporary secure storage of controlled substances; and
- Have available a Temporary Narcotics Evidence Locker Journal to enter all pertinent information.

The Evidence Officer shall:

- Ensure that the Temporary Contraband/Controlled Substance Evidence Locker remains securely locked at all times; and
- Prevent access to unauthorized personnel.

Unusual Value or Size

The CEL of jurisdiction and/or the NIU Commander shall be called immediately for instructions and assistance when:

- Seized narcotics evidence is too large to fit in the temporary Contraband/Controlled Substance Evidence Locker; and
- When any amount of marijuana plants are seized.

The Evidence Officer shall:
Make arrangements with the NIU and/or the CEL of jurisdiction for the storage of items of extreme value or unusual size that meet the following criteria:

Narcotics	Quantity
Marijuana	50 pounds or more
Cocaine	10 ounces/280 grams or more
Heroin	28 grams or more
Tablets/Pills	1000 or more of Class A, B or C

Controlled substances meeting the above criteria shall:

- Not be held for more than seventy-two (72) hours at any Temporary Contraband/Controlled Substance evidence locker or CEL unless:
  1. Authorization is granted by the NIU Commander.
- Be stored at the NIU Bunker in Framingham. If possible, the controlled substance should be submitted to the Crime Laboratory for analysis prior to being secured at the NIU Bunker.

Continued next page.

Subject	Number
Controlled Substance	**INV-11**

Controlled Substance Storage Area (Continued)

The Evidence Officer or Investigating Officer shall:

- Notify the NIU or CEL forthwith to make arrangements for the transportation of the controlled substances according to NIU procedures.

Chain of Custody

Change In the Chain of Custody

The Investigating Officer shall:

- Complete the SP 295 Narcotics Custody Form; and
- Ensure the SP 295 is attached to controlled substances involved in a temporary change of possession outside the custody of the Station/Section/Unit Evidence Officer.

Change in the chain of custody controlled substances shall:

- Be considered when controlled substances are required at judicial proceedings and are transferred to the Investigating Officer from the Station/Section/Unit Evidence Officer, CEL or NIU;
- Have entries made on the SP 295 and in the Temporary Narcotics Evidence Locker Journal (if applicable). In the event that additional space is required to accommodate entries on the SP 295, additional SP 295's shall be used and recorded as "Page 1 of 2, Page 2 of 2 etc"; and
- Require copies of the SP 295 be retained and distributed as indicated on the form.

Handling or Transport Controlled Substances

Each time controlled substances are handled or transported, members shall:

- Ensure the presence and condition of the controlled substance by examining the material without opening closed containers or breaking any seals;
- Obtain the signature of the receiving party; and
- Document the date and location on the SP 295.

Inspection of Control Substance Packaging

All members involved in the movement of controlled substances at either the Station/Section/Unit, CEL or, NIU level shall:

- Inspect the packaging for signs of tampering; and
- Immediately notify the Station/Section/Unit Commander and the NIU Commander if the packaging appears to have been tampered with.

The Station/Section/Unit Commander shall:

- Notify through channels to the Division of Standards and Training and request that an investigation be conducted.

Continued next page.

Subject	Number
Controlled Substance	**INV-11**

Chain of Custody (Continued)

Control Substance Packaging Opened

When any controlled substance evidence is opened during a court proceeding:

- A SP 655 Court Order to Open Secured and Closed Narcotic Evidence form shall be generated and kept with the opened evidence;
- The SP 655 shall include the name of the judge who requested it to be opened; and
- The SP 655 shall be signed by the Presiding Judge that ordered the evidence opened, or by either the Assistant District Attorney (ADA), or the Clerk Magistrate of the Court.

Note: The Evidence Officer may complete the SP 655, however it shall only be signed by a judge, ADA, or clerk magistrate.

Inspections

Troop/Section Commanders shall:

- Conduct monthly line inspections of all Temporary Contraband/Controlled Substance Storage areas under their control to ensure compliance.

The NIU shall:

- Annually, or as directed by the Office of the Colonel/Superintendent, conduct official, unannounced, and random inspections of all Department Permanent Controlled Substance Storage Lockers to ensure compliance

The NIU shall:

- Issue a written report with its findings and observations regarding the inspection conducted;
- A copy of this report shall be sent to:
    1. The Troop/Station/Section/Unit Commander (if applicable),
    2. The supervisor of the CEL inspected; and
    3. The NIU Commander

The Staff Inspections may:

- Conduct periodic checks of all Department Controlled Substance Lockers to ensure integrity of the system.

Training

Station/Section/Unit Evidence Officers, CEL and NIU personnel may:

- Be required to attend specified training conducted by the NIU Commander; and
- Include classroom and/or online academy training.

Subject	Number
Controlled Substance	**INV-11**

Inventories

When practicable as deemed by the Troop/Section Commander or designee, an inventory of all controlled substances may be conducted whenever a new Evidence Officer or Assistant Evidence Officer is designated.

In such instances, the outgoing and incoming Evidence Officers/Assistant Evidence Officers shall:

- Conduct an inventory jointly to verify controlled substances physically stored within that jurisdiction; and
- Document results within the Daily Administrative Journal.

References

MGL c.94C, s.47A
MGL c.22C, s.45, s.46
SP 295 Narcotics Custody Form
SP 655 Court Order to Open Secured and Closed Narcotic Evidence

Promulgated By:

Colonel Marian J. McGovern

Department of State Police
General Order

Effective Date	Number
June 17, 2013	**INV-11A**

Subject

Property and Contraband

Policy

The Department shall establish procedures for all found, unclaimed, or abandoned property including contraband held within its custody to preserve the integrity of the Department and its personnel.

All levels of supervision shall ensure strict compliance with established procedures within this policy regarding processing, storage requirements, and inspection.

Definition

Found Property: Any property discovered or found by the general public and turned over to the Department or to any police officer.

Unclaimed/Abandoned Property: Any property that comes into the possession of the Department by means of any police officer with no known owner.

Contraband (excluding controlled substances):

- May be property that is not in and of itself unlawful for a person to acquire or possess; however
- May have been acquired by the Department because of its use in an unlawful activity or manner, of its nature, or due to circumstances surrounding the person who acquired or possessed it.
  Note: Contraband in these instances shall be evidentiary and documented when applicable according to Policy and Procedure *INV-10 Evidence Collection and Preservation*.

Property Custodian: The Commanding Officer of each Station/Section/Unit shall be responsible for receiving, storing, maintaining, releasing, and accounting of all found, unclaimed, abandoned property and contraband under their command.

Subject	Number
Property and Contraband	**INV-11A**

Responsibilities

Position	Duties
Troop/Section Commanders	• Ensure the security and safeguarding of all found, unclaimed, abandoned property and contraband, held in all Stations/Sections/Units under their command.
Station/Section/Unit Commander	• Shall be designated as the "Property Custodian" of their Station/Section/Unit; • Shall be responsible for receiving, storing, maintaining, releasing, and accounting of all found, unclaimed, abandoned property and contraband in accordance with this policy; • May delegate the duties of the Property Custodian to any member under their command and designate that member to serve as the "Assistant Property Custodian" for that Station/Section/Unit; • When applicable to do so, make arrangements to the appropriate facility for: 1. Property and contraband to be tested or analyzed; and 2. Firearms to be tested by the Department's Firearms Identification Section. • Shall transport or designate the Assistant Property Custodian to transport any item requiring analysis or testing; and • Ensure that members under their command are trained and familiar with the appropriate handling and storage of all found, unclaimed, abandoned property and contraband.

Continued next page.

Subject	Number
Property and Contraband	**INV-11A**

Responsibilities (Continued)

Position	Duties
Investigating Officer	The Investigating Officer who has found, unclaimed, abandoned property or contraband shall prior to the end of their shift: • Tag each item and/or place each item in a Department Evidence bag with the required information; • Secure any contraband in the Temporary Contraband/Controlled Substances Locker; • Log the contraband in the Temporary Contraband/Controlled Substances Journal; • Ensure a complaint or case number be assigned for found, unclaimed or abandoned property; • Provide a copy of the investigative report to the Property Custodian or Assistant Property Custodian to be placed with the found, unclaimed, abandoned property or contraband; • Provide the Desk Officer with a complete inventory of any found, unclaimed, abandoned property or contraband to be logged into the Daily Administrative Journal (DAJ); Note: Found, unclaimed, abandoned property, or contraband may be given directly to the Property Custodian or Assistant Property Custodian to be secured accordingly. Whenever **evidence and/or currency** are seized, members shall adhere to Policy and Procedure: • INV-10 Evidence Collection and Preservation; and • INV-14 Seized Currency.

Subject	Number
Property and Contraband	**INV-11A**

Storage Area Provisions

Station/Section/Units Permanent Storage

The Contraband Storage Locker shall be:

- Located and alarmed to allow for proper monitoring and security thus preventing unauthorized entry; and
- Maintained to prevent damage to property, contraband or other evidence that may occur due to moisture or extreme room temperature fluctuations.

Contraband/evidence shall:

- Be stored within a secure area within the State Police facility of jurisdiction;
- Not be stored in vehicles or personal storage areas; and
- Secure perishable items requiring refrigeration within the facility's identified refrigerator.

Troop/Section Storage Area

Troop/Section Commanders shall:

- Maintain a contraband storage area within their Troop/Section Headquarters;
- The Troop/Section storage area shall be under the control of the Cases and Reports Supervisor; and
- The storage area shall be used to store contraband/property that has been forwarded and awaiting destruction or disposal.

Temporary Locker

Temporary Storage

Each Station/Section/Unit shall:

- Be provided with a Temporary Contraband/Controlled Substance Evidence Locker with twenty-four (24) hour access to all authorized personnel;
- Allow for the temporary secure storage of contraband;
- Have available a Temporary Contraband/Controlled Substances Evidence Journal to enter all pertinent information; and
- In the event that an item is too large to fit into the Temporary Contraband/Controlled Substances Evidence Locker, the Investigating Officer shall:
    1. Consult with the Property Custodian, Assistant Property Custodian or their Supervisor in locating another secure location.

Continued next page.

Temporary Locker (Continued)

Items secured in the Temporary Contraband/Controlled Substances Evidence Locker shall have an entry made into the Temporary Contraband/Controlled Substances Evidence Journal listing:

1. Investigating Officer's name;
2. Investigating Officer's ID#;
3. Defendant's name(s);
4. Defendant's DOB;
5. Case number;
6. Date seized;
7. Location where seized; and
8. A description of the item(s) including the number of items.

Chain of Custody

Change In the Chain of Custody

When the Property Custodian or Assistant Property Custodian transfers evidence, contraband or property to an Investigating Officer for judicial proceedings it shall be considered a change of possession within the chain of custody. Both the Property Custodian/Assistant Property Custodian and Investigating Officer shall:

- Ensure appropriate entries are made within the Contraband Ledger and the DAJ; and
- Ensure all of the appropriate Department forms are completed indicating the change in possession.

Documentation of Chain of Custody

The Investigating Officer shall:

- Ensure the appropriate chain of custody forms are completed for evidence involving alcohol analysis or the examination of physical evidence;
- Ensure the appropriate chain of custody form(s) accompanies evidence or contraband whenever it is involved in a temporary change of possession outside of the custody of either the Property Custodian or Assistant Property Custodian and/or the Investigating Officer;
- Ensure that a record is made into the Station/Section/Unit's Contraband Ledger and DAJ identifying the new custodian; and
- Ensure the record identifies the evidence or contraband accordingly.

Inspection Evidence or Contraband

All members involved in the movement of evidence or contraband at the Station/Section/Unit, shall:

- Inspect the packaging for signs of tampering;
- Immediately notify the Station/Section/Unit Commander if the packaging appears to have been tampered with.

Continued next page.

Subject	Number
Property and Contraband	**INV-11A**

Chain of Custody (Continued)

Chain of Custody Forms

- *SP 145 Chain of Custody: Contraband /Evidence/Property Form*: Used for all evidence (excluding controlled substances), contraband, found/unclaimed or recovered property to show the chain of custody of the item/property.
- ***Forensic Services Group Forms***
  The following forms shall be used when necessary, retained and copies distributed as indicated:
  - *Alcohol Analysis Form:* Evidence requiring the analysis of alcohol content;
  - *Evidence Submission Form:* Evidence or contraband requiring analysis; and
  - *SP 295 Drug Submission Form:* Controlled Substances requiring analysis.

Troop/Section Supervisor of Cases and Reports

The Troop/Section Cases and Reports Supervisor shall:

- Sign and date the Station/Section/Unit Contraband Ledger as the final receiver of the property;
- Ensure a red line be drawn diagonally through the ledger entry to indicate final disposition and case closed;
- Destroy contraband in an appropriate and acceptable manner in the presence of another commissioned officer; and
- Submit a written report, through channels, to the appropriate Troop/Section Commanding Officer or designee, listing the final disposition of all contraband.

Property to be Auctioned

Per Massachusetts General Law (MGL) 22c. s. 45-46, the Department may:

- Sell held properties at a public auction; and
- Only sell after six (6) months when there is no proven ownership of the property.

The Department may select a vendor to hold the public auctions in accordance with establish procedures. Information and instructions regarding the auction vendor and procedures shall be posted on DocuShare under Bulletins-*Public Auction Vendor.*

Prior to the auction, Media Relations shall promulgate a notice per (MGL) 22c. s. 45, to the necessary media news outlets and newspapers that contain the following information :

- The time and place of the auction; and
- Description of the property to be auctioned.

Subject	Number
Property and Contraband	**INV-11A**

Returning Property to Owner

When property is disposed or returned to an owner specific information shall be recorded on the SP 145 and shall be:

- Attached (original) to the report and retained at the Station/Section/Unit;
- Forwarded (copy) to the Property Custodian or Assistant Property Custodian for filing;
- Forwarded (copy) to the Troop/Section Supervisor of Cases and Reports and retained on file.

Staff Inspection Unit

The Staff Inspection Unit shall conduct periodic audits of all Department Contraband Storage Lockers to ensure the integrity of the system.

Inspections

Troop/Section Commanders or designee shall:

- Conduct biannual line inspections of all contraband storage areas under their control to ensure compliance.

The Office of the Colonel/Superintendent, may direct:

- The unannounced random inspections of all Department contraband lockers to ensure compliance.

References

MGL c.94C, s.47A
MGL c.22C, s.45, s.46
Alcohol Analysis Form
Evidence Submission Form
SP 295 Drug Submission Form
SP 145 Chain of Custody: Contraband/Evidence/Property Form

Promulgated By:

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**INV-13**

Subject

Asset Forfeiture

Policy

The Department shall adhere to state and federal forfeiture laws involving illegal activities.

Troop/Section Asset Forfeiture Officer

The Asset Forfeiture Officer (AFO) shall:

- Provide assistance to members regarding investigations when authorized by the Troop Duty Officer;
- Oversee forfeiture proceedings and manage seized assets until forfeited;
- Maintain a database and files of all seizures and forfeitures; and
- Act as a liaison with the Financial Evidence Officer (per INV-14 Seized Currency), and the Offices of the District Attorney, Attorney General, or U.S. Attorney.

Non-Field Services Sections/Units

This policy is applicable to all Department entities, except those assigned to the Offices of the District Attorney, Attorney General, U.S. Attorney, or a federal task force, and there is an internal mechanism for tracking such seized currency. Members shall follow the policy as set forth by that office or task force.

Troop/Section/Unit Commanders requesting to deviate from this policy shall forward written requests through channels to the Deputy Superintendent for approval.

Factors of Consideration

In some situations one factor alone may be insufficient to justify a seizure and may require a combination of additional factors. Some factors are:

- Suspect is evasive, or gives implausible or false answers;
- Suspect has record of narcotics charges;
- Suspect is carrying a large or unusual amount of currency;
- Suspect cannot explain where the currency came from, or what it is for;
- Suspect has a large sum of currency or an expensive vehicle and no means of income;
- Suspect denies ownership of currency;
- Currency is concealed in an unusual location; or
- A narcotics canine alerts on the currency, vehicle, or property.
  Note: A canine alert alone is not enough to establish probable cause for the seizure of currency.

Subject	Number
Asset Forfeiture	**INV-13**

Making a Seizure

Seizures may be made when there is probable cause to believe that the vehicle, currency, or other property is connected to the sale or distribution of narcotics. This authority is allowed by Massachusetts General Laws (MGL) c.94C, s.47.

Members may seize currency when there is probable cause to believe that the currency is:

- Being used or was intended for use in the procurement, processing, delivery, or distribution of drugs;
- The proceeds of sales of drugs; or
- Involved in the furtherance of criminal enterprise.

Note: Currency seized shall be processed in accordance with INV-14.

Seizing a Vehicle

The Fleet Administrator has the authority to accept or reject vehicles on behalf of the Department. Any vehicle accepted by the Department, shall be delivered to the Fleet Section for inspection according to ADM-19.

A vehicle may be seized when…	A vehicle should not be seized if…
1. An operator, owner, or occupant of the vehicle is arrested for possession with intent to distribute or trafficking: • Ten (10) pounds or more of marijuana; • Any amount of heroin; • Any amount of cocaine; or • Other controlled substances, as outlined in M.G.L. c.94C, s. 32A-G or 32I. 2. The owner knew or should have known that it was being used for such purposes.	• It is rented or leased (unless seized for evidentiary purposes); or • The owner had no knowledge that it was being used for illegal purposes. Note: The Troop AFO shall consult with the District Attorney's Office of jurisdiction and determine if there is a lien on the vehicle that an entity is willing to assume.

Use of Seized Assets

The Colonel/Superintendent may expend funds and proceeds from the Special Law Enforcement Trust Fund to:

- Defray the costs of extended investigations;
- Provide matching funds for grants; and
- Accomplish other law enforcement purpose(s).

Funds shall not be considered a source of revenue to meet operational expenses.

Subject	Number
Asset Forfeiture	**INV-13**

Troop Asset Forfeiture Process

Step	Action
1	The determination is made to seize the assets e.g., vehicle, currency, or other property.
2	All seized assets are to be secured according to Department policy.
3	The seizing member shall notify the Troop AFO. Note: The Troop Duty Officer shall be notified of all seizures and may authorize call outs of the AFO after business hours.
4	The Troop Duty Officer shall notify the Financial Evidence Officer of all currency seizures.
5	The seizing member shall prepare the necessary reports and forms.
6	The Troop AFO shall: • Confirm assets are secured with the investigating member; • Conduct an investigation to determine ownership and liens of the assets; and • Assist the Financial Evidence Officer.
7	If it is determined that the asset forfeiture proceedings shall not continue, the assets shall be returned, as soon as possible, to the lawful owner.
8	Motor vehicles seized shall be secured as directed by the Troop/Section Commander.

References

MGL c.94C
MGL c.135, s. 7, 8, 10, 11
ADM-19 Vehicle Management
INV-10 Evidence Collection/Preservation
INV-11 Contraband Substances-Storage/Handling
INV-14 Seized Currency
TRF-09 Towing
TRF-10 Vehicle Inventory
A Guide to Equitable Sharing of Federally Forfeited Property for State and Local Law Enforcement, March 1994, US DOJ

Promulgated By:

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**INV-14**

Subject

Seized Currency

Policy

The Department shall establish rigid controls and strict accountability for all seized currency coming into its custody. A non-interest bearing cashless system shall be utilized to ensure that all seized currency is properly secured, stored, and readily retrievable. Any changes in the custody of any seized currency shall be properly documented.

Applicability

This policy is applicable to all Department entities, except for the following conditions:

- Members assigned to Offices of the District Attorney, Attorney General, U.S. Attorney or federal task force; and
- An internal mechanism exists for tracking seized currency.

Troop/Section/Unit Commanders requesting to deviate from this policy shall forward written requests through channels to the Deputy Superintendent for approval.

Seized Currency

Members shall not seize less than three-hundred ($300.00) dollars from a defendant, unless the currency is seized as evidence.

Seized currency shall not include:

- Non-evidentiary currency received during custodial processing;
- Currency used for controlled purchases of contraband; or
- Currency that has independent forensic value. (i.e., currency stained with blood, bodily fluids, or other evidentiary material)

Seized currency shall be processed at the appropriate sub-station in the troop of jurisdiction.

Responsibilities

Position	Duties
Desk Officer	• Visually observe currency drop safe at start of shift for general condition and make entry into Daily Administrative Journal (DAJ) system; • Make appropriate entries into DAJ system upon seizure and retrieval; and • Notify Troop Duty Officer of seizure and provide the RAMS case number and investigating member's name.
Investigating Member	• Count currency by denomination and verify amount with a witnessing member present; • Photograph or photocopy currency for evidentiary purposes, if necessary; • Package and seal currency in a Department evidence bag (evidence bags shall be labeled 1 of 1, 1 of 2, 2 of 2, accordingly), initial the seal, ensure both members sign bag with ID numbers, include corresponding RAMS case number; • Deposit Department evidence bag with attached SP 417 Currency Custody Form and SP 418 Seized Currency Receipt into currency drop safe with witnessing member present; and • File copy of SP 417 and SP 418 with the Station Commander.
Troop Duty Officer	• Notify the Financial Evidence Officer by email of the seizure; and • Make appropriate DAJ entries.
Financial Evidence Officer	• Retrieve seized currency from the currency drop safe with a witness present, not later than next banking business day or as otherwise authorized by the Troop Commander; • Document any change in custody on SP 417; • Ensure appropriate DAJ entries are made; • Transport sealed Department evidence bag(s) to Troop HQ to verify currency amount in presence of another commissioned officer; • Report discrepancies to the Troop Commander and Station Commander and reconcile prior to deposit; • Deposit currency into cashless system on the same banking business day as retrieved; • Enter the amount of the seizure into the approved accounting program;

Continued next page.

Subject	Number
Seized Currency	**INV-14**

Responsibilities (Continued)

Position	Duties
Financial Evidence Officer	• Immediately fax a copy of the SP 12 Incident Report to the Chief Financial Officer (CFO) of the District Attorney's Office of jurisdiction; • Maintain copies of SP 12's, SP 417's and SP 418's in a dedicated folder filed alphabetically and by year; • File open and closed cases separately; and • Retain initialed sealed Department evidence bag(s) if there are discrepancies until reconciled.
Station Commander	• Notify the investigating member(s) of any discrepancy; and • Maintain copies of SP 417 and SP 418 for inspections.
Troop Commander	• Maintain a non-interest bearing account at a local banking institution; • Assign a Commissioned Officer as the Financial Evidence Officer; • Maintain historical records of members provided with combination access; • Change access combinations as required; • Conduct quarterly audits; • Conduct investigations as appropriate; and • Notify the Division Commander of any discrepancies.

Discrepancies

Seized currency shall not be deposited into the cashless system until discrepancies are identified and reconciled. All currency shall be documented by amount and denominations. The final official amount shall be determined by the financial institution of deposit.

Troop/Section Commanders shall investigate any currency discrepancies that cannot be reconciled and report findings to the Division Commander.

Return of Seized Funds

Any person requesting the return of seized currency shall:

- Request the return in writing to the Troop Financial Evidence Officer;
- Provide a copy of the court order, if applicable; and
- Receive a check in person upon presentation of positive identification. Note: the check shall indicate subject's name, case number, and troop of jurisdiction.

Seized funds shall only be returned during regular business hours Monday through Friday.

Subject	Number
Seized Currency	**INV-14**

Disposition of Currency

If no person makes a valid claim to found, unclaimed, or abandoned currency within six (6) months from the date the currency was turned into the Department, the funds shall be forwarded to the State Treasurer through channels via the Department's Fiscal Section.

Prior to forwarding the funds to the State Treasurer, the Department may deduct all reasonable charges and expenses incurred in connection with the deposit and accounting of the currency. Such deductions shall be made by the Department's Fiscal Director and documented accordingly. Any claim for return of found, unclaimed or abandoned currency after the funds have been forwarded to the State Treasurer, shall be made to the State Treasurer's Office.

All seized currency ordered forfeited through legal proceedings shall be forwarded to the Office of the Superintendent for the Special Law Enforcement Trust fund within sixty (60) days of adjudication.

Accounting and Audits

The Financial Evidence Officer shall maintain:

- Bank statements;
- An approved software accounting system;
- SP 12's, SP 417's, and SP 418's for currency received; and
- Records, documentation, or invoices of currency disbursements.

Prior to any change of command of the Troop/Section/Unit Commander, Executive Officer, or Financial Evidence Officer, there shall be a reconciliation of the accounting records and current balances with the incoming member(s).

An internal audit of all seized currency accounting records and practices shall be conducted annually by the appropriate Division Commander.

An audit of seized currency may be conducted as directed by the appropriate Division Commander or the Colonel/Superintendent.

Reports

Troop/Section/Unit Commanders shall:

- Submit a quarterly report, from the approved accounting program, to their Division Commander (due January 10, April 10, July 10, and October 10); and
- Submit a copy of the quarterly report to the Chief Financial Officer (CFO) of the District Attorney's Office of jurisdiction.

Subject	Number
Seized Currency	**INV-14**

Currency Drop Safe

Currency drop safes shall be located and maintained at each sub-station as determined by the Division Commander. Only the Troop Commander, Executive Officer, and Financial Evidence Officer shall have authorized access to the currency drop safe and combinations. Whenever the currency drop safe is opened:

- Two (2) members shall be present at all times; and
- Access and retrieval information shall be entered into the station DAJ.

Drop Safe Combinations

Troop Commanders shall be responsible for the change of safe combinations under their command.

Whenever there is a change of command, transfer or departure of a Troop Commander, Executive Officer, or Financial Evidence Officer, the access combination shall be changed.

References

INV-13 Asset Forfeiture
SP 12 Incident Report
SP 417 Currency Custody Form
SP 418 Seized Currency Receipt

Promulgated By:

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**INV-15**

Subject

Field Interview and Observation Reports

Policy

Members shall follow the established guidelines for the collection, security, and dissemination of information gathered through field interviews and observations.

Definitions

SP 73 Field Interview and Observation Report (FIO): An internal, Department report that documents information about a person, place, vehicle, event, occurrence, or any other known activity, observed by a Department member, that may be linked to suspicious or criminal activity or may be of interest to the law enforcement community.

Collection of Information

Information may be recorded on a SP 73 or any other format that is approved by the Criminal Information Section (CIS).

FIO reports are an important crime prevention and information gathering resource. Analysis of these reports is a valuable aid to investigators in uncovering leads that may result in the solving of crimes and the apprehension of criminal suspects.

The collection of information for FIO reports shall not be based solely on an individual's or group's:

- Support of a particular cause;
- Race;
- Color;
- Religion;
- Gender;
- National origin or ancestry; or
- Political affiliation.

Members collecting information for FIO reports shall not:

- Conduct random stops of persons or vehicles to gather information; or
- Employ or direct an individual to engage in any illegal activities.

Subject	Number
Field Interview and Observation Reports	**INV-15**

Public Contact

Members are encouraged to:

- Collect as much information based upon their own observations; and
- Gather as much information provided to them on a voluntary basis.

Members may:

- Detain a person or vehicle briefly when there is reasonable suspicion of criminal activity; or
- Stop and frisk a subject's outer garments for weapons when articulable facts or circumstances warrant such action, for the safety of the public and the member.

A person stopped by a member, who refuses to cooperate or answer questions, shall not be further detained without reasonable suspicion or probable cause.

SP 73 Field Interview and Observation Reports

FIO Reports should be carried by every member while on duty. Additionally:

- Members should complete a report whenever a known criminal is observed or a person, place, vehicle, event, occurrence, or any other activity is observed that would indicate criminal activity or potential criminal activity;
- A separate FIO Report shall be completed for each member of a group and for each observation made; and
- Information shall be typed or printed in black ink and its content should be as complete as possible.

Procedures for completed FIO Reports:

- Provide a copy of the FIO to the Troop/Section/Unit of jurisdiction;
- Forward the original hard copy of the FIO Report to CIS; and
- If the information within the FIO Report is related to terrorism or homeland security contact:
  1. CIS during normal business hours; or
  2. The Communications Section OIC other than normal business hours.

Security and Retention

FIO Reports shall be secured at all times by CIS. A dissemination log shall be maintained for all requests for review and dissemination of information.

Dissemination

Requests for information from the FIO database shall be made to the Commanding Officer of the CIS.

CIS shall only disseminate FIO information:

- In the furtherance of an authorized law enforcement activity;
- To authorized law enforcement or criminal justice personnel; and
- On a "need-to-know" and "right-to-know" basis per INV-08 Criminal Intelligence.

After review by either CIS, or the Communications Section OIC, information contained within an FIO Report determined to be critical, time-sensitive, or pertaining to public or officer safety shall be disseminated to law enforcement agencies, as appropriate. -

Responsibilities

Requests for dissemination shall include the:

- Date and time of the request;
- Requesting Officer's name, rank, identification (ID) number and agency;
- Case number or reason for the request; and
- Name of the person(s) or incident(s) and information sought.

The Criminal Information Section (CIS) shall:

- Respond to requests for information from FIO Reports; and
- Document requests and dissemination of information.

References

INV-08 Criminal Intelligence

Promulgated By:

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**INV-16**

Subject

Electronic Recording of Interrogations

Policy

Members shall, whenever it is practical, electronically record all custodial interrogations of suspects or interrogations of suspects conducted in places of detention.

Case Law

In *Commonwealth v. DiGiambattista*, 442 Mass. 423 (2004), the Supreme Judicial Court held that if the prosecution introduces a confession or statement that the police obtained during an interrogation of a defendant, who was either in custody or at a place of detention, and the police did not electronically record the statement, the defendant is entitled to a cautionary jury instruction.

Upon the defendant's request, the judge must instruct the jury that the State's highest court has expressed "*a preference that such interrogations be recorded whenever practicable and . . . that, in light of the absence of any recording of the interrogation in the case before them, they should weigh evidence of the defendant's alleged statement with great caution and care*." This jury instruction is required regardless of the reason that the police did not record the interrogation.

Definitions

Custody: Circumstances in which a reasonable person would believe that their freedom of action has been curtailed such that they are not free to leave.

Electronic Recording: Preservation of an interview through the use of audio or audio/video recording equipment.

Interrogation: Occurs when an officer's questions, actions or words (other than those normally attendant to arrest and custody), are reasonably likely to elicit an incriminating response from a suspect.

Place of Detention: A secure facility where persons may be held in detention in relation to a criminal charge(s) (e.g., a state police barracks, prison, jail, a department of youth services secure facility).

Suspect: A person who has either been charged with a crime or a person for whom there is a reasonable basis to believe that may in the future be charged with a crime. Witnesses, victims, and other persons who provide information to a member are not considered suspects, unless and until, there is reasonable basis to change their status.

Subject	Number
Electronic Recording Of Interrogations	**INV-16**

Applicability

These guidelines require members to record, whenever it is practical, two (2) types of interrogations:

1. Custodial interrogations of suspects; and
2. Interrogations of suspects occurring at places of detention.

Wiretap Violations

The Massachusetts wiretap statute, Massachusetts General Laws (MGL) c. 272, s. 99, generally prohibits anyone from secretly recording another person's oral statements. Accordingly, unless one of the narrow exceptions in the wiretap statute applies, a member who electronically records a suspect's interrogation shall do either of the following:

- Notify a suspect that their statements are being recorded; or
- Conduct the interrogation in such a way that it is obvious to the suspect that their statements are being recorded.

When the suspect knows, or reasonably should know, that they are being recorded, the member may record the interrogation without explicit consent to do so.

Creating a Clear and Complete Record

To the extent it is practical members should electronically record the entire interrogation of a suspect. To assist in the creation of the record, members shall do the following:

- Ensure that the recording device is functioning properly;
- Start the recording device;
- Inform the suspect that they are being recorded unless it is otherwise obvious;
- State the date, time, location, and names of persons present. If a video recording device is used which imprints the time on the tape or disk, verify that the correct time is displayed;
- State the full name of the suspect;
- Execute appropriate Department forms including Miranda warning and waiver, and waiver of prompt arraignment (if applicable); and
- If the member must suspend the recording for any reason, they shall make a record of:
    1. The reasons for stopping (i.e., taking a break or a malfunction);
    2. The time the recording device is turned off;
    3. The time it is turned back on; and
    4. What transpired while the recording device was turned off.

Continued next page.

Subject	Number
Electronic Recording Of Interrogations	**INV-16**

Creating a Clear and Complete Record (Continued)

- If the member uses or refers to documents or other items during the interrogation, the member shall describe those documents or items on the record and mark them with a unique number (similar to an exhibit number at trial) and the member's initials. If the member is unable to write on the actual document or item, the member may write on a bag, envelope, or case in which the document or item is placed, or on a piece of tape which can be attached to the document or item; and
- Conclude the recording by stating the date and the time the interrogation is completed.

Suspect Refuses to be Recorded

Refusal Given Before the Recording Device is Activated:

- If it is practical, turn on the recording device to record the refusal;
- Identify the lead member and the suspect then state the date, time, and location, inform the suspect of any applicable rights and inform the suspect of the benefit to recording, including the fact that a recording will create a clear and complete record of what was said to the suspect, and what the suspect said during the interrogation;
- Ask the suspect on the record if they are willing to make an electronically recorded statement;
- Advise the suspect if, at any time, they change their mind and decide that they do want the interview to be recorded, they should let the member know and the member shall turn on the recording device; and
- If the suspect still refuses, turn off the device, execute a signed refusal form SP 609 Refusal Form, and proceed with the interview.

Suspect Refuses to Have Their Refusal Recorded

- Advise the suspect of the benefits of electronically recording any communications;
- If the suspect objects to having their refusal electronically recorded the member shall execute a SP 609; and
- The member may proceed without recording the refusal or the interrogation.

Suspect Refuses After the Recording Device is Activated

- If, during the course of a recorded interrogation, a suspect decides that they no longer want to answer questions unless the recording device is turned off, the member shall again advise the suspect of the benefits of recording the interrogation; and
- If the suspect still refuses, the member shall turn off the recording device execute a SP 609 and proceed with the interview.

Subject	Number
Electronic Recording Of Interrogations	**INV-16**

Discretionary Decision Not to Record

A member may decide not to record an interrogation, even where it is practical to do so, if that member believes that:

- Recording the interrogation will jeopardize the safety of a member, the suspect, or any other person; or
- It is ill-advised under the circumstances to record the interrogation.

If a member decides that it is unsafe or ill-advised under the circumstances to record the interrogation, the member should:

- Advise the suspect of the potential benefits of recording the interrogation, if warranted;
- Document in the interview, or case report, the reason(s) why the interrogation was not recorded, and if the suspect was advised regarding the potential benefits of recording the interrogation.

Recording Devices

The member should choose a recording device that has removable media (e.g., tape, disk, memory card, etc.) which can be easily duplicated.

Recording Device Malfunctions

If the recording device malfunctions, the member conducting the interrogation shall make a decision whether and how to continue the interrogation, and shall document what occurred.

<u>If the recording device can be restarted or replaced immediately:</u>

- State on the record that the device malfunctioned;
- State how long the device was not working, and
- Whether or not the suspect made any statements that were not recorded.

<u>If the recording device cannot be restarted or replaced immediately:</u>

- Include in the interview or case report the fact that the device malfunctioned;
- Ask the suspect whether they wish to continue the interrogation without a recording device, or whether they wish to suspend the interrogation until an operable recording device is available;
- If the suspect consents to continuing the interrogation without a recording device, document the consent and the interrogation in some manner, such as in a signed written statement by the suspect or in the member's interview or case report; and
- Note whether or not the suspect made any statements that were not recorded.

Subject	Number
Electronic Recording Of Interrogations	**INV-16**

Inoperable or Unavailable Recording Device

If there is no recording device available or the recording device is inoperable, the member should:

- Ask the suspect whether they wish to continue the interrogation without a recording device, or suspend the interrogation until an operable recording device is available.

If it is impractical to defer the interrogation, and the suspect consents to continuing the interrogation without a recording device then:

- Include in the interview or case report the fact that no recording device was available; and
- Document the consent and the interrogation in some manner, such as in a signed written statement by the suspect, or in the member's interview, or case report.

If, under the circumstances, it is impractical to seek or obtain the suspect's consent to continuing the interrogation without a recording device, the ultimate decision to continue shall be made by the member on a case-by-case basis.

Preservation and Copying of Original Recordings

The member who conducted the interrogation shall preserve the original recording. Preservation steps include:

- Remove the storage medium from the recording device;
- Clearly label and appropriately store recordings and copies;
- If the interrogation is recorded digitally, the member shall preserve at least one (1) whole copy of the original recording file;
- As soon as it is practical, create at least one (1) exact copy of the original recording;
- Clearly label copies as such;
- Use copies, not original recordings, to make additional copies; and
- Copies, not the original, shall be used to prepare a written transcript, to comply with discovery obligations, and for all other purposes.

To the extent it is practical, statements from multiple suspects should not be recorded on the same tape or disk.

Subject	Number
Electronic Recording Of Interrogations	**INV-16**

Storage

The member shall preserve all written forms, notes, or records of all statements by a suspect that were not electronically recorded in the original case file.

All electronically recorded interrogations shall:

- Be preserved according to the state records retention law and Department policy as criminal evidence; and
- Be stored in such a manner so as to easily differentiate between original recordings and copies.

Each original and copy shall be authenticated by the interrogator with the following information:

- Date and time of recording;
- Location of the interrogation;
- Name of person interrogated;
- Name of person(s) conducting the interrogation; and
- Departmental assigned case number or incident report number.

References

Commonwealth v. DiGiambattista, 442 Mass. 423 (2004)
SP 609 Refusal Form

Promulgated By:

Department of State Police
General Order

Effective Date	Number
September 20, 2010	**INV-16A**

Subject

Eyewitness Identification

Policy

Eyewitness identification frequently plays an important role within Department investigations and it is absolutely critical that eyewitness evidence be accurate and reliable, in order to ensure that the highest possible quality of evidence is obtained.

The Department recognizes the importance of conducting and documenting eyewitness identification information in accordance with established guidelines, while recognizing that members are free to exercise discretion in adapting these guidelines to fit the unique circumstances of each case.

Definitions

Simultaneous Identification Procedure: Simultaneous identification is a procedure that displays a group of individuals or group of photographs to a witness at the same time. This allows the witness to compare all individuals or photographs before making a decision.

Sequential Identification Procedures: Sequential identification is a procedure where an eyewitness views only one member of a lineup or one photograph at a time. The witness must make a decision on each lineup member or photo before the viewing the next lineup member or photo.

Relative Judgments: Relative judgments occur when witnesses encounter a lineup in which the actual perpetrator is not in the lineup (i.e., the suspect is not the actual perpetrator). Research has shown that eyewitnesses tend to select the person who looks most like the perpetrator relative to other lineup members because they presume that the actual perpetrator will be in the lineup.

Blind Administration Procedure: A blind administration procedure where the officer/investigator who conducts the lineup has no knowledge of who the suspect is, which reduces unintentional influences. Whenever practical, this method should be used.

Field Identification (Show-Up): An eyewitness identification procedure in which a single suspect is viewed by an eyewitness shortly after the commission of a crime for the purpose of identifying or eliminating a suspect in a criminal offense.

Subject	Number
Eyewitness Identification	**INV-16A**

Definitions (Continued)

Live Lineup: An eyewitness identification procedure in which the witness to a criminal offense is asked to identify one suspect from a group of persons.

Photo Lineup/Photo Array: An eyewitness identification procedure in which the witness to a criminal offense is asked to identify one suspect from a group of photographs.

Filler: A person or photograph used in an eyewitness identification procedure not suspected of the offense and generally meets the description of the suspect.

Guidelines

Department Eyewitness Identification Guidelines may be found in DocuShare/Bulletins regarding:

- Field Identification (Showup);
- Live Lineup; and
- Photo Lineup/Array.

Department members shall adhere to established guidelines and utilize the appropriate Department forms (see References) when conducting any photo lineup, live lineup, or a field identification show-up; except for the following conditions:

- The member assigned to Offices of the District Attorney, Attorney General, U.S. Attorney or federal task force; and
- An internal mechanism exists for conducting eyewitness identification procedure.

Eyewitness Advisement

Before any eyewitness identification procedure is conducted, members shall administer a SP 645 Eyewitness Advisement. The advisement provides clear, consistent, and forceful instructions to avoid relative judgment or any prejudicial action that may influence the witness.

The Massachusetts Supreme Court *Commonwealth v. Silva-Santiago, 453 Mass. 782 (2009)* held that a photo array procedure was not per se suggestive where the police failed to use the standard advisements, sequential presentation, or a blind presenter. However the court stated that it expects such procedures, especially the standard advisements, to be used in all future identification procedures.

Subject	Number
Eyewitness Identification	**INV-16A**

References

U.S. Department of Justice, (1999) *Eyewitness Evidence, A Guide for Law Enforcement;*
The Massachusetts District Attorneys Association (September 2006), *Recommendations to Improve the Investigation and Prosecution of Cases in the Criminal Justice System.*
Commonwealth v. Silva-Santiago, 453 Mass. 782 (2009)
SP 644 Eyewitness Identification Form
SP 645 Eyewitness Advisement
SP 646 Show-Up Identification Procedure

Promulgated By:

Department of State Police
General Order

Effective Date:	Number:
August 1, 2017	**INV-17**

Subject:

Travel/Immigration Status Inquiries and Investigations

Policy

Investigating and enforcing violations of federal immigration law is not a mission of the Massachusetts State Police. Accordingly, it is not appropriate for a member of the State Police to inquire about a non-citizen's immigration or travel status for the sole purpose of facilitating that person's detention or deportation by U.S. Immigration & Customs Enforcement (ICE).

However, a member of the State Police may inquire into a person's immigration or travel status if the inquiry is part of, and reasonably likely to facilitate, the investigation of a violation of state law, federal criminal law (excluding federal immigration law), or conduct independent of immigration status that poses a threat to public safety or order. A member of the State Police may also notify federal authorities of the imminent release of a subject consistent with the limits set forth in this General Order.

Definitions

U.S. Immigration and Customs Enforcement (ICE): An agency within the Department of Homeland Security (DHS), its mission is to enforce the nation's immigration and customs laws.

Criminal Justice Information System (CJIS): A computerized system of criminal justice information, available twenty-four (24) hours a day and managed by the Commonwealth's Criminal History Systems Board.

Seizure: To take possession under compulsion of legal authority; to confiscate.

Identification Document: An article/credential that is, or purports to be, issued by a government entity, that is relied upon to record or prove the identity of its bearer. Examples may include:

- A driver's license from any state or country;
- An ICE- issued identity/status card;
- A document issued by the Massachusetts Registry of Motor Vehicles (RMV), or other official governmental motor vehicle organization; and
- A passport issued by the U.S. State Department or any other sovereign nation.

Subject	Number
Travel/Immigration Status	**INV-17**

Seizing Documents

Identification Documents may be seized from an individual only if they are:

- Contraband (including stolen, forged, or altered documents)
- The fruits or instrumentalities of a Massachusetts crime;
- Evidence of a Massachusetts crime; or
- Illegally possessed

The seized documents shall be initially processed as required under INV-10 *Evidence Collection and Preservation*. Once the case is adjudicated, seized documents shall be promptly disposed of according to Department Policy and Procedure INV-11A *Property and Contraband.* Stolen passports seized for these purposes should initially be processed like any other evidence according to INV-10 & INV-11A. Once the case is adjudicated, passports should be forwarded to the originally intended holder, or the U.S. Department of State, Passport Services, Consular Lost/Stolen Passport Section, 1111 19th St. NW, Room 500, Washington, DC 20036.

State Residency

Foreign operators may drive in Massachusetts for up to one (1) year with their foreign license if they are a visitor. An operator with an out-of-state license may drive in Massachusetts at any time, provided they do not establish residency within the Commonwealth. However, pursuant to G.L. c. 90, § 8, once a foreign operator or an out-of-state operator becomes a Massachusetts resident, he or she must immediately obtain a Massachusetts driver's license.

A member may question an operator about his/her employment, current residence, and/or tax status, when the member possesses a reasonable suspicion that a person operating on a foreign or out-of-state license has established residency in Massachusetts and the member requires the information to aid in determining if the operator is in compliance with Massachusetts law.

Out-of-State Licenses

An out-of-state license should not be seized by a member unless this document is:

- Contraband;
- A fruit or instrumentality of a crime;
- Evidence of a crime; or
- Illegally possessed.

Seized licenses shall be processed in accordance with INV-10 & INV-11A.

Determining License Status

To determine if the operator has been living in Massachusetts for longer than one year, the following checks may be performed to aid in determining an operator's current status:

- A motor vehicle violations history check (KQ);
- A criminal history check (BOP);
- Utilize the CJIS screen titled "INS" to learn when the operator entered the U.S.;
- A RMV check to determine if the operator has any license status within Commonwealth; or
- The issuance a RMV "A" or "X" number.

Note: Massachusetts RMV issues an "A" number to individuals who are unlicensed within the Commonwealth, but have received a Massachusetts motor vehicle citation; an "X" number is issued to individuals who are unlicensed within Massachusetts, but own a Massachusetts registered motor vehicle.

Foreign Licensed Operators

Massachusetts shall only honor valid licenses from countries identified within the current Massachusetts Driver's Manual "A" Appendices: *Parties to the Road Traffic Convention and the 1943 Inter-American Automotive Traffic Convention.*

This publication is available to all members via the Massachusetts Registry of Motor Vehicles web site under:
Forms & Manuals→ Driver's Manual→ Appendices "A".

International Driver's License/ Permit

An international driver's license/permit is simply a translation of an operator's foreign driver's license into English. This document is not required to operate a motor vehicle in Massachusetts.

The international license/permit is not a substitute for a person's actual driver's license issued by their country of origin. An operator who is licensed in another country is required to carry only their valid foreign driver's license.

ICE Detainers

Department members are NOT authorized to stop, arrest, and/or take an individual into custody based solely on an ICE detainer.

If an individual is in Department custody pursuant to an arrest on criminal charges or a warrant, or for any other reason, the existence of an ICE detainer for that individual does NOT grant members of the Department authority to detain the individual for any period longer than s/he would otherwise be held in Department custody.

Continued next page.

ICE Detainers (Continued)

I. Member Responsibilities

When a Department member conducts a NCIC/DCJIS query of an individual who is **already** in Department custody pursuant to arrest on criminal charges or a warrant and determines that the individual is the subject of an ICE detainer as defined in 8 C.F.R. § 287, the member shall **immediately** notify the Troop Duty Officer.

II. Troop/Duty Officer Responsibilities

The Troop Duty Officer shall instruct a Troop Dispatcher to contact ICE at (802) 872-6020 to notify ICE that an individual in custody is the subject of an ICE detainer.

The Troop Duty Officer shall monitor the status of an individual with an ICE detainer until the individual is released, transferred, or taken into custody by ICE. If ICE fails to take custody of the individual prior to the time when the individual would otherwise be released or transferred from Department custody, the individual shall be immediately released or transferred from Department custody. All such actions/inactions, and the reasons for the same shall be recorded in the appropriate daily administrative journal and/or reports.

III. Request for Voluntary Notification of Release

In certain circumstances, ICE will request, by providing *Form I-247A ("Immigration Detainer – Notice of Action")* that the Department **notify** ICE before an individual is released or transferred from Department custody. After receiving *Form I-247A* from ICE, the Troop Duty Officer shall notify ICE of the individual's impending release as early as possible and shall document the notification in the appropriate daily administrative journal and/or reports. Upon receipt of Form I-247A, the Troop Duty Officer shall also 1) relay a copy of the detainer form to any other law enforcement agency (including a jail, regional lockup, or state court) to which custody of the individual is transferred, and 2) shall notify ICE in the event of the individual's death, hospitalization, or transfer to another institution. **Under no circumstances will an individual be detained beyond the time s/he would normally be released from Department custody on the basis of the Department's receipt of *Form I-247A*.**

Continued next page.

ICE Detainers (Continued)

IV. Bail Magistrate, Court, and District Attorney Notifications

In circumstances where an individual is eligible for bail, members shall notify the Bail Magistrate that the individual is the subject of an ICE detainer.

In circumstances where an individual is transferred into the custody of the court system, the officer transporting the individual shall notify the court, district attorney's office, and other appropriate law enforcement agencies of the existence of an ICE detainer. This notification shall be documented in the appropriate daily administrative journal and/or reports.

Mandated Consular Reporting

Agreements with certain countries mandate that they be notified when their nationals are confined or detained regardless of the national's request.

When foreign nationals are involved in an incident, members shall consult "Consular Notification and Access" provided by the U. S. State Department, which is available to all members via the State Department website at:
http://travel.state.gov/consularnotification

Continued next page.

Subject	Number
Travel/Immigration Status	**INV-17**

Seizure Procedures

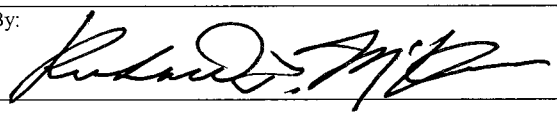
If this occurs…	Then…
The operator is arrested for operating under the influence (OUI) of alcohol and fails a breath test, or refuses a breath test.	• Process as specified by M.G.L.; and • Seize Massachusetts licenses if appropriate. **Note**: If the operator is from out-of-state and possesses an out-of-state license, do not seize the license.
The operator has a suspended or revoked Massachusetts Driver's License.	• Seize the driver's license; • Complete a RMV Form 21188 – *Report and Affidavit of an Operating After Suspension/Revocation Incident*; • Forward both the license and Form 21188 to the RMV; and If the suspended or revoked operator is operating a vehicle registered to them, seize the registration plates and forward the plates to the RMV with Form 21188.
The operator possesses/uses a forged/altered license or any official document from the Massachusetts RMV or from another country or state's department of motor vehicles.	• Seize the forged or altered documents; • Notify the State Police Compliance Unit of this violation by utilizing RMV Form #T21193 – *Affidavit of Person Obtaining License*; and • Process seized documents in accordance with INV-10 & INV-11A. Note: The operator may be charged with G.L. c. 90, §24B, c. 90, §28, or c. 267, §1- (forgery statute).
An operator presents a license from a foreign country.	See "Foreign Licensed Operators" Section.
A passenger in a vehicle presents a suspended or revoked Massachusetts license for identification purposes only.	• If the suspension/revocation is for OUI alcohol, seize the license and forward it to the RMV or destroy it; **however**, • If used for identification purposes only, the suspended/revoked license should not be seized.
The operator presents an out-of-state license, which is suspended, revoked, or expired in the operator's home state.	• Do not seize the license; • The operator may be charged with MGL Ch. 90, §10, unlicensed operation of a motor vehicle; and Obtain the CJIS printout from the operator's home state to verify the suspension or revocation for court purposes.

Subject	Number
Travel/Immigration Status	**INV-17**

References

INV-10 *Evidence Collection and Preservation*
INV-11A *Property and Contraband*
Form I-247A Immigration Detainer – Notice of Action
U.S. Department of State Publication; *"Consular Notification and Access"*
8 C.F.R. § 287
Massachusetts Driver's Manual "A" Appendices: *Parties to the Road Traffic Convention and the 1943 Inter-American Automotive Traffic Convention.*
RMV Form 21188 – *Report and Affidavit of an Operating After Suspension/Revocation Incident*;
RMV Form #T21193 – *Affidavit of Person Obtaining License*

Promulgated By:



Department of State Police
General Order

Effective Date	Number
April 23, 2009	**PRI-01**

Subject

Warrant Management

Policy

Department members shall utilize established warrant management systems in accordance with the guidelines established by this policy as well as state and federal laws.

Definitions

Commonwealth's Criminal History Systems Board (CHSB): The state agency responsible for maintaining law enforcement data communications network and systems.

Criminal Justice Information System (CJIS): A computerized system of criminal justice information, available twenty-four (24) hours a day and managed by the CHSB.

Interstate Identification Index (III): Triple III is an interstate exchange of criminal history record information maintained by the FBI.

National Crime Information Center (NCIC): Nationwide computerized system of criminal justice information managed by the FBI.

Warrant Management System (WMS): Centralized database operated by the Trial Court of the Commonwealth that provides CJIS users with access to court issued arrest warrants.

Locate: A computer entry that indicates that the wanted person or item has been apprehended or found.

Wanting Police Department (WPD): Primary police agency or Department Station entering a NCIC warrant.

Criminal Offender Record Information (CORI): A database of criminal record information where the release is regulated by state and federal laws.

CJIS Information

CJIS information shall only be used by law enforcement and criminal justice personnel in the performance of their duties.

Inquiries of a curiosity nature or other types of transactions performed for non-official purposes are strictly prohibited.

Continued next page.

Subject	Number
Warrant Management	**PRI-01**

CJIS Information (Continued)

Members in the lawful performance of their duties may rely in good faith upon the information received from CJIS and the WMS, and are not liable in any criminal prosecution or civil action.

Much of the information in the CJIS computer is codified as CORI, and its dissemination is strictly regulated by law. Employees shall not release information in violation of the CORI laws.

CJIS Representative

Commanding Officers of each Station/Section/Unit containing a CJIS terminal shall:

- Assign a member as the CJIS Representative; and
- Assign a member as the Backup CJIS Representative.

The CJIS Representative shall:

- Act as the liaison to CHSB regarding CJIS training, validation of warrant information, and password oversight;
- Assist other members in the use of the CJIS System;
- Direct members to the CJIS extranet for additional assistance; and
- Ensure all members are informed of updates, publications, or modifications to the CJIS network.

Warrant Databases

CJIS warrant information may be found in:

- WMS which contains most of the statewide warrants entered after 1995;
- CJIS/NCIC which contains information on federal, state, and nationwide warrants entered prior to 1995, including in-state parole warrants; and
- The Board of Probation (BOP) record query of an individual that may indicate a default from a court appearance.

A warrant on the WMS shall constitute notice and the printout of the warrant represents a true copy.

CJIS Inquiries

The Desk Officer or Dispatcher shall be aware that a WMS inquiry which yields a hit shall be considered probable cause to arrest when the warrant does not indicate recall or locate.

The Desk Officer or Dispatcher shall:

- Verify the warrant hit in CJIS/WMS; and
- Contact the court of issue if the warrant cannot be located.

Continued next page.

CJIS Inquiries (Continued)

The Desk Officer or Dispatcher when notified that a person has been arrested on a WMS warrant, shall:

- Place a locate against all CJIS wanted records to indicate that the wanted person has been apprehended; and
- Print a copy of the warrant.

The arresting member shall:

- Give a true copy of the warrant to a prisoner who requests a copy within six (6) hours.

Court Information for WMS

Members making a request for a WMS warrant shall provide a completed warrant application to the court of jurisdiction.

The clerk from the court of jurisdiction is responsible for the entering, recall, and removal of WMS warrants from the system.

NCIC Warrants

WMS warrants do not automatically enter into NCIC. The Department shall enter NCIC warrants in order to provide out of state access or rendition even when the warrant is located within WMS.

Any felony or serious misdemeanor warrant may be entered when:,

- The District Attorney has authorized rendition; or
- For officer safety, licensing, or employment, providing the opening notation in the remarks field is no extradition/rendition (NOEX).

All warrants entered into NCIC shall be in conformance with CJIS/NCIC and Department policy.

NCIC/NOEX warrants entered and maintained by Department entities shall be checked by designated personnel:

- Weekly for recall notices from the courts; and
- Quarterly during the months of January, April, July and October for accuracy and compliance.

NCIC/NOEX warrant file folders shall be kept and maintained by Troop Headquarters or the station of entry as the WPD, and shall contain:

- A copy of the WMS warrant;
- Driver’s license information, missing and wanted checks;
- A copy of BOP and Triple III records; and
- Any other pertinent information.

CJIS or NCIC Warrant Confirmation

A CJIS (non-WMS) or NCIC warrant that yields a hit shall not be probable cause to arrest. However, once the warrant is confirmed as active with the entering agency there may be probable cause to arrest.

When the Department receives a hit from CJIS and/or NCIC, an immediate confirmation with the agency that originated the record in the system shall be made before an arrest or seizure is made.

The Desk Officer/Dispatcher shall:

- Contact the agency that originated the record in the system by telephone to confirm the warrant; and
- Confirm the warrant following CJIS procedures.

When a request for confirmation is made for CJIS/NCIC warrants held by the Department, the Desk Officer/Dispatcher shall:

- Locate the original warrant and confirm the information following CJIS procedures ensuring the response back to the requesting agency is performed within:
  1. Ten (10) minutes for an urgent request; or
  2. One (1) hour for a routine request; or
- Cancel the warrant.

CJIS Responsibilities

Members who use the CJIS network are responsible for:

- Familiarizing themselves with the CJIS and NCIC operating manuals; and
- Maintaining bi-annual CJIS certification.

The name and Department identification (ID) number of the person requesting a BOP or Triple III shall be indicated in the "Requested by" or "Attention" fields.

Justification for BOP / Triple III Checks

Members shall only conduct BOP checks for:

- A history of violence and weapons charges to be disseminated immediately for officer safety;
- An investigation;
- Subjects under arrest; and/or
- Background checks for a legitimate law enforcement purpose.

Members shall only conduct Triple III checks for:

- Legitimate law enforcement purpose;
- Background check for a person applying for employment; and/or
- Background check of a person applying for a Firearms Identification card, or a License to Carry Firearms Permit.

Subject	Number
Warrant Management	**PRI-01**

References

MGL c.276, s.11-20, s.23A, s.29
MGL c.248, s.26
MGL c.22C, s.10
MGL c.6, s.167-178

Promulgated By:

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**PRI-01A**

Subject

Warrants, Summons, or Subpoenas

Policy

In furtherance of a legitimate law enforcement purpose, members shall serve warrants, summons, or subpoenas once they become aware of their existence, or as otherwise ordered.

Default Warrants and Bail

Type of Default Warrant	Bail
Felony or misdemeanor punishable by imprisonment for more than one-hundred (100) days.	Only by a judge of the court that issued the warrant or the court of jurisdiction holding the warrant.
Misdemeanors punishable by imprisonment for one-hundred (100) days or less.	By any person authorized to admit bail.

A subject arrested on a default warrant, who is not released on bail, shall be:
- Transported to the court of jurisdiction where the arrest was made; or
- Transported to the court that issued the warrant.

Governor's Warrants

Whenever the Department receives notification that a person wanted by the Department has been arrested in another state as a fugitive from justice:

Step	Action
1.	The Desk Officer receiving such information shall contact the Troop Duty Officer who shall contact the Detective Unit of jurisdiction.
2.	If the District Attorney authorizes the rendition of the subject named in the warrant, the Commanding Officer of the Detective Unit of jurisdiction shall: • Notify the arresting out-of-state agency of the decision by telephone and teletype as soon as possible.

Continued next page.

Subject	Number
Warrants, Summons, or Subpoenas	**PRI-01A**

Governor's Warrants (Continued)

Whenever the Department receives a Governor's Warrant from another state, it shall be forwarded to the Commander of the Detective Unit of jurisdiction.

The Detective Unit Commander shall:
- Execute the warrant by proper means; and
- Ensure all legal requirements are adhered to.

Service of Summons/ Subpoena

The service of a summons or subpoena shall be logged by the Desk Officer in the Daily Administrative Journal and shall include:
- BOP check for member's safety;
- Date and time service was executed or attempted;
- Name of member executing or attempting service;
- Name and address of person on whom legal process was served or executed; and
- Method of service or reason for non-service.

Whenever possible, the summons/subpoena shall be served by giving a copy, in hand, to the party named.

If the party is not home when the service is attempted, the summons/ subpoena:
- May be left with another responsible person residing at the residence; or
- May be left at the last place of abode of the person named.

If the person lives outside the area where service can be made and there is sufficient time, the summons/subpoena may be mailed to the last known address.

If the summons/subpoena is for a juvenile, service may be made in hand to the parent or guardian of the juvenile.

If the service of the summons/subpoena is not possible, it shall be returned to the court of issuance, with a reasonable explanation for non-service.

References

MGL c.276, s.11-20, s.23A, s.29
MGL c.248, s.26
MGL c.22C, s.10
MGL c.6, s.167-178

Promulgated By:

Department of State Police
General Order

Effective Date	Number
May 5, 2017	**PRI-02**

Subject

Custodial Inventory

Policy

Any person (subject) who comes into the custody of the Department shall be searched.

Purpose

- To protect members and subjects from harmful items or substances that may have been concealed by the subject;
- To protect members from claims of lost, stolen, or damaged property; and
- To establish and define the processing of subjects who come under the care and custody of the Department.

Inventory Protocol

Members SHALL:
- NOT physically search a subject for the sole purpose of determining the subject's gender.
- Conduct searches of transgender or intersex subjects in a respectful and appropriate manner and in the least intrusive manner possible, consistent with security needs.

Members are authorized to:
- Search a subject and remove any property from their clothing or person; and
- Search the contents of any outer garments, bags or accessories.

Members searching a subject shall:
- Inventory any documents, currency, jewelry, or valuable items found, carried or concealed by the subject;
- Record inventory on the SP 2 Custodial Property Inventory;
- If possible, inventory items in the presence of the subject;
- Have the arresting member, booking member, and the subject sign the SP 2. (If the subject refuses to sign, note the refusal and the reason, if any); and
- Properly secure the subject's property.

Member conducting the booking shall:
1. Have the subject remove:
   - Shoes, belts, ties;
   - Loose or extraneous clothing;
   - Jewelry, necklaces, neck chains; and
   - Any other article that the subject may use to escape or cause harm.
2. Before placing the subject in a cell, scan the subject with a hand-held metal detector.

Subject	Number
Custodial Inventory	**PRI-02**

Inventory Protocol (Continued)

The following items may be retained by a subject in the cell, unless a member believes it would create a hazard:

- Wedding ring;
- Currency; and
- Eye glasses, hearing aids, and prosthesis.

Valuable Property, Currency and Jewelry

The member searching a subject that has valuable property, currency or jewelry shall:

- Record the items on the SP 2 Custodial Property Inventory;
- Count currency by denomination and verify amount with a witnessing member present;
- Package and seal valuable property, currency or jewelry in a Department evidence bag (evidence bags shall be labeled 1 of 1, 1 of 2, 2 of 2, accordingly), and initial the seal;
- Secure valuable property, currency or jewelry within the appropriate prisoner belongings area while the subject remains in Department custody; and
- Provide the Desk Officer that is on duty with a copy of the investigative report and complete inventory of the valuable property, currency or jewelry to be logged into the Daily Administrative Journal (DAJ).

If a subject <u>leaves</u> the Department's custody, or is transported or transferred to another facility, and the subject's valuable property, currency or jewelry is <u>not returned</u>, the Desk Officer on duty shall immediately:

- Secure the valuable property, currency or jewelry within the Temporary Contraband/Controlled Substances Locker;
- Log the valuable property, currency or jewelry within the Temporary Contraband/Controlled Substances Journal;
- Make a log note into the Daily Administrative Journal (DAJ) of the time the valuable property, currency or jewelry was placed into the Temporary Contraband/Controlled Substances Locker;
- Notify the Troop Duty Officer; and
- Provide a copy of the investigative report to the Property Custodian or Assistant Property Custodian to be placed with the valuable property, currency or jewelry until the owner returns to collect property.

The Arresting Member shall:

- Make every effort to return the valuable property, currency or jewelry to the owner, or to a designated person identified by the owner, when the owner fails or cannot return to the Department to collect such property.

Subject	Number
Custodial Inventory	**PRI-02**

Return of Property

When the subject is released from custody their property (except seized property) shall be returned to the subject and:

- The subject shall sign the SP 2 acknowledging the return; and
- If the subject refuses to sign the form, the refusal and the reason, if any, shall be noted.

If the subject is to be transported or transferred to another facility, the transporting/transferring member shall ensure that:

- A copy of the SP 2 has been provided to the facility and/or the personnel taking custody of the subject;
- The name of the person taking custody is recorded on the original SP 2;
- The person taking custody has signed the SP 2; and
- The original SP 2 is returned to the Department facility where the subject's inventory search was conducted.

Valuable property, currency or jewelry stored with the Property Custodian or Assistant Property Custodian shall:

- Be returned to the owner on a mutually agreed upon time and date.

Container Protocols

Any closed unlocked container shall be opened and each article inventoried individually.

If a container is locked and secured, or if a container cannot be opened without damaging it, the member shall ask the subject for consent to open it.

If consent is not given, the member shall not open the container unless:

- Probable cause exists to believe that the locked container shall put the member or others in immediate risk of injury or loss of life.

If the container is not opened, it shall be inventoried as a single unit.

A member shall apply for a search warrant to open a locked container if they have probable cause to believe the container has inside it:

- Fruits or instrumentalities of a crime; or
- Evidence, contraband or weapons.

Strip Search Protocols

A "strip search" entails:

- The removal of the last layer of a subject's clothing; so
- A visual inspection can be made of all areas of the subject's body where weapons, dangerous instrumentalities, evidence, or contraband may be concealed.

The need for a strip search is based upon:

- An individual basis by the particular circumstances surrounding the arrest and probable cause to believe that the subject has contraband or weapons that may jeopardize the health and safety of the subject and/or those who may come in contact with the arrested person. The reasons for the search shall be documented in the arrest report.

Strip searches shall only be conducted:

- With the approval of a supervisor (unless exigent circumstances exist);
- Whenever practicable by two (2) members of the same gender as the subject;
- In an area that affords complete privacy (strip searches shall not be conducted outside of a Department facility, unless exigent circumstances exist);
- Out of the public view (including video cameras, windows, et cetera);
- Without any touching of the subject (although the subject may be asked to bend at the waist and spread their buttocks);
- In a reasonable, non-abusive, and professional manner; and
- Only for the duration necessary to complete the search.

Body Cavity Search Protocols

Members shall not perform physical intrusions into body cavities.

A body cavity search is:

- A search conducted pursuant to a warrant, issued by a judge, that is based on a high degree of probable cause; that
- Authorizes a medical professional to conduct an internal manual inspection of any human body cavity.

A member or supervisor seeking such a warrant must:

- Show a **high degree of probable cause** that the subject has contraband or weapons hidden in a body cavity that may jeopardize the health and safety of the subject and/or anyone that s/he may come in contact with.

Body cavity searches shall only be performed:

- By a medical practitioner in appropriate medical surroundings; and
- Pursuant to a search warrant issued by a judge that authorizes a body cavity search.

Continued next page.

Subject	Number
Custodial Inventory	**PRI-02**

Body Cavity Search Protocols (Continued)

The warrant requirement shall apply:

- Where an item may be viewed partially protruding from a body cavity.

No warrant is required when:

- A subject voluntarily and personally extracts any item from their own body cavity; and
- Cases involving exigent circumstances where medical personnel perform an operation, necessitated solely by good medical practice for medical reasons, which incidentally results in the recovery of evidence for police use.

References

SP 2 Custodial Inventory Form
Commonwealth v. Thomas, 492 Mass. 403 (1999)
Rodriques v. Furtado, 410 Mass. 878 (1991)

Promulgated By:

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**PRI-03**

Subject

Prisoner Transportation

Policy

Safety is the paramount concern when transporting prisoners. Members shall always keep in mind:

- The safety and well-being of themselves and others;
- The proper restraint of the prisoner to prevent escape or injuries; and
- The prisoner's safety and rights.

Prisoner Search Protocols

Cruisers shall be searched before and after transporting prisoners for contraband, weapons, fruits or instrumentalities of a crime, and/or evidence. A search is also part of the routine cruiser inspection at the beginning of the shift.

All individuals in custody shall be searched for weapons and contraband prior to being placed in a cruiser or otherwise transported. Never assume that someone else has searched a prisoner.

Under exigent circumstances, it may be necessary for a member to search a member of the opposite gender. Such a search shall be conducted professionally and be limited to the minimal invasion of privacy necessary. In other situations it may be more prudent to request assistance by an officer of the same gender as the prisoner, or conduct the search in the presence of others.

Cruisers

Cruisers which are routinely used to transport prisoners shall have:

- Safety barriers (prisoner cages);
- The rear passenger compartment window and locks disabled;
- Rear passenger seat belts; and
- Rear passenger door locks that cannot be unlocked from the rear passenger compartment.

When transporting a prisoner, members should not respond to calls for service unless:

- The situation clearly poses a serious risk to others; and
- The risk to prisoner is minimal.

Subject	Number
Prisoner Transportation	**PRI-03**

Prisoner Restraint Protocols

Unless extenuating circumstances dictate otherwise, members transporting prisoners shall ensure:

- Prisoners are handcuffed with their hands behind their back;
- Use alternate devices or methods when it is physically unable to handcuff someone behind their back;
- Double locked handcuffs to prevent inadvertent tightening or to avoid causing or aggravating any injuries.

If prisoners are to be transported for an extended period, members may handcuff them in front, and use a waist chain or other device to secure the hands to the waist.

Prisoner's legs may be restrained if their actions indicate that they may be a threat.

Prisoners shall not have their legs bound to their hands, except for extreme circumstances.

Prisoners should not be handcuffed or restrained to any part of the vehicle (except for use of the seat belt).

Seating Positions

Members shall:

- Ensure that prisoners being transported are visually observable at all times;
- Secure prisoners with a seat belt;
- Not transport more than two (2) prisoners at a time, unless authorized by a supervisor;
- Not transport two (2) prisoners in a cruiser without a safety barrier, unless another member is present;
- Whenever practical, transport prisoners of the opposite gender in separate vehicles; and
- Ensure prisoners of opposite gender are not transported to court in the same vehicle Massachusetts General Laws (MGL) c.276, s.53.

IF the cruiser has...	**Then, unless circumstances dictate otherwise, prisoner(s) should be placed...**
A safety barrier.	In the rear compartment, using the right seat first.
One (1) officer, one (1) prisoner, no safety barrier.	In the right front seat.
Two (2) members, one (1) prisoner, no safety barrier.	In the right front seat with the other member behind them.
Two (2) members, two (2) prisoners, no safety barrier.	One in the right front, one in the right rear seats, with the other member seated behind the driver.

Subject	Number
Prisoner Transportation	**PRI-03**

Transportation of Juveniles

Juveniles shall not be transported:

- With adult prisoners; or
- To court or other institutions in a "patrol wagon" as stipulated in MGL c.119, s.34.

Transporting Opposite Gender Prisoners

Members transporting prisoners of the opposite gender shall radio their Station/Unit Desk Officer, and have a Daily Administrative Journal (DAJ) entry made of the:

- Location;
- The number and gender of their prisoner(s);
- Preliminary charges against the prisoner(s);
- Intended destination;
- Beginning odometer mileage, and upon arrival, the ending mileage; and
- Request for back-up, if necessary.

Communication

Conversations with prisoners shall be professional and kept to a minimum.

- Conversations between prisoners shall be limited by the transporting officer for safety reasons.

Members shall not allow prisoners to use communications equipment while in transport, nor stop to allow a prisoner access to communication equipment.

Protocols for Transferring Prisoners

When transporting a prisoner to or from another agency or a court detention facility, members shall:

- Secure firearms if required by that facility's protocol;
- Remove restraining devices in the designated area;
- Positively identify the prisoner by ID, photographs or fingerprints;
- Deliver or receive the necessary documentation, paperwork, and/or information; and
- Adhere to procedures within PRI-02 Custodial Inventory regarding subject's property.

If the prisoner is a security hazard, suicide risk, or has a condition that the receiving agency or court should be aware of, the receiving agency shall be advised in writing of that condition.

Medical Considerations

If, while in transit a prisoner notifies the transporting member of an illness or injury, and if in the member's opinion an illness or injury exists and requires immediate attention, the member shall transport the prisoner to the nearest medical facility for an examination.

- The transporting member shall notify the Desk Officer; and
- Desk Officer shall notify the medical facility of the particulars prior to the prisoner's arrival.

If a prisoner is admitted to a medical facility, the Department shall provide or ensure proper security arrangements, if necessary, or arrange for the prisoner to be bailed.

If released by the medical facility, the prisoner shall be transported to the nearest station or facility, as appropriate.

When transporting a physically or mentally challenged prisoner, special care and attention may be required. The transporting member shall use discretion as to the type of restraints to be used and the Troop Duty Officer shall be notified.

Prisoner Escape Protocols

Position	Duties
Transporting Member	1. Immediately notify the appropriate Desk Officer of: • Cruiser number, member's name, rank; • Exact location; • Prisoner method of escape, escape route, and means of transportation; • Name and aliases of escapee, and a physical description including clothing; and • Criminal history and safety risk of the escapee, and the pending charges. 2. Immediately make every attempt to recapture the escapee, and if unable to do so, preserve the scene for tracking dogs and investigators.
Desk Officer	1. Immediately notify the Troop Duty Officer of jurisdiction; 2. Notify all patrols and local departments of the escape; and 3. Make the appropriate DAJ entries.

Continued next page.

Prisoner Escape Protocols (Continued)

Position	Duties
Troop Duty Officer	1. Dispatch a supervisor to the scene to: • Assume control of the recapture operation; • Investigate the circumstances of the escape; and • Prepare a report with findings and recommendations. 2. Notify: • Department Detectives Unit of jurisdiction: and • The Troop Commander.
Troop Commander	1. Notify Division Commander; 2. Administratively review report(s) for further action; and 3. Take actions to prevent reoccurrences.

Special Situations

No prisoner or individual in custody shall be allowed to participate in any operation and/or function without the specific written approval of the Division Commander.

Section/Units that conduct such operations or functions on a regular basis may request blanket authorization from their Division Commander. If such authorization is granted:

- Sufficient security shall be deployed to maintain control of the prisoner or individual;
- The intended destination shall be checked out in advance by an member;
- Control of the perimeter shall be maintained;
- There shall be minimal contact between the prisoner and others; and
- Any other measures deemed necessary by the officer-in-charge (OIC) shall be taken.

Commercial Air Transportation and Armed Members

Members shall be certified and follow the federal Transportation Security Administration (TSA) guidelines and Code of Federal Regulations (CFR) Title 49 Carriage of Weapons by Law Enforcement Officers.

Troop/Section Commanders shall ensure the following protocols are followed when members, under their command, fly on commercial airlines while armed.

1. An administrative message shall be sent to the Transportation Security Administration (TSA) by the GHQ Communications Section via the National Law Enforcement Telecommunications System (NLETS), requesting a unique alphanumeric identifier receipt for the member who will be flying armed.

Continued next page.

Commercial Air Transportation and Armed Members (Continued)

2. The member shall carry the receipt containing all the pertinent information required by TSA to be verified at the airport on the day(s) of travel.
3. The member shall also carry the appropriate number of signed original Letters of Authority from their Troop/Section Commander and surrender a letter to the airline carrier(s) when requested.
4. The Letters of Authority shall be on Department letterhead and shall include:
   - The name(s) of the member(s);
   - The dates and itinerary for fights;
   - Certification that the member(s) have completed the TSA's Law Enforcement Officers Flying Armed Program;
   - The circumstances for the need to carry a firearm; and
   - The original signature of their Troop/Section Commander and a contact number for verification.

Note: Failure to provide the unique alphanumeric identifier may result in delays due to the additional verification requirements. The airline and the pilot have the discretion to refuse armed members on any fight.

Procedure Transporting Prisoners by Commercial Airlines

When transporting a prisoner on an commercial airline flight, members shall:

- Notify TSA and the airline of the name(s) of the prisoner(s) and the accompanying member(s) at least one (1) hour before the flight;
- Notify TSA and the airline if the prisoner is considered a "high risk" at least twenty-four (24) hours, or as soon as possible, before the scheduled departure. If so, at least two (2) members shall escort the prisoner and arrive at the check-in counter at least one (1) hour before the flight. Only one dangerous prisoner is allowed on the same flight;
- Ask to board the plane first, and deplane last;
- Sit in the rear of the plane, maintaining one (1) member between the prisoner and the aisle;
- Ensure that no food, utensils, or items be given directly to the prisoner without checking the items first; and
- Not consume, nor allow the prisoner to consume, alcoholic beverages.

Note: There shall always be at least one (1) member per prisoner. At least one (1) member shall be the same gender as the prisoner.

Members shall carry:

- Department issued badge and identification card;
- A secondary valid government issued ID;
- Necessary boarding paperwork;
- Letters of Authority to travel while armed on commercial flight; and
- Adequate restraining devices.

Subject	Number
Prisoner Transportation	**PRI-03**

References

PRI-02 Custodial Inventory
MGL c.276, s.53
MGL c.119, s.34
Code of Federal Regulations (CFR) Title 49 Transportation
Transportation Security Administration (TSA) "Law Enforcement Officers Flying Armed" Program

Promulgated By:

Department of State Police
General Order

Effective Date	Number
May 20, 2016	**PRI-04**

Subject

Holding Facility Design and Inspection

Policy

The Department shall maintain holding facilities that comply with applicable laws and regulations, in order to provide a safe environment for members and prisoners.

Definitions

Holding Facility: A temporary confinement cell or lockup where prisoners are generally held for less than seventy-two (72) hours.

Prisoner: A person who has been arrested or is in the custody of the Department.

Design of Holding Facilities

Department holding facilities shall comply with Department of Public Health regulations and shall, at a minimum, be equipped with:

- Adequate lighting and air circulation;
- Access to a toilet and drinking water;
- Access to a wash basin and a bed with sanitary/fire-retardant bedding for each prisoner held in excess of eight (8) hours;
- A first-aid kit, automatic fire alarms, smoke detectors, and adequate fire suppression systems;
- Audio and electronic (Watchman) monitoring system; and
- Posted signage regarding prisoners' rights, obtaining medical services, and emergency evacuation.

Department holding facilities shall comply with the *Prison Rape Elimination Act (PREA) of 2003* and shall have signage posted advising prisoners how to report incidents of sexual abuse and/or harassment.

Sanitation

Holding facilities shall be kept clean and sanitary, and shall be inspected:

- Before use by a prisoner;
- Upon release of a prisoner, and
- As necessary to prevent the spread of communicable diseases, as outlined in GEN-05 *Communicable Diseases*.

Cells and Keys

Cells that are:

- Ready for use shall be kept open and unlocked; or
- Not usable shall be kept closed, locked, and posted.

Keys for the cells, and duplicates, shall be kept readily available at the station desk area.

Fire Prevention

- No matches, lighters, or smoking materials are allowed in any Department holding facility;
- Fire/smoke detection and suppression systems shall have written approval of fire officials;
- An emergency evacuation plan shall be written and posted; and
- At least one (1), preferably two (2), emergency exits shall be marked with a sign.

Electronic Monitoring

In addition to audio monitoring devices required by law, each holding facility shall have:

- A means of communication with the Station Desk Officer, or a panic alarm; and
- A video monitoring system so that each cell can be observed from the desk.

Guidebook

Troop Commanders shall ensure that a guidebook is kept at the desk or in the holding area of each facility, to assist the Station Desk Officer.

The guidebook shall contain information on:

- Holding facility operations;
- Procedures for escapes, fires, or suicide attempts;
- Available alternative lock-up facilities for juvenile offenders;
- The names and contact information for persons or organizations who will respond in the event of an attempted or threatened suicide; and
- The names and contact information for persons or organizations who will respond in the event of an incident of sexual assault and/or sexual harassment.

Training

Members at a location where there are holding facilities shall receive training in:

- Suicide detection, intervention, and prevention;
- PREA Standards
- Department policies regarding holding facilities, equipment and operations;
- Use of physical restraints; and
- Operation of fire suppression equipment.

Access

Non-essential persons shall not have access to the cell area, unless:

- Visiting a prisoner, as outlined in PRI-06 *Prisoner Monitoring***;** or
- No prisoners are present, and the person(s) is accompanied at all times by a member.

Maintenance, sanitation, repair, or other outside personnel may have access to cells as necessary. Afterwards, the cell area shall be inspected for tools or other items that may have been left behind.

Subject	Number
Holding Facility Design and Inspection	**PRI-04**

Inspections

An inspection of each cell for weapons or contraband shall be made immediately prior to use.

Station Commanders are responsible for ensuring:

Frequency	Item of Inspection
Daily	• Fire detection and suppression equipment (visual inspection); • Cell bars, doors, locks, windows, ventilation, lights, monitors, security devices, and first-aid kits; • Tampering or damage to facilities; • Search for weapons or contraband, and • Sanitation, including vermin and pest inspection.
Weekly	• Inspect the cell electronic monitoring device (Watchman) to ensure it is properly functioning; • Run a printout of the previous week's cell checks; • Examine the printout for compliance and discrepancies; and • Retain the weekly printouts for one (1) year.
Monthly	• Automatic Fire Alarm system test.
Semi-Annually	• Fire suppression equipment test; and • The review of the guidebook for accuracy.

Inspection records shall be maintained at the sub-station for line and staff inspections.

Station Commanders shall ensure cooperation with state and local health and fire inspectors.

To prevent inadvertent use, individual cells that do not pass inspection shall be kept closed, locked, and posted with an explanation of the problem.

Incidents

Prisoners who cause damage to the cells may be subject to prosecution under MGL c.266, s.96, Defacement or Injury to a State Building.

Station Commanders shall make written reports to their Troop Commander, of all incidents or conditions that threaten the holding facility or prisoners, or the ability of the sub-station to safely hold prisoners.

Troop Commanders shall immediately notify through channels, the Division Commander of Administrative Services, of all such incidents or conditions. The Division Commander of Administrative Services shall notify the Department of Public Health as required.

Subject	Number
Holding Facility Design and Inspection	**PRI-04**

Temporary Holding Areas

Troop Commanders may authorize such temporary holding areas for the purpose of booking and bailing prisoners, which shall provide for:

- Constant supervision of all prisoners held in temporary holding areas;
- Immovable objects that are intended for use as a restraining device;
- Access to water and restrooms;
- Separation of male, female and juvenile prisoners who are at high risk of being sexually assaulted;
- Fire prevention, evacuation, and suppression procedures; and
- Adherence to any applicable security procedures as outlined in Policy and Procedure.

References

GEN-05 Communicable Diseases
PRI-06 Prisoner Monitoring
PRI-07 Detainee Sexual Assault and Harassment
105 CMR 470
MGL c.40, s.36B
MGL c.111, s.21 and s.22
MGL c.266, s.96
Prison Rape Elimination Act (PREA) 28 CFR 115

Promulgated By.

Department of State Police
General Order

Effective Date	Number
June 14, 2018	**PRI-05**

Subject

Identification of Persons in Department Custody

Policy

All persons in department custody must be properly identified prior to release. Fingerprints offer the most reliable means of individual identification. The submission and retention of fingerprint records and other biometrics create a reliable criminal history record. **Therefore, all persons arrested shall be fingerprinted and photographed**. In addition, all persons charged with a felony shall have their palmprints recorded if recording equipment is available. Persons taken into department custody for non-criminal reasons may be fingerprinted and photographed or may be identified through other means.

Definitions

AFIS (Automated Fingeprint Identification System): The computerized biometric matching system that stores identifying biometric templates and related demographics. The State AFIS maintains the following biometric information: known fingerprints and palmprints, latent fingerprints and palmprints, booking and tattoo photos, and iris images. AFIS is operated by the State Identification Section.

AFISR: An application available from the Department of Criminal Justice Information Services via single sign-on (DCJIS SSO). This application allows the review of Massachusetts fingerprint supported arrest records and the search of recent arrest submissions. This system can be searched by OBTN, Name, SID, and FBI number.

Biometrics: Distinctive, measurable physiological characteristics used to identify individuals. Commonly collected biometrics include fingerprints, palmprints, photographs (mug shots), and iris images.

Live Scan: Electronic fingerprint capturing devices that submit fingerprints, palmprints, and associated demographics and photographs to the State AFIS and NGI.

OBTN/ SBTN (Occasion/Offense Based Tracking Number): a unique number assigned by the records management system associated with a specific event. This number allows the tracking of the individual event from arrest or summons through the state criminal history systems including AFIS and the courts.

NGI (Next Generation Identification): a biometric matching system operated by the FBI that replaces the IAFIS system creating a national electronic repository of biometric and criminal history information. www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi.

Continued next page.

Definitions (Continued)

SID (State Identification Number): A unique personal identifier based on a fingerprint ID and assigned by AFIS and the Identification Section.

UCN (Universal Control Number, formerly FBI number): Unique personal identifier based on a fingerprint ID and assigned by the FBI. This number is assigned to both criminal AND civil identities on file with the FBI.

Procedure for Properly Identifying Subjects

All persons arrested shall be fingerprinted and photographed. All persons charged with a felony shall have their palmprints recorded if recording equipment is available. Persons taken into department custody for non-criminal reasons may be fingerprinted and photographed or may be identified through other means.

Fingerprints and palmprints shall be captured and submitted to AFIS using the Live Scan device according to the *SIS-DOC 12-LIVESCAN Operational Guide*, which is located on Docushare.

The subject's booking photo/mugshot shall be captured in RAMS.

Fingerprinting shall include the recording or annotation of all fingers and may include the recording of palmprints.

The following demographic information shall be included with all fingerprint submissions:

- OBTN/SBTN
- Name,
- Date of birth,
- Sex,
- Race,
- Place of birth,
- Height,
- Weight,
- Eye color,
- Hair Color,
- Literal description of charges (not the chapter/section only),
- Date printed,
- Fingerprint official, and
- Date of arrest.

All Live Scan operators must properly log on and log off the system to prevent unauthorized access to the system. The operator logged on to the system will be documented as the fingerprint official on the official record.

Arrested persons shall not be considered eligible for bail until their fingerprints have been accepted and verified by AFIS. Fingerprint submission search results may be reviewed from the Live Scan or by viewing results in the DCJIS AFISR application. The *SIS-ADM-10 AFISR Procedural Guide* is available on Docushare.

Subject	Number
Identification of Persons in Department Custody	**PRI-05**

Special Circumstances

In instances where Live Scan is not operational or available, the subject may be:

- Transported for processing to a sub-station where Live Scan equipment is available.

When the Live Scan and/or AFIS is not available and it is impractical to transport to another location, the subject shall be:

- Processed using the traditional fingerprint card and inkpad method. The fingerprint card shall be sent immediately to the Identification Section via troop mail for manual entry into AFIS.

- In circumstances where inked fingerprints are taken, an arrested person may be considered eligible for bail consideration.

In instances when a subject's identity cannot be documented or when mutilated fingerprints are observed, the booking officer or desk officer may contact the Identification Section for review of the fingerprint record. The booking officer shall provide the SBTN/ OBTN.

Additionally, in situations when mutilated prints are observed, the Troop Duty Officer may contact the Crime Scene Services Section (CSSS) to assist in capturing full major case prints and/or tenprints to assist in offender identification.

Supervisors at the sub-station level and Cases and Reports Officer at the Troop level shall ensure:

- All officers are properly trained on the use of electronic fingerprinting/biometric capture equipment;
- All biometric processing equipment is operational;
- Proper supplies are available; and
- Biometrics are properly captured and submitted to the Identification Section.

Identification Section
59 Horse Pond Road
Sudbury, MA 01776
24 hour contact 508-358-3170

Troop Commanders shall ensure overall compliance with this General Order.

References

SIS-DOC 12 LiveScan Operational Guide
SIS-ADM 10 AFISR Procedural Guide
SIS- ADM XX Mutilated Altered Print Recognition Guide

Promulgated By:

Department of State Police
General Order

Effective Date	Number
May 5, 2017	**PRI-06**

Subject

Prisoner Monitoring

Policy

Continuous supervision is essential for maintaining and assuring the safety and welfare of prisoners while in custody. Whenever a prisoner is placed in a Department cell, the Desk Officer shall activate the cell audio and video monitoring system.

Monitoring

- The Desk Officer shall physically check all prisoners every hour, and shall use the electronic monitoring (Watchman) device during the check;
- The audio and video systems shall also be used to continuously monitor the prisoner's condition, and as a means of two-way communication with prisoners and other members in the cell area.
  Note: The system shall not be used to unnecessarily violate the personal privacy of the prisoner(s).
- Prisoners held over four (4) hours shall have meals provided at regular meal times, three (3) meals a day;
- Meals may be provided from a correctional facility, prisoner meal fund, from the prisoner's funds with their consent, or other appropriate source;
- The Desk Officer shall document within the Daily Administrative Journal (DAJ) the number, cost (if applicable), and type of meals served;
- Dishes, cups, and all utensils shall be used only once and then disposed of;
- Common cups and towels are not allowed;
- Prisoners held for over eight (8) hours shall be given access to a wash basin; and
- The Desk Officer shall provide heightened protection to vulnerable detainees to include direct sight and sound supervision. The Desk Officer shall monitor the conduct and treatment of detainees or employees who reported sexual abuse and of detainees who were reported to have suffered sexual abuse pursuant to PRI-07 *Detainee Sexual Abuse and Sexual Harassment* and PRI-07A *Detainee Sexual Abuse and Sexual Harassment Investigations, Review and Data Collection.*

Booking Process

- Firearms and Electronic Control Weapons (ECWs) **shall not** be carried on a member's person during the booking process, including (but not limited to) booking, fingerprinting, and the administration of the breath test.

Entering a Cell Area

Firearms and ECWs shall be secured before entering an occupied cell area, except when all prisoners are secured in the cells and the hourly check is being made.

Members entering the cell area alone should maintain a means of communication by:

- Verbal communication with another member;
- Portable radio; or
- Alarm or other means.

Department members shall announce themselves prior to entering the cell area containing a member(s) of the opposite sex. Staff shall not place themselves in a position where they can view the breasts, buttocks, or genitalia of a detainee of the opposite gender.

Detainees will be allowed to perform bodily functions without members or employees of the opposite gender viewing their breasts, buttocks or genitalia, except in exigent circumstances or when such viewing is incidental to routine cell checks.

Entering an Individual Cell

Members shall only open or enter an occupied cell when:

- At least one (1) other member is present;
- When releasing a prisoner from custody; or
- In the event of an emergency.

Conduct

Members should not engage in speech or behavior that could be construed as inappropriate.

Visitors

Requests for visits that do not interfere with station operations may be allowed by the station OIC. A member shall remain physically present during the visit and all visitors shall:

- Show positive identification;
- Be checked for outstanding warrants;
- Submit to a search for weapons or contraband, which shall include an inspection of their belongings before and after the visit;
- Have their name, address, and relationship documented in the DAJ;
- Only be allowed to visit the prisoner one at a time;
- Not have any physical contact with prisoners; and
- Not violate the privacy of other prisoners.

Visitation with counsel may be permitted at the discretion of the station OIC and reasonable efforts should be made to ensure privacy during these visits.

Mail/Packages

Prisoners may only receive funds, food, prescription medications, or clean clothing. All items shall be:

- Inspected for contraband and placed with the prisoner's property, or given to the prisoner as appropriate;
- Documented on a SP 2 Prisoner Inventory Form; and
- Noted in the DAJ.

Shift Change

The on-duty desk officer shall inform the incoming desk officer about the count and condition of the prisoners. Incoming desk officers shall physically verify the count and condition of prisoners prior to assuming desk duty.

Suicide Threats or Attempts

Information received from any source pertaining to a prisoner's risk of harming themselves shall be considered valid.

If the prisoner…	Then…
• Makes a suicide threat or attempt; • Has an entry in the Q5 Query; • Indicates current suicidal tendencies on the Suicide Prevention Checklist; or • Clearly exhibits signs or symptoms of suicidal behavior.	• A member shall be assigned to **physically watch** the prisoner at all times; or • The prisoner shall be transported to a medical facility for evaluation.

If a person in custody attempts or threatens suicide at a lockup facility, as outlined in Massachusetts General Laws (MGL) c.40, s.36A, the following additional responsibilities apply:

Position	Duties
Desk Officer	• Provide medical attention as necessary; • Notify the Troop Duty Officer and Station Commander; • Consult the guidebook; • Document the incident in the DAJ; and • Enter the incident into the Q5 suicide menu of the CJIS computer prior to the end of the shift.
Station OIC	• Notify, in writing, any lockup facility that the prisoner is transferred to.
Troop Duty Officer	• If needed, send a supervisor to the station to assist; • If appropriate, assign a member to guard the prisoner at the facility; • Make the appropriate DAJ entries; and • Ensure that proper procedures and MGL c.40, s.36A are followed.

Escape or Wrongful Release

If a prisoner escapes or is inadvertently released, the following actions shall be taken:

Position	Duties
Desk Officer	• Immediately notify the Troop Duty Office and Station Commander; • Notify area patrols and local departments of the escape; and • Make the appropriate DAJ entries.
Troop Duty Officer	• Dispatch a supervisor to the scene; • Notify the Troop Commander; • Notify GHQ Communications; • Notify the appropriate State Police Detective Unit (SPDU) of jurisdiction; and • Make the appropriate DAJ entries.
GHQ Communications	• Notify the Division Commander.
Troop Commander	• Ensure the Division Commander was notified; and • Review reports and take actions to prevent reoccurrences.
Division Commander	• Review reports and take actions to prevent reoccurrences.

Medical Care

Sick or injured prisoners should not be transported by the Department, unless two (2) or more members are available for the transport. It may be more prudent to await the arrival of an ambulance.

- Upon arrival of an ambulance, members shall defer medical care to the EMTs but shall retain custody and security; and
- The Troop Duty Officer shall be informed of any such incidents.

When a member observes or is informed by a prisoner that they have a medical problem that requires immediate medical treatment, the station OIC or supervisor should request an ambulance. If unsure as to whether or not a prisoner requires immediate medical treatment, members shall request assistance from trained medical personnel.

If it is an emergency or appears serious, members shall provide basic First Aid.

In the event of a sexual assault upon a detainee while in State Police custody by another detainee, staff member, employee or contractor, the responding member shall adhere to the requirements of PRI-07 *Detainee Sexual Abuse and Sexual Harassment.*

The procedures for requesting emergency health care shall be posted in a conspicuous place in English and any other language(s) prevalent within the station area.

Prisoner Death Protocols

If a prisoner dies while in a Department facility, the following actions shall be taken:

Position	Duties
Desk Officer	• Immediately notify the Troop Duty Officer and the Station Commander.
Troop Duty Officer	• Immediately notify the Troop Commander; • Immediately notify the SPDU of jurisdiction; • Notify the Medical Examiner's Office, as requested by SPDU; • Ensure that the appropriate DAJ entries are made; and • Ensure that proper procedures and MGL c.40, s.36A are followed.
State Police Detective Unit	• Respond to the scene and take command of the investigation.
Station Commander	• Submit, within four (4) days, a report of the incident to the Troop Commander, along with all other related reports.
Troop Commander	• Immediately notify the Division Commander; • Assign a Commissioned Officer to immediately assist the SPDU investigation and to conduct an Administrative Review of the incident; • Forward copies of the reports to the Medical Examiner within seven (7) days; and • Review and submit reports and recommendations to the Division Commander.
Reviewing Commissioned Officer	• Assist the SPDU; • Conduct an Administrative Review of the incident; and • Prepare a report for the Troop Commander within four (4) days. Note: The Administrative Review is to ensure that members followed Department procedures during the incident.
Field Services Division Commander	• Review reports and take actions to prevent reoccurrences; • Submit reports to the Deputy Superintendent for review and action; and • Maintain a file on prisoner deaths.

Subject	Number
Prisoner Monitoring	**PRI-06**

References

ADM-14 Personnel Investigation
UOF-06 Electronic Control Weapons
SP 2 Prisoner Inventory Form
MGL c.111, s.8 Use Common Drinking Cup
MGL c.40, s.36A Report of Death/Suicide Records
SPAM Collective Bargaining Agreement Article 27
Criminal Justice Information System (CJIS)
PRI-07 Detainee Sexual Abuse and Sexual Harassment
PRI-07A Detainee Sexual Abuse and Sexual Harassment Investigations, Review and Data Collection

Promulgated By:

Department of State Police
General Order

Effective Date	Number
May 21, 2018	**PRI-07**

Subject

Detainee Sexual Abuse and Sexual Harassment

Policy

In accordance with the *Prison Rape Elimination Act (PREA) of 2003,* the Department shall:

- Establish a zero tolerance policy toward all forms of sexual abuse and sexual harassment towards any detainee;
- Ensure that all detainees have the right to be free from sexual abuse and sexual harassment; and
- Establish a zero tolerance policy toward all forms of retaliation against anyone who reports sexual abuse and sexual harassment or who cooperates in a sexual abuse investigation.

This policy shall be made available through the Department's website and upon request.

Definitions

Prison Rape Elimination Act (PREA): Signed into law on September 4, 2003. The Prison Rape Elimination Act establishes a standard of zero tolerance for rape and sexual assault or sexual harassment in any prison, jail, police lockup, or juvenile facility.

Lockup: A facility that contains holding cells, cell blocks, or other secure enclosures that are:
(1) Under the control of a law enforcement, court, or custodial officer; and
(2) Primarily used for the temporary confinement of individuals who have recently been arrested, detained, or are being transferred to or from a court, jail, prison, or other agency.

Detainee: Any person detained in a lockup, regardless of adjudication status.

Employee: A sworn member or civilian who works directly for the Department.

Holding Cell: Any secure enclosure that is under the control of law enforcement and is primarily used for the temporary confinement of suspects who have recently been arrested.

Intersex Individual: A person whose sexual or reproductive anatomy or chromosomal pattern does not seem to fit typical definitions of male or female.

Continued next page.

Definitions (Continued)

PREA Coordinator: A management level employee who oversees, develops, and implements Department efforts to comply with the PREA standards.

Sexual Abuse: Any sexual contact or the intentional touching of the victim's or suspect's genital, anal or other intimate area for sexual arousal or gratification, or for the abuse of either party; in this directive, includes in-custody sex offenses, voyeurism, or rape or attempts; harassment, sexual harassment, neglect, discrimination and similar terms. This policy applies to sexual abuse and/or harassment of a detainee by another detainee and/or sexual abuse of a detainee by a staff member, contractor, or volunteer.

Sexual harassment includes—
(1) Repeated and unwelcome sexual advances, requests for sexual favors, or verbal comments, gestures, or actions of a derogatory or offensive sexual nature by one inmate, detainee, or resident directed toward another; and
(2) Repeated verbal comments or gestures of a sexual nature to an inmate, detainee, or resident by a staff member, contractor, or volunteer, including demeaning references to gender, sexually suggestive or derogatory comments about body or clothing, or obscene language or gestures

Transgender Individual: A person whose gender identity (i.e., internal sense of feeling male or female) is different from the person's assigned sex at birth.

Voyeurism: When a staff member, contractor, or volunteer invades a detainee's privacy for reasons unrelated to official duties, such as peering at an inmate who is using a toilet in his or her cell to perform bodily functions; requiring the detainee to expose his or her buttocks, genitals, or breasts; or taking images of all or part of a detainee's naked body or of a detainee performing bodily functions.

Department Responsibilities

The Department shall ensure that:

- An administrative or criminal investigation is completed for all allegations of detainee sexual abuse and/or sexual harassment pursuant to PRI-07A *Detainee Sexual Abuse and Sexual Harassment Investigations, Review and Data Collection*;
- Alleged detainee sexual abuse and/or sexual harassment incidents, including third-party and anonymous reports, are reported to designated investigators;
- Detainees are informed of at least one way to report sexual abuse and/or sexual harassment to a public or private entity or office that is not part of the Department, allowing the detainee to remain anonymous if so requested;
- Investigators have received special training in sexual abuse investigations pursuant to Code of Federal Regulations (CFR) 28 § 115.34.
- Develop an internal protocol appropriate for juvenile detainees where applicable; and
- Take appropriate measures to prevent retaliation against individuals who report and/or cooperate with an investigation.

Screening for Risk of Victimization and Abusiveness

In accordance with training, when booking detainees, members shall screen all detainees to assess their risk of being sexually abused by other detainees or sexually abusive toward other detainees. The screening shall be documented in RAMS/Department Records Management System.

If after screening, the member determines that the detainee may be at risk, the detainee shall be housed alone in a holding cell for the duration of his/her detainment at a State Police facility. This includes post-screening transportation in a Department vehicle to/from court, jail, prison, or other agency.

Disabled Detainees

Detainees with disabilities include detainees who are deaf, hard of hearing, blind or have low vision, and those who have intellectual, psychiatric, or speech disabilities.

Members shall take appropriate steps to ensure that detainees with disabilities have an equal opportunity to benefit from all aspects of the Department's efforts to prevent, detect, and respond to sexual abuse and sexual harassment. Such steps shall include providing access to interpreters who can interpret effectively, accurately, and impartially when necessary to ensure effective communication with detainees who are deaf or hard of hearing. In addition, members shall ensure that written materials are provided in formats and through methods that ensure effective communication with detainees with disabilities.

Detainees with Limited English Proficiency

Members shall take reasonable steps to ensure that detainees with limited English proficiency have meaningful access to information regarding the Department's policies and efforts to prevent, detect, and respond to sexual abuse and sexual harassment including by providing interpreters who can interpret effectively, accurately, and impartially.

Detainee Interpreters

No member shall use detainees as interpreters or readers or otherwise request assistance from another detainee except in limited circumstances where an extended delay in obtaining an effective interpreter could compromise the detainee's safety, the performance of first-responder duties, or the investigation of the detainee's sexual abuse/harassment allegations.

Staffing Plans

Station commanders for each barracks containing cells shall develop and document a staffing plan that provides for adequate levels of staffing, and, where applicable, video monitoring to protect detainees against abuse.
Station commanders shall consider the following factors when determining adequate staffing plans:

- The physical layout of the lock-up;
- The composition of the detainee population;
- The prevalence of sexual abuse incidents; and
- Any other relevant factor(s).

Each time the staffing plan is not complied with, the station commander shall document and justify all deviations from the staffing plan and shall forward the document with justifications to the PREA Coordinator.

First Responder Responsibilities

The first law enforcement member to respond to a report of a sexual assault or sexual harassment shall:

- Immediately separate the alleged victim and abuser;
- Take immediate action to protect the detainee from substantial risk of imminent sexual abuse;
- Keep the detainee either with the officer or in the cell and under surveillance until a supervisor can investigate and determine any further actions to take to protect the detainee;
- Follow uniform evidence protocol that maximizes the potential for obtaining usable physical evidence including preserving and protecting any crime scene until appropriate steps can be taken to collect any evidence;
- If the abuse occurred within a time period that still allows for the collection of physical evidence, request that the alleged victim not take any action(s) that could destroy physical evidence, including, as appropriate, washing, brushing teeth, changing clothes, urinating, defecating, smoking, drinking, or eating;
- Offer all victims access to forensic medical examinations performed by a Sexual Assault Forensic Examiner (SAFE), Sexual Assault Nurse Examiners (SANEs) or qualified medical practitioner without financial cost to the victim, if evidentiarily or medically appropriate;
- If the detainee is transported for a forensic examination to an outside hospital that offers victim advocacy services, ensure that the detainee be permitted to use such services to the extent available, consistent with security needs;
- Document all efforts to provide a SAFE or medical practitioner;
- Attempt to make a victim advocate from a rape crisis center or other facility available to the detainee if transported to a hospital or other medical facility consistent with security needs; and
- Accompany the victim through the forensic medical examination process and interviews.

If the first staff responder is not a law enforcement staff member, that responder shall:

- Request that the alleged victim not take any actions that could destroy physical evidence; and
- Immediately notify law enforcement staff.

Note: See also Policy and Procedure PRI-07A *Detainee Sexual Abuse and Sexual Harassment Investigations, Review and Data Collection*.

PREA Coordinated Response Plan

If a prisoner reports that he or she was sexually harassed while in a Department facility, the following actions shall be taken:

Position	Duties
First Responder	• Immediately separate the alleged victim and abuser; • Preserve and protect any crime scene until appropriate steps can be taken to collect any evidence; • Request that the alleged victim not take any actions that could destroy physical evidence, including washing, brushing teeth, changing clothes, urinating, defecating, drinking, or eating; • Take immediate action pursuant to this General Order; and • Immediately contact the desk officer.
Desk Officer	• Take immediate actions as a first responder pursuant to this General Order; • Notify, if necessary, local EMS and a local medical facility for an assessment of alleged victim's acute medical needs and to make an assessment of necessary treatment; • Immediately notify the State Police Detective Unit (SPDU)/Specialized PREA investigator(s) of jurisdiction; • Explain to the alleged victim the need for a forensic medical exam and offer the victim the option of undergoing one without any financial costs; • Make best efforts to ensure that examinations are conducted by Sexual Assault Forensic Examiners (SAFEs) or Sexual Assault Nurse Examiners (SANEs), or ensure that a qualified medical practitioner performs forensic medical examinations; • Offer alleged victim services by providing the victim with list of local sexual abuse advocates and/or crisis centers found in the Department's PREA brochure in DocuShare/PREA; • Ensure that the appropriate Daily Administrative Journal (DAJ) entries are made; • Immediately notify the Troop Duty Officer and the Station Commander; and • If the victim is transferred from the lockup to a jail, prison, or medical facility, inform the receiving facility of the incident and the victim's potential need for medical or social services, unless the victim requests otherwise.

Continued next page.

PREA Coordinated Response Plan (Continued)

Troop Duty Officer	• Immediately notify the Troop Commander; and PREA Coordinator; • Ensure proper compliance with this General Order and PRI-07A Detainee Sexual Abuse and Sexual Harassment Investigations, Review and Data Collection; • Provide for any special needs the victim may have; and • In the event that the victim is transferred from the lockup to a jail, prison, or medical facility, ensure that the receiving facility is informed of the incident and the victim's potential need for medical or social services, unless the victim requests otherwise.
State Police PREA Specialized Investigator(s)	• Respond to the scene and take command of the investigation; • Take all actions pursuant to PRI-07A Detainee Sexual Abuse and Sexual Harassment Investigations, Review and Data Collection; • Inform the victim of his or her rights under relevant policies, federal and state laws; • Safeguard the custody of evidence; • Explain to the alleged victim the need for a forensic medical exam and offer the victim the option of undergoing one at no cost; • Offer the presence of a victim advocate or other staff member during the exam; • Interview the victim and any witnesses; • Submit report(s) of investigation pursuant to PRI-07A Detainee Sexual Abuse and Sexual Harassment Investigations, Review and Data Collection; and • Document all referrals of allegations of sexual abuse or sexual harassment for criminal • investigation.
Station Commander	• Submit, within four (4) days, a report of the incident to the Troop Commander, along with all other related reports.

Continued next page.

PREA Coordinated Response Plan (Continued)

Troop Commander	• Immediately notify the Division Commander; • Assign the PREA Coordinator to immediately assist the SPDU investigation and to conduct an Administrative Review of the incident; • Forward copies of the reports to the PREA Coordinator within seven (7) of their completion; and • Review and submit reports and recommendations to the Division Commander.
Reviewing Commissioned Officer	• Assist the SPDU; • Conduct an Administrative Review of the incident; and • Prepare a report for the Troop Commander within four (4) days. Note: The Administrative Review is to ensure that members followed Department procedures during the incident.
Field Services Division Commander	• Review reports and take actions to prevent reoccurrences; • Submit reports to the Colonel/Superintendent for review and action; and • Maintain a file for PREA incident review pursuant to PRI-07A Detainee Sexual Abuse and Sexual Harassment Investigations, Review and Data Collection.

Reporting

All employees shall immediately report to their immediate supervisor:

- Any knowledge, suspicion, or information regarding an incident of detainee sexual abuse and/or sexual harassment that occurred within a Department lockup;
- Any retaliation against detainees or Department employees who reported such an incident;
- Employee neglect or violation of responsibilities that may have contributed to an incident or retaliation; and

All allegations of sexual abuse, including third party and anonymous reports, shall be reported to a designated sexual abuse investigator who shall investigate the allegation pursuant to PRI-07A *Detainee Sexual Abuse and Sexual Harassment Investigations, Review and Data Collection*.

Staff shall not reveal any information related to a sexual assault to anyone other than to the extent necessary to make treatment and investigatory decisions.

Continued next page.

Reporting (Continued)

All verbal reports sexual abuse and/or sexual harassment shall be documented by the immediate supervisor who receives a report of sexual abuse or sexual harassment pursuant to this policy.

Department employees may privately report sexual abuse and/or sexual harassment by contacting the PREA Coordinator, filing a complaint with the Internal Affairs Section, or utilizing the PREA third party contact number posted on the Department's website and on the PREA informational brochure.

Methods of reporting shall include: in-person, phone, mail, email, fax or any means by which the staff person feels comfortable in reporting to supervisory level staff and/or the PREA Coordinator. Employees are expected to report any knowledge or suspicion of abuse. The methods of reporting are expected to vary based on the situation and the individual involved. Should there be any question as to the most appropriate method, the PREA Coordinator or Supervisor should be contacted.

Abuse Reports from Outside Facilities/ Agencies

A member or employee who receives an allegation that a detainee was sexually abused and/or sexually harassed while confined at a non-Department facility, shall notify through channels:

- The Colonel/Superintendent; and
- The Department PREA Coordinator.

Colonel/Superintendent shall:

- Notify the head of the facility or appropriate office of the agency where the alleged abuse occurred;
- Make notification, as soon as possible, but no later than seventy-two (72) hours after receiving the allegation; and
- Document such notification.

Training

All employees and members who may have contact with lockup detainees shall receive training regarding:

- The Department's zero-tolerance policy and detainees' right to be free from sexual abuse and sexual harassment;
- How to fulfill their responsibilities regarding prevention, detection, reporting, and response to sexual abuse and sexual harassment;
- The right of detainees and employees to be free from retaliation for reporting sexual abuse and sexual harassment;
- The dynamics of sexual abuse and sexual harassment in confinement;
- The common reactions of sexual abuse and sexual harassment victims;
- How to detect and respond to signs of threatened and actual sexual abuse;
- How to avoid inappropriate relationships with detainees;
- How to communicate effectively and professionally with detainees, including lesbian, gay, bisexual, transgender, intersex, or gender nonconforming detainees; and
- Compliance with relevant laws related to mandatory reporting of sexual abuse.

All members shall annually review the PREA Standards Bulletin posted to DocuShare.

Continued next page.

Training (Continued)

The Department shall provide each employee with refresher training annually to ensure that all employees know the agency's current sexual abuse and sexual harassment policies and procedures.

In years in which an employee does not receive refresher training, the Department shall provide refresher information on current sexual abuse and sexual harassment policies.

Every member or employee who may have contact with detainees shall acknowledge either in written or electronic format that he or she understands the Department's PREA policies and protocols and the PREA training he or she has received.

The Department shall maintain documentation confirming that employees, volunteers and contractors understand the training they have received.

PREA Coordinator

The Colonel/Superintendent shall:

- Designate a Detective Captain within Division of Investigative Services as the PREA Coordinator; and
- Ensure the PREA Coordinator has the authority to develop, implement, and oversee the Department's effort to comply with the PREA standards in all Department lockups.

The PREA Coordinator shall:

- Annually submit a status report of PREA compliance standards, investigative training requirements and reported/investigated incidents to the Colonel/Superintendent;
- Detail any corrective action required to ensure compliance with the PREA standard;
- Keep a current list of members who receive special training in sexual abuse investigations pursuant to Code of Federal Regulations (CFR) 28 § 115.34; and
- Take necessary action to ensure Department compliance with the PREA standards subject to the Colonel's approval.

Hiring and Promoting Practices

The Department shall not hire or promote anyone who may have contact with detainees and shall not enlist the services of any contractor who may have contact with detainees who:

- Has engaged in sexual abuse in a prison, jail, lockup, community confinement facility, juvenile facility, or other institution (as defined in 42 U.S.C. 1997);
- Has been convicted of engaging or attempting to engage in sexual activity in the community facilitated by force, overt or implied threats of force, or coercion, or if the victim did not consent or was unable to consent or refuse; or
- Has been civilly or administratively adjudicated to have engaged in the activity described in the paragraphs above.

The Department shall consider any incidents of sexual abuse and/or harassment in determining whether to hire or promote an employee, or to retain the services of any contractor, who may have contact with detainees.

Continued next page.

Hiring and Promoting Practices (Continued)

Before hiring new employees who may have contact with detainees, the Department shall: (a) perform a criminal background records check on all applicants; and (b) make its best efforts to contact all prior institutional employers for information on substantiated allegations of sexual abuse, or any resignation during a pending investigation of an allegation of sexual abuse.

The Department shall ask all applicants and employees who may have direct contact with detainees about previous misconduct described in this section, in: (a) written applications and/or interviews for hiring or promotion; and (b) interviews or written self-evaluations conducted as part of reviews of current employees.

All employees shall disclose any of the misconduct described in this section. Material omissions regarding such misconduct, or the provision of materially false information, shall be grounds for termination.

Any member or employee determined to have engaged in sexual abuse or sexual harassment of detainees as defined by policy shall be subject to discipline. The presumptive sanction for having engaged in prohibited behavior under this policy is termination.

Contractors and Volunteers

The Department shall also perform a criminal background records check before retaining the services of any contractor or volunteer who may have contact with detainees and document the same. *See Vendor Acknowledgment PREA form*.

In the event that a contractor or volunteer has engaged in sexual abuse or has been convicted or adjudicated of having engaged in sexual abuse, he or she shall have no access or contact with detainees in Department custody.

The Department shall ensure that all volunteers and contractors who enter Department facilities and who may have contact with detainees have been trained on their responsibilities under the Department's sexual abuse and sexual harassment prevention, detection, and response policies and procedures including the Department's zero-tolerance policy regarding prohibited behavior.

The level and type of training provided to volunteers and contractors shall be based on the services they provide and the level of contact they have with inmates, but all volunteers and contractors who have contact with inmates shall be notified of the Department's zero-tolerance policy regarding sexual abuse and sexual harassment and how to report such incidents. All volunteers and contractors who enter the Barracks and who may have contact with detainees shall sign an acknowledgement that he or she understands the Department's zero-tolerance policy and reporting requirements.

The Department shall maintain documentation confirming that volunteers and contractors understand the Department's PREA policy and information received.

Retaliation

The Department shall ensure that all detainees and staff who report sexual abuse or sexual harassment or cooperate with sexual abuse or sexual harassment investigations are protected from retaliation by other detainees or staff, and shall designate which staff members or departments are charged with monitoring retaliation.

A member or employee who has knowledge, suspicion, or information regarding an incident of retaliation against detainees or staff who reported such an incident and any staff neglect that may have contributed to such retaliation, shall immediately report such incident or retaliation to his or her immediate supervisor.

Supervisors who receive reports of retaliation shall employ multiple protection measures, which may include:

- Cell changes or transfers for detainee victims or abusers;
- Removal of alleged staff or detainee abusers from contact with victims;
- Providing emotional support services for detainees or staff who fear retaliation for reporting sexual abuse or sexual harassment or for cooperating with investigations; and/or
- Closely monitoring detainees or staff who fear retaliation.

Each Barracks Station Commander shall monitor all employee(s) who report sexual abuse or harassment to ensure that the employee(s) are not subject to retaliatory actions by other employees and shall document the same.

Upgrades to Facilities and Technologies

When designing or updating holding cells, the Department will consider the effect of the design upon the ability to protect prisoners from sexual contact.

When installing or updating video monitoring systems, the Department will consider how the technology may enhance the ability to protect prisoners from sexual contact.

References

Prison Rape Elimination Act (PREA)
Code of Federal Regulations (CFR) 28 § 115
U.S. Department of Justice's Office on Violence Against Women publication, *A National Protocol for Sexual Assault Medical Forensic Examinations, Adults/Adolescents*
TRN-01 Training Administration
PRI-07A Detainee Sexual Abuse or Sexual Harassment Investigations, Review and Data Collection
Department of State Police Bulletin on PREA Standards
Vendor Acknowledgement PREA Form

Promulgated By:

Department of State Police
General Order

Effective Date	Number
May 5, 2017	**PRI-07A**

Subject

Detainee Sexual Abuse and Sexual Harassment Investigations, Review, and Data Collection

Policy

As the investigative agency for alleged sexual crimes committed on adults and juveniles held in a confinement setting by either the Department of Correction or Department of Youth Services, the Department of State Police shall ensure full compliance with the standards found within federal laws and mandates regarding the *Prison Rape Elimination Act* (2003).

This policy shall be made available through the Department's website and upon request.

Response

The Department shall adhere to the following requirements in regards to detainee allegations of sexual abuse and/or sexual harassment:

- Investigate allegations of sexual abuse and/or sexual harassment from the Department of Correction or Department of Youth Services;
- Investigate allegations of sexual abuse and sexual harassment from within the Department of State Police;
- Investigate allegations of sexual abuse and sexual harassment alleged by a detainee while detained at another facility;
- Follow uniform evidence protocol that maximizes the potential for obtaining usable physical evidence;
- Development of an internal protocol appropriate for juveniles where applicable;
- Offer all victims access without financial cost to forensic medical examinations performed by a Sexual Assault Forensic Examiner or qualified medical practitioner;
- Attempt to make a victim advocate from a rape crisis center available to the detainee;
- Accompany the victim through the forensic medical examination process and interviews; and
- Take appropriate measures to prevent retaliation against individuals who report and/or cooperate with an investigation.

Special Training

Department Investigators shall receive special training in detainee sexual abuse and sexual harassment investigations according to Code of Federal Regulations (CFR) 28 § 115.34, to include:

- Techniques for interviewing sexually abused or sexually harassed victims;
- Proper use of Miranda and Garrity warnings;
- Sexual abuse evidence collection in confinement settings; and
- The criteria and evidence required to substantiate a case for administrative action or prosecution referral.

Subject	Number
Detainee Sexual Abuse and Sexual Harassment Investigations, Review, and Data Collection	**PRI-07A**

Investigations

Department investigators when conducting an investigation into allegations of detainee sexual assault and/or sexual harassment, shall:

- Gather and preserve direct and circumstantial evidence, including any available physical and DNA evidence and any available electronic monitoring data;
- Interview alleged victims, suspected perpetrators, and witnesses;
- Review prior complaints and reports of sexual abuse and/or sexual harassment involving the suspected perpetrator;
- Notify their Division Commander through channels of the possible outcome when the evidence appears to support criminal prosecution;
- Make relevant information regarding the status of the investigation available to the Department and/or requesting agency so that the detainee may be kept apprised of the investigation.

When there is probable cause to believe that a detainee or a Department employee had sexual contact with another detainee in a holding cell, the Department will make a criminal referral to the District Attorney's Office of jurisdiction or to the Attorney General's Office.

A criminal investigation will not be terminated because the alleged perpetrator separates from employment with the Department.

If an outside agency investigates sexual contact, the Department will cooperate with the investigators and remain informed about the progress of the investigation.

Note: See also Policy and Procedure *PRI-07 Detainee Sexual Abuse and Sexual Harassment* for internal allegations.

Subject	Number
Detainee Sexual Abuse and Sexual Harassment Investigations, Review, and Data Collection	**PRI-07A**

Status Reports

Department Investigators who have conducted an investigation of a detainee sexual abuse and sexual harassment shall:

- Make available to the requesting agency relevant information regarding the status of an investigation;
- Document that the detainee will be informed of the investigation status by the requesting agency; and
- Retain all written reports pertaining to the administrative or criminal investigation of alleged sexual abuse or sexual harassment in accordance with the Commonwealth's retention schedule or for as long as the alleged abuser is incarcerated or employed by the agency, plus five years, whichever is longer.

Sexual Abuse Incident Reviews

The PREA Coordinator in consultation with the Incident Review Team, which shall include the Station Commander, PREA Coordinator, and other pertinent individuals, shall conduct a sexual abuse incident review at the conclusion of every investigation into allegation of sexual abuse of a detainee in Department custody. Such review shall ordinarily occur within 30 days of the conclusion of the investigation. Such review will be conducted even when the allegation has not been substantiated, unless the allegation has been determined to be unfounded.

The review will:

- Include input from supervisors and investigators as necessary;
- Consider whether the allegation or investigation indicates a need to change policy or practice to better prevent, detect or respond to sexual contact;
- Consider whether the incident or allegation was motivated by bias or gang affiliation;
- Examine the area where the incident allegedly occurred to assess whether physical barriers in the area may enable abuse;
- Assess the adequacy of staffing levels in that area during different shifts; and
- Assess whether monitoring technology should be deployed or augmented to supplement supervision by staff.

The PREA coordinator shall submit a written report to the Colonel/Superintendent with findings and any recommendations for improvement.

The Department shall implement any recommendations for improvement or document its reasons for not doing so.

Subject	Number
Detainee Sexual Abuse and Sexual Harassment Investigations, Review, and Data Collection	**PRI-07A**

Data Collection and Review

The PREA coordinator shall annually collect accurate, uniform data for every allegation of sexual abuse from each Barracks.

The incident-based data collected shall include, at a minimum, the data necessary to answer all questions from the most recent version of the *Local Jail Jurisdiction Survey of Sexual Violence* or other instrument developed by the Department of Justice and designated lockups.

The Department shall annually review data collected and aggregated in order to assess and improve the effectiveness of its sexual abuse prevention, detection, response policies, and training, including: identifying problem areas; taking corrective action on an on-going basis; and preparing an annual report of its findings from its data review and any corrective actions for each lockup, as well as the agency as a whole.

The PREA coordinator's annual report shall include a comparison of the current year's data and corrective actions with those from prior years and provide an assessment of the agency's progress in addressing sexual abuse. Upon approval of the Colonel, said report shall be made publically available upon request subject to redaction if appropriate.

The Department shall securely retain all incident based and aggregate data collected in accordance with all applicable data security policies and procedures.

All data collected shall be retained at least 10 years after the date of initial collection, unless federal, state, or local law requires otherwise.

Upon request, the Department shall provide the Department of Justice data from the previous calendar.

References

Prison Rape Elimination Act (PREA)
Code of Federal Regulations (CFR) 28 § 115
TRN-01 Training Administration
PRI-07 Detainee Sexual Abuse and Sexual Harassment
Local Jail Jurisdiction Survey of Sexual Violence

Promulgated By: 

Department of State Police
General Order

Effective Date	Number
July 5, 2017	**PRI-08**

Subject

Gender Identity and Expression

Policy

The Department strives to ensure that everyone it serves is treated with dignity, respect, and professionalism. Department employees shall not engage in conduct that denigrates or shows hostility toward an individual because of their gender identity or gender expression.

Definitions

Gender Identity: An individual's internal, deeply held sense of self as being male, female, an alternative, or no gender. Gender identity is determined by an individual's self-identification and is different from an individual's sexual orientation.

Gender Expression: External manifestations of gender identity such as an individual's name, personal pronouns, clothing, haircut, voice, and/or body characteristics.

Transgender: An umbrella term for individuals whose gender identity and/or gender expression differs from what is typically associated with the sex they were identified as at birth.

Transgender Male: A person who transitions from female to male, meaning a person who was identified as female at birth, but identifies and lives as a man. A transgender man should be referred to as a man (i.e. he, him, his), regardless of medical history or the sex listed on identification documents.

Transgender Female: A person who transitions from male to female, meaning a person who was identified as male at birth, but identifies and lives as a woman. A transgender woman should be referred to as a woman (i.e. she, her), regardless of medical history or the sex listed on identification documents.

Intersex Individual: A person whose sexual or reproductive anatomy or chromosomal pattern does not seem to fit typical definitions of male or female.

Adopted/Chosen Name: Non-birth name that an individual may use in self-reference. This may or may not be the individual's legal name and may or may not differ from the name on the transgender individual's personal documents (i.e. driver's license, passport, etc.). Department employees should be aware that the use of an adopted/chosen name does not automatically equate to an attempt to hide one's legal identity, nor does it indicate that the individual is misrepresenting themselves.

Employee: A sworn member or civilian who works directly for the Department.

Subject	Number
Gender Identity and Expression	**PRI-08**

Addressing an Individual

An individual may ask to be addressed differently from what his/her official identification documentation states. Therefore, when addressing individuals, Department employees shall adhere to the following:

- When uncertain which pronouns are appropriate, respectfully ask the individual for clarification e.g., "How would you prefer to be referred to?";
- Address the individual by the name the individual chooses, regardless of whether or not the individual has obtained legal recognition of the chosen name;
- Use the titles and pronouns appropriate for the chosen name and/or gender expression (e.g., he/him for a transgender male, she/her for a transgender female, they/them for a person with another gender identity or whose gender identity is unknown, or as requested); and
- In all situations, make every effort to comply with the individual's requests in a non-judgmental, professional manner.

Official Documentation and Reports

An employee may observe that an individual's gender identity differs from the sex indicated on the individual's identification documents.

Department employees encountering an individual wishing to be addressed differently from what is listed on official documents shall:

- Use the name and sex found on the individual's official documents in Department reports, i.e. incident reports, citations, and forms;
- Also document the individual's adopted/chosen name within the Department's Records Management System; and
- Use pronouns and descriptors consistent with the individual's gender identity when writing reports.

Searches

Department members shall adhere to Massachusetts General Laws (MGL), Department Policy and Procedures, and constitutional provisions when conducting searches upon any individual.

When Department members encounter transgender individuals, members shall:

- Not perform a search or frisk for the sole purpose of determining an individual's gender;
- Ask the individual what their preference is regarding the sex of the officer(s) searching the individual;
- Whenever practicable have two (2) officers of the preferred sex perform the search; and
- Document within the incident report the circumstances for the search, including the individual's preference regarding the sex of the officer(s) performing the search.

When an immediate cursory search for weapons is necessary for safety, it may be conducted in the field by an officer of either sex.

Subject	Number
Gender Identity and Expression	**PRI-08**

Custody

If a transgender individual is being detained in a Department cell or vehicle, no other detainee(s) shall be housed in the same cell or placed or transported in the same vehicle.

Members transporting a transgender prisoner shall radio their Station/Unit Desk Officer and have a Daily Administrative Journal (DAJ) entry made of the:

- Location;
- Preliminary charges against the prisoner;
- Intended destination;
- Beginning odometer mileage, and upon arrival, the ending mileage; and
- Request for back-up, if necessary.

Transgender individuals may be held in Department custody pending bail, transportation to another facility, or court appearance as follows:

- When there are no other prisoners in the cell block in the station where the individual is being held in custody, the transgender individual shall be placed into a cell. No other prisoners shall be placed in that cell block until the transgender individual is released from custody.
- When other prisoners are being held in the cell block at a given station, the transgender individual shall be transported to the nearest station that has no prisoners in custody. The transgender prisoner shall be placed in a cell at that station. No other prisoners shall be placed in that cell block until the transgender individual is released from custody.
- Once the booking process is complete, under no circumstances shall a transgender prisoner be secured in a public area (booking room, etc.) in view of other prisoners and shall remain separated from other prisoners at all times.

Department members shall not seize or remove appearance-related items such as clothing and undergarments, wigs, prosthetics, or make-up if those items would not be confiscated from non-transgender individuals, provided those articles and/or items may not be used to escape or cause harm to the prisoner or others or conceal weapons, illegal items, or evidence.

References

ADM-18 *Anti-Harassment/Sexual Harassment and Discrimination*
PRI-07 *Detainee Sexual Abuse and Sexual Harassment*
Rules and Regulations Article 1.3 *Code of Ethics*
Rules and Regulations Article 5.0 *Rules of Conduct*
Executive Order 526 *Order Regarding Non-Discrimination, Diversity, Equal Opportunity, and Affirmative Action*

Promulgated By:

Department of State Police
General Order

Effective Date	Number
July 12, 2018	**PRI-09**

Subject

Juvenile Detention

Policy

The Department shall ensure compliance with Federal and Massachusetts law regarding the detention of children and juveniles.

When a juvenile is arrested or placed into custodial protection, to ensure proper legal treatment, the member and his or her supervisor shall immediately review the most current version of MGL c.119, § 67 and § 39H.

Juveniles

Juvenile: A child who has not yet attained his or her eighteenth (18) birthday.

Under Age 12	A juvenile who has not yet attained his or her twelfth (12) birthday cannot be charged with a crime.
Age 12 to Age 18	A summons is the *preferred* method for bringing all juveniles to court, unless there is reason to believe the juvenile will not appear upon a summons.
Arrest Warrant	An arrest warrant will issue if the court has reason to believe the juvenile will not appear upon a summons, or if the juvenile has been summoned and did not appear, or if the juvenile violated the terms and conditions of probation.

Status Offender

Status Offender: A juvenile who engages in an unlawful activity, which, if he or she were an adult, would be classified as non-criminal. Examples of juvenile status offenders are:

- Child placed into protective custody;
- Youth curfew violations (where applicable); or
- A "Child requiring assistance" from six (6) to eighteen (18) years of age per MGL c.119 § 39H who:
  1. Repeatedly runs away from home;
  2. Repeatedly fails to obey the lawful and reasonable commands of the child's parent, guardian or legal custodian;
  3. Repeatedly fails to obey the lawful and reasonable regulations of the child's school;
  4. Is habitually truant; or
  5. Is a sexually exploited child.

Subject	Number
Juvenile Detention	**PRI-09**

Delinquent Child

Delinquent Child: A child between 12 and 18 years of age who commits any offense against a law of the Commonwealth; **provided, however, that such offense shall not include:**

- A civil infraction;
- A violation of any municipal ordinance or town by-law; or
- A first offense of a misdemeanor for which the punishment is a fine, imprisonment in a jail or house of correction for not more than six (6) months or both such fine and imprisonment.

Non-Secure Detention

Any juvenile who has not yet attained his or her eighteenth (18) birthday, a status offender, or a juvenile in protective custody under MGL c. 111B, § 8, shall be held in accordance with the requirements specified for non-secure detention of status offenders. These requirements are:

1. The area where the juvenile is held is in an unlocked, multipurpose section, such as a report writing room or office;
2. The space is in no way designed for residential use;
3. The juvenile is held long enough to complete identification, investigation, and processing and then shall be released to a parent, guardian, legal custodian, other responsible adult, or transferred to an alternative juvenile facility or court;
4. The juvenile is under continuous visual supervision until released; and
5. At no time is the juvenile to be handcuffed to any stationary object.

Note: A status offender may be handcuffed, but not to a stationary object, and shall not be considered in "secure detention".

Juveniles under 14 years of age, status offenders, or juveniles in protective custody shall not be placed in a cell.

Secure Detention

Secure detention is defined as physically detained or confined in a room, set of rooms, or a cell that has the ability to lock an individual within. Secure detention can result from either being placed in such a room and/or from being physically secured to a stationary object such as a cuffing rail/bench.

Procedures for the Detention of Juveniles

Members shall adhere to the following when detaining juvenile(s):

- A juvenile may not be held in police custody for longer than six (6) hours.
- A juvenile in Department custody should only be held long enough for members to complete the identification and booking process. Once the identification and booking process is complete, the juvenile must be either: a) transported to the juvenile court, b) released to his/her parent/guardian/custodian, or c) transferred to the custody of the Overnight Arrest Program (after 1800hrs on weeknights and anytime on the weekends/holidays).
- A juvenile who has not yet attained his or her fourteenth (14) birthday shall not be placed in secured detention for any amount of time.
- No juvenile between fourteen (14) and eighteen (18) years of age shall be placed in a cell, unless the cell has been certified by the Department of Youth Services (DYS).
- A juvenile who is securely detained in Department custody must be separated by sight and sound from adults in custody.
- A juvenile placed in Protective Custody, for ALCOHOL, **CANNOT BE SECURELY DETAINED** for any amount of time.
- A juvenile placed in Protective Custody, for Controlled Substances/Toxic Vapors, **MUST be transported to an appropriate emergency medical treatment facility.**
- A juvenile placed in custody in accordance with Child Requiring Assistance (CRA) **CANNOT be brought back to the barracks.**

Juvenile Arrest – Delinquent Offense

When a juvenile is placed under arrest, the Troop Duty Officer, or designee, shall immediately notify at least one (1) of the child's parents, or, if there is no parent, the guardian or custodian with whom the child resides or the Department of Children and Families (DCF) if the child is in its custody.

If Arrest Occurs during Court Hours	Members must complete the booking process and then transport the juvenile to the Juvenile Court of jurisdiction.
If Arrest Occurs after Court Hours	There is no longer a statutory requirement for the police to contact a Juvenile Probation Officer, and as such, the Probation Department has ceased its on-call program. Therefore, the Troop Duty Officer, or designee, will make a determination whether to release the juvenile or to detain the juvenile.

Continued next page.

Juvenile Arrest – Delinquent Offense (Continued)

If Arrest Occurs after Court Hours (Continued)	Release: If a juvenile has been arrested without a warrant and the Troop Duty Officer, or designee, determines that the juvenile should be released, such release shall be done so upon the acceptance of the written promise from the parent, guardian, custodian or a representative of DCF who will ensure the juvenile's appearance in court. The Troop Duty Officer, or designee, will ensure that members utilize the SP 122 Written Promise form to obtain the required written promise. The released juvenile shall be advised that he or she must appear in the Juvenile Court of jurisdiction on the next predetermined recognizance date for that court. The Troop Duty Officer, or designee, should refer to the appropriate barracks' current list of Juvenile Court recognizance dates. The Troop Duty Officer, or designee, shall ensure that the appropriate Juvenile Court and recognizance date are noted on the SP 122 Written Promise Form. Detain: If a juvenile between fourteen (14) and eighteen (18) years of age has been *arrested on a warrant* or if the Troop Duty Officer, or designee, *requests in writing that such a juvenile be detained*, the Troop Duty Officer, or designee, shall contact the Bail Magistrate/Bail Commissioner. In accordance with MGL ch. 119, § 67, a juvenile age twelve (12) or thirteen (13) *who has been arrested without a warrant* is prevented from being admitted to bail and therefore must be released to a parent, guardian or, custodian or a representative of DCF.
Bail	The Bail Magistrate/Bail Commissioner will set bail and/or terms and conditions of release based on the juvenile's current charge(s), circumstances of the arrest, criminal history and/or as directed by the arrest warrant.

Juveniles in police custody must be held sight and sound separate from adult detainees.

A juvenile charged with delinquency offenses *shall not be held* in a police lockup or otherwise securely detained for any *longer than six (6) hours.* If the juvenile is placed in a cell, the cell must be a Department of Youth Services certified cell.

Continued next page.

Juvenile Arrest – Delinquent Offense (Continued)

The requirement not to release a defendant for six (6) hours when arrested for a violation of MGL ch. 209A or MGL ch. 265, § 13M (Domestic Assault or Domestic Assault and Battery) or § 15D (Strangulation or Suffocation), ***DOES NOT apply to juveniles.***

A juvenile in Department custody should be held only long enough for members to complete the identification and booking process. Once the identification and booking process is complete, the juvenile must be either: a) transported to the juvenile court, b) released to his/her parent/guardian/custodian, or c) transferred to the custody of the Overnight Arrest Program (after 1800hrs on weeknights and anytime on the weekends/holidays).

- The best practice is for the six (6) hour clock to start when the juvenile is placed in police custody and ends when custody is: a) transferred to the juvenile court, b) the juvenile is released to his/her parent/guardian/custodian or c) custody is transferred to the Overnight Arrest Program.

Juvenile Unable to Make Bail / Unable to be Released

When a juvenile has been charged with a delinquency or youthful offender offense and is unable to make bail or is unable to be released and court is closed, the Troop Duty Officer, or designee, must contact the Department of Youth Services (DYS) Central Referral Line at 617-474-8150 or 617-474-8179 to coordinate DYS placement (after 1800hrs on weeknights and anytime on weekends/holidays). The Troop Duty Officer, or designee, shall ensure that DYS is provided with information regarding the juvenile's arrest and is advised of the bail amount as it relates to the Bail Fee and Bail.

If a juvenile is being held on a Bail Fee only ($40.00 - Personal Recognizance), DYS has no authority to hold the juvenile in its custody. The Troop Duty Officer, or designee, shall inform the Bail Magistrate/Bail Commissioner of this and arrangements will be made to release the juvenile without imposing a Bail Fee.

- If the juvenile is in the custody of DCF, DCF shall be notified via the DCF Hotline to take custody of the juvenile.
- If a parent, guardian or custodian refuses to take custody of a juvenile who is otherwise eligible to be released, the Troop Duty Officer, or designee, shall file a 51A and notify DCF via the DCF Hotline for placement.

DYS will provide the Troop Duty Officer, or designee, with the location of the Overnight Arrest Program.

- If the juvenile is *suffering from any medical condition(s)*, (such as: under the influence drugs/alcohol, suicidal thoughts, pepper sprayed or tasered) he/she *must be medically cleared prior to placement.*
- The Troop Duty Officer, or designee, is responsible for obtaining any current medications for the juvenile.
- The Troop Duty Officer, or designee, must provide a copy of the Booking Sheet prior to placement.

Continued next page.

Juvenile Unable to Make Bail / Unable to be Released (Continued)

It is the Department's responsibility to transport the juvenile to the Overnight Arrest Program.

It is also the Department's responsibility to transport the juvenile from the Overnight Arrest Program to the Juvenile Court before 0900 hours.

Transportation of Juveniles

Juveniles may be:

- Transported in marked or unmarked vehicles.

Juveniles shall not be:

- Transported with adult prisoners; or
- Transported to court or any other institution in patrol wagons MGL c. 119, § 34.

Jenkins Hearing

If a juvenile is arrested without a warrant and held in custody (to include while being held at the Overnight Arrest Program), for more than twenty-four (24) hours, he or she is entitled to a *Jenkins Hearing* to determine whether or not there was probable cause to make the arrest and to continue to hold the juvenile.

- The bail magistrate/bail commissioner that set bail on the juvenile cannot be the same magistrate/commissioner who conducts the *Jenkins Hearing.*
- If the juvenile will be held over twenty-four (24) hours, in order to facilitate a *Jenkin's* determination of probable cause to continue to hold the juvenile, the Troop Duty Officer, or designee, must call a magistrate/commissioner.

Special Considerations

Members may have to take extra steps to ensure that juveniles understand their rights. This may include explaining or repeating the Miranda rights, or explaining Department procedures or juvenile court procedures to the juvenile. Refer to INV-05 Special Protections for Juveniles for procedures regarding the interrogation of juveniles.

Station Juvenile Officers

Station Commanders shall:

- Designate a station court officer as the Juvenile Officer;
- Ensure that Juvenile Officers attend specialized training, if required;
- Ensure that MGL c.119, § 67 and § 39H are followed; and
- Ensure that Juvenile Officers maintain a list of predetermined recognizance dates for the Juvenile Courts in their jurisdictions. This list must be continually updated and must be provided to Troop Duty Officers.

Subject	Number
Juvenile Detention	**PRI-09**

Filing

Station/Section Commanders shall maintain a separate, secure file with all of the identifying data of each juvenile arrest and any related reports.

Records involving criminal charges against juveniles shall be maintained separately from other records.

Administrative Journal Records

The Daily Administrative Journal (DAJ) shall:

- Contain all required information except the juvenile's name, address, date of birth (DOB), and any other identifying data; and
- Under the "name" section the word "JUVENILE" shall appear, followed by a sequential number starting with "#1" for the first juvenile arrested that year.

A separate record shall be maintained that links Juvenile Arrest Journal numbers and juvenile identifying information. This record shall not be released to the public and/or media.

The DAJ shall contain only the juvenile number and no other personal data.

Reporting Juvenile Detentions

Stations that have cells approved for juvenile use are administratively required by the Executive Office of Public Safety & Security (EOPSS) to submit a monthly lockup docket, as directed within CJIS Extranet.

EOPSS may contact a station that has arrested a status or juvenile offender, to ensure compliance with the applicable holding laws. EOPSS utilizes the information to monitor the Commonwealth's compliance with state law and the Federal Juvenile Justice and Delinquency Prevention Act of 1974 and 2002. All members shall assist EOPSS as requested.

References

MGL c.119, § 39
MGL c.119, § 51A
MGL c.119, § 54
MGL c.119, § 52
MGL c.119, § 67
Jenkins v. Chief Justice of the District Court, 416 Mass. 221 (1993)
INV-05 Special Protections For Juveniles
PRI-03 Prisoner Transportation
SP 122 Written Promise to Appear

Promulgated By:

Department of State Police
General Order

Policy Date:	Number:
July 12, 2018	**PRI-10**

Subject:

Protective Custody

Policy

It is the policy of the Massachusetts State Police to comply with the requirements of Massachusetts General Law Chapter 111B and Massachusetts General Law Chapter 111E when taking an incapacitated person into protective custody.

Definitions

Incapacitated: The condition of a person who, by reason of the consumption of alcohol and/or a controlled substance, toxic vapor, or other substance other than alcohol, is:

- Unconscious;
- In need of medical attention;
- Likely to suffer or cause physical harm or damage property; or
- Disorderly.

To place someone into protective custody, an officer needs probable cause to believe that the person is incapacitated.

Intoxication alone is not sufficient to warrant a finding of incapacitation.

Assisting Officer: Member placing a person into protective custody.

Facility: Any public or private place, or portion thereof, providing services especially designed for the detoxification of intoxicated persons.

Juvenile: A child who has not yet attained his or her eighteenth (18) birthday.

Protective Custody

Pursuant to M.G.L. c.111B, § 8: Any person who is incapacitated due to consumption of alcohol may be assisted by a police officer with or without the person's consent to the person's residence, to a facility, or to a police station.

Pursuant to M.G.L. c.111E, § 9A: Any person who is incapacitated due to consumption of substance(s) other than alcohol may be placed into protective custody by a police officer without the person's consent for the purpose of immediately transporting the person to an acute care hospital or satellite emergency facility or otherwise immediately obtaining appropriate emergency medical treatment.

Subject	Number
Protective Custody	**PRI-10**

Procedure for Taking Person into Protective Custody

	111B § 8 (Alcohol)	111E § 9A (Substance other than Alcohol)
Determination of Incapacitation is a Two-Step Process	**Step One: Assessment of Incapacitation** A person who, by reason of the consumption of alcohol, is: (1) unconscious, (2) in need of medical attention, (3) likely to suffer or cause physical harm or damage property, or (4) disorderly is deemed incapacitated. **Step Two: Assessment of Intoxication** *Right to a Breathalyzer Test* (BT) - Any person assisted by a police officer to a police station shall have the right, and be informed in writing of said right, to request and be administered a breathalyzer test. *Presumption of Intoxication* - Any person who has a BT of (.10) or above is presumed intoxicated. *Sobriety Testing* - If any person has a BT of .06, .07, .08 or .09, police are authorized to administer sobriety testing in order to determine whether to release or hold the person. *Release Forthwith* – Unless there are pending charges or a warrant, any person who has a BT (.05) or less shall be released from custody forthwith *However*, if a minor registers *any* BT reading, the minor must be released to a parent, guardian, or responsible adult.	**Step One: Assessment of Incapacitation** A person who, by reason of the consumption of substance other than alcohol, is: (1) unconscious, (2) in need of medical attention, (3) likely to suffer or cause physical harm or damage property, or (4) disorderly is deemed incapacitated. **Step Two: Assessment of Intoxication** A police officer may ask a person to consent to reasonable tests of coordination, coherency of speech, and breath to determine if the person is incapacitated. A police officer may place the person into protective custody when such tests or other information or observations indicate that the person is incapacitated.

Continued on next page

Subject	Number
Protective Custody	**PRI-10**

Procedure (Continued)

	111B § 8 (Alcohol)	**111E § 9A (Substance other than Alcohol)**
Role of Police Officer when taking a person into Protective Custody:	A police officer shall assist an incapacitated person by bringing him or her to: • person's residence; • police station (will have to notify facility); or • a facility (as defined above) *NOTE:* If person is brought to police station, person has the right to: • request and be administered a breathalyzer test; and • make a phone call.	A police officer shall assist an incapacitated person by: • immediately transporting the person to an acute care hospital or satellite facility; or • obtaining appropriate immediate emergency medical treatment (EMT) for the person.
Notification of Facility	If any incapacitated person is assisted to a police station, the officer in charge, or designee, shall notify forthwith the nearest facility that the person is being held in protective custody. If suitable treatment services are available at a facility, the department shall thereupon arrange for the transportation of the person to the facility. The officer in charge, or designee, shall ensure that a Daily Administrative Journal (DAJ) entry indicates: • the name of the facility notified; and • if transportation was arranged.	N/A

Continued on next page

Subject	Number
Protective Custody	**PRI-10**

Procedure (Continued)

	111B § 8 (Alcohol)	111E § 9A (Substance other than Alcohol)
Minors	The parent, guardian or legal custodian of any juvenile to be held in protective custody at a police station, shall be notified forthwith upon his/her arrival at said station or as soon as possible thereafter. Any juvenile who is held in protective custody at a police station shall, upon request of his or her parent, guardian or legal custodian, be released to the custody of said parent, guardian or legal custodian. A juvenile placed in protective custody, for alcohol, cannot be securely detained for any amount of time. Members shall ensure that detention of juveniles shall conform to General Order PRI-09 Juvenile Detention.	The parent, guardian or legal custodian of any juvenile placed into protective custody shall be notified as soon as practicable. A juvenile placed in protective custody, for controlled substances/toxic vapors, must be transported to an appropriate emergency medical treatment facility.
Time Restraints	**No adult shall be held more than 12 hours** - No person assisted to a police station shall be held in protective custody against a person's will; provided, however, that if suitable treatment at a facility is not available, an incapacitated person may be held in protective custody at a police station until a person is no longer incapacitated or for a period of no longer than twelve hours, whichever is shorter.	A person cannot be held in protective custody beyond the time required to complete the transport of the individual to an acute care hospital or satellite emergency facility or to obtain immediate emergency medical treatment. Legislation does not provide a time frame for how long transport would take to be completed or medical treatment sought.
Use of Force	Reasonable force may be used to take a person into protective custody.	
Search and Inventory Items	Officers may search the person and immediate surroundings for weapons. Any items seized will be inventoried and returned if lawfully possessed.	

Continued on next page

Subject	Number
Protective Custody	**PRI-10**

Procedure (Continued)

	111B § 8 (Alcohol)	111E § 9A (Substance other than Alcohol)
Documentation	An entry of custody in the report narrative shall be made indicating: o the date, time, place of custody; o the name of the assisting officer; o the name of the officer in charge; o whether the person held in custody **exercised his or her right to make a phone call**; o whether the person held in custody **exercised his or her right to take a breathalyzer test**, **and** the **results of the breathalyzer test if taken**; and o the name of the facility notified and if transportation was arranged. An SP 850 Protective Custody form demonstrating subject was read and understood these rights must be completed.	An entry of custody in the report narrative shall be made indicating: o the date, time, place of custody; o the name of the assisting officer; o the name of the officer in charge; and o the name of the facility to which the person was transported.
Status of Protective Custody	Not an arrest	
Additional Considerations	Pursuant to General Order TRF-14 Operating Under the Influence -Alcohol, if a member places into protective custody a subject who has been bailed after having been arrested for OUI-Alcohol, the member shall process the subject according to MGL c. 111B and this General Order.	If a subject has been revived using naloxone (“Narcan”) and has regained consciousness, it may still be appropriate to place the subject into protective custody and transport that subject for medical attention, if the training and experience of the officer indicate that further medical attention is appropriate.

Subject	Number
Protective Custody	**PRI-10**

Non-Secure Detention

A juvenile in protective custody under MGL c. 111B, §.8, shall be held in accordance to the requirements specified for non-secure detention. These requirements are:

1. The area where the juvenile is held is in an unlocked, multipurpose section, such as a report writing room or office;
2. The space is in no way designed for residential use;
3. The juvenile is held long enough to complete identification and processing, and then shall be released to a parent, guardian, legal custodian, other responsible adult;
4. The juvenile is under continuous visual supervision until released; and
5. At no time is the juvenile to be handcuffed to any stationary object.

Note: **A juvenile in protective custody shall not be placed in a cell.** A juvenile in protective custody may be handcuffed, but not to a stationary object, and shall not be considered in "secure detention".

References

M.G.L. c.111B
M.G.L. c.111B, § 3
M.G.L. c.111B, § 8;
M.G.L. c.111B, § 10;
M.G.L. c.111E
M.G.L. c.111E, § 9A
Alfano v. Lynch, 847 F.3d 71 (CA1 2017)
Comm. v. Tomes, 400 Mass. 23 (1987)
Comm. v. O'Brien, 434 Mass. 615 (2001)
Comm. v. O'Connor, 406 Mass. 112 (1989)
PRI-09 Juvenile Detention
TRF-14 Operating Under the Influence of Alcohol
SP 850 Protective Custody

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 28, 2019	**SOC-01**

Subject

Hazardous Materials

Policy

Department personnel, unless properly equipped and trained, shall not be deployed into areas that have been contaminated, or face an immediate and substantial threat of contamination with a hazardous material.

Definition

Hazardous Materials: Chemicals, biological agents or organisms, or radiological substances that are damaging to health or property.

Responding Members

If…	Then members shall…
There is no known or potential presence of a hazardous material on scene; or There is a hazardous material on scene, but it is properly secured and poses no threat of release:	• Respond with due caution; and • Ensure that the Emergency Response Guidebook is accessible.
It is possible to ascertain from a safe distance the identity of a substance or cargo via use of placards or other identification:	• Relay information to the Desk Officer; and • Consult the Emergency Response Guidebook.
There is an immediate and substantial threat of the release of a hazardous material on scene:	• Consult the Emergency Response Guidebook for guidance as to maintaining a safe distance from the area of possible contamination.
Dangerous conditions are observed:	• Take immediate action to ensure their own safety, the safety of other responding officers or personnel, and the safety of the general public; and • Communicate the nature of the threat to the Desk Officer.

Desk Officer

Upon receiving a report of an incident that may involve a hazardous material, the Desk Officer shall make every reasonable effort to obtain available information from the scene.

The following information shall be obtained and relayed to responding members and to the Troop Duty Officer:

- The type of container/vehicle;
- Whether the container/vehicle is leaking;
- Department of Transportation (DOT) placards, labels or numbers;
- Carrier name and any information found in shipping papers;
- Local area road and weather conditions; and
- Other responding resources and/or agencies.

Upon receiving a report of an incident that may involve a hazardous material, the Desk Officer shall notify:

- Assigned patrol and other members in the area;
- Troop Duty Officer;
- Local police department;
- Local fire department; and
- Department of Fire Services-Regional Hazardous Materials Team (877) 385-0822.

Desk Officer-Actual Release or Threat of Release

On receiving a report of an incident involving the actual release or threat of release of a hazardous material, the Desk Officer shall:

- Immediately notify the Troop Duty Officer;
- Notify available resources to include: local fire department, Department of Fire Services-Regional Hazardous Materials Team, Commercial Vehicle Enforcement Section, for initial emergency hazmat actions;
- Obtain expertise from the Emergency Response Guidebook regarding:
    - Scope of contamination; and
    - Minimum safe evacuation zone for unprotected individuals prior to deploying Department personnel; and
- Notify the Massachusetts Department of Environmental Protection at (888) 304-1133 and provide the following information:
    - Location;
    - Type and quantity of material released;
    - Suspected impacts if known (catch basin, wetlands);
    - Name, address, and phone number of carrier (if known);
    - Special conditions which responders should be aware of to facilitate the safe mitigation of the release; and
    - Any other information which may be helpful.

Troop Duty Officer

The Troop Duty Officer shall:

- Dispatch a supervisor to the scene;
- Notify the Troop Commander;
- Notify GHQ Communications at (508) 820-2121; and
- When applicable, notify the Commercial Vehicle Enforcement Section at (978) 369-1004, or if after hours, GHQ Communications at (508) 820-2121.

Patrol Supervisor

Supervisors shall establish an outer perimeter, referencing the Emergency Response Guidebook and available expertise to determine an appropriate distance from the incident.

Supervisors shall:

- Ensure that Department personnel are not deployed contrary to the provisions of this policy;
- Establish a command post upwind and uphill (if possible) and at a sufficient distance from the hazard; and
- Follow incident command procedures.

GHQ Communications

If radioactive material is involved, the GHQ Communications Section shall notify the Department of Public Health Director of Radiation Control Program (617) 242-3055.

If no determination has been made as to who spilled the hazardous material, the GHQ Communications Section OIC shall notify the National Response Center (NRC) at (800) 424-8802.

Hazardous Materials Team

The head of the local fire department or designee shall activate the Department of Fire Services-Regional Hazardous Materials Team.

Available Official Expertise

The following are resources for information on hazardous materials:

- State expertise:
    - Department of Fire Services-Regional Hazardous Materials Team at (877) 385-0822;
    - Massachusetts Department of Environmental Protection at (888) 304-1133;
    - Department of Public Health Director of Radiation Control Program (617) 242-3055;
    - Bomb Squad; and
    - Commercial Vehicle Enforcement Section.

Continued next page.

Subject	Number
Hazardous Materials	**SOC-01**

Available Official Expertise (Continued)

- Federal expertise:
  - CHEMTREC at (800) 424-9300; and
  - The National Response Center at (800) 424-8802 provides emergency chemical/biological assistance twenty-four (24) hours a day.

- Additional resources:
  - Querying MQ in the task field of the CJIS computer, and entering the placard information; and
  - Consulting the Emergency Response Guidebook.

References

29 CFR 1910.120
40 CFR 311.1
527 CMR Section 1.03 (8)
U.S. Department of Transportation Emergency Response Guidebook
Criminal Justice Information System (CJIS)

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 28, 2019	**SOC-02**

Subject

Bomb Threats/Explosive Incidents

Purpose

To establish and define the role of the Bomb Squad within the Division of Investigative Services- Fire and Explosion Investigation Unit (FEIU), and to establish guidelines for utilization and activation of their members.

Policy

The Bomb Squad is tasked with rendering safe any explosive (Improvised Explosive Device (IED), military or commercial explosives) within the Commonwealth of Massachusetts. The FEIU Commander or designee is responsible for determining a response to any bomb threat.

The Department shall:

- Maintain and support a Bomb Squad comprised of members with specialized training, expertise, and equipment to include explosive detection K-9s.

The Bomb Squad shall:

- When assigned, assist officers from the Department and from other local, state, federal and military agencies to deal with potential life threatening explosive related incidents, chemical, biological, radiological and nuclear (CBRN) incidents as well as clandestine drug lab activity;
- Train first responders in explosives and IED recognition; and
- Develop, under the direction of the Section Commander, a unit specific Standard Operating Procedure (SOP) which shall be maintained and updated as necessary.

Response Guidelines

Since the validity of a bomb threat cannot be determined initially, the decision to evacuate or to re-occupy the threatened premises is the responsibility of the owner or manager of the premises or the head of the fire department or designee.

Department members shall not order an evacuation based only on a threat. If advice is sought from the Department, the recommendation should be to follow the Massachusetts Bomb Threat Response Guidance.

If a suspected explosive device or suspicious package has been located or if there is a perceived threat, the head of the fire department or designee has the authority to order an evacuation under MGL c.148.

Subject	Number
Bomb Threats/Explosive Incidents	**SOC-02**

Utilization of Bomb Squad

Bomb Squad Team members are available twenty-four (24) hours a day for:

- Rendering safe any explosive (IED, military or commercial explosives);
- Security sweeps for high profile events and visiting dignitaries;
- Response and technical assistance/advice for bomb threats;
- Weapons searches with Explosive K-9s;
- Homeland Security assignments;
- Retrieval and remediation of energetic materials to include ammunition, fireworks, gun powder, etc.; and
- Other special events/incidents as assigned.

Emergency Activation Protocol

Requests for the Bomb Squad shall be made to the Troop Duty Officer and shall include:

- The name, rank, and agency name of the requesting officer;
- The name of the primary point of contact and a direct call-back number;
- The nature of the request; and
- The exact location of the incident and any designated staging areas.

The Troop Duty Officer shall make appropriate Daily Administrative Journal entries.

Activation/ Contact

Type of Request	Contact
Emergency	• Troop Duty Office of jurisdiction.
Non-emergency	• During business hours contact the FEIU at 978-567-3310. • After business hours contact the Troop Duty Office of jurisdiction.

Authority

Any officer who encounters or seizes any bomb or other high explosive is required under MGL Chapter 266, Section 102D(a) to make immediate notification to the State Fire Marshal. Bomb Squad members shall assume complete control and authority of any explosives render-safe procedure under Incident Command System (ICS) protocols.

While at an active scene, command and control of the scene shall be exercised only by:

- Bomb Squad Commander or designee;
- FEIU Commander or designee;
- Unified Commanders on scene (ICS);
- Division of Investigative Services Commander or designee; or
- Superintendent/Deputy Superintendent.

Subject	Number
Bomb Threats/Explosive Incidents	**SOC-02**

Response Protocols

All Department members shall take appropriate measures to ensure the safety of people and property while awaiting the arrival of the Bomb Squad.

The first on-scene or investigating member shall assess the situation and determine the need for additional resources including, but not limited to:

- Local Police/Fire Department(s) as well as additional Department resources to include: Crime Scene Services, State Police Detective Unit of jurisdiction, Commonwealth Fusion Center;
- Emergency Medical Services (EMS); and
- Traffic control.

To reduce the risk of detonation, members responding to an explosives threat or incident shall NOT:

- TOUCH, MOVE or DISTURB any suspicious objects, items or packages;
- Allow anyone within three-hundred (300) feet of a suspicious device;
- Allow anyone to be in the path of possible shrapnel or flying glass;
- Utilize electronic communication devices within close proximity to the unattended/suspected item; or
- Direct flashlight beams onto a possible device or use a camera flash (in order to prevent activation by photoelectric cell).

Never rule out the possibility of a secondary or tertiary device.

Responding members shall remain on the scene until properly relieved.

Evidence Considerations

Evidence and materials collection shall be coordinated by FEIU members. Evidence custody shall remain with the lead State Police case officer.

After Action Reporting

Following the completion of any critical incident, Bomb Squad members may be debriefed.

The Bomb Squad Commander or designee is responsible for the completion of any after action reports or Bomb Squad reporting as applicable. After Action Reports shall be forwarded to the Division of Investigative Services Commander for review.

References

Massachusetts Bomb Threat Response Guidance
MGL Chapter 266, Section 102D(a)
MGL c.148

Promulgated By:

Department of State Police
General Order

Policy Date:	Number:
March 25, 2020	**SOC-03**

Subject:

Emergency Planning

Purpose

To maintain and ensure the Department's compliance with Homeland Security Presidential Directive 8 (HSPD-8) with regards to emergency planning.

Policy

The Department shall develop and implement an emergency operational response strategy to address potential public safety threat(s) or the actual occurrence(s) as identified in HSPD-8.

General Considerations

The Department must plan for foreseeable emergencies.
Certain incidents require preplanning by Troop/Section Commanders within specific operational areas. Examples of these include:

(1) A general emergency that may result from a natural or man-made disaster, including civil disorder, acts of terrorism and / or other unusual occurrences.

(2) Disasters including floods, hurricanes, earthquakes, explosions, and tornadoes.

(3) Civil disorders including rioting and other acts of violence.

(4) Planning for special operations that require general emergency planning concepts.

(5) Plans for application to site and situation specific circumstances when time allows, such as hostage or disturbances at correctional facilities.

Plans may be general initially and then become specific. In some circumstances, such as localized weather emergencies or dignitary protection details, certain information may not yet be known, but as much general information as possible should be preplanned with specifics inserted as the emergency occurs; emerging data or circumstances can be addressed as soon as they develop or can be predicted. Target areas and populations should be identified with equipment, personnel needs, the location of staging areas and emergency shelter locations identified beforehand.

Planning for emergency operations promotes efficiency. Preplanning allows for immediate and decisive action that can minimize loss of life, reduce property damage and permit involved authorities to fulfill their responsibilities. Other efficiencies include:

- Emergency equipment can be acquired and readied for deployment;
- Personnel requirements can be more accurately predicted;
- Coordination procedures can be devised and tested;
- Different strategies and tactical options can be assessed;
- Contingency responses can be developed; and
- Durable intelligence information can be assessed before the emergency occurs.

Subject	Number
Emergency Planning	**SOC-03**

General Plan Provisions

Emergency Plans should include the following provisions, as necessary:

1. Communications;
2. Situation Maps;
3. Field Command Posts;
4. Chain of Command (to include other agencies);
5. Casualty information;
6. Community Relations;
7. Public Information;
8. Rumor Control;
9. Other Agency Support & Liaison;
10. Military Support;
11. Martial Law;
12. Public Facility Security;
13. Transportation;
14. De-Mobilization Procedures;
15. Court & Prosecutorial Liaison;
16. Legal Authority;
17. Post Occurrence (Aftermath) Duties; and
18. After Action Incident Reports.

Responsibilities

Position	Duties
Colonel/ Superintendent	Shall: • Designate a Commissioned Officer as the Emergency Planning Officer; • Review and approve Emergency Operation Plans (EOPs) and Incident Action Plans (IAPs) submitted by the Emergency Planning Officer; and • Ensure that all EOPs written after October 2005 are National Incident Management System (NIMS) compliant.
Emergency Planning Officer (EPO)	Shall: • Maintain all Department emergency response plans and standard operating procedures (SOPs) devised for nuclear facilities, prisons, natural or man-made disasters, and similar circumstances; and shall also retain copies of Troop emergency response plans devised for DOC facilities; • Study, draft and maintain appropriate contingency plans for foreseeable circumstances or events for which a Department response may be required; • Prepare EOPs and IAPs and submit them to the Colonel/Superintendent; • Coordinate the creation of EOPs and IAPs with Division Emergency Planning Coordinators; • Annually review and update the EOPs and IAPs; • Ensure that all EOPs written after October 2005 are NIMS compliant;

Continued on next page

Responsibilities (continued)

Emergency Planning Officer (EPO) (Continued)	• Coordinate Department contingency planning and liaison with the Massachusetts Emergency Management Agency and the Military Division of the Commonwealth; • Ensure plans for a Department response to terrorism and civil disorder are created and maintained; • Review Department emergency response plans at least annually and report the results of this review in a written report to the Division Commander of Homeland Security and Preparedness; and • Ensure the Department maintains a minimum of a 60 day supply of: Personal Protective Equipment (PPE), decontamination and cleaning products, and individual hand sanitizers, unless otherwise directed by the Colonel.
Division Commanders	Shall: • Designate a Commissioned Officer as the Division Emergency Planning Coordinator; • Evaluate EOPs and IAPs through simulation exercises prepared by the Emergency Planning Officer; • Report deficiencies in EOPs and IAPs to the Emergency Planning Officer; and • Ensure that all EOPs written after October 2005 are NIMS compliant.

Troop/Section Commanders	Shall:
	• Designate a Commissioned or Non-Commissioned officer as the Troop/Section Emergency Planning Coordinator;
	• Evaluate EOPs and IAPs through simulation exercises prepared by the Emergency Planning Officer;
	• Report deficiencies through channels in EOPs and IAPs to the Emergency Planning Officer; and
	• Each Troop Commander shall develop, at a minimum, the framework of a plan to implement an initial response for the following types of incidents:
	  ◦ Natural or man-made disaster;
	  ◦ Civil disturbances and other unusual occurrences;
	  ◦ Hostage situations and barricaded persons;
	  ◦ VIP protection details; and
	  ◦ Other special events.

Troop/Section Emergency Planning Coordinator	Shall: • Assist the Division Emergency Planning Coordinator with the establishment of EOPs and IAPs; • Prepare and annually update, the Troop/Station/Section/Unit Emergency Planning Manual, EOPs and IAPs; and • Act as the liaison with the Division Emergency Planning Coordinator.

Subject	Number
Emergency Planning	**SOC-03**

Emergency Planning Manual

The Department shall maintain and annually update an Emergency Planning Manual for the purpose of responding to and controlling hazardous situations through the prudent use of Departmental and external resources.

The Emergency Planning Manual shall be located at every State Police facility. It shall be updated annually, or as required.

The Manual shall include all current EOPs, IAPs, operational guidelines, on site operational instructions, personnel and equipment resource inventories and other necessary information, including but not limited to:

- Personnel and skills;
- State Police property and buildings;
- Supplies (food, fuel, clothing);
- Vehicles;
- Arrest/confinement procedures;
- Topographical maps;
- Support equipment;
- Incident Command Posts;
- Field Command Posts;
- Communications;
- Miscellaneous Equipment (generators, boats, etc.);
- Fleet vehicles;
- After action reporting;
- ICS Form 205;
- ICS Form 205A-OS;
- ICS Form 206; and
- Identified Staging Areas.

Drafting Emergency Plans

When drafting an emergency response plan or SOP:

1. Describe all adverse elements.
2. Use available intelligence summaries (Fusion Center); and
3. Involve partner agencies with planning or operations, including but not limited to:

Local police departments;
Local fire departments;
Massachusetts Emergency Management Agency (MEMA);
Military Division of the Commonwealth;
MassDOT;
Massport;
Department of Corrections (DOC);
Courts;
Massachusetts Water Resources Authority(MWRA);
Department of Conservation and Recreation (DCR);
Mutual aid states (NESPAC);
Alcohol, Tobacco, and Firearms (ATF);
U.S. Secret Service;
Homeland Security;
Federal Bureau of Investigation (FBI);
National Transportation Safety Board (NTSB);
Federal Aeronautics Administration (FAA); and
U.S. Department of Defense.

Continued on next page

Drafting Emergency Plans (continued)

A plan should begin with a general assumption that an emergency will develop within the Commonwealth and:

- Normal procedures will not adequately protect life or property or preserve order; and
    - Will be beyond the capabilities of local authorities and shall require Department assistance; or
    - Will be beyond the capabilities of local authorities and the Department and may require National Guard or federal assistance to protect life and property and maintain order;
- That a national emergency may require the full resources of the Department to conduct emergency operations; and
- Immediate and decisive action is required to minimize loss of life, reduce property damage and permit involved authorities to fulfill their responsibilities.
    - Emergency equipment can be acquired and readied for deployment;
    - Personnel requirements can be more accurately predicted;
    - Intra-Department and interagency coordination procedures can be devised and tested;
    - Different strategies and tactical options can be assessed;
    - Contingency responses can be developed; and
    - Durable intelligence information can be assessed before the emergency occurs.

Planning Exercises

The expanding scope and sophistication of emergency operations, along with increased possibilities of acts of terrorism, require agency personnel to quickly act to stabilize and control emergency situations. Proactive emergency planning exercises for these circumstances shall be conducted as follows:

1. Documented annual rehearsals and training exercises regarding emergency incidents are essential for all agency personnel to be fully prepared for actual occurrences and special operations.
2. Training exercises may involve mock exercises, actual exercises, tabletop exercises, in-service training and/or Troop/Section/Unit training.
3. These rehearsals will be used to evaluate the effectiveness, efficiency and applicability of emergency plans in different situations and will include the involvement of those agencies expected to participate in the actual incident.
4. The Division Commander, designated as lead by the Colonel/Superintendent, will determine the extent, scope, and format for the exercise.
5. In the event of an actual implementation of an Emergency Plan due to a natural or man-made disaster incident, the actual implementation of the plan will replace any planned exercise.

Continued on next page

Subject	Number
Emergency Planning	**SOC-03**

Planning Exercises (continued)

6. The After Action Incident Report required for all natural or man-made disasters will serve as the critique of the Emergency Plan.
7. A documented analysis and evaluation of any Incident Command System activation incidents, as well as all intra-agency training & rehearsals, will be prepared at least every three years by the Division Commander of Homeland Security and Preparedness or designee.

Annual Training

Troop/Section Commanders shall coordinate annual emergency operations/incident command training exercises. This exercise may be limited to Troop/Section drill, or may include outside agencies such as local police/fire departments, EMS teams, state level response teams, media, non-profit agencies and other entities related to the exercise. When conducted in conjunction with other agencies, the exercise may consist of a tabletop exercise, drill, emergency operations center simulation, or functional exercise involving actual response scenarios.

Troop/Section Commanders shall submit a summary of incident command training exercises conducted to the Emergency Planning Officer no later than October 1st of each year. Upon review by the Division Commander of Homeland Security and Preparedness, the summaries shall be forwarded to the Office of the Superintendent.

The Office of the Division Commander of Homeland Security and Preparedness shall maintain a file of all incident command exercises conducted, and may recommend future training or exercises based on prior training or identified need.

Emergency Plan Availability

Any commander may request an existing emergency plan from the Emergency Planning Officer and/or from a Section/Troop headquarters.

Emergency plans containing confidential or sensitive information shall be securely maintained.

References

ICS Form 205 – Incident Radio Communications Plan
ICS Form 205A-OS – Communications List
ICS Form 206 – Medical Plan
MPAC: 46.1.1, 46.1.2, 46.1.9, 46.2.7

Promulgated By:

Col. Craig S. Mu

Department of State Police
General Order

Policy Date:	Number:
March 25, 2020	**SOC-03A**

Subject:

Emergency Operations Center (EOC)

Purpose

To provide guidance to personnel regarding the activation and operation of the Department's Emergency Operations Center (EOC).

Policy

The Department realizes the necessity of an effective response to public safety emergencies as a result of severe weather, terrorist activity, violent protest, natural and/or man-made disasters, through the prudent use of available resources.

State Police Emergency Operations Center

The Superintendent/Deputy Superintendent shall activate the EOC when deemed necessary. The EOC shall:

- Coordinate the deployment of Departmental resources in response to an emergency or incident;
- Coordinate the deployment of responding officers to an incident or an incident staging area;
- Direct the security level of response to a potential/actual threat; and
- Operate in conformance with established EOC Guidelines.

State of Emergency

Upon the declaration of a "State of Emergency" by the Governor, the Superintendent/Deputy Superintendent has the authority (within prescribed limits) to commit resources of the Department, or request resources from outside the Department, as deemed necessary, to mitigate the effects of the emergency and to minimize the disruption to public safety.

The Superintendent/Deputy Superintendent shall activate the EOC and shall establish the appropriate security level when necessary.

Upon the declaration of a "State of Emergency" after normal business hours the Watch Center Unit shall immediately notify:

- Superintendent/Deputy Superintendent;
- The EOC on-call personnel;
- Division Commanders; and
- Division of Homeland Security and Preparedness- Emergency Management Unit.

Security Level Guidelines

Upon authorization by the Superintendent/Deputy Superintendent, the EOC shall establish the appropriate security level when necessary. The EOC Director may add, delete, or modify the listed security level procedures in accordance with prevailing circumstances. Security levels and the corresponding response(s) within each level shall be determined by the specific credible information available at that time.

Subject	Number
Emergency Operations Center (EOC)	**SOC-03A**

Security Level Procedures

Level	Tasks
I	• ID Check enforced at State Police facilities and identified sites; • Note and report suspicious circumstances, packages and activities; • Ensure building integrity and security; and • Exercise heightened caution when responding to calls for service.
II	*Includes Tasks Assigned At Level I and:* • Implement physical security measures and post security personnel as appropriate; • Identify all vehicles within operational and support areas; • Conduct cursory checks for suspicious items, persons and vehicles as necessary; • Verify and inspect all inbound deliveries and services; • Check delivery and service persons for authenticity with their respective companies; • Exercise extreme caution when responding to suspicious calls for service; • Monitor potential target areas; • All personnel shall wear ID cards in State Police facilities unless in duty uniform; and • Escort all visitors (non-MSP) in State Police facilities.
III	*Includes Tasks Assigned At Levels I , II, and:* • Erect barriers and obstacles (e.g. Jersey Barriers) to control traffic; • Suspend all non-essential contract work or deliveries; • Conduct detailed searches of all operational areas and vehicles; and • Limit or restrict parking around sensitive areas and buildings.
IV	*Includes Tasks Assigned At All Levels and:* • Verify the identities of all personnel and need for access; • Deny access to all personnel not associated with local, state or federal agencies; and • Restrict/deny parking in controlled areas.

Subject	Number
Emergency Operations Center (EOC)	**SOC-03A**

Responsibilities

Position	Duties
Superintendent/ Deputy Superintendent	Shall: • Review available information provided by the EOC; • Ensure that the Department is operating at the appropriate security level; • Notify the EOC in the event that conditions warrant a change to the existing security level; • Assign the EOC Director; • Authorize the EOC Director to disseminate security level changes throughout the Department; and • Ensure EOC guidelines are developed and kept current.
Emergency Operation Center Director	Shall: • Collect and analyze information regarding Department security levels during personnel redeployment; • Forward recommendations that warrant a change to the Security Level or procedures to the Superintendent/Deputy Superintendent; • Immediately notify the Division Commanders, Commonwealth Fusion Center, Watch Center Unit, and the Emergency Planning Officer of any changes to the security level; • Disseminate security level changes to each Division/Troop/Station/Section/Unit via radio, telephone, internet, fax or any other means as necessary; and • Develop EOC guidelines as directed by the Superintendent/Deputy Superintendent.
Division Commanders	Shall: • Ensure compliance with the appropriate security level and the established procedures; and • Ensure officers under their command are informed of changes to the security level.
Troop/Station/ Section/ Unit Commanders	Shall: • Notify members who are reporting for duty or members who are re-deployed of the current security level and the established procedure(s) in place.
Sworn/Essential/ Non-essential Personnel	Shall: • Familiarize themselves with the current security level and established procedures.

Continued on next page

Subject	Number
Emergency Operations Center (EOC)	**SOC-03A**

Commonwealth Fusion Center	Shall: • Provide information to the EOC to assist in situational awareness and development of a common operating picture; • Provide the EOC with a secure, comprehensive mechanism for the timely exchange of information if requested; • Provide the EOC with accurate and timely intelligence products such as bulletins, intelligence and informational briefings, and strategic assessments; • Provide the EOC with direct analytical support for events involving precursor criminal activity; and • Provide the EOC with awareness of priority intelligence requirements and of indicators of threats to the Commonwealth.
Watch Center Unit	Shall: • Provide notification of a State of Emergency as directed by this policy; • Act as the Department's point of contact during a State of Emergency until the EOC is functional;and • Provide assistance to the EOC as directed by the Division Commander of Homeland Security and Preparedness or designee.

Promulgated By:

Col Clogg S MA

Department of State Police
General Order

Effective Date	Number
March 25, 2020	**SOC-03B**

Subject

Response to Emergency Situations

Purpose

To provide guidance for the Department's response efforts to public safety emergencies.

Policy

The Department realizes the necessity to effectively respond to public safety emergencies as a result of severe weather, terrorist activity, violent protest, natural and/or man-made disasters, through the prudent use of available resources.

Emergency Operations Center (EOC)

The Superintendent/Deputy Superintendent shall activate the Emergency Operation Center (EOC) when deemed necessary. The EOC shall:

- Coordinate logistics for Troop/Station/Section/Unit personnel redeployment; and
- Operate under established EOC Command Coordination guidelines.

Stages of Personnel Redeployment

The Superintendent/Deputy Superintendent shall authorize the EOC to initiate the following action during the potential threat or occurrence of an emergency/incident.

	If…	**Then…**
Stage I Redeployment of Personnel	A threat or occurrence of an emergency or incident raises the potential for a shift to be held over or the redeployment of sworn personnel…	• Alert personnel of potential shift hold over and/or prepare for deployment; • Temporarily re-deploy an appropriate number of sworn personnel within the affected Troop(s) and Division; and • Hold over an appropriate number of on-duty sworn personnel.
Stage II Redeployment of On-Duty Personnel	A threat or occurrence of an emergency or incident creates a situation that is expected to require additional sworn personnel deployment beyond Stage I deployment …	• Re-deploy sworn on duty personnel as appropriate from the: 1. Division of Field Services; 2. Division of Investigative Services; 3. Division of Standards and Training; and 4. Division of Administrative Services.

Continued on next page

Stages of Personnel Redeployment (continued)

Stage III Redeployment of All Sworn and Essential Personnel	A threat or occurrence of an emergency or incident requires a full deployment of sworn and essential personnel …	• Deploy all available sworn and essential personnel as necessary; and • The Superintendent/Colonel may initiate the cancellation of time-off and establish extended work hours as appropriate.

Declaration of State of Emergency

Upon the declaration of a "State of Emergency" by the Governor, sworn and essential civilian personnel (excluding personnel on suspension, injury, or other approved leaves) shall immediately:

- Contact their duty assignment supervisor or other supervising officer within the chain-of-command for specific instructions.

The Superintendent/Colonel may initiate the cancellation of time-off and establish extended work hours as appropriate pursuant to Collective Bargaining Agreement Article 8 Section 1D.

Security Level Guidelines

Upon the authorization by the Superintendent/Deputy Superintendent, the EOC may establish a specific security level in conjunction with personnel redeployment or when circumstances dictate. The EOC Director may add, delete or modify security level procedures when necessary. Refer to SOC-03A for security level guidelines.

Responsibilities

Division Commander	Shall: • Ensure compliance with the appropriate security level procedures; and • Ensure officers under their command are informed of changes to the security level.
Troop/Station/ Section/ Unit Commander	Shall: • Notify members who are reporting for duty or members who are re-deployed of the current security level and the established procedures in place.
Sworn/Essential/ Non-essential Personnel	Shall: • Familiarize themselves with the current Security Level and established procedures.
Incident Management Assistance Team	Shall: • Provide statewide incident management support for all Department emergency operations, on a 24-hour basis; and • Provide Incident Command System (ICS) compliant framework/systems to Incident Commander(s) when requested.

Subject	Number
Response to Emergency Situations	**SOC-03B**

Emergency Response ICS Framework

The Incident Command System (ICS) provides the basis for response once an incident or event requires more than a single agency response, is multijurisdictional, extends into multiple operational periods, or requires the assistance of highly trained and specialized resources to assist in the tactical response and/or management of the incident or preplanned event. Refer to SOC-03D Incident Command System (ICS)

First On Scene

The initial arriving member is critical for assessing the nature and extent of incidents, and for initiating ICS-based response when needed. Upon arrival at the incident, the initial arriving Critical Incident Responder / Supervisor becomes the Incident Commander until he/she is relieved or command is transferred. The initial arriving Critical Incident Responder / Supervisor should ensure that the following critical tasks are initiated:

- Determine nature & scope of incident;
- Establish command & a Command Post. Announce location by radio;
- Establish communications with dispatch, Troop Duty Officer and assigned officers;
- Identify and secure the Hot Zone. Announce location(s) by radio;
- Establish inner & outer perimeters. Announce location(s) by radio;
- Request resources as needed. Cancel outstanding request(s) upon arrival of requested resource(s);
- Establish and secure a staging area between the inner & outer perimeters. Announce location by radio;
- Designate a Staging Area Manager. Announce by radio;
- Consider the needs of special populations, including but not limited to:
    - schools – hospitals – nursing homes – known disabled persons;
- Reassess each step periodically; and
- Designate a Public Information Officer ("PIO"):
    - PIO: Establish and announce Media Staging Area in consultation with the Incident Commander;
    - All media inquiries shall be directed to the PIO ("Speak with one voice").

Incident Commander

Depending on the circumstances, the Incident Commander may be a Police, Fire / Rescue, EMS, federal, or other official. Where substantial police and fire/rescue objectives or resources are involved, a Unified Command will often be created, including senior fire and police officials, as well as officials from other public or private sector agencies / organizations with a major stake in the incident.

- NOTE: In the event of a Hazardous Materials incident, a Unified Command must be established. (SARA Act, 1986)

Direction from Incident Commander

All personnel responding to a critical incident, request for assistance, mutual aid request or responding to any critical incident requiring interagency assistance are subject to the direction and control of the Incident Commander, regardless of the Incident Commander's rank, department or agency. This command structure continues for the duration of the event and until the Incident Commander is relieved or command is transferred. Supervisors from all departments and agencies are responsible for implementation of this requirement.

Subject	Number
Response to Emergency Situations	**SOC-03B**

Uncontrolled Deployments

Uncontrolled deployments (sometimes referred to as self-deployment or self-dispatching), although initiated with good intentions, can create confusion, cause significant problems at crime and emergency scenes, and can lead to the destruction or inadmissibility of evidence, or injuries to self-dispatching individuals or assigned personnel. These and other forms of unauthorized and / or unreported presence at incidents / events, and unauthorized departures are inconsistent with ICS principals, and may not be eligible for compensation or reimbursement. The highest ranking supervisor responding from each agency is responsible for the control and coordination of all personnel from that agency and will coordinate that agency's response with the Incident Commander. The responding supervisor is responsible for deploying only the amount of personnel needed and requested by the Incident Commander. Department members shall not self-deploy to incidents.

Incident Command Post

The Incident Commander shall establish an Incident Command Post ("ICP," can be a building or vehicle) and advise dispatch of that location. Dispatch shall advise all on-scene and responding personnel of that information. The Incident Commander shall remain at and operate from the ICP. The Incident Commander may move the ICP if its location is threatened by expanding circumstances or hazards. If moved, its new location must be announced immediately to all personnel and to dispatch.

Liaison Officer

The Incident Commander shall designate a Liaison Officer, who shall be the point of contact between all Critical Incident Responders and the Incident Commander. The Liaison Officer shall meet and brief all responding Agency Representatives at a location to be determined, such as the ICP or the Staging Area.

Staging Area

The Incident Commander shall establish a Staging Area between the inner and outer perimeters. It should be large enough to accommodate the required resources and close enough to the incident to make tactical deployments effective and timely. All responding resources shall respond to the Staging Area for check-in unless otherwise directed by the Incident Commander. Resources should not respond to the ICP unless directed to do so by the Incident Commander or his designee.

Staging Area Manager

The Incident Commander shall designate a Staging Area Manager, who shall have authority for check-in and accountability of Critical Incident Responder arrivals and departures. The Staging Area Manager will remain in and operate from the Staging Area. All Critical Incident Responders shall report immediately upon arrival to the Staging Area Manager, and remain in the Staging Area until properly assigned.

Dispatch Notifications

Dispatch shall notify critical incident responder agencies of:

- the location, type and known extent of the emergency;
- the name, rank and agency of the Incident Commander;
- the location of and directions to the Incident Command Post and the Staging Area;
- the name and agency of the Staging Area Manager; and
- the name, agency and location of the Operations Section Chief (if a Unified Command is established).

Subject	Number
Response to Emergency Situations	**SOC-03B**

Requesting Assistance

When requesting critical incident assistance, Incident Commanders, Staging Area Managers and dispatchers should scale requests properly.

- Avoid issuing generalized calls for help; and
- Specify by name which agencies are being asked for assistance, how many personnel and any specialized skills needed (e.g.: negotiators, search-and-rescue, entry-team, etc.), along with requested special equipment types.

Reporting to Staging Area

All arriving Critical Incident Responders shall immediately report to the Staging Area Manager (SAM) located at the Staging Area for check-in. The SAM shall record the names, rank, agency, specialty, and equipment brought with them on NIMS ICS 211 Check-In-Form or other document.

After arrival and check-in at the Staging Area, one supervisor from each responding agency should report to the Incident Command Post or other location designated by the Incident Commander or Liaison Officer. That individual will serve as the responding agency's representative. That person should have authority delegated from his / her agency to make decisions on the deployment of his / her resources.

The SAM must carefully consider where arriving personnel are to park their vehicles. Blocking of streets, bridges, underpasses, etc., may hinder rapid arrival of essential emergency vehicles. Arriving personnel shall park where designated by the SAM.

Arriving personnel shall remain at the Staging Area until assigned by the Incident Commander or relieved.

Demobilization

Personnel located at the Staging Area who intend to demobilize from the incident shall contact the SAM and await his / her authorization before departing.

Agency Representatives wishing to demobilize their resources from the incident shall contact the Liaison Officer and await his / her authorization before departing; demobilization must be accomplished through and according to the direction of the SAM.

A proper demobilization plan shall be completed to accurately record departing personnel and resource check-out time, notation of any apparent physical injuries or critical incident stress-related concerns, and include notations of any damaged or lost equipment. NIMS ICS 221 Demobilization Check-Out Form or other suitable document should be utilized.

Unified Command

A determination must be made promptly whether to continue under an Incident Commander, or via establishment of a Unified Command. If a Unified Command is established, a single, coordinated Incident Action Plan (IAP) must be agreed upon, and an Operations Section Chief designated by agreement to implement it. The Incident Commander remains in command until relieved by the Unified Command.

The Incident Commander or Unified Command must delegate the Planning Section Chief (PSC) to begin or expand the planning process by developing a single consolidated Incident Action Plan with appropriate NIMS ICS 204 Assignment forms for each responding resource that will be assigned to a Division or Group Supervisor, or Strike Team or Task Force Leader.

Subject	Number
Response to Emergency Situations	**SOC-03B**

ICS Support

All supervisors from Critical Incident Responder agencies have a continuing duty to support ICS-based operations, particularly with regard to unity of command, for the duration of the incident or event.

References

SOC-03A – Emergency Operation Center (EOC)
The National Incident Management System (NIMS)
Commonwealth of Massachusetts "Recommended Protocol For Managing Initial Response To Critical Incidents, April 2014"

Promulgated By:

Col. Clay S. M...

Department of State Police
General Order

Effective Date	Number
March 25, 2020	**SOC-03C**

Subject

Response to Civil Disturbances

Purpose

To provide guidance for the Department's response to civil disturbances.

Policy

The Department realizes the necessity of an effective response to any civil disturbance through the prudent deployment of available Departmental resources.

Definition

Massachusetts General Laws c.269 s.1:

- An unlawful assembly exists when five or more persons, being armed with clubs or other dangerous weapons, or ten or more persons, whether armed or not, are unlawfully, riotously, or tumultuously assembled.
- An "Order to Disperse" shall be given to persons unlawfully assembled before any action can be taken against them.

Civil Disturbances Initial Inquiries

Whenever any law enforcement agency requests the assistance of the Massachusetts State Police for civil disorders, riots, etc., a request to such effect shall be made through channels to the Office of the Superintendent/Deputy Superintendent. The following minimum information is required:

- Requesting department, rank and name of the caller;
- Name of authorizing official and a call-back number;
- Specific facts surrounding the incident:
  1. Location;
  2. Number of officers on-scene/enroute;
  3. The reason or purpose for the disturbance; and
  4. Number of people causing the disturbance and whether armed, violent, or hostile.

Civil Disturbances Response

The "Order to Disperse" shall be given by the Incident Commander at the scene. The restoration of public peace should be accomplished first through persuasion. If necessary, force may be employed.

Crowd control objectives:

- Protect life and property;
- Contain and isolate the disturbance;
- Disperse as expeditiously as possible;
- Prevent re-grouping or re-entry; and
- Identify and take action against law violators.

Officers shall keep in mind the limitations imposed upon the Department in private business sector strikes.

Responsibilities

Position	Duties
Responding Officer	Shall: • Report with the current duty uniform and riot gear; • Report to the Incident Commander on-scene for instructions when responding in plainclothes; • Be issued additional restraining devices, as necessary, by the Supply Section; • Field search prisoners prior to entering an established Field Processing Area; and • Submit all appropriate reports using the incident case number as issued by the Incident Commander.
On-scene Department Incident Commander	Shall: • Order or verify that an "Order to Disperse" was issued to all persons to immediately and peaceably disperse; • Take necessary action if the crowd fails to disperse after being ordered to do so; • Request additional personnel and support through the Division Commander of Field Services; • At no time attempt to accomplish a police objective, unless sufficient forces are present to support such objective; • Establish a Field Processing Area when necessary; • Assign officers (e.g., security, intake, booking, evidence control, photo/ fingerprint, court officer, clean-up, etc.) as needed, to maintain a Field Processing Area; and • Prepare and submit an "After Action Report" within 24 hours after termination of all Departmental activities.
Division Commander of Field Services	Shall: • Ensure adequate uniformed personnel and tactical support remain in the affected area during and after order is restored for such period of time as deemed necessary by the Colonel/Superintendent; and • Ensure any further disruptions are addressed as expeditiously as possible.

Mass Arrests Logistics

The following procedures shall be used when a situation requires multiple arrests:

- Normal arrest procedures shall be used for all arrested individuals;
- All arrested individuals shall be subject to the appropriate bail procedures;
- Arrested individuals shall be expeditiously taken to a Field Processing Area;
- For record keeping purposes and whenever feasible, the arresting officer's name shall be written on the photograph of each individual they have arrested;
- As soon as possible, transport arrested individuals to an appropriate place of temporary confinement or released after booking as directed by judicial authorities;

Continued on next page

Subject	Number
Response to Civil Disturbances	**SOC-03C**

Mass Arrests Logistics (continued)

- Food, water, medical and sanitation needs shall be tended to as soon as reasonably possible;
- The face sheet/arrest report and Prisoner Property Inventory Form shall be sent with the transporting officer to the place of confinement or release;
- The court of jurisdiction and the appropriate District Attorney's office shall be apprised of the situation; and
- Contraband or evidence shall remain with an assigned Evidence Control Officer.

After Action Report

An After Action Report shall be prepared by the Incident Commander assigned to the scene. It shall begin with a numerical, chronological listing of all arrested individuals and shall contain, at a minimum:

- Number and source of complaints;
- Verbatim instructions given to the crowd and the name of the officer giving them;
- Department personnel on scene and their respective duties;
- Names of arresting officers and individuals arrested;
- Contraband and evidence seized;
- Damage to private/public property;
- Injuries to police/public; and
- Private/public agencies/personnel involved.

References: MPAC: 46.1.2

Promulgated By:

Col. Clay J. M...

Department of State Police
General Order

Effective Date	Number
March 25, 2020	**SOC-03D**

Subject

All Hazards Incident Command Framework

Policy

The Department recognizes the Incident Command System (ICS) as a valid incident management system for use at the scenes of all emergency incidents. Regardless of the size or complexity of an incident, emergency responders must employ good management techniques to ensure an effective response and an efficient, safe use of resources. ICS helps emergency responders accomplish these goals.

While ICS is normally associated with responses to emergency incidents, the Department further recognizes that ICS can be applied to a wide variety of incidents requiring Department response.

Members shall use the incident management strategies outlined in this policy for all multiagency and multi-jurisdictional responses. In addition, and when applicable, members are encouraged to use these strategies for responses to incidents involving only the Department.

Purpose

To provide guidance for the Department's response efforts to emergencies and incidents.

Incident Command System Defined

ICS is an emergency incident management system that was originally developed by the fire services in the 1970s in response to a series of wildland fires in California. Over the years, ICS was refined by the fire services and emergency management organizations into an "all-risk" system that is now used for managing a wide variety of emergencies. Many police agencies throughout the nation have begun to include ICS principles in their incident management strategies.

The Federal Emergency Management Agency (FEMA) defines ICS as:

"An incident management system consisting of procedures for organizing personnel, facilities, equipment, and communications at the scene of an emergency."

- The system is based upon traditional business management principles such as planning, directing, organizing, coordinating, communicating, delegating, and evaluating. ICS provides a common organizational structure, or framework, within which participating agencies can work toward accomplishing common goals and objectives. While the system works well in all types of emergency incidents, its primary benefit is found in managing incidents of a multiagency or multi-jurisdictional nature.

- The federal government requires an ICS to be used at the scenes of hazmat incidents. This regulation has been promulgated by the Occupational Safety and Health Administration (OSHA) at 29 CFR 1910.120.

Major Components of the Incident Command System

- Common Terminology: Responding agencies can communicate at the scene of an emergency only if they have a common understanding of the terminology used by the various emergency responders. Common names are established and used for personnel, equipment, and facilities operating in and around the incident area.
- Modular Organization: An incident management system is valuable only if it can adapt to changing conditions at the scene of an incident. A common characteristic of emergency situations is that they seldom remain constant; the incident often will expand or contract. A modular organizational structure will allow the incident response to grow in direct proportion to the complexity of the incident. Conversely, the structure of the response can be scaled back as conditions improve and resources are no longer needed.
- Integrated Communications: Effective communications at the scene of an incident is essential for proper incident management. Whenever possible, responding agencies should be able to talk directly to each other through common radio channels. Furthermore, command personnel must be able to personally interact to formulate effective response strategies.
- Command Structure: ICS recognizes the key ingredient to any emergency response is to have an effective command structure to manage personnel and other resources. The command function may be organized in one of two ways:
- A *single command* involving one person may be used when there is no overlap of jurisdictional boundaries or when a single commander is designated by the agency with overall management responsibility for the incident. This person is normally referred to as the Incident Commander.
- Under a *unified command* structure, all involved agencies contribute to the command process by sharing management responsibility. A unified command structure is the preferred method when responding to emergencies of a multiagency or multi- jurisdictional nature. Even with a unified command structure, however, one person will still be in overall charge of the event.
- Span of Control: Span of control is defined as the number of subordinates one supervisor can manage effectively. ICS recommends that one person can properly supervise no more than three to seven subordinates, with the optimum number being five. Command officers must anticipate span of control problems and prepare for them as the modular organizational structure of the incident response expands.
- Consolidated Action Plan: ICS requires every emergency response to have a consolidated action plan.
    - For small incidents, this may be something as simple as the Incident Commander having a cognitive plan. For large scale events, the incident response may require a written plan, even as the event is unfolding.

Continued on next page

Major Components of the Incident Command System (continued)

- ICS requires all plans to address strategic goals and tactical objectives.
  - A strategy is the overall plan that will be used to control the incident.
  - Strategic goals are broad in nature.
  - Tactical objectives are the tasks that must be accomplished to achieve strategic goals. Objectives are specific and measurable.

  For example, in a prison riot where inmates have overcome the guard staff and gained control of a cell block, the following goals and objectives might be established:

  - Strategic Goal: Retake control of the affected sections of a riot-torn prison by using the minimum amount of force necessary.
  - Tactical Objectives:
    - Secure the outer perimeter of the prison to ensure only authorized ingress and egress.
    - Mobilize a sufficient number of Department personnel to contain the uprising.
    - Secure unaffected housing units within the correctional facility.
    - Activate a counteraction involving tactical team members.
    - Ensure all injured persons receive appropriate medical attention.
    - Assist correctional authorities in restoring the facility to a sense of normalcy.
- Designated Incident Facilities: ICS recognizes that designated incident facilities can greatly assist the Incident Commander in managing the incident. For instance, a Command Post is designated to serve as the on-scene location from which all incident operations are directed. Similarly, staging areas are established to designate where available resources should report for assignment. Other facilities are established as the need arises.
- Comprehensive Resource Management: The Incident Commander is responsible to ensure all resources currently available are used effectively and efficiently. Resource management requires that the safety of personnel is given the highest priority. Incident Commanders must continually evaluate and adjust the deployment of resources at all incidents. If additional resources are needed to manage the incident, the Incident Commander must ensure they are obtained in a timely manner.

Incident Command System Functional Areas

The organizational structure of ICS requires the establishment of five key functional areas. In a small, single command structure, the Incident Commander will be able to perform all five functions. In a large scale event, however, the Incident Commander will designate section chiefs to manage the responsibilities of the various areas.

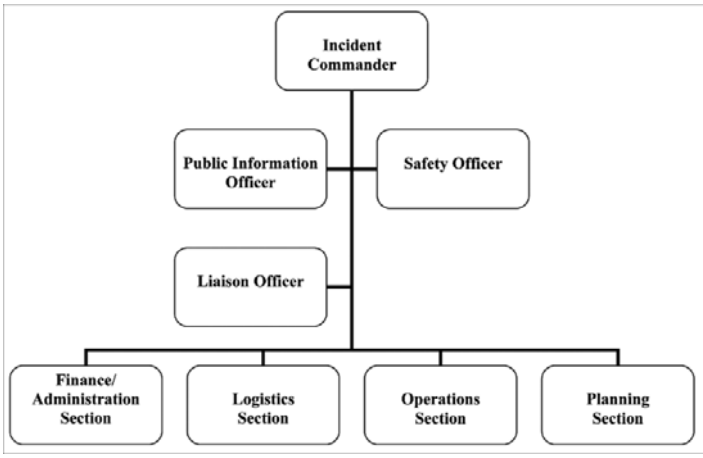
Continued on next page

Incident Command System Functional Areas (continued)

Command: Incidents are commanded by an Incident Commander, normally from the agency having primary jurisdiction, who is responsible for the management of all incident operations. As previously discussed, command may be established either through a single or unified command structure. The Incident Commander is responsible for the following activities:

- Assessing incident priorities.
- Determining strategic goals and tactical objectives.
- Developing and implementing the incident action plan.
- Developing an appropriate organizational structure.
- Managing resources.
- Coordinating overall emergency activities.
- Ensuring scene safety, proper liaison with other agencies, and disseminating information to the news media.

NOTE: In some large scale events, Incident Commanders must delegate authority to ensure the above responsibilities are properly addressed. Any functions not specifically delegated by the Incident Commander remain the responsibility of the Incident Commander. Any one or all of the functional areas depicted in the following diagram may be established as the need arises.



Operations Section: The Operations Section is responsible for the management of all tactical operations at an incident. The most common reason for staffing operations is to relieve span-of-control concerns for the Incident Commander. Some incidents may become so complex that the Incident Commander may no longer be able to solely supervise all operational aspects of an incident. An Operations Section Chief will be able to assist the Incident Commander by:

- Assisting in development strategic goals and tactical objectives for the incident;
- Developing operational plans;
- Requesting or releasing resources through the Incident Commander;
- Consulting with the Incident Commander about the overall incident action plan;
- Keeping the Incident Commander informed of the progress of the incident and the status of resources;
- Supervising the Staging Area Manager.

Continued on next page

Incident Command System Functional Areas (continued)

Planning Section: The Planning Section is responsible for the collection, evaluation, dissemination, and use of information about the development of the incident and the status of resources. Planning includes an assessment of the current situation and a projection of future conditions. Members in the Planning Section maintain information about resources committed to the incident and projected resource requirements. The modular nature of ICS also allows the planning function to be expanded in scope to include the following Subdivisions or Units:

- Resource Unit: The Resource Unit provides answers to the following questions which are important to the Incident Commander: What resources (personnel and equipment) are currently committed to the incident? Where are these resources assigned? Are all personnel accounted for at shift changes? Are additional resources necessary? Where can they be obtained?

- Situation Analysis Unit: Members in the Situation Analysis Unit analyze the incident as it progresses. They help the Planning Section Chief and the Incident Commander develop a consolidated action plan and determine if the plan is being followed and whether the plan of action is having the desired effect. Members of this Unit will also offer alternatives to the Incident Commander in those situations where the original plan must be modified.

- Documentation Unit: The Documentation Unit is responsible for recording the incident and protecting all documents relevant to the incident. Examples include Incident Reports, Communication Logs, CLEAN Messages, Injured Employee Statements, correspondence, and directives from various sources. In all incidents, thorough documentation is essential to permit proper after-action analysis. In major emergency incidents, a member should be assigned to collect information for the After-Action Report while the incident is still ongoing. This will ensure the availability of appropriate documentation for reporting purposes and will also ensure a timely completion of the After-Action Report (refer to Chapter 3).

- Demobilization Unit: The Demobilization Unit should begin preparing for the orderly and controlled withdrawal of resources from the scene of the emergency while the incident is still unfolding. This will ensure that resources are properly managed and that the scene is returned to a state of normalcy as soon as possible after the incident has terminated.

- Technical Specialists: Technical specialists should be included in the planning function whenever expertise is needed beyond the levels maintained by the Incident Commander and their immediate subordinates. Examples include hazmat personnel, engineers, industry representatives, explosives technicians, and radiation experts.

- CISM: Crisis Incident Stress Management Team personnel should also be included in the planning function.

Continued on next page

Incident Command System Functional Areas (continued)

Logistics Section: The Logistics Section is responsible for providing facilities, services, and materials to sustain the incident response. The logistical needs of the members assigned to an incident will grow in direct proportion to the size, duration, and complexity of the incident. The Logistics Section Chief may elect to establish functional Units to perform the following roles:

- Communications Unit: The Communications Unit will perform a vital role by developing and overseeing the operation of the communications infrastructure. Members of this Unit will ensure that proper equipment is available and that it is performing to acceptable standards. They will maintain the operational readiness of all radio, telephone, and CLEAN System communications at the Command Post and other incident facilities.

- Facilities Unit: The Facilities Unit will ensure the availability of adequate buildings and shelter for incident operations. Included in this category are such matters as Command Post location and operation, feeding and housing areas, sanitary facilities for field operations, and other fixed facilities necessary for the successful management of the incident.

- Procurement and Supply Unit: This Unit orders the equipment and supplies required for incident operations and maintains ongoing inventory and control of these resources. Examples in this category include clerical supplies such as paper and pens, as well as tactical supplies such as ammunition and tear gas.

- Food Unit: Incidents that operate for an extended period of time will require the procurement of food for participating personnel. In smaller incidents, this role may be handled within the Procurement and Supply Unit, e.g., when sandwiches are obtained for a 12-hour operation. However, for incidents that may extend for days, the Incident Commander and Logistics Section Chief may elect to contract food services from a local vendor. A Food Unit within the Logistics Section would be responsible for making the necessary arrangements.

- Other Service and Support Units: Other service and support Units can be added to the Logistics Section as the need arises.

Finance/Administrative Section: The Finance/Administrative Section is responsible for tracking all incident costs and evaluating the financial considerations of the incident. Financial considerations for a major Department mobilization can be extensive, especially when the Department tries to seek reimbursement for the operation or when detailed records must be prepared for budgetary or planning purposes. The Section Chief has the responsibility to document all incident costs and to provide guidance to the Incident Commander on financial issues that impact incident operations. As with other functional areas, the Finance/Administrative Section can be subdivided into Units to manage matters such as timekeeping, billing, and cost accounting.

Expansion: Not all of the above functional areas may be needed during an incident response. However, Incident Commanders must be prepared to expand their organizational structure if the need arises.

Incident Priorities

A member serving in the capacity of the Incident Commander has numerous duties and responsibilities to perform. These responsibilities will vary depending upon the nature of the incident and the number of available resources. One aspect of the emergency response that will not vary, however, is the recognition of three incident priorities. Regardless of the nature of the incident, the following priorities WILL ALWAYS be addressed in an emergency incident response:

- Life Safety: Life safety is the first priority for any emergency incident. This includes not only the safety of any victims involved in the incident, but also the safety of response personnel and populations surrounding the incident scene. Incident Commanders must place life safety above all other considerations of emergency incident management.
- Incident Stabilization: The Incident Commander's second priority is to formulate a strategy to stabilize the incident. Incident stabilization involves the development of a plan to minimize the effect the incident may have on the surrounding area and populations (e.g., with incidents of civil disorder, this priority will involve isolation of the perpetrators and containment of the disorder to prevent it from spreading; a hazmat response team might stabilize an incident by containing the spill at the scene of a crash and preventing runoff into nearby waterways).
- Property Conservation: Property conservation involves achieving strategic goals and meeting tactical objectives at an incident while minimizing property damage and inconvenience to uninvolved citizens. While this priority is clearly important, it should not weigh as heavily with the Incident Commander as the previous priorities of life safety and incident stabilization. Nevertheless, an emergency incident cannot be considered successfully managed if the Incident Commander does not give this priority proper consideration.

NOTE: In addition to the above priorities, restoration of traffic flow for incidents occurring on or around highways must be considered when normal traffic patterns are disrupted. Major highway incidents often create substantial disruptions to traffic, and it is the Incident Commander's responsibility to restore normal or limited traffic flow around the scene as soon as possible. Refer to TRF-05 Traffic Incident Management for additional guidance.

Incident Command Summary

When using the Incident Command System (ICS), members must be cognizant that the system is a management tool. ICS does not replace sound command decision making at the scene of an incident; it does not avoid the need for proper training and education; and it does not eliminate the need for establishing positive interagency relationships. The system does provide a broad management framework under which one agency or many agencies can operate at the scene of an emergency.

ICS makes the best use of available resources. Resources are essential to the management of any emergency incident. Some incidents, such as a minor non-reportable motor vehicle crash, can be managed with no resources other than the member assigned to make a record of the crash. Other incidents, such as a major prison disturbance, may require hundreds of personnel resources and dozens of pieces of equipment to successfully resolve the incident. ICS helps the on-scene commanders manage the resources at their disposal.

Continued on next page

Subject	Number
All Hazards Incident Command Framework	**SOC-03D**

Incident Command Summary (continued)

ICS does not, in any way, cause an agency to relinquish authority at the scene of an incident. On the contrary, this system recognizes the valid role that all emergency response agencies play at the scene of an incident. ICS further establishes a system in which the various responders can perform their individual roles in a unified manner with the other agencies represented at the scene.

ICS can be effective only when all members of an organization practice ICS principles in their day-to-day responses to emergency situations. ICS works best when members apply the principles taught in training to small, frequently occurring events, such as traffic collisions and minor crime scenes. As a result of this constant repetition and familiarity, members are then better able to manage the large-scale events such as prison riots and motor vehicle crashes involving multiple fatalities. ICS operating principles become so well established that they soon become an integral part of all incident management.

ICS Support

All supervisors from Critical Incident Responder agencies have a continuing duty to support ICS-based operations, particularly with regard to unity of command, for the duration of the incident or event.

For incidents falling within the primary jurisdiction of the Department, the highest ranking Department member at the scene shall assume the role of Incident Commander. However, to ensure command continuity, the temporary involvement of a higher-ranking member at the scene will not automatically require that member to assume the role of Incident Commander. If, in the opinion of the higher ranking member, the situation dictates that he/she remain at the scene, then the higher ranking member shall assume the role of Incident Commander.

Supervisors shall monitor the status of all incidents and ensure that an appropriate management strategy is employed.

ICS Training

The Commandant of the State Police Academy shall ensure Basic Incident Command System training is made part of the Recruit Training Curriculum.

References

The National Incident Management System (NIMS)
MPAC: 46.1.2, 46.1.4, 46.1.5, 46.1.6, 46.1.7

Promulgated By:

Col. Craig S. Mann

Department of State Police
General Order

Effective Date	Number
July 11, 2011	**SOC-04**

Subject

Lost/Missing Person Searches

Policy

Every incident involving a lost and/or missing person shall be treated as a potential emergency event that may require a rapid and coordinated response of specialized personnel and equipment.

Members should understand that every lost and/or missing person incident has the potential of being or becoming a criminal investigation; members shall treat the scene of each incident as a potential crime scene.

If the missing person is identified as a child age seventeen (17) or younger and there is evidence of abduction, the Amber Alert Coordinator shall be notified.

Stage One Response Protocol

Upon receiving a report of a lost/missing person and/or receiving a request for Department assistance in locating a lost/missing person, the Desk Officer shall immediately gather as much information as possible, including, but not limited to:

- Name, age, and address of the missing person;
- Description of appearance/clothing;
- Activity at time of disappearance;
- Place Last Seen (PLS);
- Reporting person's information;
- Physical or general health condition;
- Any mental or cognitive deficiencies e.g., Alzheimer disease, dementia, or autism;
- Does the missing person have an electronic tracking transmitter;
- Involvement of any weapon;
- Requesting agency point of contact including their call back telephone number; and
- Action taken so far.

Continued next page.

Subject	Number
Lost/Missing Person Searches	**SOC-04**

Stage One Response Protocol (Continued)

Position	Duties
Desk Officer	• Dispatch the appropriate patrols; • Notify the Troop Duty Officer of all requests; • Broadcast all pertinent information over the radio; and • Make appropriate Daily Administrative Journal (DAJ) entries.
Troop Duty Officer	• Dispatch a supervisor to the scene; • Dispatch K-9 to the scene; • Make appropriate DAJ entries; • Check on the availability of Air Wing; • Dispatch Department members trained and equipped with electronic tracking receivers, when it is determined the missing person is equipped with an electronic tracking transmitter; • Dispatch other resources as needed; • Conduct an assessment of the "search urgency" by reviewing the current information. The following conditions may indicate a high search urgency: 1. Child under twelve (12) years of age; 2. Adult over seventy (70) years of age; 3. Mentally challenged individuals; 4. Physical conditions or health issues; 5. Extreme or deteriorating weather conditions; 6. Time of day; 7. Persons determined to be at risk to themselves; and 8. Other pertinent factors. • Ensure that a SP 622 Lost/Missing Person Questionnaire is completed by on-scene personnel.

Subject	Number
Lost/Missing Person Searches	**SOC-04**

Stage Two Response Protocol

Upon the need for a more comprehensive response as determined by:

- The requesting agency;
- The responding members; or
- Based upon a search urgency analysis.

The Troop Duty Officer shall request, through the GHQ Communications Section, that the Tactical Operations Commander or designee be contacted for a Stage Two Response.

The Tactical Operations Commander or their designee shall approve all Stage Two requests prior to any Stage Two Response activation orders.

When authorized, the Tactical Operations Commander or designee shall activate:

- Additional resources from within Tactical Operations (SERT, IMAT, Air Wing, Canine, Mounted, etc.) or
- Outside resources (Environmental Police, Department of Conservation and Recreation, Civilian Volunteers, etc.); or
- Other resources as needed.

Reference

SOC-04A Amber Alert Activations
TOP-01 tactical Operations Command and Control
TOP-09 Incident Management Assistance Team
SP 622 Lost/Missing Person Questionnaire

Promulgated By:

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**SOC-04A**

Subject

AMBER Alert Activation

Policy

The Department shall initiate an AMBER Alert for cases of child abduction, where the child's life is in imminent danger of serious bodily harm or death, and specific criteria supporting the AMBER Alert Activation have been met.

Amber Alert Criteria

America's Missing Broadcast Emergency Response (AMBER) Alerts shall only be activated when:

- A child, seventeen (17) years of age or younger has been abducted;
- The child is in danger of serious bodily harm or death; and
- There is enough descriptive information to believe an AMBER Alert will help locate the child.

Note: AMBER Alerts are <u>not intended</u> for missing child incidents, runaways, or child custody situations.

Activation Procedures Duties / Responsibilities

Position	Responsibilities
First Responding Officer	• Conduct an initial scene assessment to determine if the AMBER Alert Criteria has been met; • Verify witness(s) observations to the abduction; • Notify the Desk Officer with specific information and request an immediate AMBER Alert Activation; and • Remain at the scene until relieved by a supervisor.
Desk Officer	• Dispatch the appropriate patrols; • Notify the Troop Duty Officer of jurisdiction with the specific information for an AMBER Alert Activation; • Broadcast pertinent information via the radio; and • Enter the AMBER Alert Activation request into the Daily Administrative Journal (DAJ).

Continued next page.

Subject	Number
AMBER Alert Activation	**SOC-04A**

Activation Procedures Duties / Responsibilities (Continued)

Position	Responsibilities
Troop Duty Officer	• Complete the AMBER Alert Activation Form and fax to GHQ Communications Section OIC; • Follow up fax with a call to GHQ Communications to ensure the fax has been received; and • Assign a supervisor to respond to the scene, who shall act as a liaison with the AMBER Alert Activator and/or Coordinator.
GHQ Communications Section OIC	• Notify the AMBER Alert Activator and AMBER Alert Coordinator with the specific information received from the AMBER Alert Activation Form; • Notify the Media Relations officer-on-call when an AMBER Alert Activation Request is received; • Notify the Division Commanders of Field Services and Investigative Services when an AMBER Alert Activation has been authorized; • Initiate the AMBER Alert Activation procedures when authorized; and • Enter the information into NCIC if the Department is the initiating agency.
AMBER Alert Activator	• Review the Massachusetts Child AMBER Alert Activation Form information; • Contact the Troop Duty Officer or requesting police department if further information is needed to support an activation; • Authorize the AMBER Alert Activation when specific criteria warrant such activation; • Notify the submitting Troop or local department when the AMBER Alert Activation is authorized or denied; and • Complete an after action report on all activations and forward: 1. The original to the Division Commander of Investigative Services.

Continued next page.

Subject	Number
AMBER Alert Activation	**SOC-04A**

Activation Procedures Duties / Responsibilities (Continued)

Position	Responsibilities
AMBER Alert Coordinator	• Oversee the AMBER Alert Activation Process within the Department; • Select the Massachusetts Child AMBER Alert Committee; • Act as a backup AMBER Alert Activation Officer; • Maintain a database on all requests; • Notify Division Commander of Investigative Services of all activations; • Review all requests for AMBER Alert Activations; • Complete an after action report on all activations; and • Submit findings through channels to the Office of the Superintendent.
Superintendent	• Assign a member as the AMBER Alert Coordinator; and • Assign Commissioned Officers from the Division of Investigative Services as the AMBER Alert Activator.

References

SOC-04 Lost/Missing Person Searches
National Center for Missing and Exploited Children (NCMEC)

Promulgated By:

Department of State Police
General Order

Effective Date	Number
July 22, 2014	**SOC-05**

Subject

Special Considerations

Policy

In accordance with international, federal, and state laws, the following are entitled to special considerations and/or immunities:

- Diplomatic and consular officers;
- Foreign Nationals;
- Individuals requesting political asylum;
- Military personnel; and
- Elected officials.

Diplomatic and Consular Officers

Diplomatic Immunity

Diplomatic Immunity is a principle of international law accorded to duly-accredited diplomatic officers, their families, and their servants that afford them qualified exemptions from local jurisdictional prosecution.

Federal law grants members of foreign diplomatic missions and consular posts privileges and immunities in their offices, private residences, as well as in their papers and correspondence.

Members may consult the U. S. Department of State web site and search for the publication ***Diplomatic or Consular Immunity****- Guidance for Law Enforcement and Judicial Authorities (Revised July 2011)* for further information.

Identification

Foreign nationals who enjoy privileges and immunities possess a valid diplomatic passport issued by their country with a diplomatic "A" or "G" visa.

Other formal documents of identity issued by the U.S. State Department includes a (3¾" x 2½") card with photo which depicts:

- Blue border - Diplomatic officers and their families;
- Green border - Embassy administrative and technical staff and their families; or
- Red border - Consular officers, employees and their families.

Vehicle Registration

The State Department has revised the diplomatic and consular license plates. These plates may or may not designate consular or diplomatic codes to correspond to the owner's privileges and immunities. Members may consult

Continued next page.

Vehicle Registration (Continued)

the U.S. Department of State web site and search for the publication ***Diplomatic or Consular Immunity****- Guidance for Law Enforcement and Judicial Authorities (Revised July 2011)* for further information.

Members shall:

- Not tow or boot any vehicle bearing a diplomatic or consular license plate, however, the vehicle may be moved to the nearest safe location for reasons of public safety.

Diplomatic Immunity Incidents

The following individuals shall not be detained, handcuffed, or arrested:

- Diplomatic agents or their administrative and technical staff;
- Diplomatic level staff of the United Nations; or
- Family members of any of the above.

Exception: Reasonable restraints may be applied in emergency circumstances involving self defense, public safety, or the prevention of serious criminal acts.

Incidents involving foreign diplomatic and consular personnel shall be fully documented to assist the State Department in subsequent prosecution or expulsion.

Civil Infractions

No person is exempt from being issued a citation for a civil motor vehicle violation.

Diplomatic Immunity and OUI

If…	Then…
Operating Under the Influence and has a diplomatic "A" or "G" visa.	Sobriety tests may be offered but not compelled. Do not allow the person to drive, however, a member may: • Transport operator to a police station to arrange for safe transport; or • Contact a taxi, friend, or relative of the individual to drive, or assist in making arrangements.

Notifications

When any foreign diplomatic official, members of their family, or staff are involved in any State Police action the Troop Commander shall:

- Immediately notify their Division Commander; and
- Notify the State Department at (202) 895-3682 or call the telephone number listed on the reverse of the subject's identity card issued by the U.S. Department of State, if after regular business hours.

Subject	Number
Special Considerations	**SOC-05**

Foreign Nationals

Introductions

The State Department requires assistance from state and local police in carrying out certain international obligations arising from the arrest, detention, or death of foreign nationals (citizens of other countries).

For the purposes of consular notification, foreign nationals include lawful permanent resident aliens of the United States who have a resident alien registration card (commonly known as a "green card").

When foreign nationals are involved in an incident, members shall consult *"Consular Notification and Access"* provided by the Department of State, and are available to all stations via the web site at:

- http://travel.state.gov/consularnotification

International Drivers Licenses

Some foreign nationals, while in the United States, may legally drive using their country's license for up to one (1) year from the person's date of entry into the country, unless they establish permanent residency or employment in this country.

Massachusetts shall only honor valid licenses from countries identified within the current Massachusetts Driver's Manual Appendices:

- *Parties to the Road Traffic Convention and the 1943 Inter-American Automotive Traffic Convention*.

This publication is available to all members via the Massachusetts Registry of Motor Vehicles web site under:

- Forms & Manuals→ Driver's Manual→ Appendices "A".

This also applies to private vehicle registrations, when accompanied by a plaque indicating the country of origin.

An operator with a valid driver's license from Germany or Switzerland shall be considered to be duly licensed to operate in Massachusetts.

Foreign Nationals Arrest or Detention

Position	Duties
Member	• The arrest or detainments of a foreign national immediately notify a supervisor.

Continued next page.

Foreign Nationals Arrest or Detention (Continued)

Position	Duties
Supervisor	• Inform the detainee of their right to have their government notified; • Notify the Troop Duty Officer of the detention and of the notification of the detainee's rights; and • Subject to laws and Department procedures, allow consular officers to visit and converse with the detainee.
Troop Duty Officer	• Notify the Troop Commander; and • If the detainee requests, or if it is mandated, notify the appropriate consulate or embassy without delay, and document the notification.

Mandated Reporting

Agreements with certain countries mandate that they be notified when their nationals are confined or detained regardless of the national's request. These countries are listed in *"Consular Notification and Access"* provided by the Department of State, and are available to all stations via the web site at:

- http://travel.state.gov/consularnotification

Contact information for Foreign Consular Offices within the U.S. can be found at:

- http://travel.state.gov/law/consular/consular_745.html

Station Commanders shall ensure that the Consular Notification and Access List is updated and available in the guidebook.

Questions

Members who have questions regarding Consular Notification may contact U.S. Department of State at (202) 485-7703 or after regular business hours the Department of State Operations Center at (202) 647-1512.

Ship and Aircraft Incidents

If a ship or aircraft registered in a foreign country crashes within the United States, the nearest consular offices of that country shall be notified immediately.

Deaths of Foreign Nationals

Article 37 of the Vienna Convention on Consular Relations requires that if federal, state or local government officials become aware of the death of a foreign national in the United States, they must ensure that the nearest consulate of that national's country is notified of the death. Members who become aware of such incidents in the course of their duties shall make appropriate notification in a timely manner.

Subject	Number
Special Considerations	**SOC-05**

Requests for Political Asylum

Asylum

Protection and immunity from extradition granted by the United States to a foreign national who is unable or unwilling to return to their country of nationality because of persecution or a well-founded fear of persecution on account of race, religion, nationality, membership in a particular social group, or political opinion.

Request for Asylum

If approached by a foreign national seeking asylum:

Step	Action
1	Prevent attempts at forced repatriation, and try to make the person feel comfortable and safe: • Offer protection; and/or • Invite the person to the nearest Department station or facility.
2	Obtain personal data/history: • Name, nationality, date and place of birth, and any documents; • Whether person is alone or with a group; and • Whether person has family, friends, or relatives nearby.
3	Notify a supervisor and the Troop/Section/Unit Commander of the situation.
4	Notify U.S. Immigration and Customs Enforcement (ICE) Boston office (617) 565-3100/3104 to transfer the case.

Elected Officials

National Senators and Congressional Representatives

U.S. Senators and Representatives shall in all cases, except treason, felony, and breach of peace, be privileged from arrest during their attendance at the session of their respective houses, and in going to and returning from the same; and for any speech or debate in either house, they shall not be questioned in any other place. *(U.S. Constitution Article 1, section 6, clause 1.)*

Massachusetts State Senators and State Representatives

No member of the House of Representatives or Senate shall be arrested, or held to bail while going to, returning from, or attending the General Assembly. (Massachusetts Constitution Part 2 C.1 §3 Articles 10 & 11.)

If…	Then
A Senator or Representative, as outlined above, is en route to an official function associated within the scope of their duties:	• Release forthwith; and • Take action at a later date.
OUI or endangering public safety:	• Normal arrest process.

Subject	Number
Special Considerations	**SOC-05**

Elected Officials

Notification

The Troop Commander shall immediately notify the Division Commander and the Office of the Superintendent when any elected or appointed official is arrested or detained for a crime.

Military Personnel

Exceptions To License Requirements

Members shall be aware that Massachusetts General Laws (MGL) c.90, s.5B, s.9B, and s.10 allow several exceptions to license and registration requirements for members of the Armed Forces and their spouses.

References

MA Constitution - Pt. 2 C.1 §3 Articles 10 & 11
MGL c.85, s.2C
MGL c.40, s.22D
U.S. Constitution Article 1, section 6, clause 1
22 USC 254 Diplomatic Relations Act
U.S. Department of State Publication: *"Consular Notification and Access"*
U.S. Department of State Publication: *Diplomatic or Consular Immunity*- Guidance for Law Enforcement and Judicial Authorities (Revised July 2011)
Massachusetts Registry of Motor Vehicles: *Parties to the Road Traffic Convention and the 1943 Inter-American Automotive Traffic Convention*

Promulgated By:

Department of State Police
General Order

Effective Date	Number
July 29, 2014	**SOC-06**

Subject

Administration of Naloxone Hydrochloride (Narcan)

Policy

This policy shall establish protocol for Department members, in order to reduce life-threatening emergency of fatal opioid overdose, where medical professionals are not readily available, by administering naloxone hydrochloride.

Department members shall assist any person who may be suffering from an opioid overdose. Department members trained in accordance with this policy shall make every reasonable effort, to include the use of naloxone combined with First Responder Training, to revive the victim of any apparent drug overdose.

Definitions

Naloxone Hydrochloride or Narcan - An opioid receptor antagonist and antidote for opioid overdose administered in intramuscular, intranasal or intravenous forms. The intranasal form, using prefilled syringes compatible with Mucosal Atomization Device, is permitted for use by first responders under Massachusetts Office of Emergency Medical Services Statewide Protocol Standing Orders.

Mucosal Atomization Device – Used to deliver a mist of atomized medication that is absorbed through the nasal mucosa into a person's blood stream and into the brain and cerebrospinal fluid.

Opioids – Reduce the intensity of pain signals to the brain and affect those brain areas controlling mood, memory, reward and emotion, which diminishes the effects of a painful stimulus, but also can result in addiction. Opioids at high doses reduce the drive to breathe, which can result in inadequate oxygen to the brain and overdose. Medications that fall within this class include hydrocodone, oxycodone, morphine, codeine, and related drugs e.g., heroin potent illicit derived from morphine that is prohibited for medical use in the United States.

Continued next page.

Subject	Number
Dispensing of Naloxone Hydrochloride (Narcan)	**SOC-06**

Definitions (Continued)

Opioid Overdose – An acute condition including but not limited to decreased level of consciousness, respiratory depression, coma, or death resulting from the consumption of an opioid, or another substance with which an opioid was combined, or that a layperson would reasonably believe to be an opioid-related drug overdose that requires medical assistance.

Universal Precautions - is an approach to infection control to treat all human blood and certain human body fluids as if they were known to be infectious for HIV, HBV and other blood borne pathogens.

Training

Department members issued Naloxone Hydrochloride (Narcan), shall:

- Be trained by the Department's Medical Unit on the topic of responding to persons suffering from an apparent opioid overdose and the use of Naloxone Hydrochloride (Narcan); and
- Receive refresher training every two (2) years that may be done in conjunction with First Aid/CPR Training.

Training shall follow recommendations from the Office of Emergency Medical Services (EMS) - Department of Public Health, *Administrative Requirements Manual AR-2-100* as amended.

Issue of Naloxone

Department members who are authorized shall:

- Carry Naloxone Hydrochloride (Narcan) kit with a Mucosal Atomization Device according to EMS Statewide Treatment Protocols;
- Follow Naloxone Hydrochloride (Narcan) and First Responder training conducted by the Department's Medical Unit;
- Store Naloxone Hydrochloride (Narcan) kit with their first aid kits, however, during extreme hot and cold temperatures or when on extended leave, kits should be removed from vehicles and maintained at room temperature (59-86 degree F) away from direct sunlight;
- Report missing, damaged or expired Naloxone Hydrochloride (Narcan) kits to their immediate supervisor;
- Dispose of MAD syringes and Naloxone Hydrochloride (Narcan) vials in a biohazard sharps container; and
- Request replacement Naloxone Hydrochloride (Narcan) kits through channels to the Department's Medical Unit.

Immediate Supervisors shall:

- Document in writing any reports of missing, damaged or expired Naloxone Hydrochloride (Narcan) kits; and
- Forward the documentation through channels to their Division Commander's Office for further action in coordination with the Officer-In-Charge (OIC) of the State Police Medical Unit.

Subject	Number
Dispensing of Naloxone Hydrochloride (Narcan)	**SOC-06**

Use of Naloxone

When dispensing Naloxone Hydrochloride (Narcan) Department members shall:

- Maintain universal precautions;
- Follow training received from the Department's Medical Unit on protocols and procedures for the administration of Naloxone Hydrochloride (Narcan);
- Ensure SP 900 Naloxone Hydrochloride (Narcan) Administration Incident Record is completed for each Naloxone administration and forward through channels to the Department's Medical Unit.

Medical Unit

The Department's Medical Unit shall:

- Ensure Department members receive training in the dispensing of Naloxone Hydrochloride (Narcan) according to EMS and the Statewide Treatment Protocols;
- Authorize and supply members with Naloxone Hydrochloride (Narcan) kits as needed;
- Ensure SP 900 Naloxone Hydrochloride (Narcan) Administration Incident Record is forwarded to the identified Medical Director of the Naloxone Hydrochloride (Narcan) Program; and
- Keep training records of all Department members authorized to dispense Naloxone Hydrochloride (Narcan).

References

105 Code of Massachusetts Regulations (CMR) 171.165
105 Code of Massachusetts Regulations (CMR) 700.003
SP 900 Incident Report for the Administration of Naloxone Hydrochloride (Narcan)
Office of Emergency Medical Services(EMS)- Department of Public Health: *Administrative Requirements Manual AR-2-100 (3/27/2014)*

Promulgated By:

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**SOC-07**

Subject

Domestic Abuse

Policy

The Department shall adhere to the Massachusetts Domestic Violence Law Enforcement Guidelines 2001.

Definitions

Abuse: For the purposes of this policy, abuse is defined by Massachusetts General Laws (MGL) c.209A, s.1 as the occurrence of one or more of the following acts between family or household members:

- Attempting to cause or causing physical harm;
- Placing another in fear of imminent serious physical harm; or
- Causing another to engage involuntarily in sexual relations by force, threat, or duress.

Family or Household Members: Persons who:

- Are or were married to one another;
- Are or were residing together in the same household;
- Are or were related by blood or marriage;
- Have a child in common regardless of whether they have ever married or lived together; or
- Are or have been in a substantive dating or engagement relationship, including same sex relationships.

Response

Domestic abuse situations are considered a high priority and require that members immediately respond to the scene. Notifications shall be made to the department of jurisdiction as appropriate with an offer made of Department assistance.

The State Police Detective Unit (SPDU) of jurisdiction shall be notified of all domestic abuse cases involving serious bodily injury or injury which results in a death.

Continued next page.

Response (Continued)

Position	Duties
Desk Officer /Dispatcher	• Whenever possible, two (2) members should be dispatched to the scene; • Provide available information as requested: 1. Existence of any warrants or protective orders, or record of criminal history; 2. Any other relevant information of prior incidents or likelihood of firearms being present; and 3. Record of Firearms Identification Cards and/or Licenses To Carry Firearms issued to resident(s); and • Notify the Troop Duty Officer. Note: A response shall not be terminated based on a follow-up call from the complainant.
Responding Member(s)	Whenever there is reason to believe that a family or household member has been abused, or is in danger of being abused, members shall: • Arrest the abuser where probable cause exists; • Request medical treatment if appropriate; • Activate the Emergency Judicial Response System (EJR); • Remain on the scene; • Immediately provide the abuse victim with copy of a SP 500 Abused Persons Notice of Rights; • Assist victim and dependent children to a safe place; • Provide referral information for programs, shelters, and counseling to victims; and • Inform victim that abuser may be eligible for bail.

Supervisor Responsibilities

Supervisors shall ensure the provisions of MGL c.209A, as well as these guidelines, are adhered to:

- That an incident report has been filed, even in cases where no arrest was made; and
- That calls which are received as allegations of domestic abuse or a domestic disturbance are not reclassified because no probable cause to arrest existed. Incident reports shall be filed in those cases as well.

If upon review of an incident report, it is believed that probable cause exists, the supervisor shall:

- If required, ensure that a follow-up investigation is conducted;
- Ascertain that appropriate referrals are provided to the victim; and
- Ensure that criminal charges are initiated according to MGL c.209A.

Notice of Rights

The investigating member shall immediate provide abuse victims with adequate notice of rights. The notice shall consist of:

- Handing the victim a copy of SP 500; and
- Reading the victim their rights.

When the victim's native language is not English, every attempt shall be made to provide the statement in their native language.

Confidentiality

A plaintiff's residential address and workplace address shall appear on the court order and be accessible to the defendant unless the plaintiff specifically requests that this information be withheld from the order.

Members assisting in emergency abuse prevention orders shall be cognizant of victims' confidentiality rights and requests.

Service of Orders

Service of orders shall be made in hand, unless otherwise ordered by the court. Orders shall be:

- Served promptly upon receipt. If service is initially unsuccessful, the Department shall continue to attempt service until it is completed. Service of orders shall not be delayed in order to be served by a specialized officer or unit; and
- Returned to the court promptly.

The victim's safety shall be considered in the timing of the service of the order. Members should encourage the victim to contact an advocate (either through the District Attorney's (DA) Office of jurisdiction, SAFEPLAN, or the local battered women's program) in order to develop a safety plan around the service of the order.

Troop/Station/Section/Unit Commanders shall maintain a record of all attempts at service.

Out of State Orders

Persons who violate out of state abuse orders, or violate Massachusetts abuse orders in another state, may be charged criminally for contempt in the Commonwealth of Massachusetts.

- In assessing probable cause, a member may presume the validity of the protection order issued by another jurisdiction when the member has been provided with:
  1. A copy of the order by any source; and
  2. A statement by the victim that such order remains in effect.

A protective order issued in another jurisdiction (as defined in MGL c.209A, s.1) shall be given full faith and credit in the Commonwealth. Therefore, members shall make a warrantless arrest of any person, when the member has probable cause to believe there is a violation of an emergency, temporary or permanent vacate, refrain from abuse, stay away or no-contact order, or judgment issued by another jurisdiction.

Firearms

In domestic abuse incidents, members shall seize all firearms in accordance with SOC-07A Domestic Abuse Arrest/Investigations.

Vacate Orders and Court Orders to Retrieve Belongings

Once a vacate, no contact, stay away, or refrain from abuse order is issued, members shall not accompany any party to the property without specific judicial authorization. A vacate order may include the following requirement:

- The defendant shall not damage any of the plaintiff's belongings, or those of another occupant, and shall not interfere with any utilities or mail delivery to the plaintiff.

The defendant in the vacate order may be allowed to retrieve their belongings under the following conditions and shall:

- Have a court order allowing for the retrieval; and
- Not be allowed to use this as a means of harassing the victim.

The victim/defendant shall have prior notice by the Department, and shall agree to the timing of the retrieval.

Note: Members need to keep in mind that certain behaviors by the victim or the defendant, while at the residence, may constitute a violation of the protective order. Repeated visits may also constitute a violation. The purpose of the restraining order is to keep the defendant away from the plaintiff. If the defendant repeatedly returns to collect their belongings, it is defeating the purpose of the protective order.

In cases where one party has a court order that allows them to return to a residence in order to retrieve their belongings, members shall:

- Accompany the victim to ensure the order is executed: and
- Ensure the victim is free from harassment or abuse by the defendant.

Referral Information

Troop/Station/Section/Unit Commanders shall ensure that referral information for programs, shelters, and counseling for victims are identified within their respective jurisdictions and available within the guidebook.

Subject	Number
Domestic Abuse	**SOC-07**

Confidential Programs Locations

A domestic abuse program is defined as any refuge, shelter, office, safe home, institution, or center established for the purpose of offering assistance to victims of abuse through crisis intervention, medical, legal, or support counseling.

The location and street address of all domestic abuse programs are absolutely confidential and shall not be revealed in any criminal or civil proceeding.

Under no circumstances shall law enforcement officers release information to anyone, other than another law enforcement officer or a victim, regarding the location of a domestic abuse program.

References

SOC-07A Domestic Abuse Arrest/Investigations
SP 500Abused Person's Notice of Rights
Massachusetts Domestic Violence Law Enforcement Guidelines 2001 (Revised)
Chapter 164 of the Acts of 2000: An Act Relative to the Crime of Criminal Harassment
MGL c.209A, s.8, as amended by c.236 s.24 of the Acts of 2000.
MGL c.209A
MGL c.233, s.20K
MGL c.233, s.20L
MGL c.265, s.43 Stalking
MGL c.277, s.62B Stalking; jurisdiction

Promulgated By:

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**SOC-07A**

Subject

Domestic Abuse Arrest/Investigations

Policy

The Department shall respond and investigate allegations of domestic abuse while ensuring the rights and safety of all those involved.

Arrest Guidelines

The safety of the victim and any children shall be paramount in any decision to arrest, and in the timing of the arrest. The decision to arrest shall be based on whether or not probable cause exists that the crime occurred, not on whether or not the victim wishes to seek complaints or wishes to testify at a future date.

Mandatory Arrest: Members shall make a warrantless arrest of any person the member witnesses or has probable cause to believe has violated an emergency, temporary or permanent vacate, refrain from abuse, stay away or no-contact order, or a judgment, suspension, surrender and/or a protection order issued by any jurisdiction.

Arrest Preferred: When there are no refrain from abuse, vacate, stay-away, or no-contact orders or judgments in effect, arrest shall be the preferred response whenever a member witnesses or has probable cause to believe that a person has committed:

- A felony;
- An assault and battery of a family or household member in violation of Massachusetts General Laws (MGL) c.265, s.13A;
- A misdemeanor involving abuse, as defined in MGL c.209A;
- An assault and battery or permits another to commit an assault and battery upon an elder or a person with a disability in violation of MGL c.265, s.13K;
- An assault and battery with or without a dangerous weapon on an individual under the protection of an abuse prevention order, as defined in MGL c.265 s.13A(b)(iii) and 15A(c)(iii); or
- An assault on an individual who is known to be pregnant, or there is reason to know is pregnant.

Continued next page.

Subject	Number
Domestic Abuse Arrest/Investigations	**SOC-07A**

Arrest Guidelines (Continued)

When probable cause to arrest exists and the suspect has fled the scene, the member shall:

- Have the Desk Officer/Dispatcher advise area patrols and all local police departments as appropriate;
- Attempt to make a warrantless arrest; and
- Seek an arrest warrant from the appropriate court, as soon as possible.

A statement from a police department that probable cause to arrest exists shall be honored by another police department. When probable cause exists to believe a crime involving abuse occurred, members shall not advise the victim to seek complaint applications on their own.

Investigations

Members responding to domestic abuse calls shall follow the guidelines established in SOC-07 Domestic Abuse and ensure an investigation includes:

- Information about the suspect's ownership, access to, or presence of any firearms, and their location;
- Relationships of all parties at the scene, including names and DOB of children present, or those in the household;
- The phone number of the victim's residence and include the number within the incident report so the bail bondsman or court personnel may inform the victim of the defendant's release on bail; and
- Informing the victim that if they intend to leave the residence, and desire to be informed of the abuser's release on bail, they must provide a contact number.

Members shall be aware that thorough documentation of the crime scene condition is critical to the prosecution.

Defendant Information

Members shall provide information regarding a defendant's dangerousness to the Prosecutor for use at arraignment such as:

- Criminal history;
- Restraining, no-contact or other protective orders currently in effect against the suspect;
- Possession of, or past use of weapons;
- Threats of serious physical harm against the victim, other family members, or pets; or
- Attempts or threats to commit suicide.

Arrest of a Caretaker

In cases involving abuse of a child, a person with a disability, or an elder, members shall:

- Address the issue of whether or not the victim can be left alone safely, if the abuser is arrested; and
- Contact the respective protective agency in order to arrange for temporary care, if the child, person with a disability, or the elder cannot be left alone.

In situations involving allegations of abuse of children, the disabled, or the elderly refer to SOC-07C Abuse of Children/Disabled/Elderly.

Subject	Number
Domestic Abuse Arrest/Investigations	**SOC-07A**

Substantive Dating Relationship

Members shall gather enough information to determine whether or not a substantive dating relationship exists and examine the following factors when making this determination:

- The length of time of the relationship;
- The type of relationship;
- The frequency of interaction between the parties; and
- If the relationship has been terminated by either person, the length of time that has elapsed since the termination of the relationship.

If it is determined that a substantive dating relationship exists or did exist, then the member shall:

- Take proper action, including arrest when appropriate, regardless of whether the victim seeks a restraining order.

In cases where there is no substantive dating relationship, another crime such as stalking or criminal harassment, may have been committed.

Dual Arrests

Dual arrests, like the issuance of mutual restraining orders, are strongly discouraged because they trivialize the seriousness of domestic abuse and increase the danger to victims. In the majority of cases, an effective investigation will reveal the dominant aggressor. Members shall:

- Attempt to identify the dominant aggressor bearing in mind the difference between offensive and self-defense injuries; and
- Take action based on that determination.

A member arresting both parties is required by law to submit separate and detailed arrest reports indicating the basis for the dual arrest.

Members investigating an incident of domestic violence shall not discourage requests for law enforcement intervention by threatening, or otherwise indicating all parties will be arrested.

Incident Reports

Incident reports shall be made whether or not an arrest results. Upon request to the Department, reports shall be made available to the victim at no cost. Prosecution and subsequent legal action can be greatly aided by documentation and description of:

- Physical injuries; and
- Photographs of the injuries.

Members shall note the presence of children in the household and other information gained through the investigation.

Subject	Number
Domestic Abuse Arrest/Investigations	**SOC-07A**

Confidentiality

The Department shall ensure the confidentiality of domestic abuse victims by safe guarding certain information including, but not limited to:

- Information regarding the identity of a victim or children;
- Any medical information;
- Statement by witnesses; or
- Keeping a separate record of the victim's address and phone number, if the victim will be seeking to hide from the abuser.

Victims of domestic abuse have a strong privacy interest in this type of information whether contained in the initial incident report or supplemental reports. Domestic abuse reports shall only be released to the victim and the District Attorney's Office of jurisdiction. Any other requests for a domestic abuse report shall be forwarded to the Department's Legal Section.

Firearms

Firearms at the scene of a domestic abuse incident.

If...	Then...
The responding members are informed that a firearm or weapon has been involved in the dispute	• Seize the weapon as evidence of the crime.
The weapon is not reported to have been involved in the dispute	• Request that the firearm or weapon be placed in the Department's custody temporarily.

A consent search is permitted by law in all jointly controlled or accessible areas. Members shall:

- Take temporary custody of the firearm or weapon to alleviate the threat of serious violence; and
- Ascertain whether a firearm is lawfully possessed.

If the member determines that the weapon cannot be seized, then:

- A judge can order the defendant to surrender all firearms, and their Licenses To Carry (LTC) Firearms including their Firearms Identification Card (FID); or
- The issuing authority may revoke or suspend the LTC or FID, which would then allow for the seizure of the firearms.

In all domestic abuse cases, the investigating member shall advise the licensing authority that the subject of the license is suspected of abuse. Notice may be made by mailing or faxing a copy of the incident report to the local licensing authority after authorization from the Department's Legal Section.

Continued next page.

Subject	Number
Domestic Abuse Arrest/Investigations	**SOC-07A**

Firearms (Continued)

Abuse Prevention Orders
Upon issuance of any order under MGL c.209A Abuse Prevention Orders, members shall:

- Immediately take possession of all firearms, rifles, shotguns, machine guns, and ammunition, including any LTC and FID, owned or controlled by the subject of the order; and
- Ensure that the order has been completely vacated prior to returning weapons and permits.

Violations of Orders
In the interest of immediacy and the statutory mandate to arrest, members shall:

- Make a warrantless arrest of any person the member witnesses or has probable cause to believe has violated an order, including a violation which stems from the possession of weapons.

Seizure and Storage of Firearms
Every department within the Commonwealth shall honor another department's request for assistance in seizing the above listed items regardless of which department is named within the order. The department named within the order shall be responsible for the storage of the seized items or the delegation of storage to an authorized facility.

Orders Against Law Enforcement Officers
In cases involving police officers that are defendants in Abuse Prevention Orders, the defendant must relinquish all firearms, including departmental weapons, to the department serving the order.

Federal Firearms Provisions

The Colonel/Superintendent shall be notified whenever a member identifies a case involving certain circumstances of which federal action can be taken. Members shall be cognizant of the following federal provisions:

Persons Named in Protective Orders
Under the Federal Crime Control and Law Enforcement Act of 1994, it is unlawful for an individual subject to a permanent restraining order involving intimate partners to receive, ship, transport, or possess guns (including handguns, rifles, and shotguns) or ammunition, that traveled through interstate commerce.

Misdemeanors Involving Domestic Violence
Under 18 USC s.922(g)(9), it is unlawful for any person convicted of certain misdemeanor crimes involving domestic violence to ship, transport, possess, sells, or otherwise dispose of, or receive firearms or ammunition.

Federal Felon in Possession Of A Firearm
Under 18 USC s.922(g)(1), "Felon in possession of a firearm," it is unlawful for any person who has been convicted in any court of a crime punishable by imprisonment for a term exceeding one year to possess any gun or ammunition.

Property

The relationship of the parties and their property interests complicate domestic abuse situations. When a party to a domestic dispute is accused of removing, or attempting to remove property from the dwelling, or is accused of damaging or destroying property, the member shall:

- Conduct an investigation to determine the civil or criminal consequences; and
- Take appropriate action if criminal (e.g. malicious destruction of property).

Police Officers from Other Jurisdictions

In cases involving police officers from other jurisdictions, the investigation shall follow the guidelines established within this policy and SOC-07. The supervisor shall:

- Immediately notify the OIC of the employing department;
- Ensure information is entered into the RAMS system, the Daily Administrative Journal and other appropriate reports;
- Secure the local weapon until returned to the involved Department; and
- Forward a copy of the report to the Chief of Police of the involved officer, through the Department's Legal Section

References

SOC-07 Domestic Abuse
SOC-07B Domestic Abuse Involving MSP Members
SOC-07C Abuse of Children/Disabled/Elderly
MGL c.209A, s.6(7).
MGL c.265, s.13A
MGL c.265, s.13K
MGL c.265, s.15A

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 17, 2013	**SOC-07B**

Subject

Domestic Abuse Involving Members

Policy

The Department shall ensure that all reports of alleged domestic abuse by members are thoroughly investigated.

The Department shall respond and investigate allegations of domestic abuse while ensuring the rights and safety of all those involved.

Involved Member

Any member, upon being notified that they are a defendant in any protective order or modification thereof, or upon becoming aware that they have been accused of abuse, shall:

- Immediately notify their duty assignment supervisor (pursuant to Rules and Regulations), naming the investigating department, if any;
- Surrender Department issued License To Carry (LTC) Firearms and/or weapons and any other state or federal firearms licenses to the responding supervisor; and
- Within twenty-four (24) hours, make written notification, through channels, to their Division Commander. A copy of the protective order or modification shall also be attached to the documentation.

Responding Member

All members responding to incidents of alleged domestic abuse involving members of the Department shall:

- Take immediate action to ensure the safety of the victim;
- Call a supervisor of higher rank than the involved member to the scene;
- Remain on the scene until relieved by the responding supervisor;
- Ensure that all provisions of Massachusetts General Laws (MGL) 209A are followed, including arrest, when necessary; and
- Submit a detailed report of observations and statements made, prior to the end of their shift.

Subject	Number
Domestic Abuse Involving Members	**SOC-07B**

Responding Supervisor

Whenever a member is alleged to have committed abuse, a supervisor of higher rank than the accused member shall be assigned to conduct a criminal investigation. When a protective order is issued, or when the supervisor has reason to believe that the member committed abuse, the supervisor shall immediately:

- Relieve the accused member from duty;
- Seize all Department issued use of force weapons, pursuant to Departmental Rules and Regulations;
- Seize all other firearms and/or weapons at the scene;
- Seize member's LTC, and any other state or federal firearms licenses;
- Notify the member's Troop/Section Commander;
- Seize Department issued vehicle and conduct a vehicle inventory;
- Identify outstanding protective orders against the accused member;
- Ensure that all provisions of MGL 209A are followed, including arrest and further investigation, when appropriate;
- Forward LTC and any other state or federal firearms licenses to the Administrative Investigator;
- Complete an incident report prior to the end of their shift and forward to the Troop/Section Commander; and
- Ensure the complaint has been documented in a To/From format and fax to the Division of Standards and Training (DST) prior to the end of their shift.

Division Commander's Responsibilities

When an abuse prevention order is issued, or when there is reason to believe that the member committed abuse, the Division Commander shall:

- Assign a Commissioned/Staff Officer to conduct an administrative investigation;
- Immediately ensure that the accused member is or has been relieved from duty pursuant to Departmental Rules and Regulations;
- Convene a Duty Status Hearing, pursuant to Department Rules and Regulations; and
- Review reports and initiate additional investigations as necessary.

Administrative Investigation

In all incidents where a member has been accused of abuse, a thorough administrative investigation shall be conducted by a Commissioned/Staff Officer, preferably of higher rank than that of the accused member. The investigation shall include, but not be limited to the following:

- Identify all outstanding and expired protective orders against the accused member;
- Collect and review all reports, affidavits, and records pertaining to the allegations of abuse; and
- Interview the victim and other witnesses.

Other duties of the Administrative Investigator include:

- Working with the criminal investigator (if any) to ensure that the provisions of MGL 209A are adhered to, including criminal action or arrest when appropriate;
- Ensuring appropriate referral information has been given to the victim regarding battered women's programs, emergency shelter, counseling services, and court based advocacy services;
- Forwarding all available documents to the Duty Status Board;
- Attending all court proceedings and maintaining contact with any assigned prosecutor or probation officer; and
- Forwarding copies of all reports to the Internal Affairs Section upon completion of the investigation.

Division of Standards and Training

In domestic abuse cases involving Staff Officers, the DST Commander shall notify the Colonel/ Superintendent.

Subject	Number
Domestic Abuse Involving Members	**SOC-07B**

Complaint Notification to DST

In addition to any other required reports, all complaints of domestic abuse involving members shall be documented and submitted to the Division of Standards and Training (DST).

Member	Action
Member Receiving Complaint	**Internal Complaints** Internal personnel complaints originating within the Department, shall: • Be documented in a To/From format; • Faxed to the Division of Standards and Training within twenty-four (24) hours from the date of the To/From; • Submit a copy through channels to the appropriate Troop/Section/Unit Commander; and • Forward the original copy to the Division of Standards and Training.
Administrative Investigation	The Commissioned/Staff Officer conducting the administrative investigation shall: • Document the complaint in a To/From: • Fax to DST at 508-820-2149 within 24 hours of receipt; • Forward a copy through channels to the appropriate Troop/Section/Unit Commander; and • Forward the original to DST.

References

ADM-14 Personnel Investigation
SOC-07 Domestic Abuse
SOC-07A Domestic Abuse Arrest/Investigations
SOC-07C Abuse of Children/Disabled/Elderly
Rules and Regulations
SPAM Collective Bargaining Agreement Article 27

Promulgated By:

Department of State Police
General Order

Effective Date	Number
July 22, 2014	**SOC-07C**

Subject

Abuse of Children/Disabled/Elderly

Policy

The Department shall investigate all allegations regarding the abuse of children, the disabled, and the elderly, to ensure the safety and rights of all those involved.

Mandated Reporting

Investigating members shall make mandated reports by immediately contacting the designated agency with an immediate oral report, and shall submit a report in writing **within forty-eight (48) hours** after the initial oral report. Members shall contact:

- Department of Children and Families (DCF) whenever they have reasonable cause to believe that a child under the age of eighteen (18) has been abused or neglected shall:
    1. Call to make an oral report Monday-Friday during the hours of 9:00 A.M. to 5:00 P.M. to the nearest DCF Office found at the bottom of the revised DCF form *"Report of Child(ren) Alleged to be Suffering from Serious Physical or Emotional Injury by Abuse or Neglect"*; or
    2. Call to make an oral report after 5:00 P.M. Monday-Friday and twenty-four (24) hours on weekends and holidays to the Child-At-Risk-Hotline 1-800-792-5200; and
    3. Submit the written report by either by mail or fax within forty-eight (48) hours to DCF. To assist in the written notification of child abuse/neglect, DCF has establish a form *"Report of Child(ren) Alleged to be Suffering from Serious Physical or Emotional Injury by Abuse or Neglect"*. This form can be obtained from DocuShare under Bulletins or from the DCF website: www.mass.gov/dcf .
- Disabled Persons Protection Commission whenever they have reasonable cause to believe that a caretaker has abused/neglected a disabled person, between the ages of eighteen (18) and fifty-nine (59). At any time call (800) 426-9009.
- Executive Office of Elder Affairs whenever they have reasonable cause to believe that someone age sixty (60) or older has been abused/neglected. At any time call (800) 922-2275.

Subject	Number
Abuse of Children/Disabled/Elderly	**SOC-07C**

Notifications

Troop Duty Officers shall notify the State Police Detective Unit of jurisdiction in cases where abuse of children, the disabled, and/or the elderly involve serious bodily injury or results in death.

Arrest of a Caretaker

In cases involving abuse of a child, a disabled person, or an elderly person, members shall:

- Address the issue of whether or not the victim can be left alone safely, if the abuser is arrested; and
- Contact the respective protective agency in order to arrange for temporary care, if the child, the disabled person, or the elderly person cannot be left alone.

References

SOC-07 Domestic Abuse
SOC-07A Domestic Abuse Arrest/Investigations
SOC-07B Domestic Abuse Involving MSP Members
MGL c.119, s.51A
MGL c.19C, s.10.
MGL c.19A, s.14-26.
Department of Children and Families (DCF) *"Report of Child(ren) Alleged to be Suffering from Serious Physical or Emotional Injury by Abuse or Neglect"*

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 28, 2019	**SOC-09**

Subject

Terrorism/WMD Incidents

Policy

The preservation of life and the prevention of injury shall be recognized as high priorities in responding to terrorist incidents, including those involving Weapons of Mass Destruction.

Terrorism

Terrorism is the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

WMD

Weapons of Mass Destruction (WMD) can be chemical, biological, radiological, nuclear or explosive (CBRNE) weapons that have potential for creating mass casualty incidents.

SP 2810 Form

All Members shall keep a copy of the SP 2810 Crime Scene Threat Assessment Worksheet folded inside the Emergency Response Guidebook in their cruiser. Copies of SP 2810 shall be maintained at each Department facility or within the Emergency Response Guidebook to be accessible to Desk Officers and Troop Duty Officers.

Responding Members

When…	Then…
Responding to routine calls for service:	• Respond with due caution; callers may lack a complete understanding of the situation and may not convey the existence of on-scene hazards.
There is the potential that a terrorist or WMD event is occurring:	• Ensure the safety of all responders and the public; and • When possible, review SP 2810 and relay pertinent information to the Desk Officer.
Relaying information from the SP 2810:	• Utilize the most secure channel of communication at your immediate disposal; and • If it is necessary to relay information via radio, request a Code 1.

Continued next page.

Subject	Number
Terrorism/WMD Incidents	**SOC-09**

Responding Members (Continued)

When…	Then…
On-scene hazards threaten life or health:	• The preservation of life and the prevention of injury shall be of the highest priority.
Members inadvertently encounter a potentially contaminated area:	• Avoid contact; • Minimize exposure; • Never purposefully touch, taste or smell any object, package, or container, etc; • Warn others; • If possible, isolate area; and • Stay upwind and uphill.
Issues arise concerning the crime scene or the securing of evidence:	• Contact the Troop Duty Officer for guidance.

Desk Officer

If…	Then…
A report is received involving a potential terrorist or WMD event:	• Transmit the most detailed information possible to all responding members; and • Relay all available information from the scene to the Troop Duty Officer, assigned patrols, local police, and fire departments.

Troop Duty Officer

If…	Then…
A report is received involving a potential terrorist or WMD event:	• Relay all available information from the scene to GHQ Communications and the Troop Commander (who shall contact the Division Commander); • Contact the local fire department to activate Department of Fire Services-Regional Hazardous Materials Team (877)385-0822; • Contact the Department State Police Detective Unit (SPDU) of jurisdiction; and • Ensure that the area hospitals are advised.
The incident involves a suspected explosive device or a suspicious package:	• Contact the Bomb Squad; and • Refer to SOC-02 Bomb Threat/Explosives Incidents.

Continued next page.

Subject	Number
Terrorism/WMD Incidents	**SOC-09**

Troop Duty Officer (Continued)

If…	Then…
The incident involves a hazardous material:	• Contact the local fire department to activate Department of Fire Services-Regional Hazardous Materials Team (877)385-0822; and • Refer to SOC-01 Hazardous Materials.
Issues arise concerning the crime scene or the securing of evidence:	• Contact the SPDU of jurisdiction; and • The Division of Investigative Services (DIS) representative shall be designated the officer-in-charge.

GHQ Communications Section

If…	Then…
A report is received involving a potential terrorist or WMD event:	In addition to duties required by other written directives, the GHQ Communications Section shall notify: • The Office of the Superintendent; • The Division of Investigative Services and Field Services Commanders; • Media Relations; • The Commonwealth Fusion Center; • Massachusetts Emergency Management Agency (MEMA); and • Department of Fire Services-Regional Hazardous Materials Team; and • The National Guard Civil Support Team, if needed.
The incident involves a suspected explosive device or a suspicious package:	• Contact the Bomb Squad; and • Refer to SOC-02 Bomb Threat/ Explosives Incidents.
The incident involves a hazardous material:	• Contact the local fire department to activate Department of Fire Services-Regional Hazardous Materials Team (877)385-0822; and • Refer to SOC-01 Hazardous Materials.

Subject	Number
Terrorism/WMD Incidents	**SOC-09**

DIS

If...	Then...
A preliminary investigation into a reported potential terrorist or WMD event reveals a hoax or an unsubstantiated incident:	• The Division of Investigative Services shall prepare an after action report within forty-eight (48) hours in order to make use of "lessons learned."

References

SOC-01 Hazardous Materials
SOC-02 Bomb Threat/ Explosives Incidents
SP 2810 Crime Scene Threat Assessment Worksheet
U.S. Department of Transportation Emergency Response Guidebook

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 28, 2019	**SOC-10**

Subject

Clandestine Drug Laboratory Response

Purpose

To define the role of the Clandestine Laboratory Enforcement Team (CLET) and establish guidelines for the utilization and activation of team members.

Policy

The Department recognizes the inherent dangers of clandestine drug laboratories and sets forth the following procedures to be followed by all Department members. These procedures are in compliance with Federal Occupational Safety and Health Administration (OSHA) Standards and are designed to limit dangers to Department members and the public.

Definitions

Clandestine Lab (Clan Lab): The operation at any location consisting of chemicals, mixtures, or processes designed or intended to synthesize, extract or convert illegal or controlled substances to include but not be limited to:

- Methamphetamine, Ecstasy, LSD, Fentanyl, THC and other illegal drugs.

Clandestine Laboratory Enforcement Team (CLET): A multi-agency team of law enforcement officers and certified chemists who have completed the Drug Enforcement Agency (DEA) Basic Clandestine Laboratory Certification School.

Site Safety Officer: A CLET member who has completed the DEA Advanced Site Safety School. The Site Safety Officer is responsible for the safe operation and adherence to DEA procedures at clan lab sites.

Utilization of CLET

CLET is available when requested, to assist members from the Department and those from other local, state, and federal agencies for:

- Known or suspected clan labs or their investigations;
- Execution of search warrants at clan lab locations;
- Training personnel relative to clan labs; and
- Other special events as assigned by the Commander of the Division of Investigative Services or designee.

Subject	Number
Clandestine Drug Laboratory Response	**SOC-10**

CLET Activation Protocol

Requests for CLET services shall be made to the Troop Duty Officer and shall include:

- The name, rank, and agency name of the requesting officer;
- The name of the primary point of contact and a call-back number;
- The nature of the request; and
- The exact location of the incident and any designated staging areas.

The Troop Duty Officer shall contact:

- the Department's CLET Leader, or designee; and
- the on-call member of the State Police Detective Unit of jurisdiction.

The CLET Leader, or designee, shall:

- Assess the situation;
- Activate the necessary Department's CLET members, to include the Department's chemists, and
- Contact the DEA CLET Coordinator.

Note: The CLET Leader shall maintain the current list of certified CLET members.

Activation/ Contact Number

During business hours: contact MSP Fire and Explosion Investigation Unit (978)567-3310.

After business hours: contact Troop Duty Office.

Authority

No member of the Department shall enter a known/suspected clan lab site unless:

- Authorized by a CLET Site Safety Officer; or
- Imminent or immediate danger exists to others.

CLET members shall assume complete control and authority of all identified clan lab sites.

While engaged in clan lab operations, CLET members shall take direct orders only from the:

- CLET Leader or designee;
- Site Safety Officer;
- DEA Clan Lab Coordinator;
- Division of Investigative Services Commander or designee; or
- Colonel/Superintendent.

Subject	Number
Clandestine Drug Laboratory Response	**SOC-10**

Operational Protocols

Department Members

Department members who discover or are advised of a suspected clan lab shall:

- Immediately notify the Troop Duty Office;
- **NOT** attempt to touch, turn off, adjust or otherwise manipulate any switches, controls or other materials within the suspected clan lab;
- Secure the area around the suspected clan lab and remain at a safe distance from the lab; and
- Remain on the scene until properly relieved.

CLET Leader

The CLET Leader, or designee, after assessing the situation, shall determine the need for additional resources including, but not limited to:

- Local Fire Department(s);
- MSP Bomb Squad;
- Department of Fire Services Hazardous Materials Team;
- Emergency Medical Services (EMS); and
- Traffic mitigation and controls.

CLET Members

CLET members shall:

- Assist and advise on-scene Incident Commander by recommending actions, coordinating resources, and/or providing appropriate documentation related to an on-going incident; and
- Provide assistance by coordinating internal or external agency resources that can be utilized to respond, mitigate, and/or recover from an incident in accordance with Incident Command System (ICS) protocols.

The Site Safety Officer shall coordinate and work with Department and CLET members from other agencies to respond to mitigate and recover Clandestine Drug Laboratory scenes in accordance with CLET Standard Operating Procedure (SOP).

Evidence Considerations

The collection of evidence, contraband and materials shall be coordinated by CLET members in consultation with chemists (either state or federal).

The Department member or local officer who is the case officer shall ensure evidence preservation and custody.

Subject	Number
Clandestine Drug Laboratory Response	**SOC-10**

After Action Reporting

Following the completion of any critical incident, CLET members shall conduct a debriefing.

The CLET Leader, the Site Safety Officer, or designee, is responsible for the completion of any after action reports or CLET reporting as applicable. After Action Reports shall be forwarded to the Division of Investigative Services Commander or designee for review.

References

29 CFR 1910.120 Occupational Safety and Health Administration Standard

Promulgated By:

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**SUP-01**

Subject

Jurisdiction/Mutual Aid

Policy

The Department shall ensure that its members are informed of the limits of their police authority and shall work in cooperation with other law enforcement agencies.

Jurisdiction

The Department has sole and/or concurrent jurisdiction within the territorial boundaries of the Commonwealth.

Limits on Jurisdiction

No member may be used or called upon for service at any industrial dispute unless actual violence has occurred therein, and then only by written order of the Governor.

Members shall not exercise police powers on a reservation or other property of the United States of America unless requested by the person in charge of the reservation or property.

Members have no police powers in any Massachusetts Correctional Institution (MCI) facility, except by direction of the principal officer.

New England State Police Administrators Compact

The Commonwealth of Massachusetts has entered into a mutual aid agreement with State Police agencies in adjoining states. The agreement, known as the New England State Police Administrators Compact (NESPAC), provides for:

- Cooperation and assistance in detecting and apprehending those engaged in criminal activity;
- Establishing and maintaining an information sharing system to be accessed by participatory agencies;
- Mutual aid and assistance in the event of police emergencies; and
- The granting of powers, duties, rights, privileges, and immunities of police personnel when rendering such aid.

Requests for Mutual Aid

When approved by the Colonel/Superintendent, Department personnel or other resources may be provided at no cost to other law enforcement agencies.

Continued next page.

Subject	Number
Jurisdiction/Mutual Aid	**SUP-01**

Requests for Mutual Aid (Continued)

When any other law enforcement agency requests mutual aid from the Department, the initial request should contain:

- Nature and duration of the request;
- Contact information for requesting department's officer-in-charge (OIC); and
- Expenditures, if any, which shall be borne by the requesting agency.

The Troop/Section/Unit Commander or designee shall be responsible for determining which personnel shall be dispatched to the incident while maintaining adequate Department services within their command.

Requests by the Department

In the event of an unusual, natural, or man-made emergency situation, the Colonel/Superintendent shall request authorization from the Executive Office of Public Safety and Security:

- To seek assistance from any appropriate state agency;
- To seek assistance from the Massachusetts National Guard; and
- To grant personnel from outside the Department powers as a State Police Officer.

State of Emergency

Upon declaration of a "State of Emergency" by the Governor, all members (excluding personnel on suspension, injury, or other approved leaves) shall immediately contact their duty assignment supervisor, or other supervising officer within their chain-of-command, for specific instructions.

After Action Reporting

The Commanding Officer/OIC rendering assistance shall make a complete and accurate accounting which shall include, at a minimum:

- Number/names of members assigned, and time expended;
- Specific action taken; and
- Equipment utilized.

The Colonel/Superintendent may require a Division Commander or a Troop Commander to complete an After Action Report on significant incidents to determine if:

- Established Rules & Regulations, Policies & Procedures, orders and directives were followed;
- Available resources (personnel, equipment, etc.) were utilized in the most effective and efficient manner possible;
- Whether there is any deficiency or inadequacy in training, supervision, or policy which needs correction, enhancement, or adoption; and
- Conclusion(s), opinion(s), and recommendation(s).

Promulgated By:

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**SUP-03**

Subject

Media Relations

Policy

The Department shall provide the media and the public with information on Department operations and administration, ensuring that individual rights are protected.

Dissemination of Information

Employees shall treat official business of the Department as confidential. Information shall only be disseminated according to established procedures. Employees shall not:

- Disseminate information in violation of Rules and Regulations; or
- Disseminate information prohibited by this policy.

Driver's Privacy Act

The release of information obtained through any state motor vehicle database shall not be released to non-law enforcement personnel.

Significant News or Events

The Office of the Colonel/Superintendent or Media Relations shall be the authorized source for the dissemination of all press releases.

When a member is involved in an incident or significant event that may be considered of interest to the public, the member or the Desk Officer shall contact Media Relations to provide the necessary information.

Examples of such incidents or events may include, but are not necessarily limited to:

- A significant arrest or investigation;
- Search or rescue;
- Motor vehicle crash with fatal or life-threatening injuries; or
- Large scale law enforcement operation.

Any inquiries from the media about such types of incidents shall be referred to Media Relations.

Media Relations

Troop/Section/Unit Commanders shall assist Media Relations with:

- Coordinating news conferences;
- Preparing and conducting news releases in the absence of a Media Relations member; and
- Positive news stories involving the Department.

Information for Dissemination

Information generally appropriate for members to disclose to the media and the public includes:

- Typical crash information:
  1. Names of the occupants involved, if over eighteen (18) years of age;
  2. Cause of crash if known; and
  3. Degree of injuries- minor, serious, or no injuries occurred.
     Note: Do not give out specific injuries of any occupant due to privacy rights.
- Road and weather information;
- Information from the public log (except for prohibited information as outlined within this policy);
- The time and place of arrest;
- An arrested adult's name, age, town, charges and bail status; and
- The name and rank of the investigating and arresting members (except for undercover officers), assisting agencies and the length of the investigation.

Division/Troop/Section Commanders shall:

- Approve, coordinate and/or release information concerning confidential investigations, operations, and emergency/crisis situations to Media Relations.

It is preferred that the Office of the Attorney General (AG), District Attorney (DA) Offices, the Office of the State Fire Marshal (OSFM), or other outside agencies generate news releases regarding a crime or arrest of concern to that specific office, in coordination with Media Relations, when members of the Department are involved.

Members assigned to the AG, DA, OSFM, or other agencies shall:

- Not become unilaterally involved in media relations efforts unless approved by the Office of the Colonel/Superintendent or Media Relations.

If the AG, DA, OSFM, or other agencies choose not to make a news release, Media Relations may do so when authorized by the Office of the Superintendent.

Media Interviews

Media interviews shall be conducted by the highest ranking or most experienced member on-duty in the order of:

- Media Relations;
- Troop/Section/Unit Commander;
- Troop/Section/Unit Duty Officer; or
- A Supervisor, with training or experience in giving interviews.

Note: Troopers shall not be compelled to do television or radio interviews against their wishes.

Continued next page.

Media Interview (Continued)

After consultation with Media Relations personnel, members may give limited interviews:

- To accredited news personnel at the scene of a vehicle crash or criminal incident, if there is no interference to the ongoing investigation; or
- Concerning information regarding road and weather conditions.

Members shall wear the uniform of the day, including the appropriate cover. Members working in a plain clothes assignment shall be appropriately dressed.

All other interviews shall be approved/coordinated through Media Relations.

Prohibited Information For Release

Employees **shall not** release or give out information on:

- The prior criminal records or driver's history of a person, or the existence or nonexistence of a prior criminal record except:
  1. To other federal, state, or municipal law enforcement agencies as authorized by the Criminal Offender Record Information (CORI) laws; or
  2. To warn the public of imminent danger from such a person; or
  3. In connection with serious or violent offenses, to expedite the location and apprehension of such a person.
- The identity of a deceased victim before confirmation has been received that the next of kin has been notified according to ADM-13 Notification of Medical Examiner and/or Next of Kin;
- The name or address of a juvenile (refer to INV-05 Juvenile Operations for definition) who is a suspect, defendant, complainant, or victim;
- The name or biographical information of the victim of a sexual crime;
- The name or photograph of an undercover officer;
- The existence or contents of any confession, admission, or statement given by a suspect, however, it may be stated that the defendant denies the charges. Note: This does not apply to statements made by the defendant to representatives of the news media or general public;
- Opinions about the guilt, innocence, character, or reputation of a suspect;
- Statements predicting or influencing the outcome of the trial;
- The results, refusal, or failure to submit to any examinations or tests;
- Statements or opinions concerning the credibility or testimony of prospective witnesses;
- Information that may adversely affect an investigation or prosecution of a case;
- Information about ongoing litigation;
- Any medical information;
- Causes of death until officially determined by the Medical Examiner;
- Handicapped individuals per MGL c.41 s.98F; or
- Other information as outlined in the Rules and Regulations.

Subject	Number
Media Relations	**SUP-03**

Photographs

The news media may photograph a person in custody. However, members shall not:

- Pose prisoners for news photographs;
- Allow prisoners to be photographed in Department facilities; or
- Allow prisoners to be photographed in other facilities against the wishes of the owner.

Members should not interfere with photographing or televising of a defendant in a public area, unless such activities:

- Interferes with their official duties; or
- Violate a court order.

Media Relations shall be contacted:

- Before the release of any photograph of Department employees; and
- Before the release of any photograph of a suspect or defendant.
  Note: Members shall be mindful that booking photos are considered part of a subject's CORI record and the release of these photos is restricted.

The release of photographs of Department undercover officers shall only be approved by the Colonel/Superintendent or the Deputy Superintendent.

Access to Crime And Crash Scenes

Representatives of the news media shall not be permitted to interfere with investigations or the efficient flow of traffic. However, news media representatives may be:

- Granted access to crime or emergency scenes; and
- Allowed to locate their vehicles and equipment at points nearer to a scene than permitted by normal traffic.

Permission for media access to a scene occurring in a private dwelling or other area generally not open to the public shall:

- Be obtained from lawful authority over the premises including government entities, such as the Turnpike or Port Authority; and
- Be controlled by a supervisor in command of the scene ensuring the particular needs of the investigation take precedence.

Note: Most accredited news reporters and photographers have identification cards that are issued by their respective employer.

References

ADM-13 Notification of Medical Examiner and/or Next of Kin
MGL c.6, s.167-178 (CORI Law)
MGL c.41, s.98F Daily Logs; Public Records
18 USC 2722 Driver's Privacy Protection Act

Promulgated By:

Department of State Police
General Order

Effective Date	Number
July 11, 2011	**SUP-04**

Subject

Employee Assistance Unit

Policy

The Department has a responsibility to ensure the safety of our employees and to contribute to their psychological and physical well-being. The Department shall offer to employees and their families, professional assistance, training, peer counseling, and professional referrals.

Availability

The Employee Assistance Unit (EAU) is available to all Department employees and family members, twenty-four (24) hours a day by calling (978) 975-0794 or the GHQ Communications Section at (508) 820-2121.

Members of the EAU are available:

- To meet employees who request assistance at a mutually acceptable location;
- Provides training to recruit training classes; and
- To provide specialized training upon request.

Responsibility

Employee Assistance Unit members shall:

- Not represent themselves to any third party as the Department's agent for purposes of adjudication, placement or disposition; and
- Not be held responsible for decisions made by any employee receiving EAU services that prove to be in violation of Department rules, regulations, policies, or procedures.

In no event shall a member's involvement with the Employee Assistance Program abrogate their responsibility to conform or comply with rules, regulations, policies and procedures.

Accordingly, and in furtherance of EAU's commitment to recovery and good health, EAU members shall:

- Remind anyone receiving such services that compliance with rules, regulations, policies, and procedures must remain a primary factor in all personal decisions.

Subject	Number
Employee Assistance Unit	**SUP-04**

Confidentiality

It is critical for the success of the Employee Assistance program that confidentiality of case information be maintained. The EAU shall ensure that information obtained from an employee remains confidential, **unless failure to disclose such information could cause a clear and present danger to the safety or security of an individual, the public, or the Department**.

Members of the EAU have the same confidentiality privileges and prohibition on disclosures of information as licensed social workers.

Reports

Written and oral reports shall contain only that information that is pertinent to an ongoing evaluation.

Every effort shall be made to avoid any undue invasion of privacy.

Procedure

Supervisors should remain alert for signs of unhealthy stress in their employees, particularly when involved in a high trauma incident. Reactions to stress may appear immediately after an incident; however, they may not appear for hours, days, or even weeks later.

Supervisors should notify the EAU as soon as possible, but no later than eighteen (18) hours following occurrences of:

- Critical incidents that may evoke extraordinary emotion;
- On or off duty death, serious injury, or serious illness of an employee;
- Unusual death or violence to a child, or a victim known by an employee;
- Use of force incidents involving death or serious injury;
- Fatal accidents involving Department vehicles, or pursuits;
- A prolonged rescue situation that ends in failure; or
- When an employee's work performance appears to be affected by stress.

In any high trauma incident where an employee is affected, or is likely to be affected, supervisors should:

- Assign a support employee, preferably a friend, to the employee for close contact;
- Isolate and remove the employee from the scene of the incident, if possible;
- Ensure against unnecessary repetition of statements and accounts of the incident by the affected employee;
- Assist the employee in preparing the official report; and
- Monitor the employee's condition closely over the following weeks and months for signs of unhealthy stress.

Employees may be referred to the EAU when they may not be aware of the adverse impact, or suppress the need for psychological care.

Subject	Number
Employee Assistance Unit	**SUP-04**

Administrative Leave/ Temporary Modified Duty

Any employee directly involved in a high risk situation that may adversely affect personal or professional conduct may be placed on Administrative Leave or Administrative Duty by the Colonel/Superintendent.

The EAU may recommend members for placement on Temporary Modified Duty as approved by the Colonel/Superintendent. This is a management action used to deal with stress for the individual and the organization, and allows the member to refocus and cope with the situation in a healthy and positive manner.

Commanding Officers shall consult with the EAU prior to the employee resuming regular duties.

References

MGL c.112, s.134, s.135, s.135A, s.135B
Bernard v. Commonwealth**,** 424 Mass. 32 (1996)
ADM-18 Anti-Harassment/Sexual Harassment and Discrimination

Promulgated By:

Department of State Police
General Orders

Effective Date	Number
April 10, 2019	**SUP-05**

Subject

State Police Chaplain Corps

Purpose

To establish guidelines for the responsibilities, organization, and qualifications of chaplains assigned to the Massachusetts State Police Chaplain Corps.

This policy supersedes any previous promulgated Superintendent's Memorandums regarding this subject.

Policy

The State Police Chaplain Corps:

- Is a voluntary support service;
- May assist, but is not intended to replace or impede the efforts of the Department's Employee Assistance Unit and/or the Office of the Ombudsman; and
- Shall provide non-denominational spiritual support and counseling as sought, regardless of gender, ethnicity, religious preference, affiliation, or beliefs.

All members of the State Police Chaplain Corps shall take and affirm an Oath of Office prior to the initial performance of duties.

Oath of Office

I solemnly promise that I will faithfully and diligently perform the duties of Police Chaplain for the Department of the Massachusetts State Police, and that I will provide ministry to the officers of the department and to the citizens of the community as I am called upon.

I will strive to set an exemplary standard of ethical and moral conduct and not use my position of Police Chaplain to proselytize or to gain personal advantage, and will minister to all persons without religious bias.

I will acknowledge those appointed in a position of authority within the department and will serve them with loyalty, and will be supportive of the officers with whom I serve and will be subject to their authority when on duty and will accept the responsibility willingly and without reservation, so help me God.

Subject	Number
State Police Chaplain Corps	**SUP-05**

Requests for Service

The Office of Superintendent shall:

- Coordinate requests for services of the State Police Chaplain Corps with the Director of the State Police Chaplain Corps.

Administrative and Programmatic Oversight

Administrative oversight shall:

- Be conducted by a Commissioned Officer assigned to the Office of the Superintendent.

Programmatic oversight shall:

- Be conducted by the Commanding Officer of the Employees Assistance Unit (EAU) or designee.

Availability

The State Police Chaplain Corps provides services that are available on a twenty-four (24) hour basis for Department employees, when seeking guidance and comfort, or at times of illness, injury, or death.

The Department Chaplains may be contacted through the:

- Communications Center at 508-820-2121;
- Department Telephone Directory; or
- The EAU.

State Police Chaplains shall respond to a critical incident or crime scene when:

- Officially notified by the Department; and
- Render services to only those employees requesting such service.

Upon arriving at a scene, State Police Chaplains shall:

- Immediately identify themselves as a State Police Chaplain, and display the issued Department Identification Card to Officer-In-Charge (OIC) or designee;
- Only enter an active scene when prior approval has been granted from the OIC or designee; and
- As soon as practicable, notify the Commanding Officer of EAU or designee as to such response.

Responsibilities

State Police Chaplains shall be available to provide support and guidance to Department employees. Their duties shall include, but not be limited to:

- Visits to injured or hospitalized personnel;
- Participation at funeral services;
- Provide counseling at the request of an employee;
- Assist in making serious injury or death notifications upon request of the Department;

Continued next page.

Subject	Number
State Police Chaplain Corps	**SUP-05**

Responsibilities (Continued)

- Maintain strict confidentiality of all Department matters;
- Provide follow-up assistance to employees of the Department at times of crisis; and
- Participate in Department functions as requested, (i.e. promotional ceremonies, award ceremonies, etc.).

Designation

The Colonel/Superintendent may designate individuals as State Police Chaplains and shall determine the appropriate number of chaplains.

State Police Chaplains shall serve at the discretion of the Colonel/Superintendent on a voluntary basis and shall not receive compensation.

The Colonel/Superintendent shall designate a Chaplain as Director of the Chaplain Corps to oversee the duties and responsibilities of assigned State Police Chaplains and the program.

Qualifications

Qualifications for State Police Chaplains are:

- Affiliation with a recognized, organized religion;
- Demonstration of sufficient experience in community pastoral and parish work;
- Possession of a Bachelor of Arts and Masters of Divinity degree from an accredited college or seminary;
- Possession of a valid Massachusetts Driver's License and access to a properly registered and insured motor vehicle;
- Successful completion of a background investigation (no individual with a past criminal conviction for any offense shall be designated a Department Chaplain); and
- Attend training(s) as required by the Commanding Officer of EAU.

Director of the Chaplain Corps

The Director of the State Police Chaplain Corps shall:

- Coordinate and monitor the activities of the Chaplain Corps; and
- Conduct bi-annual meetings to share information, discuss goals and objectives, and other issues of interest.

References

Department of State Police *Rules and Regulations*

OFFICIAL:

Kerry A. Gilpin
Colonel/Superintendent

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**SUP-06**

Subject

Binding Written Agreements

Policy

All Memorandum of Understandings, Mutual Aid Agreements, or any other type of binding written agreements (collectively referred to as "MOUs") between the Department and outside organizations, including any state or federal agency, shall only be authorized and signed by the Colonel/Superintendent.

MOU Process

Position	Responsibilities
Troop/Section/Unit Commander	• Carefully review the MOU; and • If approved, forward to their Division Commander.
Division Commander	• Review the forwarded MOU; • Either approve the MOU or recommend changes to the language or terms; • Forward the approved MOU to the Chief Administrative Officer; and • Be responsible for the MOU oversight and renewal.
Chief Administrative Officer	• Review the forwarded MOU; • If need be, return the MOU and supporting documentation to the Division Commander with any recommendations; • Forward a copy of any MOU that pertains to a grant program to the Fiscal Grants Manager and the Strategic Planning Section; and • Forward the approved MOU to the Chief Legal Counsel.

Continued next page.

Subject	Number
Binding Written Agreements	**SUP-06**

MOU Process (Continued)

Position	Responsibilities
Chief Legal Counsel	• Review the forwarded MOU; • Submit the reviewed MOU with any recommendations to the Colonel/ Superintendent; • If approved by the Colonel/ Superintendent forward the MOU to the outside agency for signature; • Return a copy of the approved and signed MOU package to the Division Commander and Chief Administrative Officer; and • Retain all signed original MOU documentation for archives.
Colonel/ Superintendent	• Approve all MOUs involving the Department; and • Return signed MOUs to the Chief Legal Counsel.

Written Agreement Sign-Off Sheet

The SP 480 Written Agreement Sign-Off Sheet shall be:

- Attached to all MOU's;
- Submitted through channels; and
- Signed off by all appropriate employees prior to signature by the Colonel/Superintendent.

Property Inventory

Commanding Officers shall ensure that any property acquired as the result of an MOU shall be inventoried and treated in accordance with ADM-30 Asset Management.

Control and Authority

All MOUs for Department law enforcement services shall clearly identify the nature and extent of services to be provided and shall stipulate that the Colonel/Superintendent maintains control and authority over all Department personnel including, but not limited to:

- Hiring;
- Discipline;
- Transfers;
- Promotions;
- Assignments;
- Training; and
- Dismissal.

Subject	Number
Binding Written Agreements	**SUP-06**

Services Provided

All MOUs shall include provisions for services provided, but not limited to:

- Training;
- Equipment;
- Facilities;
- Functions and activities to be performed; and
- Duties and responsibilities.

Financing and Budget

Fiscal accounting shall be clearly articulated to avoid confusion and misunderstandings and shall include, but not be limited to the following:

- Salaries, indirect costs, and fringe benefits;
- Training and equipment costs;
- Maintenance of cost accounting records;
- Issuance of fiscal reports;
- Time and manner of payment for services; and
- Procedures for the disposition of revenues generated by Department law enforcement activity.

Records

MOUs shall specify the types of records required, the frequency of reporting, and the means for maintaining them.

Duration

All MOUs shall include:

- Effective beginning and termination dates or conditions;
- Procedures for modification or amendment; and
- Procedures for termination, if necessary.

Employee Rights

Participation in any MOU shall not penalize the rights of any Department employee.

References

ADM-30 Asset Management
ADM-47 Grant Approval Process
SP 480 Written Agreement Sign-Off Sheet

Promulgated By:

Department of State Police
General Order

Effective Date	Number
July 11, 2011	**SUP-12**

Subject

Office of the Ombudsman

Policy

The Ombudsman Program provides a confidential, neutral, and informal process to help resolve work-related issues. It is a dispute resolution system that offers employees formal and informal options for addressing work-related problems and concerns. Although the program is an alternative channel of communication, it is designed to complement, not replace or circumvent the Department's formal resolution options.

Definitions

Confidential Communications: Communications, or a source of communication, which are intended to be held in secret.

Privileged Communications: Communications that occur in a context of legal or other recognized professional confidentiality.

Office of the Ombudsman

The Office of the Ombudsman reports to the Colonel/Superintendent. The primary role of an Ombudsman is to act as a designated neutral in order to facilitate fair and equitable resolutions regarding work-related problems and concerns.

An Ombudsman shall:

- Attempt to provide informal conciliation, when appropriate;
- Not use the names of individuals without their permission;
- Exercise discretion on whether to act upon a concern of an employee;
- Maintain objectivity and impartiality; and
- Keep professionally current and competent in areas that relate to the role of an Ombudsman and the practices of the Department.

The Ombudsman shall attempt to identify options within the Department to resolve issues brought forth. This includes creating innovative solutions, when possible, or referring individuals to other available Department processes.

Availability

An employee may contact an Ombudsman and leave a confidential voice message at 508-988-7025.

Subject	Number
Office of the Ombudsman	**SUP-12**

Responsibility

An Ombudsman shall:

- Not represent themselves to any third party as the Department's agent for purposes of adjudication, placement or disposition; and
- Not be held responsible for decisions made by any employee receiving Ombudsman services that prove to be in violation of Department rules, regulations, policies, or procedures.

In no event shall a member's involvement with an Ombudsman abrogate their responsibility to conform or comply with rules, regulations, policies and procedures.

Accordingly, and in furtherance of an Ombudsman commitment to recovery and good health, Ombudsman shall:

- Remind anyone receiving such services that compliance with rules, regulations, policies, and procedures must remain a primary factor in all personal decisions.

Confidentiality

Communications with the Office of the Ombudsman are considered privileged. That privilege cannot be waived, **unless failure to disclose information that was obtained from an employee could cause a clear and present danger to the safety or security of any individual, the public, or the Department.**

Complaints and Department Investigations

The Ombudsman has the responsibility to consider the concerns and rights to privacy of all parties potentially involved in a dispute. The Ombudsman does not take action on calls, letters, or other communications that are anonymous. However, the Department shall be notified of any alleged criminal conduct committed by an employee.

No acts of reprisal or retaliation shall be tolerated against any employee of the Department as a result of contact with the Office of the Ombudsman.

Records

The Office of the Ombudsman does not keep case records for the Department and maintains only those notes necessary to manage an ongoing case. The Office of the Ombudsman adheres to the Standards of Practice and the Code of Ethics of The Ombudsman Association (TOA).

To protect the principle of privileged communications, the Department shall **vigorously resist** any effort to compel testimony or obtain notes or other records from an Ombudsman. To ensure maximum legal protection, the Ombudsman shall immediately contact the Legal Section upon knowledge or receipt of any document indicating efforts to compel testimony or obtain documentation.

The Office of the Ombudsman shall:

- Prepare a quarterly and annual statistical report for the Office of the Superintendent; and
- Protect the confidentiality and anonymity of the involved parties within submitted reports.

Supervisors

Supervisors shall:

- Ensure that employees under their supervision are aware of the Office of Ombudsman's confidential services in assisting with work-related problems;
- Provide support and commitment to the role and function of the Department's Ombudsman; and
- Be accessible to the Ombudsman to help in the resolution of work-related problems, as necessary.

Employees

Contacts with the Office of the Ombudsman need not be reported to a supervisor, as the program is accessible outside of the chain of command. An employee may contact the Office of the Ombudsman when seeking:

- Accurate information about Department policies, procedures, practices, or other issues;
- Informal advice on matters that they prefer to discuss without being "on the record"; and
- Assistance with work-related problems.

An employee who seeks the assistance of an Ombudsman may withdraw from the process at any time.

Contacts with an Ombudsman are voluntary and shall not jeopardize the employee's job security or promotional opportunities.

References

Bernard v. Commonwealth 424 Mass. 32 (1996)
The Administrative Dispute Resolution Act of 1995
MGL c.112, s.134, s.135, s.135A, s.135B
ADM-18-Anti-Harassment/Sexual Harassment and Discrimination

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 14, 2018	**TOP-01**

Subject

Special Operations Command and Control

Purpose

To define the command and control of Special Operations and to provide guidance to Department members who are involved in any incident that involves (or may involve) the utilization of any Special Operations resource.

Policy

Special Operations may be comprised of the following Sections/Units/Teams:

- Special Tactical Operations Team;
- Crisis Negotiations Team;
- Mounted Unit;
- Canine Unit;
- Underwater Recovery Team;
- Special Emergency Response Team;
- Motorcycle Unit;
- Commercial Vehicle Enforcement Section;
- Collision Analysis and Reconstruction Section;
- Traffic Programs Section; and
- Motor Vehicle Regulatory Section.

The Colonel/Superintendent reserves the right to modify the Special Operations' Sections/Units/Teams.

For the purpose of command and control, members of Special Operations Sections/Units/Teams shall be accountable to one chain of command while performing Special Operations functions or assignments.

Continued next page.

Subject	Number
Special Operations Command & Control	**TOP-01**

Policy (Continued)

All Department personnel must be cognizant of the fact that tactical operations are inherently hazardous and require specific understanding of the risks, risk management, and the various capabilities and limitations of Department resources. Special Operations Section/Unit/Team Commanders and their members are specially trained and equipped to meet specific standards applicable to their assigned positions within the various disciplines.

Activation Protocol and Response Procedures

Any emergency request for Special Operations resources shall include:

- The requesting agency's name;
- The requesting party's name and rank;
- The name and direct call-back number of the primary point of contact;
- The nature of the request; and
- The exact location of the incident and any designated staging areas.

Position	Responsibilities
Responding Member(s)	• Assess the situation, taking any actions necessary to eliminate immediate danger to others; • Contain and isolate the suspect(s) in the immediate area; • Advise the Desk Officer and request resources as necessary; • Gather and report as much tactical information as possible; and • If applicable, assume command and control until relieved by proper authority.

Continued on next page.

Subject	Number
Special Operations Command & Control	**TOP-01**

Activation Protocol and Response Procedures (Continued)

Station Desk Officer	• Advise Troop Duty Officer of request; and • Log entries into Daily Administrative Journal.
Patrol Supervisor	• Establish and secure perimeter as soon as possible; • Order evacuations, if necessary; • Establish liaison with local agency at scene; and • Ensure that only a single chain of command has control of the inner perimeter or scene.
Patrol Supervisor	**Additionally for significant events**: • Coordinate activities with outside jurisdictions (federal, state, municipal); • Establish a Command Post away from bystanders and the news media; • Assign a member as the media liaison until members from the Media Relations Section arrive; • Communicate accurate and current information on a regular basis to Troop Duty Officer; and • Upon conclusion of the incident, preserve the crime scene.
Troop Duty Officer	• Notify GHQ Communications Section; • Dispatch Patrol Supervisor if necessary; • Log request in Daily Administrative Journal; • Notify Troop Commander. • Notify appropriate Special Operations Section/Unit/Team Commander or designee of the request; and • Activate/notify Special Operations Section/Unit/Team members and others as requested by Section/Unit/Team Commander or designee.
Special Operations Section/Unit/Team Commander or designee	• Contact initial requesting party to determine appropriate response; and • Brief the Special Operations Commander /designee to obtain operational approval.

Continued on next page.

Subject	Number
Special Operations Command & Control	**TOP-01**

Activation Protocol and Response Procedures (Continued)

Special Operations Commander/designee	• Approve/deny activations/deployments; and • Contact Division of Field Services Commander.
Division of Field Services Commander	• Notify the Office of the Superintendent when appropriate; and • Activate other resources as needed.

Risk Management

Special Operations missions involve the likelihood of encountering potentially life-threatening hazards. All Special Operations Section/Unit/Team members shall exercise the best possible operational risk management strategies to:

1. Identify and assess hazards;
2. Develop controls to reduce hazards or risks; and
3. Use strategies to mitigate risk exposure and to safeguard the public and public safety personnel.

Removal from Assignment

Any member assigned to a non-biddable position with a Special Operations Section/Unit/Team may be removed at the discretion of the Colonel/Superintendent or designee.

Public Relations Requests

Requests for Special Operation resources for ceremonial, static or operational demonstrations, public relations displays, or other events shall be made in writing and approved by the Commander of the Division of Field Services.

After Action Reporting

When so directed, Special Operations Section/Unit/Team Commanders are required to submit mission/incident specific After Action Reports to the Special Operations Commander/designee for review.

All After Action Reports shall be in a format approved by the Special Operations Commander.

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 17, 2013	**TOP-02**

Subject

Special Tactical Operations Team

Purpose

To establish and define the role of the Special Tactical Operations Team within the Division of Field Services-Special Operations and establish guidelines for activation and utilization of their resources.

Policy

The Special Tactical Operations (STOP) Team shall:

- When requested and approved, assist members from the Department and those from other local, state, and federal agencies; and
- Develop, under the direction of the Team Commanding Officer, team specific Standard Operating Procedure (SOP) that shall be created, maintained, and updated as directed by the Special Operations Commander.

Definitions

Incident Command Post: A location where members may safely and effectively manage a scene, ideally equipped with a telephone, parking area, rest room, and effective radio communications for tactical team members.

Inner Perimeter: The immediate area of operations where violence or hostile actions are most likely to occur.

Outer Perimeter: A designated area outside the immediate area of operations which limits access and prevents harm to others.

Utilization of Resources

The STOP Team is available for:

- Emergency or critical incidents that may require a specialized response.

Subject	Number
Special Tactical Operations Team	**TOP-02**

Operational Protocols

The designated Incident Commander (IC) shall:

- Attempt to isolate and contain the incident by establishing the initial inner and outer perimeter; and
- Continually assess the situation in conjunction with the STOP Team Commander or designee to determine the need for additional resources and to adjust tactics as required to resolve the incident.

The Inner Perimeter:

- First responding members in the inner perimeter shall normally be replaced by STOP Team members once they arrive at the scene; and
- The Special Operations Commander or designee and STOP Team Commander or designee shall determine what personnel are required to safely manage the outer perimeter and scene.

The Outer Perimeter:

- No Department member on the outer perimeter shall discharge their weapon once the STOP Team has assumed control and authority of the Inner Perimeter unless:
  1. Ordered by the STOP Team Commander or designee; or
  2. When necessary upon the threat of death or serious bodily harm.

Building Entry:

When the STOP Team has made entry into a building, all other responding Department members shall:

- Not aim, fire, or discharge a firearm into the building; and
- Take a position of cover.

The STOP Team Commander or designee shall:

- Have the primary responsibility to determine the type of equipment (including weapons) used by the STOP Team members.

Command and Control

When engaged in STOP Team operations, missions, and/or training the command and control concerning deployment and operational tactics utilized shall be:

- Determined by the STOP Team Commander or designee; or
- Special Operations Commander or designee.

Subject	Number
Special Tactical Operations Team	**TOP-02**

Evacuations/ Witnesses	In some instances, it may be necessary to evacuate nearby civilians. Witnesses or those who may provide situational awareness and/or intelligence may be requested to remain at or near the Command Post.
References	Policy and Procedure TOP-01 Command and Control

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 17, 2013	**TOP-03**

Subject

Crisis Negotiation Team

Purpose

To establish and define the role of the Crisis Negotiation Team within the Division of Field Services-Special Operations and establish guidelines for activation and utilization of their resources.

Policy

The Crisis Negotiation Team shall:

- When requested and approved, assist members from the Department and those from other local, state, and federal agencies; and
- Develop, under the direction of the Team Commanding Officer, team specific Standard Operating Procedure (SOP) that shall be created, maintained and updated as directed by the Special Operations Commander.

Definitions

Incident Command Post: A location where members may safely and effectively manage a scene, ideally equipped with a telephone, parking area, rest room, and effective radio communication for team members.

Negotiator: A specially trained member of the Crisis Negotiation Team who utilizes crisis management techniques in an effort to stabilize extremely dangerous and volatile circumstances.

Utilization of Resources

The Crisis Negotiations Team is available for:

- Crisis, hostage, or barricaded incidents that can potentially be resolved through dialogue; and
- Other special events/incident as assigned by Special Operations Commander or designee.

Subject	Number
Crisis Negotiation Team	**TOP-03**

Operational Protocols

Crisis Negotiations Team shall:

- Utilize a philosophy of containment and negotiation;
- Assume control of the negotiations process once they arrive on-scene;
- Manage any personnel or individuals involved in the negotiations process; and
- Report to and remain operationally accountable to the Incident Commander.

Useful information related to the operational area include:

- The layout of the building;
- Size and Number of rooms/spaces;
- Ventilation, food, and water supplies; and
- Observation points, approach, and escape routes.

Useful information related to perpetrator(s) and/or hostage(s) include:

- Names, number, age, gender, size, and physical condition;
- Behavior and emotional state (rational, tolerant, aggressive, ambivalent, etc.);
- Criminal record/weapons access/ownership;
- Purpose of act (terrorist, criminal, mentally disturbed); and
- Any stated plans, demands, or motivation.

Additional Response Guidelines

In addition to the response protocols outlined in TOP-01 Special Operations Command and Control, members shall follow these additional guidelines.

Position	Duties
Responding Member(s)	• Assess the situation, taking no aggressive action unless there is an immediate danger to others; • Contain and isolate the suspect(s) in the immediate area; • Attempt to slow the pace of events, and open and establish communication with suspect(s); and • Gather and report as much tactical information as possible.

Continued on next page.

Subject	Number
Crisis Negotiation Team	**TOP-03**

Additional Response Guidelines (Continued)

Position	Duties
Patrol Supervisor	• Request through the Troop Duty Officer the Crisis Negotiation Team; and • Designate a member to research utility shut-offs, if necessary;
Incident Commander	• Work with the Crisis Negotiation Team, • Attempt to maintain as much control as possible over the movements and behavior of the suspect(s); and • Attempt to defuse the situation while affecting the safe release of any hostages.

Evacuations/ Witnesses

In some instances, it may be necessary to evacuate nearby civilians. Witnesses or those who may provide situational awareness and/or intelligence may be requested to remain at or near the Command Post.

References

Policy and Procedure TOP-01 Command and Control

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 17, 2013	**TOP-04**

Subject

Mounted Unit

Purpose

To establish the role of the Mounted Unit within the Division of Field Services-Special Operations and establish guidelines for activation and utilization of their resources.

Policy

The Mounted Unit shall:

- When requested and approved, assist members from the Department and those from other local, state, and federal agencies; and
- Develop, under the direction of the Unit Commanding Officer, unit specific Standard Operating Procedure (SOP) that shall be created, maintained and updated as directed by the Special Operations Commander.

Utilization of Resources

The Mounted Unit is available for:

- Patrol and law enforcement services;
- Search and rescue;
- Crowd Control; and
- Other special events/incidents as assigned by the Special Operations Commander or designee.

Operational Protocols

The Mounted Unit Commander or designee shall:

- Determine the use of animals and equipment during inclement weather; and
- Consult with the Incident Commander regarding search patterns and/or other Special considerations.

References

Policy and Procedure TOP-01 Command and Control

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 17, 2013	**TOP-05**

Subject

Canine Unit

Purpose

To establish and define the role of the Canine Unit within the Division of Field Services-Special Operations and establish guidelines for activation and utilization of their resources.

Policy

The Canine Unit shall:

- When requested and approved, assist members from the Department and those from other local, state, and federal agencies; and
- Develop, under the direction of the Unit Commanding Officer, unit specific Standard Operating Procedure (SOP) that shall be created, maintained and updated as directed by the Special Operations Commander.

Utilization of Resources

The Canine Unit is available for:

- Conducting building searches for hidden offenders;
- Assisting in the arrest of dangerous or violent offenders;
- Tracking/locating suspect(s), lost and/or missing person(s);
- Locating criminal evidence or hidden instrumentalities;
- Locating cadavers;
- Detecting the presence of concealed narcotics, explosives, or arson related accelerants;
- Crowd control;
- Homeland Security related missions; and
- Other special events/incidents as assigned by the Special Operations Commander or designee.

Subject	Number
Canine Unit	**TOP-05**

General Protocols

- Only that amount of force that reasonably appears necessary to apprehend or secure a suspect shall be used. Handlers and their dogs are required to adhere to procedures that properly control their potential use of force and channel their specialized capabilities into legally reasonable crime prevention and control activities;
- Canine handlers are responsible for determining whether a situation justifies canine use and the appropriate Special measures that should be taken;
- Employees shall not pet a canine except with the permission of the canine handler;
- No employee is to tease or agitate any canine unless performed as part of a training exercise;
- The canine shall not enter any State Police facility except for a specific police purpose;
- Whenever a canine is used in a special situation, Incident Commanders shall confer with canine handlers and members shall heed the directions of the canine handler;
- Canines shall not be handled by anyone other than their assigned handler, except in emergency situations;
- **No** commands shall be given to a canine by anyone other than the canine handler except in emergency situations; and
- **No** employee shall enter a canine cruiser while a canine is present, except at the direction and in the presence of the canine handler.

Building Search Protocols

Canines may be utilized for locating suspects in buildings or other structures. To optimize building searches, and if possible, the:

- Perimeter should be secured by the requesting patrol personnel;
- Owner should be contacted to ascertain the layout;
- Tenants, workers, or unnecessary personnel should be removed;
- Heating, air-conditioning, or other blowing units should be shut off so as not to interfere with the canine's scent;
- Entrances and exits should be monitored, and communications limited once entry is made by the search team; and
- Canine handler shall ensure notification has been made to all personnel prior to deploying a canine into any building or structure.

Tracking Protocols

Canines may be utilized for tracking. To facilitate tracking:

- Identify and mark the location where the subject was last seen;
- Avoid foot or vehicular movement in the immediate area;
- Set-up an initial perimeter to be searched; and
- Protect all items of clothing that shall be used for scent acquisition purposes.

Subject	Number
Canine Unit	**TOP-05**

Drug Detection Protocols

Public Facilities: Random exploratory sniffing of luggage, packages, or other inanimate objects may be conducted in public facilities such as:

- Airports/Transportation terminals (bus, train, marine);
- Commercial vehicle weigh stations; and/or
- Government buildings.

Public Schools: The use of drug detection canines in public schools is permitted only when authorized by the Division of Field Services Commander or designee, and if:

- The school administrator and the local police chief, if applicable, request and approve such use; and
- A search is limited to inanimate objects in public areas and the exterior of student lockers, unless reasonable suspicion exists to gain admission to an area.

Motor Vehicles: Drug sniffing canines may be used to sniff motor vehicles during:

- A commercial vehicle inspection; and/or
- A valid motor vehicle stop when reasonable suspicion exists to believe that the operator or passengers are in possession of illegal narcotics.

Canine Bites and Injuries

In the event that a Department canine bites or injures any party, the canine handler shall contact the Troop Duty Officer, who shall immediately dispatch a supervisor and Crime Scene Services to the scene to conduct an investigation and take color photographs.

The supervisor shall forward appropriate information including the SP 376 Use of Force Report to the Division of Field Services Commander and Canine Unit Commander prior to end of their shift.

Reference

SP 376 Use of Force Report
Policy and Procedure TOP-01 Command and Control

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 17, 2013	**TOP-06**

Subject

Underwater Recovery Team

Purpose

To define the role of the Underwater Recovery (Dive) Team within the Division of Field Services-Special Operations and establish guidelines for activation and utilization of their resources.

Policy

The Dive Team shall:

- When requested and approved, assist members from the Department and those from other local, state, and federal agencies; and
- Develop, under the direction of the Team Commanding Officer, team specific Standard Operating Procedure (SOP) that shall be created, maintained and updated as directed by the Special Operations Commander.

Utilization of Resources

The Dive Team is available for:

- Underwater sweeps for hazardous or improvised explosive devices;
- Active search and rescue;
- Water-safety and survival instruction;
- Evidence location and recovery;
- Body location and extrication;
- Vehicle/vessel location and recovery;
- Underwater survey for security purposes;
- Underwater obstruction identification and removal;
- Homeland Security related missions; and
- Other special events/incidents as assigned by the Special Operations Commander or designee.

Operational Protocols

Because of the inherent risks involved in diving operations:

- No dive shall be undertaken until a diving supervisor and at least two (2) divers are present and prepared to dive; and
- The Dive Team Commander or designee at the scene shall make the final determination as to whether a mission shall be undertaken or terminated due to changing conditions.

Subject	Number
Underwater Recovery Team	**TOP-06**

Witnesses

In some instances, it may be necessary to evacuate nearby civilians. Witnesses or those who may provide situational awareness and/or intelligence may be requested to remain at or near the Command Post.

References

Policy and Procedure TOP-01 Command and Control

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 14, 2018	**TOP-07**

Subject

Air Wing

Purpose

To define the role of the Air Wing within the Division of Homeland Security and Preparedness and establish guidelines for activation and utilization of their resources.

Policy

The Air Wing shall:

- When requested and approved, assist members from the Department and those from other local, state, and federal agencies; and
- Develop, under the direction of the Air Wing Commanding Officer, a unit specific Standard Operating Procedure (SOP) that shall be created, maintained and updated as directed by the Planning, Preparedness, and Response Section Commander.

Utilization of Resources

The Air Wing is available for:

- Search and rescue for lost, missing, or endangered persons;
- Photographic and video missions, documentation and video downlink;
- Motor vehicle enforcement and patrol;
- Incident command situations;
- Drug eradication efforts, including surveillance;
- Transportation of specialized equipment and personnel;
- Transportation of government officials;
- Criminal investigations;
- Dignitary protection;
- Fire services support;
- Homeland security related missions; and
- Other special events/incidents as assigned by the Division of Homeland Security and Preparedness Commander or designee.

Subject	Number
Air Wing	**TOP-07**

Operational Protocols

The Colonel/Superintendent, or designee, shall authorize all requests for out-of-state travel in department aircraft.

In accordance with Federal Aviation Regulations, the Air Wing Commander or flight crew members may decline, cancel, or terminate any request or mission due to:

- Safety, weather, distance;
- Type of request beyond aircraft or members capability;
- Availability;
- Mechanical maintenance of the aircraft; or
- Determination that use of aircraft is not the appropriate resource after operational risk management assessment is completed.

This policy shall not preclude the use of the aircraft in any other circumstances at the direction of the Air Wing Commander consistent with the Air Wing SOP.

Command and Control

When engaged in Air Wing operations, missions, and/or training, the command and control concerning deployment and operational tactics utilized shall be determined by:

- Air Wing Commander or designee; or
- Division of Homeland Security and Preparedness Commander or designee.

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 28, 2019	**TOP-07A**

Subject

Small Unmanned Aircraft Systems (UAS)

Policy

To define the operation of small Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) within the Department of State Police.

To establish guidelines for the utilization and activation of UAS.

To develop, under the direction of the Department UAS Program Manager, unit-specific Standard Operating Procedures (SOPs) that shall be created, maintained and updated, as directed by the UAS Program Manager.

UAS missions shall:

- Not facilitate the use of any weapons and/or dispersal payloads;
- Comply with the United States Constitution, the Massachusetts Declaration of Rights, and all relevant and applicable laws; and
- Comply with all applicable Department Policies and Procedures, Rules and Regulations, and unit-specific SOPs.

Privacy

A UAS shall not be intentionally used for viewing, recording or transmitting images and/or video in a criminal investigation at any location or property where a person has a *reasonable expectation of privacy* unless:

- A warrant or court order has been approved for the search of the property;
- Consent by the owner or person responsible for the property is obtained; or
- Exigent circumstances exist, including but not limited to: search and rescue missions, tactical missions, crash scenes, crime scenes, fire scenes, hazmat scenes and natural disasters.

Prohibited Uses

Department UAS shall not be used for the following:

- To target a person based solely on individual characteristics, such as, but not limited to race, ethnicity, national origin, religion, disability, gender or sexual orientation;
- To harass, intimidate or discriminate against any individual or group; and/or
- To conduct personal business of any type.

Definitions

Small Unmanned Aircraft (UA): A UA weighing less than 55 pounds, including everything that is onboard or otherwise attached to the aircraft, and can be flown without the possibility of direct human intervention from within or on the aircraft.

Remote Pilot- in- Command (Remote PIC): A person who holds a remote pilot certificate with a UAS rating and has final authority and responsibility for the operation and safety of a UAS operation conducted under 14 CFR 107.

Visual Observer (VO): A person acting as a flight crew member who assists the small UA remote PIC to see and avoid other air traffic or objects aloft or on the ground.

Remote Pilot Certificate: A person acting as a remote PIC of a UAS in the NAS under 14 CFR 107 must obtain a Remote Pilot Certificate with a UAS rating issued by the Federal Aviation Administration (FAA) prior to UAS operation.

UAS Program Manager: A Department member designated by the Colonel to oversee implementation, management, training, documentation and adherence to current FAA regulations for all Department-owned UAS. The UAS Program Manager shall create unit-specific SOPs and ensure the safe operation of all Department unmanned aerial systems.

Utilization of Resources

Consistent with this policy, applicable laws and unit-specific SOPs, Department authorized UAS may be utilized for missions including, but not limited to, the following:

- Search and rescue for lost, missing, or endangered persons;
- Photographic and video documentation missions;
- Motor vehicle crash investigations / crash scene mapping;
- Criminal investigations and crime scene mapping;
- Tactical response missions (e.g., hostage rescue/barricaded subject);
- Providing an aerial visual perspective to assist officers in providing direction for crowd control, traffic incident management, special circumstances, and tempory perimeter security;
- Fire Services support;
- Homeland Security-related missions; and
- Other special events/incidents as assigned by the Division Commander, Unit Commander and/or UAS Program Manager or designee, consistent with and as permitted by law.

Statistics, Records and Audits

The Department UAS Program Manager shall:

- Ensure that yearly statistics are kept for all UAS missions; and
- Ensure that flight and training records are properly maintained by the appropriate Unit Commander responsible for the use of the unit-specific UAS and forwarded to the UAS Program Manager.

Licensing, Certification and Registration

The Department UAS Program Manager shall:

- Ensure that all unit-specific remote pilots hold a Remote Pilot Certificate with a UAS rating issued by the FAA under 14 CFR 107; and
- Ensure that all UAS are registered with the FAA as required by 14 CFR 107.

Operational Protocols

The UAS Program Manager, the appropriate Unit Commander or the Remote PIC may decline, cancel, or terminate any UAS request or mission due to:

- Safety, weather, visibility;
- Type of request is beyond the UAS or member's capability;
- Availability;
- Mechanical maintenance of the UAS;
- Determination that use of UAS is not the appropriate resource after operational risk management or resource assessment is completed; or
- Determination that use of the UAS is in violation of this policy or Massachusetts General Laws.

All UAS missions will be flown in compliance with all current FAA Regulations including but not limited to 14 CFR 107. The Remote PIC has final authority and responsibility for the operation and safety of a UAS operation conducted under 14 CFR 107.

Training

The State Police UAS Program Manager or designee shall:

- Ensure that all training and licensing is compliant with current FAA regulatory requirements including but not limited to 14 CFR 107.

Department members selected to be Remote PICs shall:

- Be properly trained and licensed as required by 14 CFR 107;
- Satisfy and maintain all the conditions of the Certificate of Authorization (COA) issued by the FAA if applicable;
- Have working knowledge of the airspace intended for operations and Air Traffic Control communication requirements; and
- Have the ability to obtain and interpret weather information.

Department members selected to be Visual Observers (VO) shall:

- Be properly trained according to standards set by the UAS Program Manager or designee that comply with FAA current regulatory requirements if any; and
- Satisfy and maintain all the conditions of the COA issued by the FAA if applicable.

Subject	Number
Small Unmanned Aircraft Systems (UAS)	**TOP-07A**

Accident Notification and Investigation:

In the event of a crash/incident involving fatalities, injuries, property damage, damage to the UAS or UAS fly-away, the Remote PIC shall:

- Report the crash/incident immediately to the appropriate Unit Commander and UAS Program Manager or designee;
- When applicable, notify the FAA in compliance with 14 CFR 107; and
- Complete and submit an incident report to the UAS Program Manager and appropriate Unit Commander.

The UAS Program Manager shall:

- Review all documentation and reports;
- Complete a summary report with conclusions and recommendations; and
- Forward all documentation through channels to the Colonel/Superintendent.

Mission Approvals

UAS mission requests shall be authorized by either:

- The appropriate Unit Commander or designee;
- The UAS Program Manager or designee; or
- The appropriate Division Commander.

Note: The Remote PIC has final authority and responsibility for the operation and safety of a UAS operation conducted under 14 CFR 107.

Authorized Equipment

Only Small UAS approved by the UAS Program Manager shall be authorized for use by members of the Department and/or for Department use.

Digital Data preservation

All digital data including but not limited to photographs, video, and/or flight data shall be processed and maintained according to existing Department policies and preservation of evidence procedures.

References

14 CFR 107
Department Policy and Procedure, *TOP-01 Command and Control*
Department Rules and Regulations

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 14, 2018	**TOP-08**

Subject

Marine Unit

Purpose

To define the role of the Marine Unit within the Division of Homeland Security and Preparedness and establish guidelines for activation and utilization of their resources.

Policy

The Marine Unit shall:

- When requested and approved, assist members from the Department and those from other local, state, and federal agencies; and
- Develop, under the direction of the Marine Unit Commanding Officer, a unit specific Standard Operating Procedure (SOP) that shall be created, maintained and updated as directed by the Planning, Preparedness, and Response Section Commander.

Utilization of Resources

The Marine Unit is available for:

- Patrol and law enforcement services;
- Search and rescue;
- Waterborne surveillance/undercover operations;
- Underwater recovery (dive) operations support;
- Homeland security related missions; and
- Other special events/incidents as assigned by the Division of Homeland Security and Preparedness Commander or designee.

Operational Protocols

The Marine Unit Commander, shall assign authorized Marine Unit members who are designated and trained to:

- Operate State Police vessels and their associated motors, trailers, and equipment.

For all Marine Unit missions a member shall be designated as Boat Captain per the Unit's SOP. The Boat Captain shall:

- Be responsible for the safety of the vessel and all on-board.

The Marine Unit and the designated Boat Captain(s) shall:

- Collaborate with the Underwater Recovery Team Commander or designee to ensure a safe and efficient environment for all dive operations.

Subject	Number
Marine Unit	**TOP-08**

Command and Control

When engaged in Marine Unit operations, missions, and/or training, the command and control concerning deployment and operational tactics utilized shall be determined by:

- Marine Unit Commander or designee; or
- The Division of Homeland Security and Preparedness Commander or designee.

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 28, 2019	**TOP-09**

Subject

Incident Management Assistance Team

Purpose

To define the role of the Incident Management Assistance Team (IMAT) within the Division of Homeland Security and Preparedness and establish guidelines for activation and utilization of its resources.

Policy

The IMAT shall:

- When requested and approved, assist members from the Department and those from other local, state, and federal agencies; and
- Develop, under the direction of the Unit Commander, a team specific Standard Operating Procedure (SOP) which shall be created, maintained and updated as directed by the Division of Homeland Security and Preparedness Deputy Division Commander.

Utilization of Resources

The IMAT is available for:

- Large scale law enforcement operations;
- Lost or missing persons search and rescue missions;
- Extended recovery operations;
- Homeland Security-related missions; and
- Other special events/incidents as assigned by the Division of Homeland Security and Preparedness Deputy Division Commander.

Operational Protocols

IMAT members shall assist and advise on-scene Incident Commanders in the coordination and command and control of personnel and assets during the response to, mitigation of and/or recovery from an incident in a manner consistent with the Incident Command System (ICS) and the National Incident Management System (NIMS).

Subject	Number
Incident Management Assistance Team	**TOP-09**

Responsibilities

Position	Responsibilities
IMAT Coordinator	• Shall be a commissioned officer from the Division of Homeland Security and Preparedness; • Shall be supported by members of the DHSP IMAT; • Shall review the qualifications of all potential members and, select Troop IMAT members who will also be available to the Department as IMAT members; • Maintain a list of all Department IMAT members, in combination with DHSP IMAT members and Troop IMAT members; • Shall assist the Troop IMAT Officer in planning for IMAT support at planned Troop events; • Shall assist the Troop IMAT Officer with response to unplanned Troop events; • At the request of the Troop IMAT Officer, shall provide the requesting Troop with IMAT support from the list of Department IMAT personnel for planned and unplanned events; • Shall plan IMAT training for all Department IMAT members; and • Shall identify and recommend IMAT equipment purchases through channels to the Colonel/Superintendent.
Division of Field Services Troop IMAT Officer	• Shall be a commissioned officer that is appointed by the Troop Major from the Division of Field Services; • Shall identify and recommend to the Department's IMAT Coordinator a team of 5 subordinates as members of the Troop's IMAT; • Shall attend Troop planning meetings and report on anticipated IMAT staffing requirements to the Department's IMAT Coordinator; and • Shall make immediate notification to the Department IMAT Coordinator of Troop IMAT responses to unplanned events.
Department IMAT Members	• Shall provide the Department IMAT Coordinator with their current qualifications for selection and retention as Department IMAT members; • Shall respond to requests for Troop and Department IMAT responses; • Shall attend Department IMAT Training; and • Shall assist their Troop IMAT Officer when requested.

Subject	Number
Incident Management Assistance Team	**TOP-09**

References Homeland Security – National Incident Management System (NIMS) October 2017

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 17, 2013	**TOP-10**

Subject

Special Emergency Response Team

Purpose

To establish and define the role of the Special Emergency Response Team within the Division of Field Services-Special Operations and establish guidelines for activation and utilization of their resources.

Policy

The Special Emergency Response Team (SERT) shall:

- When requested and approved, assist members from the Department and those from other local, state, and federal agencies; and
- Develop, under the direction of the Team Commanding Officer, team specific Standard Operating Procedure (SOP) that shall be created, maintained and updated as directed by the Special Operations Commander.

Utilization of Resources

SERT is available for:

- Search and rescue efforts;
- Special event crowd control;
- Area security operations;
- Fugitive searches;
- Prison and civil disturbances;
- Extended recovery operations support;
- Wilderness searches requiring advanced land navigation techniques;
- Homeland Security related missions; and
- Other special events/incidents as assigned by the Special Operations Commander or designee.

Subject	Number
Special Emergency Response Team	**TOP-10**

Operational Protocol

Search patterns and/or other tactical considerations shall be:

- Determined by the Incident Commander; after
- Consultation with the SERT Commander or designee.

References

Policy and Procedure TOP-01 Command and Control

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 17, 2013	**TOP-11**

Subject

Emergency Management Unit

Purpose

To establish and define the role of the Emergency Management Unit within the Division of Field Services-Special Operations and establish guidelines for activation and utilization of their resources.

Policy

The Emergency Management Unit shall:

- When requested and approved, assist members from the Department and those from other local, state, and federal agencies; and
- Develop, under the direction of the Commanding Officer, unit specific Standard Operating Procedure (SOP) that shall be created, maintained and updated as directed by the Special Operations Commander.

Utilization of Resources

The Emergency Management Unit is available for:

- Multi-agency resource management and coordination;
- Assistance and/or support with exercise planning and evaluation;
- Major event coordination support;
- Natural disaster response, recovery and mitigation coordination;
- Emergency evacuation coordination support;
- Advanced incident management training;
- Homeland Security related missions; and
- Other special events and/or incidents as assigned by the Special Operations Commander or designee.

Subject	Number
Emergency Management Unit	**TOP-11**

Operational Protocols

The Emergency Management Unit shall:

- Serve in a liaison capacity between the Department and the Massachusetts Emergency Management Agency (MEMA) and other local, state, federal, private emergency management partners;
- Ensure the liaison position is staffed when requested by the Director of MEMA during the activation of the State Emergency Operations Center; and
- Reports through channels to the Colonel/Superintendent.

References

Policy and Procedure TOP-01 Command and Control

Promulgated By:

Department of State Police
General Order

Effective Date	Number
July 22, 2014	**TOP-12**

Subject

Motorcycle Unit

Purpose

To establish and define the role of the Motorcycle Unit within the Division of Field Services-Special Operations and establish guidelines for activation and utilization of their resources.

Policy

The Motorcycle Unit shall:

- When requested and approved, assist members from the Department and those from other local, state, and federal agencies; and
- Develop, under the direction of the Unit Commanding Officer, unit specific Standard Operating Procedure (SOP) that shall be created, maintained and updated as directed by the Special Operations Commander.

Utilization of Resources

The Motorcycle Unit is available for:

- Escorts;
- Patrol and law enforcement services;
- Crowd control;
- Traffic control;
- Homeland Security related missions; and
- Other special events/incidents as assigned by the Special Operations Commander or designee.

Operational Protocols

The Motorcycle Unit Commander or designee may decline, cancel, or terminate any request or mission due to:

- Safety, Weather, Distance;
- Type of request beyond motorcycle or personnel capability;
- Availability; or
- Determination that the use of motorcycles is not the appropriate resource after operational risk management assessment is completed.

Subject	Number
Motorcycle Unit	**TOP-12**

Troop Assigned Motorcycles

Division of Field Services (DFS) members assigned to motorcycle duty within a troop shall:

- Attend and successfully complete Certification Courses and Periodic Training as designated by the Motorcycle Unit Commander and approved by the Special Operations Commander.

References

Policy and Procedure TOP-01 Command and Control

Promulgated By:

Department of State Police
General Order

Effective Date	Number
November 5, 2008	**TRF-01**

Subject

Mission, Goals, and Objectives

Policy

All members are responsible for facilitating the safe and expeditious flow of traffic.

Mission

To develop and implement data-driven, multidisciplinary strategies to maximize the safety of the users of the roadway system.

Traffic Law Enforcement

Goal

- Minimize the incidence of offenses committed on the roadways and to promote voluntary compliance with traffic laws.

Objectives

- Minimize the number of crashes and the resulting fatalities, injuries, and property damage through uniform, consistent, and active enforcement;
- Maximize training, selective enforcement, and criminal operations to reduce the number of driver errors, traffic violations, and the overall crime rate; and
- Maximize the utilization of traffic data, crash reports, and citation information as key identifiers for personnel deployment and selective traffic enforcement.

Traffic Crash Management

Goal

- Minimize the incidence of loss of life, personal injury, and property damage resulting from crashes.

Objectives

- Maximize planning and coordinate programs by systematically obtaining data about collisions, roadways, drivers, and other required information;
- Minimize the severity of personal injuries and safeguard the lives and well-being of persons involved in collisions by providing basic medical and other emergency services;
- Minimize the number of driver errors and traffic violations by determining the cause(s) of collisions and taking appropriate enforcement action; and
- Minimize secondary crashes and/or delays by clearing crash scenes as rapidly as possible.

Subject	Number
Mission, Goals, and Objectives	**TRF-01**

Traffic Direction and Control

Goal

- Minimize delays to highway users resulting from crashes, construction, or other impediments.

Objectives

- Maximize the presence of personnel and equipment at locations and times conducive to enhancing traffic safety and flow;
- Maximize the expeditious flow of traffic by maintaining a high degree of officer and cruiser visibility while on patrol or specific assignment;
- Minimize and prevent collisions by eliciting the assistance of transportation officials and other law enforcement agencies to resolve problems as quickly and efficiently as possible;
- Maximize the direction of traffic through the use of signs, signals, and mechanical devices to regulate, coordinate, and detour traffic; and
- Maximize inter-agency relationships by sharing knowledge and information with other law enforcement, transportation, and academic officials involved in the transportation system so as to be better able to identify opportunities and resolve problems as quickly and efficiently as possible.

Traffic Safety Education

Goal

- Maximize the knowledge of highway users through Department announcements and provide information on risks, losses, and hardships associated with unsafe driving practices.

Objectives

- Maximize the awareness among the general public of the risk of damage, economic losses, and hardships associated with crashes and/or arrests resulting from unsafe driving;
- Minimize crashes and traffic violations committed by the general public through comprehensive training and education programs in unison with media informational efforts; and
- Maximize the public's safety by providing education on the importance of safety precautions, and promoting good driving practices such as wearing safety belts.

Subject	Number
Mission, Goals, and Objectives	**TRF-01**

Traffic Ancillary Services

Goal

- Maximize service to highway users in need of aid or information in a timely manner.

Objectives

- Maximize public safety by diligently patrolling assigned areas and rendering assistance when needed;
- Minimize the dangers to a stranded motorist by obtaining appropriate and timely assistance;
- Maximize public acceptance and respect by courteously providing information; and
- Maximize public awareness of traffic safety information through Department Public Service Announcements (PSA's) and community relations efforts.

References

Massachusetts Strategic Highway Safety Plan

Promulgated By:

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**TRF-02**

Subject

Patrol

Policy

The Department shall provide twenty-four (24) hour a day patrol coverage of state and interstate highways, as well as other areas of primary jurisdiction. The Department shall also be available to assist other agencies when required.

Patrol Function

The purpose of the patrol function is to:

- Protect life and property;
- Respond to emergencies and other calls for service;
- Investigate crimes;
- Ensure the safety of motorists and pedestrians; and
- Assist other members, police departments, and government agencies.

Deployment

Members may be deployed based upon the documented need for services. Criteria to be used for the assignment of personnel are:

- Crime: Number of crimes, type, and severity;
- Calls For Service: Number of specific incidents, time, and type;
- Jurisdiction: Geography and demographics of the area;
- Crash Data: Number of crashes, type and severity;
- Roads: Type and miles of roadways; and
- Coverage: Sufficient patrols are available to ensure officer safety.

Roll Call

Supervisors or Station Desk Officers should conduct a roll call with shift members, preferably at the start of each shift. Roll call information may include items such as:

- Review of Department written orders and directives;
- Administrative or teletype messages;
- Legal updates;
- Patrol information; and
- Investigative bulletins.

Patrol Responsibilities

The safety of members and the public are a paramount concern at all times.

Members shall:

- Maintain high visibility for general deterence of criminal and traffic violations;
- Familiarize themselves with their patrol area;
- Know the location of hospitals, local police departments, and other such facilities;
- Utilize various routes of travel to promote the visibility concept and to minimize predictability;
- Remain in their assigned patrol area, unless otherwise authorized or directed;
- Check vehicles parked within their patrol area, on the highway, and in rest areas (see ADM-46 Sexual Activity in Public Places), particularly at night and during periods of extreme or inclement weather to ascertain if the motorist/occupants are in need of assistance;
- Be alert to and report hazards within their patrol area, such as: road debris, inoperative traffic lights, missing traffic signs, fallen trees, or icy roads; and
- If the condition or hazard is of an emergency nature, the member should remain at the scene until the situation has been resolved, or the member is relieved by another member, entity, or as ordered.

Supervisors shall provide support to members to ensure their safety and efficiency while on patrol.

Desk Officer Responsibilities

Desk Officers shall:

- Enter the proper Roll Call information into the Daily Administative Journal (DAJ) including officers present and accounted for;
- Notify the Troop Duty Officer as appropriate;
- Take appropriate action to address reported hazards/situations; and
- Enter information as required into the DAJ.

Assisting Motorists

All members, regardless of duty assignment, shall be constantly alert for motorists who may appear to need assistance. Whenever a disabled motor vehicle is observed, members shall stop, unless a call or assignment prohibits them from doing so.

- Members are not required to perform mechanical work, change flat tires, jump-start vehicle batteries, unlock doors, etc.

If a disabled vehicle presents a clear and present danger, further traffic problems, and/or the possibility of a traffic crash, it may be pushed off the roadway and onto the shoulder, median, or breakdown lane. Members shall:

- Ensure that when pushing a disabled vehicle sufficient care is taken to prevent unnecessary damage; and
- Use only vehicles modified with extended front push bumpers.

Continued next page.

Assisting Motorists (Continued)

Members shall remain with the disabled vehicle and its occupants until assistance arrives, or they are assigned to a higher priority call for service.

- Members may allow stranded motorists and/or occupants to remain in a Department vehicle for safety and warmth; additionally
- Members may transport operators and/or occupants to another location for their safety or to a location where arrangements may be made for further assistance.

When encountering an unattended/abandoned motor vehicle members shall:

- Stop and make a visual check of the vehicle; and
- Make a RMV CJIS/NCIC inquiry into the status of the vehicle.

If the vehicle is properly registered and does not appear to be stolen or pose a risk to public safety, a courtesy check sticker shall be completed and affixed to the vehicle, on the upper left corner of the rear glass, where it can be readily identified by other members.

When asked to provide directions, guidance, or general information, members shall conduct themselves in a courteous and professional manner.

References

Rules & Regulations 5.5
ADM-46 Sexual Activity in Public Places
Criminal Justice Information System (CJIS)

Promulgated By:

Department of State Police
General Order

Effective Date	Number
November 5, 2008	**TRF-03**

Subject

Selective Traffic Enforcement

Policy

The Department shall use special enforcement patrol duties as an effective technique to meet our highway traffic safety goals and objectives.

Selective Traffic Enforcement

The primary purpose of selective traffic enforcement is to:

- Regulate traffic flow;
- Reduce traffic crashes; and
- Improve the safety of roads and highways.

Assignments shall be based upon:

- Crash data;
- Frequency of traffic violations;
- Traffic volume;
- Citizen complaints; and
- Any other pertinent information.

Traffic law enforcement depends upon the public and judicial acceptance of our efforts. Selective enforcement shall be fairly applied to create a climate of compliance with motor vehicle laws.

The selective enforcement performance standards for members shall be based upon the goals and objectives of the mission.

It is important to understand that both a quantitative and a qualitative emphasis are integral parts of selective enforcement.

Troop Commanders

Troop Commanders may utilize any of the following selective enforcement techniques, or combinations thereof, based upon the Traffic Program Officer's and/or Traffic Program Section's reports.

- Aerial patrol by the Air Wing;
- Speed reduction with speed measuring devices;
- Removing intoxicated drivers through saturation patrols, sobriety checkpoints, and other approved methods;
- Commercial vehicle enforcement conducted by the CVES;
- Joint operations in unison with other law enforcement agencies; and
- Education and information with electronic and print media releases and public presentations on traffic safety.

Subject	Number
Selective Enforcement	**TRF-03**

Traffic Programs Section

The Traffic Programs Section shall provide assistance and guidance to Troop Commanders on the selective enforcement activities to be conducted. This shall occur on a monthly basis and may include, at a minimum:

- Analysis of traffic crash investigations/reports;
- Analysis of traffic enforcement activities;
- Determining selective enforcement activities and programs success; and
- Review and revision of selective enforcement objectives.

Troop Traffic Programs Officer

The Troop Traffic Programs Officer is responsible for providing the traffic analysis for their respective Troop in conjunction with the Traffic Programs Section as stated above. The summaries shall include:

- Time and location of crashes;
- Causal factors; and
- Types of violations noted.

Station Commanders

Station Commanders shall utilize this traffic information for the scheduling of members for selective enforcement.

- Routine patrol assignments shall be planned based upon available assets in order to maximize the patrol effort of members not specifically assigned to other duties; and
- The assignment and deployment of members to selective enforcement should complement rather than replace regular patrols.

Promulgated By:

Department of State Police
General Order

Effective Date	Number
May 10, 2012	**TRF-04**

Subject

Motor Vehicle Pursuits

Purpose

This policy provides guidelines for the pursuit of motor vehicles.

Policy

A motor vehicle pursuit is justified when the necessity of the apprehension of a suspect outweighs the risk created by the pursuit.

Officers shall continually evaluate all circumstances surrounding a pursuit. If the degree of danger to the public, the pursuing officer(s), and/or the suspect(s) is greater than the necessity for immediate apprehension, a pursuit should not be initiated, or if in progress terminated.

Definitions

Vehicular Pursuit: An active attempt by an officer in an authorized emergency vehicle to apprehend a fleeing suspect who is actively attempting to elude the police.

Densely Populated Area: An established city or town that is thickly settled and/or comprised of a business district marked by compactness, pedestrian and vehicular traffic.

Prohibited Pursuits

Pursuits of motorcycles **shall be prohibited**, unless the suspect poses an imminent threat of death or serious bodily harm to the public or officers.

When a member initiates or signals the operator of a motorcycle to stop for a motor vehicle violation and recognizes that the violator is refusing to stop, the member shall:

- Terminate any further pursuit, unless the suspect poses an imminent threat of death or serious bodily harm to the public or officers.

The Troop Duty Officer shall:

- Immediately assume command and control when circumstances result in a request for a CODE 1 regarding pursuit of a motorcycle; and
- Terminate the pursuit, unless the suspect poses an imminent threat of death or serious bodily harm to the public or officers.

Subject	Number
Motor Vehicle Pursuits	**TRF-04**

Initiating a Pursuit

If a violator fails to stop when signaled to do so and operates in such a manner as to avoid capture, officers must first recognize the potential risk to public safety before initiating a pursuit. Consideration should be given to tactics that reduce the opportunity for a suspect to flee apprehension.

If the degree of danger to the public, the pursuing officer(s), and/or the suspect(s) is greater than the necessity for immediate apprehension a pursuit should not be initiated or, if in progress terminated.

Factors to consider include:

- Probability of apprehension;
- Type of vehicle being pursued;
- Offense;
- Availability of assistance;
- Speed and driving behavior;
- Presence of passengers;
- Location, visibility, weather, road conditions, and the time of day;
- Volume of vehicular and pedestrian traffic; and
- Other circumstances or conditions which mitigate or aggravate hazards associated with the pursuit.

Termination of Pursuits

Officers shall immediately terminate a pursuit when any of the following conditions exist:

- When a pursuit for a civil infraction, misdemeanor, or non-violent felony enters into a densely populated area or heavily congested roadway;
- If radio communications with the Troop Duty Officer cannot be established or lapse during the pursuit;
- When the initiating officer or Troop Duty Officer determines that the risks of continuing the pursuit are outweighed by the risk to public safety; or
- When ordered to do so. Termination orders shall be immediately acknowledged.

When an officer terminates a pursuit they shall immediately deactivate all emergency visual and audible systems.

Subject	Number
Motor Vehicle Pursuits	**TRF-04**

Pursuit Responsibilities

Position	Duties
Primary Pursuit Officer	Shall: • Request a **CODE 1** and broadcast cruiser number, location, direction of travel, speed and traffic conditions; • Activate all emergency visual and audible systems; • Provide the original reason for the attempt to stop the motor vehicle and a vehicle description; • Continually broadcast the location, direction, speed, and road conditions; • Operate cruiser in accordance with General Order ADM-19A Vehicle Use and Maintenance and MGL c.89 s.7B and continually re-evaluate the risk to public safety; • Advise the Troop Duty Officer and render assistance to any civilian vehicle involved in a crash; • Assistance to injured parties shall take precedence over the continuation of the pursuit; and • Conduct a comprehensive follow-up investigation in the event the operator eludes apprehension. **<u>Out of State Pursuits</u>** • Officers shall not pursue a fleeing vehicle across the territorial boundaries of the Commonwealth and into another state for a misdemeanor; and • Officers may pursue felony suspects into other states only when authorized by the Troop Duty Officer.
Station Desk Officer	Shall immediately: • Notify the Troop Duty Officer of a pursuit and request **CODE 1**; • Receive, record, and coordinate information on the pursuit and the pursued vehicle with the Troop Duty Officer and other law enforcement agencies; and

Continued next page.

Subject	Number
Motor Vehicle Pursuits	**TRF-04**

Pursuit Responsibilities (Continued)

Position	Duties
Station Desk Officer	• Ensure that all pertinent information regarding the pursuit is entered into the Daily Administrative Journal (DAJ) and forwarded to the Troop Duty Officer.
Assisting Pursuit Officer(s)	Shall immediately: • Notify the Troop Duty Officer of their participation in the pursuit; • Maintain a safe distance behind the primary unit, but be close enough to provide aid; and • Assume radio communication if and when required. <u>Only two (2) State Police vehicles may engage in active pursuit.</u> The Troop Duty Officer may permit additional State Police officers to assist in a pursuit if they determine extraordinary circumstances exist. State Police vehicles not directly engaged in the pursuit, but in close proximity to the pursuit shall immediately notify the Troop Duty Officer. These officers shall position themselves on alternate/parallel roadways to provide assistance in the event the suspect eludes the pursuing officer(s) or flees on foot; or as otherwise directed by the Troop Duty Officer.
Troop Duty Officer	Shall immediately: • Initiate a **CODE 1**; • <u>Personally broadcast</u> that they have assumed "command and control" of the pursuit; • Ascertain the cruiser number(s) of the involved officer(s); location, direction of travel, speed, and traffic conditions; • Determine the original reason for the attempt to stop the motor vehicle; • Obtain the vehicle description, including plate number, if known, and number of occupants; • Continually evaluate the risk to the public, and the pursuing officer(s), as such risks relate to the necessity for immediate apprehension;

Continued next page.

Subject	Number
Motor Vehicle Pursuits	**TRF-04**

Pursuit Responsibilities (Continued)

Position	Duties
Troop Duty Officer	• Utilize State Police Air Wing (if available); and • Direct State Police K-9 units to respond to the general area (if available). **Mandatory Termination** In the event the Pursuit Officer fails to transmit the required information to the Troop Duty Officer, said Duty Officer shall terminate the pursuit. If the degree of danger to the public, the pursuing officer(s), and/or the suspect(s) is greater than the necessity for immediate apprehension, a pursuit should not be initiated, or if in progress, terminated. **Authority** Regardless of the rank of the pursuing officer, the Troop Duty Officer shall remain in command and control of the pursuit for the entire duration. **Inter-Troop Pursuits** The Troop Duty Officer of jurisdiction shall assume command and control once the pursuit enters their Troop. Adjoining Troop Duty Officers shall be notified of pursuits that are in close proximity to their jurisdiction and may enter into their area of responsibility. When a pursuit enters into another Troop the originating Duty Officer shall remain in command and control until the adjoining Troop Duty Officer personally broadcasts that they have assumed "command and control" of the pursuit. **Note: Only the Duty Officer from the originating Troop shall complete the pursuit evaluation.**

Continued next page.

Subject	Number
Motor Vehicle Pursuits	**TRF-04**

Pursuit Responsibilities (Continued)

Position	Duties
Troop Duty Officer	**Inter-Jurisdictional Pursuits** Troop Duty Officers shall notify other law enforcement agencies when a State Police pursuit is within their primary jurisdiction. They shall factor into their consideration any additional information bearing on the pursuit provided by said law enforcement jurisdiction. Request for their assistance or; • Courtesy notification with NO participation requested. **Out of State Pursuits** If a felony has been committed, the Troop Duty Officer may authorize the pursuing officer(s) to continue to pursue into another state. If this occurs, the Troop Duty Officer shall immediately: • Notify the law enforcement agency of jurisdiction and request their assistance; • Require that the first out-of-state law enforcement vehicle that joins the pursuit become the primary pursuit vehicle; and • Direct the Massachusetts State Police vehicle to become a backup unit; and • Direct the MSP officer(s) involved to return to the Commonwealth as soon as the pursuit investigation is terminated. **Crash Investigations** The Troop Duty Officer shall assign a supervisor to investigate all crashes associated with a State Police pursuit.

Other Law Enforcement Agency Pursuits

Once a law enforcement agency notifies the State Police that they are in pursuit the caller must be identified and specifically asked:

- Whether they are making a request for State Police assistance; or
- Making a courtesy notification with NO State Police participation requested.

Once a request for assistance is made, the Troop Duty Officer shall determine if the State Police shall participate. If approval is granted, State Police officer(s) shall act as a secondary unit to the other agency's officer unless otherwise directed by the Troop Duty Officer.

All State Police officers directly or indirectly involved in a pursuit initiated by another law enforcement agency shall adhere to all of the requirements established in State Police General Orders, as well as Rules and Regulations.

Subject	Number
Motor Vehicle Pursuits	**TRF-04**

Pursuit Driving Tactics

Deliberate Contact – Shall be prohibited unless specifically authorized and ordered by the Troop Duty Officer, Troop Commander, or Command Staff Member and where the suspect poses an imminent threat of death or serious bodily harm to the public or officers.

Tire Deflating Devices – Should be considered as an effective option for bringing a pursuit to conclusion for passenger vehicles only. The use of these devices is prohibited for motorcycles, buses, and trucks. (Refer to TRF-21 for additional details.)

Caravanning - Only two (2) State Police vehicles may engage in active pursuit. The Troop Duty Officer may permit additional State Police officers to assist in a pursuit if they determine extraordinary circumstances exist.

Units Paralleling – Additional State Police officers may operate with emergency visual and audible systems activated and assist by paralleling the pursuit or pre-position themselves at likely avenues of escape. These assisting units are strictly prohibited from direct/active pursuit unless specifically authorized by the Troop Duty Officer.

Passing – Attempts to pass another police vehicle are strictly prohibited, unless the police vehicle is disabled or ordered by the Troop Duty Officer.

Spacing – All units in pursuit shall space themselves at a safe distance to ensure proper braking and reaction time.

State Police Motorcycles – SHALL NOT become involved in a pursuit.

Unmarked State Police Vehicles – Officers operating unmarked State Police vehicles shall only engage in pursuits if they are equipped with emergency visual and audible systems and shall allow a marked/semi-marked unit to assume the primary pursuit position at the earliest opportunity. The unmarked vehicle shall then become the assisting unit until an additional marked/semi marked State Police vehicle can assume the secondary role. Once two (2) marked/semi marked State Police vehicles have become actively involved in the pursuit, the unmarked vehicle shall immediately disengage from the pursuit unless specifically authorized by the Troop Duty Officer to continue involvement in the pursuit.

Reckless/Hazardous Driving – Officers shall not duplicate the reckless operation displayed by fleeing suspects. Officers are strictly prohibited from wrong way operation.

Subject	Number
Motor Vehicle Pursuits	**TRF-04**

Post Pursuit Documentation and Review

Position	Duties
Pursuit Officer	Provide the Troop Duty Officer with relevant information so they can complete the SP 343 Pursuit Evaluation Form.
Troop Duty Officer	• Ensure that the Desk Officer has entered all pertinent information into the DAJ and the entry is forwarded to Troop Headquarters; • Complete all required entries in the Troop Headquarters DAJ; • Ensure that the Troop Headquarters DAJ entry is included in the Daily AM Report; • Complete the electronic RAMS Pursuit Evaluation; and • Ensure a follow-up investigation occurs for suspects who elude apprehension.
Deputy Superintendent	• Appoint members to the Pursuit Review Committee.
Pursuit Review Committee	• Examine each pursuit and ensure compliance with this policy and report their findings to the Deputy Superintendent.

References

ADM-19A Vehicle Use and Maintenance
TRF-12 Traffic Crash Investigation
TRF-21 Tire Deflating Devices
MGL c. 89 s.7B

Promulgated By:
Colonel Marian J. McGovern

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**TRF-04A**

Subject

Foot Pursuits

Policy

Members shall continually evaluate all circumstances surrounding a pursuit. If the degree of danger to the public, the pursuing officer(s), and or member(s) is greater than the necessity for immediate apprehension, a pursuit shall not be initiated, or if in progress, terminated.

Criteria for Foot Pursuits

Mere flight by an individual not otherwise suspected of criminal activity shall not serve as the sole justification for engaging in an extended foot pursuit, or for a significant commitment of Department assets.

Alternatives to Foot Pursuits

In deciding whether or not to initiate or continue a foot pursuit, a member should continuously consider reasonable alternatives to pursuit based upon the circumstances and resources available, including:

- Containment of the area;
- Canine search;
- Saturation of the area with additional patrol personnel;
- Air Wing support;
- Apprehension at another time when the identity of the suspect is known or other information is available that would likely allow for later apprehension; and
- The need to immediately apprehend the suspect does not reasonably appear to outweigh the risk in continuing the pursuit.

The team concept of using two (2) or more officers should be used whenever possible.

If exigent circumstances exist, it is generally recommended that a single member keep the suspect in sight from a safe distance and coordinate containment.

Continued next page.

Subject	Number
Foot Pursuits	**TRF-4A**

Alternatives to Foot Pursuit (Continued)

Foot pursuits are inherently dangerous and require heightened officer safety awareness, common sense and sound tactics.

Before initiating a foot pursuit, member(s) shall contact the station of jurisdiction and at a minimum, provide the following information:

- Member's identification (e.g. cruiser number) and exact location;
- Reason for the pursuit and current direction of travel;
- Number and description of suspects; and
- Whether the suspect is known or believed to be armed.

Members should consider, if the situation allows, removing the keys from the ignition of Department vehicle and/or the suspect's vehicle before commencing the tracking of the suspect operator.

Unless there is an immediate threat to another officer or a member of the public, members shall not initiate a foot pursuit under the following conditions:

- The member has no portable radio, no means of communicating or loses communications with other members or duty station;
- The member is alone and the subject has fled into the woods or an unoccupied building;
- When two (2) or more members become separated, lose visual contact with one another, or obstacles separate them to the degree that they cannot immediately assist each other should a confrontation take place;
- The member loses possession of their weapon or other essential equipment;
- When the member is unsure of their location and direction of travel;
- When pursuing multiple suspects and the pursuing members(s) do not reasonably believe that they would be able to control the suspects should a confrontation occur; or
- When ordered to do so by the Troop Duty Officer.

Promulgated By:

Department of State Police
General Order

Effective Date	Number
November 5, 2008	**TRF-05**

Subject

Traffic Incident Management

Policy

The Department shall use Traffic Incident Management protocols to minimize the congestion and delay caused by highway incidents.

Traffic congestion causes safety concerns due to the increased risk of secondary crashes, resulting in economic losses, which can adversely impact the quality of life.

Every effort should be made to minimize this cost, in addition to the impact to public safety and the inconvenience to motorists of the Commonwealth.

Applicability

Every incident requires that certain management activities be performed. Even if the incident is small, Traffic Incident Management protocols are applicable to some degree.

The system should always be applied, even to routine incidents to:
- Create familiarity with the system;
- Be prepared for escalation; and
- Increase awareness of the risks that exist in all incidents.

Goal and Objectives

Goal: Use "Quick Clearance" to restore the normal traffic flow as quickly and safely as possible.

Objectives:
- Coordinate and expedite emergency response to incidents;
- Save lives, preserve property and minimize damage to the environment by the use and implementation of standard procedures and/or agreements;
- Improve scene management to facilitate quick clearance of incidents;
- Provide timely, accurate information to other agencies and roadway users about roadway conditions and alternate routes through the use of media, MassHighway's Advanced Traveler Information System (ATIS), and other systems; and
- Minimize the impact of non-recurring incidents through the use of pre-planned alternate routes.

Subject	Number
Traffic Incident Management	**TRF-05**

Unified Command

Incidents occur without regard to jurisdictional boundaries requiring a well integrated, unified command approach to managing the incident scene.

Roadway crashes, fire, and hazardous material incidents usually require a multi-jurisdiction, multi-agency response. Individual agency responsibilities and authority are normally confined by jurisdiction or function by statute.

Unified Command requires all responding agencies to have a functional responsibility that contributes to:

- Ensuring safety of ALL emergency responders;
- Determining overall incident objectives;
- Ensuring joint planning;
- Implementing strategy chosen for clearing the incident;
- Ensuring integrated tactical operations are conducted;
- Maximizing all assigned resources; and
- Re-opening the affected roadway as quickly and efficiently as possible to minimize congestion delays resulting from the incident.

First-On-Scene

There are certain duties and responsibilities required of the first-on-scene member that are critical to initiating the appropriate response necessary to successfully manage an incident.

1. **Initiate Communication of incident with exact location-** Give brief description of incident, route number, direction, town, exit number or mile marker, landmark.
2. **Evaluate the incident-** Type of incident and potential number of injured, traffic conditions, lanes that are blocked, best access to scene:
   - **I.** If a commercial motor vehicle (bus or truck) is involved the Department of Transportation Number is required.
   - **II.** In case of hazardous material releases then the type, estimated amount, tank rupture and placard number is required.
3. **Communicate the evaluation**- Communicate the evaluation and the need for additional responders to the sub-station of jurisdiction.
4. **Secure the scene**- Secure the scene by whatever means available (cruiser, cones, etc.) to prevent further injury or property damage to the motoring public.
5. **Perform First Responder Duties**- Provide basic medical care; (e.g. CPR, first aid), until the arrival of more qualified EMS personnel.
6. **Assume Incident Command (IC) duties until relieved-** Begin to initiate IC responsibilities until the appropriate IC agency arrives. The first-on-scene member shall brief the relieving Incident Commander on the situation.

Subject	Number
Traffic Incident Management	**TRF-05**

Traffic Incident Management Response Framework

Department members shall:

- **Perform First-On-Scene Duties-** All members, when first arriving on the scene of a roadway crash, shall be prepared to assume the first-on-scene duties.
- **Assist in Securing the Scene-** The first responding member shall immediately take charge and secure the scene pending the arrival of the assigned patrol or supervisory personnel to whom the responsibility shall be surrendered.
- **Perform First Responder Duties-** Provide basic medical care; (e.g. CPR, first aid), until the arrival of more qualified EMS personnel.
- **Assume IC Duties When Appropriate**- The senior member at the scene shall assume IC duties. In the event that a fire, explosion, HazMat, or serious threat of fire, explosion, or HazMat is encountered, the responsibility for the "immediate scene" shall fall to the Senior Local Fire Department Official. Department personnel should be aware that Incident Command shall be transferred back to the Department once the fire, threat of fire or Hazardous Material has been removed.
- **Support Unified Command As Necessary-** Paramount to the successful management of any critical incident is cooperation among all of the agencies participating in the operation. Department members shall be aware that Incident Command might be rotated with an official of another agency (such as Fire or MassHighway).
- **Control Scene Access/Egress-** This may include providing escorts for emergency vehicles and equipment necessary for clearing the scene of the injured and any obstructions or hazards.
- **Implement Alternate Routes-** Redirect the flow of traffic from the incident when necessary. Members are reminded that when alternate routing is initiated, which may affect local communities, additional personnel may be needed to augment the local police department at strategic locations to safely move large volumes of traffic within the local community.
- **Assist the Public Information Coordinator-** In order to facilitate the movement of traffic around and away from the incident, the media should be contacted. The Department's Media Relations shall dispatch qualified personnel to the scene of major incidents, if available, and shall provide support to on-scene personnel. The IC shall designate a Public Information Coordinator, normally a member from Media Relations, to interface with the media at the incident.

Continued next page.

Subject	Number
Traffic Incident Management	**TRF-05**

Traffic Incident Management Response Framework (Continued)

- **Conduct Incident Investigation-** The initial responding member, a member designated by the IC, or the assigned patrol of jurisdiction shall complete any and all reports required pursuant to established Department policy and procedure.
- **Participate In After Action Review/Debriefing-** All Department personnel involved shall be available for any after-action review of the incident. Members shall be prepared to discuss their roles and actions during the management of the entire incident.

Traffic Control

When conducting manual traffic control, members shall ensure that their presence and purpose are clear and obvious, and that they use traffic direction and control signals that are easily understood to ensure the safe and efficient flow of traffic.

Members conducting manual traffic control shall:

- Wear issued retro-reflective outerwear and employ a flashlight when warranted;
- Position themselves in a safe location so they can be seen by all;
- Stand straight, with a military-like bearing facing traffic, and be alert to their duties and conditions around them;
- Use clear and simple signals to direct traffic; and
- Start or stop one lane of traffic at a time on multiple lane roads, before proceeding to start or stop the next lane of traffic.

At the scene of critical incidents, members should assist by diverting vehicles around or away from the incident and allow medical and fire personnel room to operate. Roadway closures should be as short as possible; quick clearance techniques shall be employed whenever practicable.

Temporary traffic control devices, including portable signs, moveable barriers, and other apparatus, may be deployed to assist members in the safe and efficient flow and control of traffic. This is mainly applicable for pre-planned events, or long-term road closures.

In most circumstances, planning a road closure beforehand can reduce the length of the closure.

References

Unified Response Manual for Roadway Traffic Incidents

Promulgated By:

Department of State Police
General Order

Effective Date	Number
November 5, 2008	**TRF-07**

Subject

Motor Vehicle Stops

Policy

Necessary precautions shall be taken for every motor vehicle stop to ensure the safety of all. Members shall use these guidelines as well as their training and experience to determine specific actions for each situation.

Racial and Gender Profiling

All motor vehicle stops shall be in compliance with ADM-47 Identification and Prevention of Racial and Gender Profiling.

Marked Cruiser Motor Vehicle Stops

Members in marked cruisers shall:

- Activate the emergency lights and siren, as necessary;
- Select a safe location, if possible, to stop a violator; and
- Position the cruiser behind the violator at a safe and reasonable distance, or as circumstances require.

Unmarked or Low-profile Cruiser Motor Vehicle Stops

Members operating unmarked/semi-marked cruisers should be aware that motorists might not recognize them as police members and may refuse or be reluctant to stop. These motorists may drive to areas with increased population, illumination or to a local police station before feeling safe enough to stop.

Members shall:

- If in uniform, wear the appropriate cover while signaling the motorist to stop during the contact;
- Request assistance from a marked cruiser if the motorist does not comply; and
- Advise the Troop or GHQ Communications Center of the situation. In many instances people may use cellular phones to call 911 to ascertain the member's authenticity.

Subject	Number
Motor Vehicle Stops	**TRF-07**

Felony Stops

Members making felony or high risk stops shall conduct the stop in accordance with established training guidelines, and if practical:

- Contact the station Desk Officer giving the location, direction of travel, description of the vehicle and occupants(s), and the reason for the stop;
- Request a Code 1 if necessary;
- Position the cruiser in a manner that provides protection and cover; and
- Make an effort to conduct the stop with back up.

Assisting members shall not give additional commands, unless necessary for officers' safety. They shall remain in position to cover the primary member, who shall issue the instructions to the vehicle occupant(s).

Approaching a Vehicle

When approaching a vehicle, members shall be aware of their environment and alert to oncoming traffic. Members shall:

- If in uniform, wear the appropriate cover;
- Ensure the portable radio is on;
- Approach in a manner that affords maximum protection; and
- Remain alert for any sudden or suspicious movement within the vehicle.

Operator Contact

Members shall:

- Speak to the operator from a safe position;
- Inform the operator of the reason for the stop;
- Remain professional and courteous;
- Avoid unnecessary conversation that may lead to verbal confrontations; and
- Assist the operator in safely re-entering the traffic flow.

Member Safety

To maximize safety, the operator and occupants of the stopped vehicle shall be instructed to remain in the vehicle except for:

- An arrest;
- Situations where the member has specific articulable facts and reasonable suspicion that causes the member to be apprehensive for their safety or that of the public;
- Specialized enforcement functions;
- When conducting a field interview; or
- Other situations as necessary.

If individuals refuse to stay in the vehicle, they shall be directed to a position of safety off the roadway, away from the cruiser, but within view of the member.

If a member is stopping a vehicle which they have good reason to believe may pose a threat to the member or the public, they shall follow the felony stops procedure.

Subject	Number
Motor Vehicle Stops	**TRF-07**

References

TRF-04 Motor Vehicle Pursuits
Comm. V. Williams 46 Mass. App. Ct. 181, 1999
Comm. V. Gonsalves 46 Mass App. Ct. 186, 1999

Promulgated By:

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**TRF-08**

Subject

Citations

Policy

Citations shall be issued in accordance with Policy and Procedure ADM-04 State Police Authority and Massachusetts General Law (MGL) c. 90C.

Issuance of Citation

The specific enforcement action taken should be predicated upon the offense. Traffic enforcement action shall be taken at the time and place of the occurrence, unless:

- The vehicle could not be stopped;
- Additional time or information is necessary to determine the nature of the violation or identity of the operator; or
- Other extenuating circumstances exist at the time of the violation.

Members shall fill out all applicable fields within a citation including:

- The gender of the operator;
- One applicable authorized code when identifying the operator's race; and
- If a non-inventory motor vehicle search is conducted the appropriate block shall be checked "yes or no."

Under no circumstances shall the race block contain unauthorized codes, remain unfilled, or contain inappropriate notations such as "unknown."

Issuing Member's Responsibilities

Issuing members shall:

- Complete appropriate sections of the traffic citation accurately and legibly;
- Forward the citations to the appropriate court/station of jurisdiction at or before the completion of their tour of duty;
- Ensure the Department copy is submitted to the appropriate court officer; and
- Record citation information onto the PayStation Citation Entry Form.

Members assigned to a station within the Division of Field Services shall utilize the station code of their assigned station in the approved format (e.g., A-1 Andover is SA-1). Members assigned to a section or unit not in Field Services shall use the station identifier approved by their Division Commander.

Subject	Number
Citations	**TRF-08**

Court Officer's Responsibilities

Court Officers shall:

- Forward warning copies to the Registry of Motor Vehicles (RMV) forthwith;
- Mail or deliver civil infraction copies to the Registrar not later than the end of the sixth (6^{th}) business day after the date of the violations;
- Forward criminal complaint/summons to the court of jurisdiction not later than the end of the sixth (6^{th}) business day after the date of the violations; and
- File the Department copy.

Supervisor's Responsibilities

Supervisors shall:

- Review citations for accuracy, legibility, and compliance with statutory requirements; and
- Ensure that unacceptable/unprofessional patterns are immediately addressed.

Station/Section/ Unit Commander's Responsibilities

Station/Section/Unit Commanders shall:

- Maintain a Control Journal for all citation books received and issued;
- Review citations for accuracy, legibility, and compliance with statutory requirements;
- Review the citation data entered into the PayStation Citation Entry application by members under their command;
- Submit monthly/quarterly compliance reports as directed by the Traffic Stop Data Collection Technical Support Manual located on DocuShare;
- Ensure all citation copies are classified, distributed, and delivered to the RMV and the appropriate court(s), as required by statute;
- Retain all Department citation copies in station files for a period of three (3) years; and
- Ensure that unacceptable/unprofessional patterns are immediately addressed.

Troop Traffic Programs Officer's Responsibilities

Troop Traffic Programs Officers shall:

- Maintain and forward up-to-date traffic/legal information as appropriate;
- Maintain a Control Journal for the issuance of citation books; and
- Maintain Monthly Troop Traffic Law Enforcement Statistical Summaries prepared in accordance with the requirements of the Division of Field Services.

Troop/Section Commander's Responsibilities

Troop/Section Commanders shall:

- Review monthly/quarterly compliance reports to ensure that the members under their command are in compliance with the provisions of this policy; and
- Ensure that unacceptable/unprofessional patterns are immediately addressed.

Subject	Number
Citations	**TRF-08**

Division Commander's Responsibilities

Division Commanders shall:

- Establish internal guidelines for procedural review to ensure that the personnel under their command are in compliance with the provisions of this policy.

Recreational Vehicles

Members shall take appropriate enforcement action for violations committed by operators of off-road recreational vehicles (snowmobiles, dirt bikes, all-terrain vehicles, etc.,) observed and/or reported to them.

All MGL c. 90B violations shall be entered upon the standard RMV citation, or an application for complaint may be made with the District Court of jurisdiction.

The standard uniform citation can be utilized as a complaint application for a recreational vehicle operated on a public way in violation of MGL c. 90B s.25.

Note: If needed, under the Executive Office of Energy and Environmental Affairs, the Massachusetts Environmental Police may be called for assistance at (800) 632-8075.

Voidance of Citations

If an error is made while writing a citation, or if a citation becomes accidentally damaged, it may be administratively voided by the issuing member. The member shall:

- Print "VOID" on all copies of the citation;
- Provide a full explanation in writing (To/From) before the end of their tour of duty and submit it to their first line supervisor for review; and
- Record the voided citation in the PayStation Citation Entry application.

If satisfied with the explanation provided, the supervisor shall approve the "VOIDED" citation and the explanation for such action. The voided citation and explanation shall be returned to the Registrar forthwith.

References

ADM-04 State Police Authority
MGL c. 90C Procedure for Motor Vehicle Offenses
Traffic Stop Data Collection Technical Support Manual

Promulgated By:

Department of State Police
General Order

Effective Date	Number
June 14, 2018	**TRF-09**

Subject

Towing

Purpose

To establish and define guidelines for State Police officers engaged in towing vehicles.

Policy

Public safety is the Department's primary concern and shall guide the application of this policy. When authorized to remove vehicles, officers shall remove such vehicles to an area which shall ensure the safety and well being of the occupants, security of the vehicle, and allow for safe and efficient flow of traffic.

All personnel and approved tow companies shall adhere to and comply with all Division Commanders' Standard Operating Procedures relating to towing, as well as the Department of State Police Tow Service Agreement SP 357.

Nothing in this policy shall prevent personnel assigned to Troop F from adhering to Massport towing regulations.

Causes for Removal

Officers are authorized to remove (or cause to be removed) any vehicle found upon a road/state highway when:

- The vehicle was stolen or taken without the owner's consent;
- The vehicle is disabled as to constitute an obstruction to traffic and/or is an obvious hazard;
- The operator of the vehicle is arrested and the vehicle would be left unattended on a public way;
- The vehicle is improperly parked or standing in violation of a state or municipal law or regulation;
- The operator of the vehicle is not properly licensed and there are no properly licensed occupants;
- The vehicle is not validly registered or insured;
- The vehicle, in its current condition, is too hazardous or dangerous to be driven;
- The vehicle is impounded/towed pursuant to MGL or state or federal court order; and/or
- Adverse weather conditions or other emergency reasons necessitate the removal in the interest of public safety, or when requested by the Massachusetts Highway Department or other agency having jurisdiction over maintenance of the roadway.

Continued on next page

Subject	Number
Towing	**TRF-09**

Causes for Removal (continued)

Public safety is of paramount importance when considering the time, manner, and method of off-loading and/or towing a large vehicle. The key determinants are current and impending road, weather, and traffic conditions.

All crash/recovery scenes should be cleared as quickly as possible in order to return the highway to its normal traffic flow. If necessary, cargo may be pulled/pushed to adjacent shoulders/medians before the vehicle is towed.

The off-loading and/or towing of large trucks involved in crashes and recoveries on high density/congested roadways should be avoided during peak commuter hours (0600-0900 hours and 1500-1830 hours) as it may contribute to additional delays and/or crashes.

Responsibilities of the Officer Towing a Vehicle

Officers shall inquire if there is a preference for a particular tow company and it shall be honored unless:

- The emergency requires expediency;
- Traffic conditions require immediate removal; and
- The response time of the tow company requested would be unreasonably long in the opinion of the on-scene officer(s) and safety dictates its removal.

When no request for preference is expressed, the officer shall inform the Station Desk Officer who will dispatch a tow company from the Station's Tow Company List that is approved to provide the required service.

Depending upon time of day, weather, or other variables, the officer shall remain with a disabled vehicle and its occupants until assistance arrives, or until the officer is assigned to a higher priority call for service. The officer may transport the occupant(s) to a safer location to make their own arrangements, if it is agreeable to the occupants.

If the officer at the scene makes an informed observation that a particular on-scene tow company is unable to safely and expediently remove a vehicle; they may request the services of the nearest available State Police Tow Company capable of handling the job.

When applicable, officers shall inventory the towed vehicle in accordance with TRF-10.

Responsibilities of the Station Desk Officer

The Station Desk Officer shall appropriately record the following via RAMS:

- The registration number and state;
- The location from which the vehicle was towed from including time and date;
- Make and description of the vehicle;
- The cause for removal;
- The name or identification number of the officer or proper authority requesting such removal; and
- The towing company name.

The officer requesting the tow shall notify or cause to be notified, the owner of record as soon as possible.

Responsibilities of the Station Commander

Station Commanders shall establish a Station Tow Company List based upon fair and equitable standards including, but not limited to: minimum response times, the maximum allowable number of tow companies, the provisions of this policy and all Division Commanders' Standard Operating Procedures relating to towing.

Fair and equitable standards shall include:

- A consideration of the financial and administrative burden of maintaining and administering the Station Tow Company Lists;
- The public interest and necessity for the prompt removal of wrecked, crashed, and disabled vehicles from the roadway;
- The maximum number of tow companies on a Station Tow List shall not exceed ten companies unless authorized by the Troop Commander; and
- Any additional factors that a Station Commander deems reasonably necessary.

Station Commanders shall be responsible for the oversight of station tow companies in their station areas and may suspend, terminate, and/or place on probation any station tow company consistent with the requirements of all Division Commanders' Standard Operating Procedures relating to towing and the State Police Tow Service Agreement SP 357.

Station Commanders shall appoint a Station Tow Officer to assist with the administration of this policy and to maintain records of all tow agreements and associated documents.

Station Commanders shall also maintain all required records necessary for the administration of this General Order and all Division Commanders' Standard Operating Procedures relating to towing.

Station Commanders, or his/her designee, may establish exclusive tow zones during natural or man-made emergencies in order to maximize public and officer safety.

Responsibilities of the Troop Commander

The Troop Commander shall ensure the effectiveness of the towing process by monitoring personnel under his/her command. The Troop Commander, or his/her designee, as Troop Tow Officer shall:

- Perform random line inspections;
- Order an immediate indefinite suspension without advance notice (until such time as the deficiencies have been satisfactorily corrected) for an event where a tow company's actions have resulted in a threat to public safety;
- Hold and preside over hearings relative to the appeal of a Station Commander's decision or suspension. The Troop Tow Officer may preside over appeal hearings at the discretion of the Troop Commander;
- Notify the tow company in writing of all decisions; and
- Ensure that Station Commanders maintain all records and Tow Service Agreements required by this General Order and all Division Commanders' Standard Operating Procedures relating to towing.

Subject	Number
Towing	**TRF-09**

References

Division Commanders SOP- TOWING
SP 357 – Tow Service Agreement
TRF-10 – Vehicle Inventory
MGL c.90, s.22C
720 CMR 9.04

Promulgated by:

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**TRF-10**

Subject

Vehicle Inventory

Policy

Any vehicle ordered towed, or in the custody of the Department, shall be inventoried and properly documented in order to protect:

- The vehicle and its contents;
- The Department and tow company against false claims of lost, stolen, or vandalized property; and
- The member(s) and the public from dangerous items that might be in the vehicle.

When to Inventory a Vehicle

An inventory is a non-investigative procedure in which the contents of a vehicle are itemized, and the condition of the vehicle is noted.

The Department shall inventory any vehicle ordered towed, removed, or impounded:

- As outlined within TRF-09 Towing;
- When involved in a crash, and the owner is unable to care for it;
- Pursuant to a lawful arrest when the vehicle would be left unattended; or
- As a seizure - the vehicle is subject to statutory forfeiture or lawful seizure pursuant to a governmental interest, such as:
  1. A seizure pending forfeiture;
  2. Company or corporation distress warrant; or
  3. The vehicle was used in the commission of a crime, as an instrument of a crime, or is stolen.

The inventory process should be conducted at the scene before towing the vehicle. If the scene is not safe or practical, the process may be done at another location, however the inventory shall be done within a reasonably short period of time.

Inventory Not Necessary

A motor vehicle inventory need not be taken if the vehicle is:

- Legally parked and locked;
- Abandoned and locked;
- Removed by a third party; or
- Disabled with the operator and/or occupants present, and is towed at their request.

Subject	Number
Vehicle Inventory	**TRF-10**

Inventory Procedure

The standard inventory procedure shall consist of a detailed inspection of the interior and exterior of the vehicle for damaged and missing parts, as well as to locate and record the contents of the vehicle. The following areas shall be inventoried:

- The interior of the vehicle;
- The glove compartment and trunk (unless they are locked and there is no key available); and
- The exterior of the vehicle for missing or damaged parts.

The inventory listing of personal items and valuables shall extend to all storage areas and compartments that are accessible to the operator or occupants. This encompasses:

- All open areas, including the floor areas, the area in and around the instrument panel and the rear deck above the rear passenger seat, the open area under the seats, the glove compartment and trunk, and other places where property is likely to be kept.

All closed but unlocked containers shall be opened, and each article inventoried individually.

Locked containers shall be inventoried as a single unit.

If an owner and/or operator requests to remove or entrust their possessions to another person, without it impeding the towing or impoundment process, such request may be granted, unless the member has probable cause to seize the items.

Search Warrants

A search warrant shall be obtained before the search of a locked container or forcing open a locked glove compartment or trunk, unless:

- Consent to open the container is obtained from its owner; or
- The member has probable cause to believe that such locked container shall put the member or others in immediate risk of injury or loss of life.

Subject	Number
Vehicle Inventory	**TRF-10**

Responsibilities

Position	Duties
Members	• Locate and secure any monies or articles of value that cannot be secured by the tow company; • Accurately record on the motor vehicle inventory form a complete listing of the general condition of the vehicle and its contents; • File the form in the station of jurisdiction; 1. Records shall be kept for one (1) year; and 2. Filed by date. • A copy of the form may be filed with any report of investigation; • Make, or cause to be made, any necessary administrative journal entries; • Ensure that all articles taken for safekeeping are stored in an appropriate container and secured in the station; and • An article of value may be left with the vehicle, if the owner so requests, by storing it in the trunk.
Station Commanders	• Provide a central location for members to file the motor vehicle inventory forms, and periodically review the forms for compliance with this policy; and • Ensure that property secured during the inventory procedure is returned to the rightful owners, as appropriate, and not kept longer than necessary.
Troop Commanders	• Strictly enforce the motor vehicle inventory procedure in order to avoid arbitrary application of the policy.

References TRF-09 Towing

Promulgated By:

Department of State Police
General Order

Effective Date	Number
October 1, 2019	**TRF-11**

Subject

Automatic License Plate Recognition

Purpose

The purpose of this policy is to establish guidelines and procedures for the proper use and application of the Automatic License Plate Recognition (ALPR) System within the Department of State Police (Department). Additionally, it is the purpose of this policy to provide Department personnel with guidelines and principles for the collection, access, use, dissemination, and retention of ALPR information to ensure that the information is used for legitimate law enforcement purposes only and the privacy, civil rights, and civil liberties of individuals are not violated.

Policy

The availability and use of the ALPR System provides opportunities for the enhancement of law enforcement agencies' productivity, effectiveness, and protection of public and officer safety.

The Department shall only utilize the technology in furtherance of official and legitimate law enforcement operations and public safety. All Department Employees shall abide by the guidelines set forth herein when using the ALPR System.

Definitions and Acronyms

Automatic License Plate Recognition (ALPR): Automatic license plate recognition technology uses high-speed cameras combined with sophisticated computer algorithms capable of converting the images of license plates to electronically readable data. The ALPR System captures an image of a license plate and converts it to a text file using Optical Character Recognition (OCR) technology. The technology also compares the digital images of license plates to the CJIS-NCIC Hot file database. The ALPR System is configured as either fixed, mobile, or portable.

Alert: A visual and/or auditory notice that is triggered when the ALPR System receives a potential hit on a license plate.

Alert Data: Information captured by an ALPR relating to a license plate that matches the license plate on a hot list.

ALPR Data: Scan files, alert data, and any other documents or data generated by, or obtained through, utilization of the ALPR System.

ALPR Data Query Logs: A record of a search or query of ALPR data.

Continued next page.

Definitions and Acronyms (Continued)

Hit: An alert that a license plate matches a record maintained in the ALPR database related to stolen vehicles, wanted vehicles, or other alert type files that support investigation or which have been manually registered by a user for further investigation.

Hot List: License plate numbers of vehicles of interest, such as stolen vehicles, unregistered vehicles, vehicles owned by persons of interest, and vehicles associated with AMBER Alerts, Missing Child Alerts, Missing College Student Bulletins, Silver Alerts, Incapacitated or Endangered Persons, Be On Look Out (BOLO), Attempt To Locate (ATL), and Wanted or Missing Person broadcasts or bulletins in which a license plate number is included, or other license plate numbers of interest entered by the Department or an authorized officer.

Hot List Download: The method by which the hot list data is transferred to a computer within a law enforcement vehicle.

Optical Character Recognition (OCR): The technology that supports the automated reading and digitizing of images of license plates that are captured by the ALPR System.

Authorized Uses

The provisions of this policy are provided to support authorized uses of ALPR information. Authorized uses may include, but are not limited to, the following:

- Investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime;
- Enhance Department's AMBER/SILVER or other law enforcement alerts and real-time response capability by deploying and networking ALPRs across the state to more rapidly identify and locate vehicles related to potential child-abduction or other serious crimes;
- Alert law enforcement that a particular license plate on a "hot list" (e.g., a stolen vehicle or a vehicle associated with a wanted individual) is in close proximity to an ALPR to dramatically reduce the recovery time of stolen vehicles and assist in locating dangerous and wanted individuals;
- Identify plates associated with potential witnesses and/or victims of crime;
- Support the Department's homeland security mission by protecting critical infrastructure from individuals who intend to damage or disrupt the systems and locations that allow for travel and the free flow of commerce;
- Identify vehicles linked to stolen license plates or other motor vehicle traffic violations;

Continued next page.

Authorized Uses (Continued)

- Provide situational awareness for law enforcement related to public safety or otherwise relevant to their authorized duties;
- Support local, state, federal, and tribal public safety departments in the identification of subjects associated with/as targets of criminal investigations;
- Support law enforcement response to critical incident responses and special events;
- Support special operations, such as high-crime-area patrols, gang investigation/suppression, operating under the influence initiatives, enforcement details, directed criminal investigations, and other investigations; and
- Support emergency and public safety situations including, but not limited to terrorist threats, kidnappings, missing persons, and felons actively traveling to or from a crime scene.

ALPR Administrator

The Division Commander of Field Services (DFS) shall:

- Designate a Commissioned Officer as the ALPR Administrator; and
- Ensure the ALPR Administrator has oversight for the ALPR System deployment, operations, and maintenance.

The ALPR Administrator shall be responsible for the following:

- Ensuring the proper selection of the personnel approved to operate the ALPR System and maintaining an adequate number of trained and authorized users;
- Authorizing any requests for ALPR System use or data access according to Department policy;
- Coordinating with all Divisions to ensure resources are available and deployed to meet Departmental investigative needs; and
- Ensuring that designated, trained personnel check equipment on a regular basis to ensure functionality, camera alignment, and removing from service any equipment that falls outside expected functionality until deficiencies are corrected.

The ALPR Administrator shall:

- Designate users who have been properly trained in the use and operational protocols of the ALPR System;
- Allow access to the ALPR System for those users with an approved login and password; and
- Ensure that any changes in hardware, software, policy, or law are the subject of continuing in-service training or bulletins.

Subject	Number
Automatic License Plate Recognition	**TRF-11**

ALPR Procedures

The use of ALPR technology shall be approved by the Colonel/Superintendent or designee.

ALPR System and information shall be:

- Accessed and used only for official and legitimate law enforcement purposes;
- Used for searches of historical ALPR data, in accordance with this policy and other Department policies or regulations where applicable; and
- Used for searches of ALPR data by members of this Department or by other law enforcement agencies through the ALPR Administrator.

ALPR Operations

Members using the ALPR System shall:

- Ensure, at the start of each shift, the ALPR System has been updated with the most current hot lists available;
- Verify, prior to use, the aim of the ALPR camera(s) to ensure it is focused on the correct lanes of traffic;
- Ensure ALPR equipment be cleaned and maintained according to the manufacturer's recommendations; and
- Notify the ALPR Administrator of any malfunctions.

ALPR Alerts/Hits

The member shall, prior to initiation of a stop, based on an ALPR Hit or Alert:

- Visually verify that the vehicle plate number matches the plate number run by the ALPR System, including both:
  1. Alphanumeric characters of the license plate; and
  2. The state of issue.

- Verify the current status of the plate through:
  1. The Commonwealth's Criminal Justice Information System (CJIS), or
  2. National Crime Information Center (NCIC), or
  3. Department's Records Management System (RMS), or
  4. Other appropriate source of data, when circumstances allow, or as soon as practicable.

License plate numbers and date/time location collected through an ALPR may not be, when taken alone, sufficient to identify the individual associated with the vehicle. The Department may be able to link the ALPR information to an individual through additional use and combination with other information, such as a check of vehicle registration. Thus, even though the ALPR information the Department accesses may be the result of an ALPR system's automated collection of license plate numbers, it is the investigative process that identifies individuals.

Manual Entry of Data/Manual Hot List

Manual entries may include, but should not be limited to:

- AMBER Alerts;
- Missing Child Alerts;
- Missing College Student Bulletins;
- Silver Alerts;
- Be On Look Out (BOLO);
- Investigative needs;
- Attempt To Locate (ATL); or
- Wanted or Missing Person broadcast or bulletin in which a license plate number is included.

Manual entries entered into the ALPR System shall be:

- Manually updated when the information changes or is no longer current;
- Documented with the specific reason by the member;
- Documented with agency case number; and
- Given a retention date of 1 year or less.

ALPR Data: Logs, Sharing, Dissemination, and Retention

The following process shall apply to ALPR Data:

- A Query Log is internally maintained by each instrument for each transaction;
- Data can be accessed, retrieved, or shared for official and legitimate law enforcement business only; and
- Retention of data shall be determined by the Department of Criminal Justice Information Services (DCJIS) Policy.

The Department will prohibit access, use, or dissemination of ALPR information for:

- Any purpose that violates the Constitution or laws of the United States or the Commonwealth of Massachusetts, including the protections of the Fourth Amendment;

- Based solely on an individual's or organization's religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their race, ethnicity, citizenship, place of origin, age, disability, gender, gender identity, sexual orientation, or other classification protected by law;

- Non-law enforcement or personal purposes;

- The purpose of prohibiting, infringing upon, or deterring individual activities protected by the First Amendment, such as freely practicing one's religion, freedom of speech and peaceful assembly, freedom of the press, and the right to petition the government for the redress of grievances;

Continued next page.

ALPR Data: Logs, Sharing, Dissemination, and Retention (Continued)

- Harassing and/or intimidating any individual or group;
- Targeting of any individual or group by means of camera placement or data use in a discriminatory manner; and
- Any other access, use, disclosure, or retention that would violate applicable law, regulation, or policy.

The Department protects all ALPR information as personally identifiable information (PII) because ALPR information may be combined with other information to specify a unique individual (i.e., the identity of an individual could be directly or indirectly inferred by using information that is linked or linkable to that individual).

Information Quality Assurance

Original ALPR information will not be altered, changed, or modified in order to protect the integrity of the data. Any changes will be maintained as a separate and additional record, and such record will be identified as having been modified.

The Department will correct, notate, delete, or refrain from using ALPR information the Department originated and found to be erroneous or deficient. Originating agencies external to the Department are responsible for reviewing the quality and accuracy of the ALPR information provided to the Department and must take reasonable steps to correct or amend the information upon learning that it is inaccurate or deficient.

The Department will advise the appropriate point of contact, in writing or electronically, when its ALPR information is alleged, suspected, or found to be erroneous or deficient.

Security

The following shall apply to ALPR system and information security:

- The Department of Criminal Justice Information Services of the Executive Office of Public Safety and Security will operate ALPR servers in a secure facility protected from external intrusion and will utilize secure internal and external safeguards against network intrusions. Any access to DCJIS ALPR information from outside the facility will be allowed only over secure networks;
- The Department and DCJIS will store ALPR information in a manner that ensures that it cannot be added to, modified, accessed, or purged except by personnel authorized to take such actions;
- Access to Department ALPR information will be granted only to personnel whose positions and job duties require such access and who have successfully completed a background check and training;

Continued next page.

Subject	Number
Automatic License Plate Recognition	**TRF-11**

Security (Continued)

- Usernames and passwords to ALPR information are not transferrable, must not be shared by Department personnel, and must be kept confidential;
- Queries made to the Department's ALPR information will be logged into the system identifying the user initiating the query. All user access, including participating agency access, and queries are subject to review and audit; and
- The Department and DCJIS will maintain an audit trail of accessed, requested, or disseminated Department-held ALPR information. An audit trail will be kept for a minimum of one-year of requests for access to ALPR information for specific purposes and of what ALPR information is disseminated to each individual in response to the request.

State Central Repository

The Department has agreed to:

- Electronically submit captured ALPR data to the state repository maintained by the DCJIS at the Commonwealth's Public Safety Data Center.

The Department and its users agree to the terms of this policy and to the Commonwealth of Massachusetts *Global Justice and Public Safety Information Sharing Policy* of the DCJIS.

Policy Review

The ALPR Administrator shall be responsible for:

- The annual review of this policy and the procedures contained herein; and
- Making recommendations through channels to the Colonel/Superintendent or designee, for any necessary amendments.

As use of the technology progresses, the Department shall continue to monitor and assess the appropriateness of this policy, as new technology may raise both legal and technological issues.

References

Executive Office of Public Safety and Security (EOPSS) - *The Commonwealth of Massachusetts Global Justice and Public Safety Information Sharing Policy*
Executive Office of Public Safety and Security (EOPSS) - Department of Criminal Justice Information Services - *Automatic License Plate Recognition System Central Repository Companion Policy.*

Promulgated By: Colonel Kerry A. Gilpin

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**TRF-12**

Subject

Crash Investigations

Policy

To establish guidelines for traffic crash reporting and investigations

Definitions

Crash: A motor vehicle collision with any other vehicle, object, or person.

Crash Investigation: The systematic recording and examination of the involved vehicles, the roadway, and human factors, to determine the cause of the collision, contributing factors, and determination of violations of law.

Crash Reporting: The basic data collection needed to identify the operators and the particulars of every crash referred to Massachusetts General Laws (MGL) c.90 s.26.

Crash Reconstruction: The technical analysis of all available information and physical evidence to determine how and potentially why the crash occurred.

Commercial Motor Vehicle: A motor vehicle used in commerce, and designed or used to transport passengers or property, which has a gross vehicle weight rating (GVWR) of 10,000 or more pounds, or which is designed to transport more than eight (8) passengers (including the driver), or which transports hazardous materials and is required to be placarded in accordance with federal law.

Serious Bodily Injury: Any bodily injury which creates a substantial risk of death or which involves either total disability or the loss or substantial impairment of some bodily function for a substantial period of time.

Reporting Requirements

Members shall conduct an on-scene investigation and complete Registry CRA-65 Motor Vehicle Crash Report whenever a crash results in:

- A death;
- Personal injury;
- Any violation of law exists;
- Any damage occurs to a Federal/State/Municipal vehicle; or
- Property damage per MGL c. 90 s.26.

For crashes not meeting the above requirements members shall assist the operator(s) with the exchange of any pertinent information and safely clear the crash scene. Members may utilize a SP 256 Crash Data Exchange Form.

Station Desk Officer

Desk Officers shall:

- Dispatch members as needed to respond to the scene of any reported crash;
- Make an entry into the Daily Administrative Journal (DAJ) on all calls for service with appropriate findings;
- Make every attempt to identity callers for investigative purposes;
- Contact MassHighway to respond with necessary equipment (such as arrow boards, cones, curiosity screens, message boards, signage, etc.);
- Notify the Troop Duty Officer of any serious injury or fatal crash;
- Ensure Media Relations is made aware of any serious injury or fatal crash by faxing the SP 640 Serious Crash Fact Sheet directly to Media Relations and GHQ Communications; and
- Notify the Registrar of Motor Vehicles of all crash fatalities immediately through the CJIS "FATAL" screen.

Responding Members

All responding member(s) shall:

- Exercise sound judgment in proceeding to the scene;
- Position the cruiser and/or flares in such a manner as to provide maximum protection for the crash scene;
- Render first aid to the injured, pending arrival of emergency medical personnel;
- Direct traffic safely around crash scene;
- Retain charge of the scene pending the arrival of the assigned patrol, department of jurisdiction, or any supervisory personnel;
- Ensure roadway is clear of debris e.g., flares, cones; and
- Expedite quick road clearance re: TRF-05 Traffic Incident Management.

Primary Investigating Officer's Responsibilities

In addition to the above duties the primary investigating member shall:

- Comply with all reporting procedures;
- Take appropriate enforcement action when sufficient evidence exists;
- Notify the Troop Duty Officer if the crash results in serious injury or death;
- When applicable, utilize findings and measurements determined by the Collision Analysis and Reconstruction Section (CARS) member as the official record for reference throughout the investigation;
- Request to the station of jurisdiction an entry into the DAJ documenting the time cleared and when traffic is back to normal; and
- Submit a CRA-65 to a supervisor, within ten (10) days for approval.

Troop Duty Officer

Upon notification of a crash resulting in serious injury or death, as appropriate notify:

- On call member from CARS;
- Crime Scene Services;
- The District Attorney's Office of jurisdiction; and
- Media Relations.

Troop Duty Officers shall follow the CARS call-out protocol set forth by the CARS Commander.

Note: Ensure that MassHighway has been contacted to respond with necessary equipment when CARS members are responding to crashes on limited access highways.

Station Commander

Station Commanders shall:

- Review all reports for accuracy, completeness, and legibility; and
- Ensure the reports are forwarded to the Registrar of Motor Vehicles within fifteen (15) days.

Crash Reported at Construction Sites

When a crash occurs on the scene of a construction detail under the control and jurisdiction of the Department, the Desk Officer shall:

- Dispatch a patrol to investigate and take appropriate action; or
- If the detail officer is not involved in the crash, assign the member working the detail to investigate the crash when no patrol is available.

Reports for Death or Serious Injury

Motor vehicle crashes occurring on a public way resulting in death or serious injury require an incident report that may include:

- Observations from eye witnesses;
- Observations of hospital personnel;
- Forensic evidence (of operation) such as fingerprints, hair, blood, clothing fibers, etc. that places the occupants accordingly;
- Seat positions;
- Matching damage to the interior of the vehicle to defendant's and passenger's injuries;
- Evidence from occupant protection devices such as seat belts and air bags;
- Evidence of contact with glass in the vehicle;
- Any other pertinent information or evidence; and
- Preliminary findings from the CARS reconstructionist.

Off-Road/ Recreation Vehicles

Off road recreational vehicle crashes occurring on public ways shall:

- Be investigated and reported on the standard CRA-65; and
- The standard uniform citation can be utilized as a complaint application for a recreational vehicle operated on a public way in violation of MGL c. 90B s.25.
  Note: If needed, under the Executive Office of Energy and Environmental Affairs, the Massachusetts Environmental Police may be called for assistance at (800) 632-8075.

Crashes occurring on private property that involve a motor vehicle, or an off-road recreational vehicle, and resulting in death or serious injury shall:

- Be investigated and reported following the same reporting requirements and procedures set forth for death and serious injury crashes.

Crashes involving only property damage that occur on private property, not open to the general public, shall not require an investigation.

Collision Analysis and Reconstruction Section

CARS may be used for the following purposes:

- When any crash involves a fatality;
- When any serious injury crash involves a strong possibility of criminal charges being filed;
- When any Department vehicle collision involves serious injury/death;
- When any serious injury occurs at a work zone where a member is working a paid detail;
- When any Department pursuit results in serious injury or death;
- Upon request by another police department/agency;
- Upon request of the District Attorney's Office, Fire Marshal's Office, or Attorney General's Office for assistance in forensic mapping of crime scenes; and
- As directed by the Troop/Section Commander.

CARS shall:

- Assist the primary investigator and shall not assume full responsibility for any investigation, unless ordered to do so by the Troop/Section Commander; and
- Forward an approved copy of the final report to the primary investigator for proper filing.

Local Cruiser Crash Investigations

Upon a request for a crash investigation involving a local police department, the request shall:

- Be made by the officer-in–charge (OIC) of the requesting department to the Troop Duty Officer.

Troop Duty Officers shall:

- Assign a supervisor (preferably of a higher rank than the officer involved) to conduct a crash investigation.

Continued next page.

Local Cruiser Crash Investigations (Continued)

Investigating Officers shall:

- Conduct an investigation and determine the cause;
- Take immediate enforcement action as necessary;
- Prepare an incident report;
- Submit the incident report together with a CRA-65 for review to the Troop Commander within seventy-two (72) hours of the crash.

Troop Commanders shall:

- Upon approval, forward a copy of the crash investigation to the local police department chief or designee for final disposition.

Crashes/ Commercial Motor Vehicles

Troop Duty Officers shall notify the Commercial Vehicle Enforcement Section (CVES) of all significant commercial motor vehicle crashes when they:

- Cause a major disruption of normal traffic;
- Involve serious injury or a fatality;
- Cause extensive property damage;
- Involve hazardous or radioactive materials;
- Involve violations of law; or
- Are requested by the investigating officer.

The "Truck and Bus Information" section of the CRA-65 shall be completed by the primary investigator with CVES assistance.

Crashes with Deer and Disposition

Eligible Person: A resident of Massachusetts who is an operator or an occupant of a vehicle that strikes a deer.

Members shall be aware that 321 CMR 2.04 allows an eligible person, to salvage the deer in accordance certain stipulations.
Members shall:

- Ascertain if there is an eligible person who wishes to take possession of the deer;
- Advise the eligible person to immediately notify the Massachusetts Environmental Police;
- Ensure an DAJ entry includes the name, address, and telephone number of the eligible person; and
- Notify MassHighway if no eligible person is available to, or declines to take possession of the deer carcass.

Release of Crash Reports

Private Individuals/Businesses

Private individuals, whether representing a business or themselves, are required to obtain crash reports from the Registry of Motor Vehicles.

Instructions for obtaining crash data can be found on the internet at: http://www.mass.gov/rmv/forms/accrecform.pdf.

State Employees/Representatives

Members shall release unredacted crash reports to:

- Employees of the Massachusetts Highway Department when an official(s) appears in person and is properly identified.

Representatives of private companies, under State contracts, responsible for repairs may be allowed to access crash report/record information available at Department facilities, under the following conditions:

- For the purpose of identifying monetary liability in crashes which resulted in damage to the infrastructure of the State highway system;
- Crash reports shall be accessed and copied under the supervision of a Department member; and
- The Station Commander, or designee, shall be responsible for blacking out, the dates of birth and operator license numbers of all parties contained within the crash report.

Specific questions or concerns about the applicability of the Public Records Law or any other statute authorizing or restricting access to such material shall be directed to the Department's Legal Section at (508) 820-2311.

References

49CFR part 172, sub-part F.
MGL c. 90 s.26 & c. 90 s.29
321 CMR 2.04 Salvage, Disposition , and Possession of Deer Killed
Criminal Justice Information System (CJIS)

Promulgated By:

Department of State Police
General Order

Effective Date	Number
July 22, 2014	**TRF-14**

Subject

Operating Under the Influence-Alcohol

Policy

To promote traffic safety through the detection, arrest and prosecution of persons operating a motor vehicle while under the influence of alcohol.

Definitions

Breath Test Operator (BTO): A member certified to administer a breath test in accordance with 501 CMR 2.00.

Officer-in-Charge of Instruments (OIC): A BTO, designated by a Troop Commander responsible for maintaining station/unit breath test devices.

Office of Alcohol Testing (OAT): Established within the Department's Forensic Services Group that oversees the State's Breath Test Device Program and Breath Test Operator Training.

Preliminary/Portable Breath Test Device (PBT): A breath test device, used to administer a screening test, that is capable of quantifying the amount of alcohol in a breath sample or calibration standard.

Standardized Field Sobriety Test(s) (SFST): A test or tests administered to a person prior to arrest and designed to assist in the detection of impairment due to alcohol.

Standardized Field Sobriety Tests

- These tests should be administered by the member, if able, in accordance with training and the procedures outlined in the SFST Manual; and
- A PBT Device when used as a field sobriety test should be the **last** test administered.
  Note: Please refer to TRF-14B Preliminary/Portable Breath Test Device for further information.

Post Arrest Breath Tests

All post arrest breath tests shall be conducted:

- By a certified BTO, however refusals maybe entered by either a certified BTO or by an uncertified Department employee;
- In accordance with 501 CMR 2.00 and Massachusetts General Laws (MGL) c. 90 s. 24;
- In accordance with training and operational procedures developed by the OAT;

Continued next page.

Subject	Number
Operating Under the Influence-Alcohol	**TRF-14**

Post Arrest Breath Tests (Continued)

- At the station of jurisdiction in which the arrest was made; or
- At any station or department having an operational breath test device; or
- In the Department's Breath Alcohol Testing (BAT) vehicle.

Note: If the result of the post arrest breath test is 0.05% BAC or less, there shall be a permissible inference that such defendant was not under the influence of intoxicating liquor, and they shall be released from custody forthwith per MGL c. 90 s. 24, unless other charges support continued incarceration.

Blood Tests

Individuals arrested for operating under the influence (OUI) of alcohol and being treated at a medical facility licensed under MGL c. 111 s. 51 may be offered an opportunity to submit to a blood test in lieu of a breath test.

Refusals

If after being advised of their rights and the consequences of refusing to submit to a test, the individual refuses to submit to a test, none shall be given.

- All refusals, breath and blood, shall be entered into the Breath Alcohol Testing System (BATS) and noted in the Daily Administrative Journal (DAJ);
- Once a refusal is entered into the BATS, no test shall be given;
- Refusal may be entered by a certified BTO or by an uncertified Department employee;
- Refusals shall be witnessed by a third party other than the defendant and the refusal officer; and
- The refusal witness shall be noted within the report and BATS.

Protective Custody

Subjects who have been bailed, after having been arrest for operating under the influence and are placed into protective custody, the Arresting Officer or Desk Officer shall:

- Process the subject according to MGL c. 111B;
- Re-enter the protective custody into the DAJ: and
- Ensure an SP 850 Protective Custody form is completed with a separate report and log entry made.

Subject	Number
Operating Under the Influence-Alcohol	**TRF-14**

Responsibilities

Position	Duties
Arresting Member	• Advise the prisoner of their rights and consequences as outlined in the Statutory Rights and Consent form during the booking process; • If certified as a BTO, administer the breath test; • If not a certified BTO, ensure the breath test is administered by a certified BTO; • If the arrestee refuses to submit to a breath test, enter the refusal into the BATS; • If data entered into BATS is found to be incorrect, complete a BATS Data Correction Form, and fax to the RMV and OAT; • Complete all required documents and reports; and • Ensure arrestee is given suspension notification(s) if they fail the evidential breath test or refuse to submit to a breath test. Note: All required documents and reports shall be completed and signed by the arresting member and/or BTO.
Breath Test Operator	• If the arrestee refuses to submit to a breath test, enter the refusal into the BATS; • Administer a breath test in accordance with Chapter 90, §24 and 501CMR 2.00; • If data entered into BATS is found to be incorrect, complete a BATS Data Correction Form, and fax to the RMV and OAT; • Complete all required documents and reports; and • Ensure arrestee is given suspension notification(s) forthwith. Note: All required documents and reports shall be completed and signed by the arresting member and/or BTO.
Desk Officer	• Notify the bail commissioner and advise them if the prisoner requests to exercise their rights per MGL c. 263 s. 5A; and • Make appropriate entries into the DAJ.

Continued next page.

Subject	Number
Operating Under the Influence-Alcohol	**TRF-14**

Responsibilities (Continued)

Position	Duties
Supervisor	• Ensure compliance with this policy and the completion of all required documents and reports.
Troop Traffic Programs Officer	• Document the date, time and location of each OUI related arrest and crash within their Troop; and • Maintain monthly OUI related reports as may be required by the Traffic Programs Section.
Troop Commander	• Designate OIC of Instruments and ensure they perform all assigned duties regarding station/unit breath test devices; and • Oversee the OUI enforcement efforts within their jurisdiction.
Officer-in-Charge Instruments	• Provide guidance and assistance to BTOs and members entering refusal data; • Ensure arrestee has been suspended if they fail the evidential breath test or refuses to submit to a breath test; • Ensure station/unit breath test devices, supplies, and current reference manuals are maintained and readily accessible; • Troubleshoot breath test devices and perform periodic tests as prescribed by OAT; • Maintain calibration stations for members who have been issued PBTs; • Coordinate with both OAT and individual members for all breath test devices certifications, calibration, repairs, and loaner/replacement units; • Maintain station records of all periodic tests performed as prescribed by OAT; and • Testify as the Keeper of Records in all prosecutions within their jurisdiction.

Subject	Number
Operating Under the Influence-Alcohol	**TRF-14**

References

TRF-14B Preliminary/Portable Breath Test Device
SP 850 Protective Custody Form
MGL c. 90 s. 24, c.111 s. 51, c.111B s. 7, c.111B s.8, c.263 s.5A
C.M.R 501 2.00 (Safe Roads Act)
Office of Alcohol Testing-Case Law Updates
Statutory Rights and Consent Form
BATS Data Correction Form
Breath Test Operators Manual
Preliminary Breath Testing Manual
Standardized Field Sobriety Testing Manual

Promulgated By:

Department of State Police
General Order

Effective Date	Number
July 22, 2014	**TRF-14A**

Subject

Operating Under the Influence-Drugs

Policy

To promote traffic safety through the identification, arrest, and prosecution of persons found to be operating a motor vehicle while under the influence of a drug(s).

Definitions

Drug Recognition Expert (DRE): A member who has successfully completed a National Highway Traffic Safety Administration (NHTSA) approved program and is certified by the International Association of Chiefs of Police (IACP) as a Drug Recognition Expert.

DRE Department Coordinator: A member designated by the Division of Standards and Training as the program coordinator responsible for DRE selection, retention, training, and protocols.

Drug: Any substance, when taken into the human body, which impairs the mental or physical abilities of the person taking it. This definition does not include the ingestion of ethyl alcohol.

Categories of Drugs:
- Central Nervous System (CNS) depressants;
- Central Nervous System (CNS) stimulants;
- Hallucinogens;
- Dissociative anesthetics,
- Narcotic analgesics;
- Inhalants; and
- Cannabis.

Requests for DRE

A request for the assistance of a DRE shall be made to the Troop Duty Officer. If approved, the Troop Duty Officer shall:
- Ascertain if a DRE is working; and
- If available, have the DRE respond to the requesting member/agency.

Subject	Number
Operating Under the Influence-Drugs	**TRF-14A**

Criteria for a DRE Evaluation

The investigating member may request a DRE, through the Troop Duty Officer, when any of the following circumstances exist:

1. The detainee is under arrest and being charged with Operating Under the Influence in violation of Massachusetts General Laws (MGL) c.90 s.24, if :
   - The detainee displays signs and symptoms of impairment associated with drug use; or
   - The detainee refused to submit to a breath test, or submits to a breath test with the result less than .08 BAC, and drug use is suspected; or
   - The detainee consents to a DRE evaluation.

2. Cases involving arrests or investigations for violations of MGL c.94C possession of drugs (that may or may not be associated with a driving offense), if:
   - The detainee consents to a DRE evaluation;
   - The DRE's opinion may help establish an affirmative link between the subject and the drugs; and
   - The requesting member provides the Troop Duty Officer with a substantial rationale for the services of a DRE.

3. In any other cases where a DRE may be beneficial.

Responsibilities

Position	Duties
Drug Recognition Expert	• Ensure that the individual's statutory rights are communicated and understood; • Conduct an evaluation consistent with the twelve (12) step protocol as set out in the DRE Program; • Ensure that a parent, guardian, or legal custodian is present for juveniles who are under the age of eighteen (18) years; • Complete a Drug Influence Evaluation Report to be submitted with the arrest report; and • Forward a copy to the Department DRE Coordinator.
Department DRE Coordinator	• Develop a standard operating procedure (SOP) to include training, protocols, and the selection process of DRE officers; and • Maintain a list of DRE trained members.

Specimen Collection

When consent is given, the DRE shall collect a urine sample using the following procedures:

Step	Action
1	• The defendant shall sign the SP 606 Consent to Toxicology form.
2	• Use a sterile specimen container.
3	• Adults shall be escorted to a cell with a toilet; or • Juveniles shall be escorted to a restroom, not a cell.
4	• The DRE shall collect the specimen from the subject ensuring that there is no opportunity for specimen tampering or adulteration; • If the DRE is not of the same gender as the subject then: 1. A request shall be made for the assistance of another member who is of the same gender as the subject; 2. The assisting member shall collect the subject's specimen and transfer the specimen to the DRE; and • The DRE shall ensure the proper chain of custody is reflected on all documentation regarding specimen collections.
5	• Once the sample is deposited into the container, the DRE shall: 1. Seal the container; 2. Indicate on the container the subject's name, time and date; 3. Place the container into a plastic evidence bag; 4. Place copies of the SP 604 Drug Influence Evaluation Report and the SP 603 Toxicology Request Form with the evidence bag; 5. Secure the evidence bag and container within the evidence refrigerator at the Troop Headquarters; 6. Request the Troop Duty Officer to make an entry into the Daily Administrative Journal of the evidence being secured at the Troop Headquarters; and 7. Ensure the specimen is transported to the Department Crime Laboratory for analysis as soon as is practical.
6	• The arresting member shall enter the sample as evidence into the Evidence Control System.

Subject	Number
Operating Under the Influence-Drugs	**TRF-14A**

References

SP 603 Toxicology Request Form
SP 604 Drug Influence Evaluation Report
SP 606 Consent to Toxicology
MGL c.90, s.24
MGL c.94C
MGL c.111, s.51
MGL c.111B, s.7 and s.8
MGL c.263, s.5A
CMR501 2.00 (Safe Roads Act)
Statutory Rights and Consent Form
Commonwealth v. Hampe, 646 Mass. N.E.2d 387 (1995)
Commonwealth v. King, 429 Mass. 169 (1999)
Commonwealth v. O'Connor, 406 Mass. 112, 115, 546 N.E.2d 336 (1989)
Commonwealth v. McGeoghegan, 389 Mass. 137 (1983)
Breath Test Operators Manual
Breath Test Re-certification Manual
Standardized Field Sobriety Testing Manual
Preliminary Breath Testing Manual

Promulgated By:

Department of State Police
General Order

Effective Date	Number
July 22, 2014	**TRF-14B**

Subject

Preliminary/Portable Breath Test Devices

Purpose

To provide guidance for the proper use, documentation, and maintenance of Preliminary/Portable Breath Test (PBT) instruments.

Policy

All devices approved and issued by Traffic Programs Section shall be operated and maintained in accordance with approved Department training.

Definitions and Acronyms

Officer-in-Charge (OIC): The keeper of the breath test records for instruments assigned to their individual barracks or unit.

Office of Alcohol Testing (OAT): Established within the Department Forensic Services Group that oversees the State's Breath Test Device Program and Breath Test Operator training.

Preliminary/Portable Breath Test Device (PBT): A breath test device, used to administer a screening test, that is capable of quantifying the amount of alcohol in a breath sample or calibration standard.

Preliminary/Portable Breath Test Operator: A member trained to administer preliminary breath test.

Calibration and Certification

OIC and members issued a PBT Device shall:

- Successfully complete an operator training program;
- Adhere to Department of State Police guidelines for PBT Device maintenance and operation;
- Perform accuracy checks monthly according to Department of State Police guidelines;
- Ensure that a PBT Device is taken out of service immediately when found not to be working properly;
- Notify Traffic Programs of a PBT Device taken out of service and in need of repair thus following repair arrangements made by OAT; and
- Ensure the PBT Device is certified annually, at the Office of Alcohol Testing, as directed by the Traffic Programs Section.

Subject	Number
Preliminary/Portable Breath Test Devices	**TRF-14B**

Records

OIC and members issued a PBT Device shall:

- Ensure records are maintain within their assigned station/unit per Department of State Police training; and
- Forward copies of the monthly accuracy checks to the Traffic Programs Section.

Traffic Programs Section

The Traffic Programs Section shall maintain an inventory of all issued PBT Devices and the inventory shall include:

- The member's station or unit assigned;
- Model and serial number of each PBT Device; and
- The Department Inventory Control number.

Testimony

Members should be aware that the following elements may be required in court testimony:

- Date, time, test number, subjects name and result of the blood alcohol contents percentage (BAC %);
- Department SP 691 Preliminary/Portable Breath Test (PBT) Log;
- The PBT Device was operating properly;
- The PBT Device was properly calibrated and certified;
- The training, qualifications and certification of the member; and
- PBT Device was used as the **last** field sobriety test.

Limitations

The acceptance of PBT Devices within the court system is dependant upon the member's :

- Proper care and effective use of the PBT Device;
- Appropriate PBT Device training and certification; and
- Use in combination with Standardized Field Sobriety Tests.

References

SP 691 Preliminary/Portable Breath Test (PBT) Log
Commonwealth v. Gary F. Goller, Trial Court Dept. Concord D.C. Docket No. 9647-CR-2063
Commonwealth v. Blais 428 Mass. 294 (1998)
National Highway Traffic Safety Administration (NHTSA) *DWI Detection and Standardized Field Sobriety Testing*

Promulgated By:

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**TRF-15**

Subject

Sobriety Checkpoints

Policy

When utilized, Sobriety Checkpoints shall be conducted in conformance with judicial guidelines.

Key Considerations

In the preparation and execution of any Sobriety Checkpoint, the following considerations shall receive special attention:

- Motorist safety shall be assured;
- Motorist inconvenience shall be minimized;
- The action undertaken shall be in accordance with a written plan devised by supervisory personnel and developed prior to implementation of the checkpoint;
- Selection of vehicles to be stopped shall not be arbitrary;
- Advance public notice shall be given to reduce motorist surprise, fear, and inconvenience; and
- A trained Commissioned Officer shall be in charge.

Site Safety

The Officer In Charge (OIC) of the Sobriety Checkpoint shall ensure compliance with the following Work Zone Safety Guidelines:

- Physical barriers shall not be used;
- Sufficient warning signs shall be placed ahead of the checkpoint to provide advance notice for on-coming vehicles;
- Signs should be illuminated or constructed of highly reflective material;
- Sufficient road flares, reflectors, or cones should be used to safely control traffic;
- Auxiliary and/or sufficient street lighting should be in place to illuminate the checkpoint;
- There shall be sufficient law enforcement presence to reduce fear and apprehension, minimize inconvenience, and ensure compliance;
- All officers shall be in uniform;
- All officers shall wear an issued traffic vest, reflectorized belt, or other high visibility clothing;
- Officers shall position themselves so they can be easily observed by motorists;
- Officers shall give visual stop/start commands;
- Marked cruisers shall be utilized as site safety vehicles;
- All cruisers shall have operable visual emergency warning devices; and
- Cruisers shall be positioned in compliance with the predetermined plan.

Continued next page.

Site Safety (continued)

Vehicles shall be waved through the Sobriety Checkpoint without stopping when:

- Traffic is backed up to the safety officer; or
- A commercial vehicle with a gross vehicle weight rating (GVWR) greater than 10,000 pounds causes sight obstructions.

Vehicles which are transporting flammable liquids (including compressed gas as a motor fuel), hazardous materials or explosives as the cargo or a part thereof shall not be parked within three-hundred (300) feet of any portion of the check-point where flares are being utilized. In addition, such vehicles shall be allowed to pass through the checkpoint without stopping.

Site Selection

Individual site selection shall be made based upon selective enforcement identifiers of alcohol related traffic crashes or prior OUI violations such as:

- Time;
- Day of the week; and
- Location.

Site selection data for each Sobriety Checkpoint shall be retained by the Troop Traffic Programs Officer for a period of five (5) years.

Safety considerations for the site location should include:

- Motorist/officer safety;
- Sight visibility;
- Traffic volume and pattern;
- Operator reaction time; and
- Operator stopping distance.

Parking lots, rest areas, or wide shoulders immediately adjacent to the Sobriety Checkpoint should be available and accessible for use as a screening area. This shall ensure that vehicles can be directed out of the normal flow of traffic without creating a traffic safety hazard.

Advance Notification

The OIC shall coordinate activities with Media Relations to ensure that:

- Announcements to the appropriate electronic and print media shall be made, at a minimum, three (3) business days prior to the implementation;
- The press release provides the overall purpose of the Sobriety Checkpoint, thereby allowing the Department to gain the public acceptance, support, cooperation, and voluntary compliance of the endeavor;
- The press release specifies the county the Sobriety Checkpoint shall be conducted in, but does not detail the precise location or hours of implementation; and
- Any inquiries pertaining to the Sobriety Checkpoint are referred to the appropriate Troop Commander.

Subject	Number
Sobriety Checkpoints	**TRF-15**

Operational Plans

Individual Sobriety Checkpoint plans shall be prepared in advance of the date of actual implementation. These plans shall include, at a minimum:

- Date;
- Time and duration;
- Site selection and justification;
- Set patterns of vehicles to be stopped;
- Personnel, assignments, and responsibilities;
- Training for this particular sobriety check-point;
- Field sketch detailing the Sobriety Checkpoint logistics and site configuration;
- Notifications; and
- Equipment and materials needed.

These plans shall be strictly adhered to. There shall be no arbitrary or random modification of Sobriety Checkpoint procedures.

Officers may make suggestions for changes due to extenuating circumstances, but only the OIC can authorize and approve any changes in plans.

All officers shall be briefed and trained on details of the specific plan prior to the start of each Sobriety Checkpoint.

Operational plans shall be maintained at the Troop Headquarters and retained for a period of five (5) years. A copy shall be forwarded to the Traffic Programs Section.

Site Configuration

Site configuration shall be as follows:

- Each Sobriety Checkpoint shall have a clearly marked warning sign;
- All signs, signals, markers, traffic cones, flares, or reflectors shall be placed in accordance with the Work Zone Safety Guidelines;
- The position of the cones, flares, or reflectors should guide vehicles to the appropriate lane of travel and are parallel to the stop location; and
- The position of the cones, flares, or reflectors around the stop location should provide as much protection to the officers in that location as possible.

Subject	Number
Sobriety Checkpoints	**TRF-15**

Stopping Vehicles

The selection of vehicles to be stopped shall be either:

- Every vehicle; or
- A set pattern, e.g., every other, every third vehicle, or other set number desired.

Vehicles stopped at the checkpoint should be greeted for a period of one (1) minute or less.

The operator and/or passengers shall remain within the vehicle to minimize the intrusion.

If there is reasonable suspicion, based upon articulable facts, that the operator and/or passenger(s) is committing or has committed an OUI violation or other violation of law, that vehicle shall be directed from the normal flow of traffic and the offender(s) checked further.

Cruisers

All Department vehicles shall be placed at Sobriety Checkpoint in such a manner as the OIC deems appropriate for safety purposes.

Personnel

The number of uniformed officers needed for a Sobriety Checkpoint shall vary according to site and take into consideration visible authority, motorist safety, and minimizing inconvenience.

There shall only be one (1) Commissioned Officer as the OIC of a Sobriety Checkpoint.

Responsibilities

Position	Duties
Division Commander of Field Services	• Annually, confer with the Traffic Programs Section regarding the efficiency of Sobriety Checkpoints; • Make a determination as to whether or not such checkpoints shall be utilized as a component of the OUI Countermeasures Program; and • Issue a Division Commander's Order directing all Troop Commanders to gather intelligence regarding potential sites for the deployment of checkpoints during the coming year, if such checkpoints are to be utilized.
Troop Commanders	• Shall designate a Commissioned Officer to conduct the site selection and operational planning for each Sobriety Checkpoint; • Approve the written operational plan and site selection; and • Designate a Commissioned Officer to be the OIC of the Sobriety Checkpoint.

Continued next page.

Responsibilities (Continued)

Position	Duties
Sobriety Checkpoint OIC	Ensure: • The safety of all motorists and officers in the OUI checking area; • Motorists are directed into the checking area for screening by at least one (1) officer; • At least one (1), preferably two (2) officers interact with motorists during the screening process; • Motorists not arrested are released as quickly as possible; and • Arrested motorist's vehicles are inventoried and towed in accordance with existing policy or are released to a legal driver/passenger.
Safety Vehicle Officer(s)	Shall: • Position the safety vehicle(s) prior to the start of the checkpoint setup; • Observe traffic for vehicular operation indicating OUI; • Observe traffic to forewarn other officers and motorists of impending dangerous drivers approaching; • Observe traffic for violations of law and notify the OIC; • Ensure that visual warning devices are activated; and • Monitor traffic for backup. Note: Speed measuring devices may be used by the safety officer.
Sobriety Checkpoint Screening Officers	Shall: • Be courteous and polite when interacting with motorists. The element of voluntariness reduces the intrusiveness of the procedure; • All contacts shall be kept brief, with a short greeting such as "Good evening, this is a State Police Sobriety Checkpoint. Sorry for the inconvenience, thank you." The inconvenience to motorists must be minimized; • Guide motorists to the screening area to ensure the safety of all other officers and motorists within the OUI checking area; and • Ensure the safety of motorists being checked further by directing them to an appropriate location to park in the OUI checking area.

Continued next page.

Subject	Number
Sobriety Checkpoints	**TRF-15**

Responsibilities (Continued)

Position	Duties
Sobriety Checkpoint Screening Officers	• Minimize the inconvenience of motorists by screening them for OUI as efficiently as possible and administering the standard field sobriety tests, horizontal gaze nystagmus test or portable breath test device (PBT). If all elements of the OUI violation have been clearly established, the member shall arrest the subject, and follow Department arrest procedures.

References

M.G.L. c. 90, s.24
Commonwealth v. McGeoghegan 449 N.E.2d 349
TRF-09 Towing
TRF-10 Motor vehicle Inventory
TRF-14 Operating Under the Influence - Alcohol
MassHighway Work Zone Safety Guidelines

Promulgated By:

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**TRF-16**

Subject

Speed Measuring Devices

Policy

The Department shall use speed measuring devices as part of the strategy to reduce motor vehicle crashes and enhance public safety within the Commonwealth.

Use

The safety of the member, traffic violator, and motoring public shall be of primary concern whenever selecting locations for speed enforcement operations.

- Light Detection and Ranging (LIDAR) and Radio Detection and Ranging (RADAR) devices should not be used during inclement weather.

Calibration and Certification

All members using a LIDAR, or RADAR, or any other speed measuring device shall successfully complete the basic operator training program and receive certification prior to use.

- Members shall follow the manufacturer's guidelines for the maintenance and operational procedures of the devices;
- Members shall perform calibration checks at the beginning and end of each shift, and periodically as needed to ensure accuracy. If the device is not working properly, it shall be taken out of service immediately until repaired; and
- LIDAR and RADAR devices shall be certified annually, as directed by the Traffic Programs Section.

Records

Certificates and documentation of maintenance, calibration, and certification shall be maintained by the assigned member, or at the station.

Speedometer

Speedometers shall be checked by using a speed measuring device:

- Periodically;
- After cruiser service, specifically including transmission work or new tires; and
- If a question of accuracy arises.

Troop Traffic Programs

The Troop Traffic Programs Officer shall maintain an inventory of all speed measuring devices within the Troop. The inventory shall include:

- Member assigned the unit;
- Serial number of the unit; and
- The Department Inventory Control number.

Testimony

Members should be aware of the following elements that may be required in court testimony:

- The time, location, and direction of travel of the violator vehicle;
- The identity of the violator;
- The make, model, and color of the violator's vehicle;
- The visual estimate and the confirmation of the speed by the speed measuring device;
- The device was operating properly;
- The device was properly calibrated and certified; and
- The training, qualifications, and certification of the member.

Limitations

The effective use of speed measuring devices and their acceptance by the public and courts is dependent upon the member's:

- Understanding the factors that limit the accuracy of the device;
- Appropriate training and certification; and
- Proper care and use of the equipment.

References

Commonwealth v. Whynaught, 377 Mass. 19 (1979)

Promulgated By:

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**TRF-17**

Subject

Emergency Roadblocks

Policy

At times, situations arise which may necessitate the utilization of an emergency roadblock. Many factors have to be considered prior to implementation of a roadblock, to ensure officer and public safety.

Only Commissioned Officers may approve and authorize the implementation of an emergency roadblock.

Definitions

Roadblock: A deliberate obstruction by physical means at one or more selected points on a roadway.

Activation and Implementation

Many factors need to be considered before the implementation of a roadblock. The decision to use a roadblock shall be based upon:

- The seriousness of the known/alleged crime;
- The number of members available to be assigned;
- The sufficiency of information and descriptions of wanted persons and vehicles;
- The elapsed time between the known/alleged criminal act and the time of reporting to the Department or other law enforcement agencies; and
- Any other pertinent facts.

Upon implementation of an emergency roadblock:

- A Patrol Supervisor shall be dispatched and shall assume command at the scene of the roadblock;
- If available, the Air Wing should provide aerial assistance.

Fixed Roadblocks

Fixed roadblock barricades may consist of any strong structure augmented by any combination of signs, signals, markers, reflectors, or flares, and may include the strategic positioning of cruisers on the roadway.

- No member shall remain in a cruiser utilized as a fixed roadblock; and
- Firearms may be made ready for use.

Subject	Number
Emergency Roadblocks	**TRF-17**

Circle System

The Circle System is designed to completely contain the suspect in a given area by blocking every possible avenue of escape.

Typically two (2) circles are established; an inner circle and an outer circle. The radius of the circles is determined by the estimated time that has elapsed from the commission of the crime. The locations of blocking points are then determined by using the crime scene as a center and drawing circles around it.

- The inner circle is the area immediately surrounding the crime scene; and
- The outer circle is set up to apprehend the fugitive if they get through the inner circle.

Incident Commanders/Supervisors shall assign members to:
- Patrol the area between the two circles;
- Staff blocking points established at major intersections and highways;
- Stop all traffic and interview each operator; and
- Use cover-contact techniques as appropriate.

Observation Techniques

It may be more desirable to slow traffic, as this enables members to check vehicles and occupants without bringing traffic to a complete stop.

Department vehicles should be parked at forty-five (45) degree angle with the traffic flow. In this position members can observe traffic and maintain mobility.

Blocking Two-Lane Roads

To stop traffic traveling in only one direction, Department vehicles should be:
- Parked at a forty-five (45) degree angle with the traffic flow;
- Partially on the roadway; and
- Blocking the lane to be stopped.

Light traffic can be stopped in both directions with this system. However, in heavy traffic it may be necessary to set up this blocking method on both sides of the road. This second roadblock should be close enough, approximately seventy-five (75) yards away, and in sight of the first roadblock.

If signs and other warning devices are used, consideration should be given to the sight and stopping distances and the need for the element of surprise.

Blocking Roads at Night

At night, the member assigned as the contact officer shall:
- Stay off the roadway and out of oncoming headlights;
- Wear safety vest or high visibility clothing;
- Ensure roadblock lighting does not blind oncoming motorists; and
- Use cover-contact techniques as appropriate.

Subject	Number
Emergency Roadblocks	**TRF-17**

Blocking Multi-Lane Roadways

The blockade procedure for one side of a multi-lane highway is basically the same as for a one or two lane roadway.

A major difference is in the placement of signs and other warning devices.

- Because of greater speeds, the signs should be placed further away from the cruisers to allow motorists time to stop safely;
- If used, at least two (2) signs should be placed on both sides of the roadway facing towards oncoming traffic; and
- Flares and other warning devices should be arranged to funnel traffic into one or more lanes.

Promulgated By:

Department of State Police
General Order

Effective Date	Number
July 8, 2009	**TRF-20**

Subject

Department Vehicle Crashes

Policy

The Department shall document, within the Records Activity Management System (RAMS), all Department vehicle crashes in accordance with this policy.

The Department shall objectively investigate all vehicle crashes, in order to ensure that each crash investigation reflects the Department's commitment to impartiality and integrity.

Definitions

Cruiser Crash: A motor vehicle crash involving any Department vehicle, or any vehicle assigned to Department personnel, including civilian personnel.

Damage to a Department Vehicle: Non-crash damage, e.g. broken window or vandalism to an unattended vehicle. This includes windshield damage incurred as a result of debris from an unidentified or natural source.

Type I Crash: A minor cruiser crash not meeting any of the conditions of a Type II crash.

Type II Crash: A vehicle crash involving:
- Any injury or fatality to any party; or
- The issuance of a citation/criminal complaint; or
- Estimated damage over $1000 to any vehicle or property; or
- Any civilian employee operating a Department vehicle.

Registry of Motor Vehicle (RMV) Forms: Department operators shall:
- Identify themselves as operator number one; and
- List the operator's address as:
  Department of State Police
  470 Worcester Road
  Framingham, MA 01702; and
- The owner's name and address shall be listed in accordance with the vehicle's registration.

Note: When a crash involves more than one Department operator, the investigating supervisor shall determine the numerical designation of each operator, such as Operator Number One, Operator Number Two, and so on.

Subject	Number
Department Vehicle Crashes	**TRF-20**

Damage to Department Vehicle

Employees discovering/incurring damage to their assigned Department vehicles shall:

- Notify the sub-station of jurisdiction and request an entry to be made into the Daily Administrative Journal (DAJ);
- Report the damage, as soon as practicable, to their immediate supervisor and the Fleet Administrator per ADM-19A Vehicle Use and Maintenance.

Note: Any damage to a vehicle caused by a person arrested or a person summonsed to court shall be reported to the Fleet Section, in order to collect restitution. The investigating officer shall document the damage and take out appropriate criminal charges.

Type I Procedure

Employee	Duties
Member Involved in Crash	*Preliminary Procedures* • Immediately report the crash to the sub-station of jurisdiction; • If the Department vehicle was damaged, have photographs taken (not necessarily at the scene); • Ensure queries of license and registration data are done through the Registry databases and take appropriate action as necessary (See Type II); • Complete and submit within RAMS, the SP 425 Preliminary Documentation of Cruiser Crash prior to the completion of tour of duty; and • Completed reports shall be reviewed by the member's Station/Unit Commander prior to submission to Troop/Section Major; and • Complete and mail the original Registry form CRA-23, to the Registry of Motor Vehicles (RMV) within five (5) days. *Completed Documentation* • Completed documentation shall include: 1. To/From reporting the circumstances, to include the date the Registry CRA-23 was forwarded to the RMV; 2. A copy of the Registry CRA-23; and 3. Troop Mechanic's report and photographs. • Completed documentation shall be forwarded to their Troop/Section Major within five (5) days.

Continued next page.

Type I Procedure (Continued)

Employee	Duties
Desk Officer	• Document the crash within the DAJ as a Type I Cruiser Crash activity; and • Notify the Troop Duty Officer.
Troop Duty Officer of Jurisdiction	• Document the crash within the DAJ; • Authorize operator to document crash; or • Assign a supervisor to investigate, preferably of higher rank than the member involved, from the Division of Field Services. **Note: Whenever a supervisor is assigned to investigate a cruiser crash, Type II procedures shall be followed.**
Involved Member's Station/Unit Commander	• Shall review reports for accuracy and completeness prior to submission to the Troop/Section Major.
Troop/Section Major	*Preliminary Documentation* The Troop/Section Major of the involved member shall: • Review the SP 425 upon receipt or no later than one (1) business day following the crash; • Ensure the Cruiser Crash is reclassified within RAMS from a Type I to a Type II if warranted; • Consult with the Major of jurisdiction within the Division of Field Services, to assign a supervisor to conduct a Type II Investigation when so determined; • Ensure that only a supervisor shall issue any citations related to the cruiser crash. *Completed Documentation* Upon receipt of all documentation the Troop/Section Major shall within RAMS: • Fill out the appropriate section of the SP 377; • Make findings and recommendations; and • Forward all documentation to the involved member's Division Commander within twenty-one (21) days of the crash.

Subject	Number
Department Vehicle Crashes	**TRF-20**

Crash in Personal Vehicle

On-duty Department employees involved in a crash while operating their personal vehicles shall immediately inform their duty assignment supervisor of the crash when:

- They are authorized to operate their personal vehicle within the scope of their duties; and
- They are entitled to mileage pay for that travel.

Within five (5) days of the crash, the employee shall provide their duty assignment supervisor with a copy of the RMV CRA-23 and all other pertinent documentation and forward a copy to the Legal Section.

When a Department employee is injured in a crash that meets the criteria listed above, the injury shall be investigated as an on-duty injury.

Type II Procedure

Employee	Duties
Employee Involved in Crash	• Immediately report the crash to the sub-station of jurisdiction; • Preserve the scene, if safety and traffic concerns allow; • Members shall not take any enforcement action except to prevent parties from unlawfully leaving; • Complete and mail the Registry CRA-23 to the RMV within five (5) days; • Ensure their Station/Unit Commander has reviewed completed reports prior to submission; and • Complete and forward the following printed reports to the investigating officer within five (5) days (unless incapacitated): 1. To/From reporting the circumstances, to include the date the Registry CRA-23 was forwarded to the RMV; 2. A copy of Registry CRA-23; and 3. Commonwealth's Form 1 Notice of Injury (if injured).
Desk Officer	• Document the crash within the DAJ as a Type II Cruiser Crash activity; and • Notify the Troop Duty Officer.

Continued next page.

Type II Procedure (Continued)

Employee	Duties
Troop Duty Officer of Jurisdiction	• Document the crash within the DAJ; • Assign a supervisor from within the troop to investigate, preferably of higher rank than the member involved. • If appropriate, notify the involved employee's Troop/Section Major or designee; and • Make arrangements for other assistance at the scene (Photographs, crash reconstruction, etc.).
Investigating Supervisor	*Preliminary Investigation* • Take command of the crash scene and investigation; • Have photographs taken of the scene and/or the damage; • Ensure queries of license and registration data are done through the Registry databases; • Take appropriate action on violations of law (e.g. citations); • Complete and submit the SP 425 within RAMS, prior to the completion of tour of duty; and • Complete and forward SP 624 Initial Injury Report if necessary. (Refer to ADM-11B Injury Reporting) *Completed Investigation* Forward reports to Troop Commander within fifteen (15) days from the date of the crash: • Registry CRA-65; • SP 209 Supplementary Cruiser Crash Report; • Troop Mechanic's Report and photographs of damage; • If applicable, towing bills; • If applicable, the SP 37 Statement In Support of Claim, Section 8; • All other reports, photographs, copies of citations, etc; and • If employee is incapacitated complete: 1. SP 37 Sections, 1-7, and 2. Commonwealth's Form 1.

Continued next page.

Type II Procedure (Continued)

Employee	Duties
Involved Member's Station/Unit Commander	Shall review reports for accuracy and completeness prior to submission to the investigating supervisor.
Troop Commander of Crash Jurisdiction	*Preliminary Investigation* The Troop Commander shall: • Review the SP 425 upon receipt or no later than one (1) business day following the crash. *Completed Investigation* The Troop Commander shall within RAMS: • Make findings and recommendations; • If applicable, fill out the appropriate sections of the SP 37; • If applicable, fill out the appropriate sections of the SP 377 in RAMS; • Send a copy of the SP 37 and Commonwealth's Form 1 to Occupational Health if appropriate; and • Forward the completed report to the involved member's Division Commander within twenty-one (21) days of the crash.

Involved Employee's Division Commander

Division Commanders shall:
- Review all Type I and II reports including findings and recommendations;
- Complete appropriate sections of SP 377 in RAMS;
- Take corrective action when appropriate;
- Submit completed reports to the Division of Standards and Training within thirty (30) days of the crash; and
- Send a copy of the completed reports to the Fleet Section.

Division of Standards and Training

The Division of Standards and Training Commander or designee, shall:
- Complete appropriate section of SP 377 in RAMS;
- Ensure reports are complete and are filed within the Records Section; and
- If reports are not complete, return to the Division Commander for reconciliation.

The Commanding Officer or designee, of the Emergency Vehicle Operation Center (EVOC) shall within RAMS:
- Fill out and submit the appropriate section of the SP 377 when remedial training is completed.

Subject	Number
Department Vehicle Crashes	**TRF-20**

Records Section The Records Section shall maintain all hard copies of reports and investigations upon receipt from the Division of Standards and Training.

References

SP 37 Statement in Support of Claim
SP 209 Department Supplementary Cruiser Crash Report
SP 377 Cruiser Crash Review Form
SP 425 Preliminary Investigation of Cruiser Crash
CRA-23 Motor Vehicle Crash Operator Report
CRA-65 Motor Vehicle Crash Police Report
Commonwealth's Form 1 Notice Of Injury

Promulgated By:

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**TRF-21**

Subject

Tire Deflation Devices

Policy

The Department may use tire deflation devices in specific circumstances to reduce the speed and duration of pursuits in order to reduce the risk of injury to persons and/or damage to property.

Definitions

Tire Deflation Device: A device that, when driven over, causes one or more tires of a vehicle to safely deflate.

Channelizing: A technique where objects are placed in the anticipated path of a pursued vehicle in order to alter its direction.

Utilization of Tire Deflation Devices

Tire Deflation Devices shall:

- Only be deployed by a member trained in its use;
- Only be deployed if the device has a recovery cord;
- Be readily accessible in the event of an emergency; and
- Not be used to stop a motorcycle, tractor trailer, bus carrying passengers, or vehicle with less than four (4) wheels unless:
  1. The suspect and/or vehicle poses an imminent threat of death or serious bodily harm to the public or officers; or
  2. When specifically authorized and ordered by the Troop Duty Officer, Troop Commander or a Command Staff Member.

Site Selection

Tire deflation devices shall not be used at intersections or in locations where geographic configurations (such as curves and steep embankments) increase the risk of injury to the suspect or occupants of other vehicles.

Deployment Notification

A tire deflation device shall only be deployed when:

- The pursuing member has been informed of the location of deployment; and
- Has acknowledged this information on the radio.

Covert Deployment

Situations where it is prudent to covertly disable a vehicle with a tire deflation device may include:

- Stolen vehicles;
- Serious felony arrest warrants and/or charges; and
- Hostage or kidnapping situations.

Subject	Number
Tire Deflation Devices	**TRF-21**

Recovery of Tire Deflation Device(s)

A deployed tire deflation device(s) shall be safely removed from the roadway after the fleeing vehicle passes. Members shall not enter into the travel lane until all traffic is clear and it is safe to retrieve the device from the roadway. The deployed device(s) shall not be left unattended in the roadway.

Duty of Pursuit Member(s)

On approach to the deployment area the pursuing member(s) shall proceed cautiously and adjust the cruiser speed as necessary to:

- Allow time for the removal of the tire deflation device; or
- Respond to sudden evasive or unpredictable maneuvers by the fleeing vehicle.

After clearing the deployment area the member(s) may increase cruiser speed, if necessary.

Maintenance of Tire Deflation Device

Members assigned tire deflation devices shall maintain them according to the manufacturer's guidelines and specifications.

Non-functioning parts/units shall be forwarded to the Troop Clerk for replacement, unless otherwise indicated.

Reporting

Members shall report all deployments:

- To the Troop Duty Officer of jurisdiction; and
- To the Emergency Vehicle Operations Center (EVOC) via SP 601 Tire Deflation Device Evaluation Form.

The Troop Duty Officer shall report the use of a tire deflation device and the results on the RAMS pursuit database.

Damage to Vehicles or Property

The Troop Duty Officer shall assign a supervisor to investigate any related damage to any other vehicle or property.

Third party owners of any damaged vehicle or property shall be advised to contact the Legal Section for guidance in filing a claim at (508) 820-2311.

References

SP 601 Tire Deflation Device Evaluation Form

Promulgated By:

Department of State Police
General Order

Effective Date	Number
May 21, 2018	**TRF-22**

Subject

Escorts and Relays

Policy

The Department may authorize escorts or relays to provide added security, expedite the delivery of special items, and ensure the safe and efficient movement of traffic.

General Guidelines

The Division of Field Services Commanding Officer shall have operational control of all escorts and relays.

Routine requests for escort or relay services shall be approved as outlined below. All emergency requests for escort or relay services shall be forwarded to the Troop Duty Officer.

Members shall not initiate or commence any escort or relay without permission from the Troop Duty Officer.

Routine Requests

If the request is for…	Then the request should be forwarded to…
• Any sub-division of the United States Government; • Executive Security; • Political or high-profile figures; or • Nuclear, Radiological, Biological, Hazardous, and/or Sensitive Materials.	Troop "S" Commanding Officer, or his/her designee.
• Funerals, parades, etc.; • Public Safety vehicles; or • Other instances where an escort or relay is in the public interest.	Troop Commander
• Oversize vehicles; or • Unusual cargo.	Troop Detail Officer

Whenever possible, the request shall be in writing and include the trip route and any other pertinent information. Notification of an escort or relay shall be made to any affected Troop.

Emergency Requests

Legitimate requests for unscheduled Department escort or relay services may include:

- Protection of life;
- Medical personnel;
- Other law enforcement agencies; or
- Valuable cargo, which may include blood, life saving medicines, human organs and tissues, or other materials as required by law.

The Troop Duty Officer shall notify the GHQ Communications Section of every escort or relay that extends beyond the troop area.

Emergency escort of ambulances or private vehicles shall be avoided except when a life is in jeopardy. Permission to escort shall be sought immediately from the Troop Duty Officer.

Escort of Nuclear, Radiological, Biological and/or Sensitive Materials

The movement of nuclear, radiological, biological and/or other sensitive materials, in and through the Commonwealth, may require the utilization of an escort.

When an escort is recommended by the Massachusetts Department of Public Health, the Commanding Officer of Troop "S" or his/her designee shall develop an Operations Plan that will ensure the following steps are undertaken:

- Notify the Division Commander of Field Services;
- Notify the Division Commander of Homeland Security and Preparedness;
- Notify the Division Commander of Investigative Services;
- Notify the Emergency Management Unit;
- Assign a Commissioned Officer from Special Operations as the escort Incident Commander / OIC;
- Ensure that Commercial Vehicle Enforcement Section (CVES) personnel provide appropriate inspections of the vehicle(s) to be escorted. CVES personnel will accompany the escort for the duration of the escort;
- Contact the Division Commander of Homeland Security and Preparedness to request a dedicated Air Wing unit to provide aerial surveillance for the duration of the escort if deemed necessary;
- Assign Special Tactical Operations (STOP) Team personnel to coordinate appropriate security measures. STOP Team personnel will, as appropriate, utilize armored or other assigned vehicles during the escort;
- Assign the Motorcycle Unit, as appropriate, to facilitate the movement of the escort; and
- Assign other Special Operations assets as appropriate.

(Continued next page.)

Escort of Nuclear, Radiological, Biological and/or Sensitive Materials (Continued)

The Emergency Management Unit shall coordinate the escort with the following entities, as appropriate:

- Special Operations Commanding Officer;
- CVES;
- Air Wing;
- STOP Team;
- Motorcycle Unit;
- Criminal Information and Intelligence Section-Commonwealth Fusion Center;
- Troop Commanders of each Troop through which the escort will travel;
- Communications Section;
- Fiscal Section;
- State Police agency of adjoining state(s) through which the escort will travel;
- Police Department of the receiving/departing community;
- Police Department of adjoining communities, as appropriate;
- Massachusetts Department of Public Health Radiation Control Program;
- Shipping/receiving company; responsible financial party; and
- Additional notifications, as appropriate.

The Criminal Information and Intelligence Section Commanding Officer, or his/her designee, shall assign personnel to:

- Conduct open source research related to the shipment;
- Query internal databases to determine if the Commonwealth Fusion Center has any relevant information pertaining to the shipment;
- Contact a representative of the federal Department of Homeland Security's Intelligence and Analysis Section to determine if his/her agency has any relevant information pertaining to the shipment;
- Contact a representative of the Federal Bureau of Investigation's Boston Field Office to determine if his/her agency has any relevant information pertaining to the shipment;
- Contact a representative of the Boston Regional Intelligence Center to determine if his/her agency has any relevant information pertaining to the shipment; and
- Report all results and significant findings to the Emergency Management Unit's Commanding Officer.

Troop Commanders of each Troop through which the escort travels shall:

- Provide notification to communities, as appropriate; and
- Provide uniformed personnel, as appropriate, to facilitate the movement of the escort through the Troop.

Communications Section shall:

- Assign a SOPs channel for escort personnel to utilize.

Subject	Number
Escorts and Relays	**TRF-22**

Escort Request for Charitable Events

At least thirty (30) days in advance, organizers of a legitimate charity shall provide the Paid Detail Officer of jurisdiction a written plan and sign a SP 618 Motorcycle Escort Waiver.

The written plan shall contain:

- The date of the event, routes of travel and the anticipated number of participants;
- Number of Department members requested for escort;
- Notification to local and state authorities, and media in writing;
- Proof of the required one million dollar bond to cover the event; and

Acknowledgement that participants shall obey all traffic laws during the duration of the event.

Outlaw Motorcycle/ Criminal Gangs

The Paid Detail Officer shall consult with the Criminal Information and Intelligence Section if it appears that the event organizers, or likely participants, have an association with criminal activity.

Outlaw motorcycle/criminal gangs shall be barred from obtaining Department escorts.

References

ADM-25 Paid Details
SP 618 Motorcycle Escort Waiver

Promulgated By:

Department of State Police
General Order

Effective Date	Number
September 18, 2018	**TRN-01**

Subject

Training Administration

Policy

The Department shall provide training that will develop the skills necessary for the safe, professional and effective performance of its personnel, and that is designed to promote and maintain the professionalism and operational readiness of the Department.

The Department shall ensure that all employees successfully complete compulsory training as required by law and the Colonel/Superintendent.

State Police Academy

The State Police Academy is commanded by the Deputy Division Commander of Standards and Training, who is responsible for ensuring that all training is conducted in accordance with Department directives and applicable laws.

Academy Staff Responsibilities

The Academy Staff shall:

- Identify, develop, and evaluate training and educational programs;
- Assist in the development of lesson plans for all Department training courses;
- Provide necessary training to Department employees and the law enforcement community;
- Meet all federal, state and Department mandated training requirements;
- Provide training to develop the skills necessary for the safe, professional and effective performance of its employees;
- Provide career development opportunities for employees; and
- Maintain training records for employees, including attendance records.

Attending Training

Employees assigned to all training programs shall:

- Report at the specified time and location with the proper uniform/attire and materials;
- Be returned to their duty assignment for failing to report as directed and may be subject to disciplinary action; and
- Attend non-mandatory training programs only as approved in accordance with Departmental guidelines.
  Note: Changes in work schedules for the purpose of training shall be in accordance with the Collective Bargaining Agreement.

Subject	Number
Training Administration	**TRN-01**

Training Requests

Massachusetts State Police personnel, requesting to attend a training program that has *any* costs associated with it and/or is held outside of the Department, shall comply with the following:

- ***At least forty-five (45) days prior*** to the anticipated date of the requested training, ***each traveler*** shall submit, through channels to their Division Commander:
    1. A To/From requesting approval;
    2. A completed *SP 371 Travel Training Endorsement Sheet;*
    3. A completed *Commonwealth of Massachusetts Travel Authorization Form* (TAF Form Primary);
        - ***NOTE***: *Section 9 "Travel Itinerary and Justification*" must include a ***thorough*** explanation of how the travel will benefit the Commonwealth;
        - ***NOTE:*** *Section 10 "Expenses"* must be completed even if the cost of the Travel/Training will be paid by personal funds, Commonwealth funds, or federal/ Other State Funds;
    4. If the travel and/or training is funded by a private entity, a completed *Disclosure by Non-Elected Public Employee of Travel Expenses Serving a Legitimate Public Purpose* form;
        - ***NOTE***: ***Each traveler*** must estimate and account for expenses in the "*Itemization and explanation of amounts offered"* section when travel/training is funded by a private entity; and
    5. **All** supporting documentation (i.e. training fees and agenda; lodging and transportation estimates; meal reimbursement rates and other appropriate expenses as specified in the member's appropriate Collective Bargaining Agreement.)

- When estimating expenses, it is the responsibility of the traveler to ascertain and account for taxes and fees associated with hotel reservations, car rentals, etc. It is also the responsibility of the traveler to minimize all costs associated with travel and training.

- If the training is out-of-state, personnel should review on Docushare the Executive Office of Administration and Finance *Out Of State Travel Guidelines.*

The Division Commander, or designee, within five (5) days of receipt of the training request shall forward approved requests and accompanying documentation to:

- The Deputy Superintendent; and
- The Department's Leave Coordinator per ADM-11E Leaves of Absence.

Subject	Number
Training Administration	**TRN-01**

State Police Academy Coordinated/ No Cost Training

Massachusetts State Police personnel, requesting to attend training that is coordinated by the State Police Academy and has no costs associated with it, **need not** submit To/From and travel forms as described in the previous section. Instead, personnel, interested in attending such training, shall complete the *MSP Professional Development Registration* form which will be attached to the State Police Academy e-mail that announces such training. Personnel shall submit the **completed** *Registration* form to the State Police Academy.

Expense Reimbursement

Reimbursement for expenses shall be made only if prior written approval has been received from the Deputy Superintendent.

In order to be reimbursed for expenses, *each* traveler must submit to the Fiscal Section a completed *Employee Travel/Training/ Reimbursement Voucher Input Form* along with all necessary receipts and paperwork.
Note: The reimbursement amount should not exceed the previously authorized expenditure.

Testing

Instructors shall use competency based testing with performance objectives designed to measure the participant's ability and knowledge of course related skills. Participants shall be advised of minimum acceptable standards prior to the administration of such tests.

Remedial Training

Employees who fail to meet required standards of performance shall be required to participate in remedial training, as soon as possible.

The goal of remedial training is to ensure that employees demonstrate the knowledge, ability, and skills to achieve an acceptable level of performance.

Employees, who fail to attend assigned remedial training, and/or who fail to achieve acceptable levels of performance, shall be subject to disciplinary action.

Records

In order for the Department to maintain complete and accurate training records, commencing January 1, 2012, employees shall:

- Forward copies of training certificates or records of attendance for non-Department training to:
    1. The State Police Academy (SPA); and
    2. Their Station/Section/Unit Commanding Officer.
- Ensure that copies of certificates or records of attendance for any future non-Department trainings are forwarded to:
    1. The State Police Academy (SPA); and
    2. Their Station/Section/Unit Commanding Officer.

Note: If available, employees are encouraged to forward training records acquired before January 1, 2012, to their Commanding Officer and the SPA for insertion into their Individual Training files.

Continued next page.

Subject	Number
Training Administration	**TRN-01**

Records (Continued)

Station/Section/Unit Commanding Officers shall:

- Ensure that all employees under their command have an Individual Training File that is retained and updated within the Station/Section/Unit; and
- Ensure that the Individual Training File is administratively forwarded together with the employee's Attendance Calendar(s) and the Employee Evaluation System (EES) Fact File when, transferred out of the Station/Section/Unit.

The Academy Commandant shall be responsible for maintaining current Department training records. Such records shall include, but not be limited to:

- Name, rank, ID#, and duty assignment of Department employees attending all training programs;
- Name and agency of non-department personnel attending all training programs;
- Attendance records;
- Name of instructor and course lesson plan;
- Individual records of performance evaluations administered with associated results; and

The type of certificates received, if any.

References

ADM-11E Leaves of Absence
TRN-04 Professional Development
SP 371 Travel Training Endorsement Sheet
Commonwealth of Massachusetts Travel Authorization Form (TAF Form Primary).
Disclosure by Non-Elected Public Employee of Travel Expenses Serving a Legitimate Public Purpose form
Executive Office of Administration and Finance *Out Of State Travel Guidelines*

Promulgated By:

Department of State Police
General Order

Effective Date	Number
April 23, 2009	**TRN-02**

Subject

Recruit Training

Policy

Prior to assuming duties as a sworn State Police Trooper, recruits shall be assigned to, and satisfactorily complete a recruit training class. This class shall be held at the State Police Academy and fulfill the requirements as prescribed by Massachusetts General Laws and the Colonel/Superintendent.

Recruit Handbook

The Academy Commandant shall, prior to the commencement of a recruit training class, prepare and distribute to each recruit a handbook containing the following information:

- Recruit performance expectation;
- The rules and regulations governing the conduct of recruits while assigned to the Academy; and
- The method for determining the final overall average score of each recruit which shall be used to establish the class standing of each trainee.

Recruit Class Curriculum

The Academy Commandant shall develop a recruit class curriculum including, but not limited to:

- Constitutional principles, criminal law and procedure, motor vehicle law;
- Department operations, Rules and Regulations, Policies and Procedures;
- Use of force, including firearms;
- Emergency vehicle operations;
- CPR/First Responder training;
- Principles of leadership;
- Report writing, court testimony and communications skills;
- Cultural diversity and ethics; and
- Physical fitness and wellness.

Authorized Use of Recruits

The Colonel/Superintendent may authorize the use of recruits assigned to the State Police Academy to tasks not requiring law enforcement powers.

References

MGL c.22C

Promulgated By:

Department of State Police
General Order

Effective Date	Number
November 5, 2008	**TRN-03**

Subject

Field Training Program

Policy

The Department shall provide a Field Training Program for the transition from the controlled learning environment of the Academy to the responsibilities and duties of a State Trooper.

Field Training Program

The Field Training Program shall be twelve weeks in duration, or as prescribed by the Colonel/Superintendent. Successful completion of the program is contingent upon satisfactory attendance and performance.

Probationary troopers may be assigned to three (3) Field Training Officers, on different shifts, as set forth in the Field Training Program. Exceptions may be made for specific operational and training reasons.

Excessive absenteeism shall be reported to the Field Training Administrator and may result in termination of the probationary trooper.

Academy Commandant

The Academy Commandant is responsible for the administration of the Field Training Program. The Academy Commandant shall coordinate the selection of an appropriate number of Field Training Officers (FTOs) through the Division of Field Services.

Prior to the commencement of the Field Training Program, the Academy Commandant shall develop and provide training to Station Commanders and FTOs. This training shall, at a minimum:

- Provide an overview of the current Academy recruit training program reinforcing:
  1. The mission of the Department;
  2. Fundamental training values;
  3. Department goals and objectives; and
  4. Instructions on the administration and reporting requirements of the Field Training Program.

Subject	Number
Field Training Program	**TRN-03**

Field Training Administrator

The Academy Commandant shall designate a member of the Academy Staff as the Field Training Administrator. The Field Training Administrator shall be responsible for:

- The management of the Field Training Program;
- The development and distribution of the Field Training Program Manual; and
- Coordinating the selection of Field Training Officers with Troop Field Training Coordinators.

Troop Commander

The Troop Commander shall:

- Appoint a member to serve as the Troop Field Training Coordinator; and
- Allow the Troop Field Training Coordinator to modify their work schedule to effectively manage the Field Training Program.

Troop Field Training Coordinator

The Troop Field Training Coordinator shall:

- Administer the Field Training Program;
- Act as the liaison with the Field Training Administrator; and
- Review the Daily/Weekly Observation Reports on a weekly basis.

Station Commander

Station Commanders shall:

- Administer the Field Training Program within their sub-station;
- Review and approve all submitted FTO evaluations;
- Forward the approved evaluations to the Troop Field Training Coordinator; and
- Immediately notify the Troop Field Training Coordinator of any issues that arise during the Field Training Program.

Field Training Officer

The FTO performs a critical role in the development of the new trooper and shall be responsible for:

- Providing an effective learning environment through leadership and experience;
- Providing an opportunity to realistically apply the knowledge, ability, and skills acquired during academy training;
- Providing an example that promotes professionalism, public respect, and confidence;
- Complying with the procedures established in the Field Training Program; and
- Assessing the performance of probationary trooper and providing remedial instruction as necessary.

Subject	Number
Field Training Program	**TRN-03**

Field Training Program Manual

The Field Training Program Manual shall:

- Be provided to Station Commanders and FTOs prior to the commencement of the Field Training Program;
- Clearly define the responsibilities of the FTO; and
- Provide specific direction concerning the knowledge, ability, and skills to be taught, performed and assessed.

Selection Process

The identification and selection of the FTOs is critical to the success of the Field Training Program.

Selection Process:

- Station Commanders shall recommend to the Troop Commander members who demonstrate integrity, character, and commitment to the Field Training Program;
- Troop Commanders shall approve and forward the final list of FTOs to the Commander of the Division of Field Services; and
- The Division of Field Services Commander shall forward the names of the approved FTOs to the Academy Commandant.

Evaluations

Station Commanders and FTOs shall ensure that all written evaluation forms are submitted in accordance with the Field Training Program Manual.

All deficiencies that may impact the ability of the probationary trooper to safely and successfully complete the Field Training Program shall be brought to the attention of the Station Commander immediately.

Completion of Program

After twelve (12) weeks, the Station Commander shall forward a recommendation to the Field Training Administrator which shall include a conclusion as to:

- The probationary Trooper is capable of working on their own; or
- An extension of the Field Training Program is necessary; or
- Termination of employment is appropriate.

The Troop Commander shall forward all recommendations for termination to the Colonel/Superintendent, through channels after consultation with the:

- Field Training Officer(s);
- Station Commander;
- Troop Field Training Coordinator; and
- Field Training Administrator

Promulgated By:

Department of State Police
General Order

Effective Date	Number
May 10, 2012	**TRN-04**

Subject

Professional Development

Policy

The Department recognizes the necessity of continuous education and training in order to maintain and enhance the knowledge, abilities, and skills of its employees.

This shall be accomplished, in part, through an ongoing professional development program to include regular in-service training.

Compulsory Training

The Department shall provide compulsory training to all members.

The Deputy Division Commander of Standards and Training, shall:

- Ensure that an annual training assessment is conducted to identify the training and educational needs of the Department;
- Ensure the Academy Staff develops a training curriculum, based on annual training assessment; and
- Forward the training curriculum, through channels, for review and approval by the Colonel/Superintendent.

Members shall attend compulsory training on dates assigned. Members who fail to attend may be subject to discipline.

In-service training may be conducted at the State Police Academy or any site approved by the Colonel/Superintendent.

Online Academy

The Online Academy Unit within the Academy shall:

- Be responsible for the development and distribution of online training;

Employees are encouraged to submit recommendations for training topics to the Online Academy Unit.

Subject	Number
Professional Development	**TRN-04**

Professional Development

The Department shall identify and develop training programs to be presented internally which shall provide its employees with the opportunity to expand or enhance their knowledge, abilities, and skills in specialized areas, or upon promotion.

The Academy Staff shall be responsible for:

- Development and/or administration of courses in accordance with the procedures outlined in TRN-01 Training Administration;
- Maintaining a current schedule of professional development courses on the intranet website;
- Maintaining accurate attendance records for members who have attended training; and
- Forwarding to respective Troop/Section Commanders the accurate attendance records for members who have attended training upon completion of training.

Employees may attend training or seminars intended to improve their professional abilities. Employees requesting to attend professional development courses shall adhere to the procedure outlined within TRN-01 Training Administration. Authorization to attend may be granted based upon the applicability of the program and available Department resources.

Training Records

In order for the Department to maintain complete and accurate training records commencing, January 1, 2012, employees shall:

- Forward copies of training certificates or record of attendance for non-Department training to:
    1. The State Police Academy (SPA); and
    2. Their Station/Section/Unit Commanding Officer.
- Ensure that copies of certificates or records of attendance for any future non-Department trainings are forwarded to:
    1. The State Police Academy (SPA); and
    2. Their Station/Section/Unit Commanding Officer.

Note: If available, employees are encouraged to forward training records acquired before January 1, 2012, to their Commanding Officer and the SPA for insertion into their files.

Station/Section/Unit Commanding Officers shall:

- Ensure that all employees under their command have an Individual Training File that is retained and updated within the Station/Section/Unit; and
- Ensure that the Individual Training File is administratively forwarded together with the employee's Attendance Calendar and the Employee Evaluation System (EES) Fact File when, transferred out of the Station/Section/Unit.

Subject	Number
Professional Development	**TRN-04**

Training for Civilian Employees

The Director of Human Resources shall develop and maintain guidelines related to the training and education of civilian employees.

All newly appointed civilian employees shall receive training in the following areas, at a minimum:

- Mission, goals and objectives of the Department;
- Applicable Department policy, procedure, rules, regulations and guidelines (e.g. workplace violence, harassment);
- Department expectations and the civilian employees performance evaluation program; and
- Responsibilities and rights of employees.

The Department shall provide training to civilian employees in accordance with law, Department policy and as requested by the Director of Human Resources. The Academy shall coordinate the presentation of training to civilian employees, as requested by the Director of Human Resources.

References

TRN-01 Training Administration

Promulgated By:

Colonel Marian J. McGovern

Department of State Police
General Order

Effective Date	Number
June 11, 2020	**UOF-01**

Subject

Use of Force

Policy

Members shall use, or are authorized to use, only that force which is *objectively reasonable* to:

- Effect an arrest;
- Restrain or subdue an individual resisting a lawful seizure; or
- Protect themselves or others from physical harm.

Members should assess each situation to determine which action shall best bring the incident under control, using only that amount of force that is reasonably necessary.

Any technique or hold that is, by application or duration, intended to prevent an individual's ability to breathe or prevent blood flow to an individual's head in a manner the member knows or should reasonably know will create a substantial risk of death or serious bodily harm constitutes lethal force.

If a member observes another member engaging in an unauthorized or excessive use of force, the observing member has an affirmative duty to intervene and attempt to stop the unauthorized or excessive use of force.

Members shall administer and secure medical aid after any use of force, if necessary and practical.

Definitions

Objectively Reasonable: This term means that, in determining the necessity for and appropriate level of force, officers shall evaluate each situation in light of the known circumstances, including, but not limited to, the seriousness of the crime, the level of threat or resistance presented by the subject, and the danger to the officer, subject, or community. The reasonableness of a particular use of force must be judged from the perspective of a reasonable officer on scene, rather than with the 20/20 vision of hindsight. Determining reasonableness of force must allow for the fact that police officers are forced to make split second judgments in circumstances that are tense, uncertain and rapidly evolving. The force used must be reasonable under the circumstances known to the officer at the time force is used.

Continued next page.

Subject	Number
Use of Force	**UOF-01**

Definitions (Continued)

Less Lethal Force: Use of force that is not intended to cause serious bodily harm/serious physical injuries or death.

- Members are authorized to use less lethal force in accordance with the law and the contents of this policy.

Lethal Force: Use of force intended to inflict serious bodily harm/serious physical injuries or death.

- Members are authorized to use lethal force in accordance with the law and the contents of this policy.

Sensitive Population Groups: Sensitive population groups include those who reasonably appear to be, or are known to be, children, elderly, medically infirm, pregnant, or users of a cardiac pacemaker.

Compliant Individual: An individual who is fully cooperative with a Department member.

Passively Resistant Individual: An individual who is uncooperative but does not use physical strength or body movement to resist a Department member.

Actively Resistant Individual: An individual who uses physical strength and/or body movement to resist a Department member. Examples of active resistance include pulling, turning, or walking away from an officer.

Assaultive Individual (Bodily Harm): An individual who attempts to injure a Department member or another person or engages in conduct that has the potential to injure a Department member or another person.

Aggravated Assaultive Individual (Serious Bodily Harm/Death): An individual who engages in conduct that is likely to produce death or serious bodily harm to a member of the Department or another person.

Use of Force Responses

(Note: *Use of Force responses need not be exercised in progression*.)

Determining the level of force necessary may depend on resistance levels and circumstances. Factors in this decision include, but are not limited to:

- Subject vs. member - relative to age, size, physical condition, skill level;
- Subject's drug and alcohol use;
- Weapons - type, proximity;
- Seriousness of offense;
- Exigent circumstances; and

Number of potential assailants vs. number of police on the scene.

Continued next page.

Subject	Number
Use of Force	**UOF-01**

Use of Force Responses (Continued)

(Note: *Use of Force responses need not be exercised in progression*.)

If the subject is…	Then the response may include…
Compliant	• Verbal commands
Passively Resistant	• Verbal commands; and/or • Contact control techniques.
Actively Resistant	• Verbal commands; • Contact control techniques; • Compliance techniques; • Distraction techniques; • Oleoresin Capsicum (OC) Spray, according to training; • Laser activation of Electronic Control Weapon (ECW) according to training; • Spark display of Electronic Control Weapon (ECW) according to training; and • Drive Stun deployment of Electronic Control Weapon (ECW) according to training.
Assaultive-Bodily Harm	• All of the above responses; • Striking techniques; • Probe deployment of Electronic Control Weapon (ECW) according to training; and • Any other Department approved less lethal force equipment.
Aggravated Assaultive - Serious Bodily Harm /Death	• All of the above responses; and • Lethal force.

Continued next page

Subject	Number
Use of Force	**UOF-01**

Use of Force

Verbal Commands - Commands and gestures designed to:
- Effect compliance; and
- Express the member's intent.

Contact Control Techniques: Touch techniques (carrying and guiding) not designed to produce pain compliance.

Compliance Techniques:
Techniques authorized by the Department that may be used to achieve compliance and/or control of an actively resistant or assaultive subject.

In exigent circumstances, other compliance techniques may be used.

Distraction Techniques: Techniques intended to temporarily break the mental focus of an actively resisting individual and create an opportunity for the member to apply a compliance or control technique. Distraction techniques may be similar to striking techniques, but they differ in *intent* and *intensity*. The *intent* is to take the subject's focus off of their chosen method of resistance so that the member can bring them under control, unlike a striking technique, where the intent is to stop an assault. The *intensity* is, therefore, less than it would be with a striking technique. The intensity of the distraction technique should be limited so as not to create substantial trauma or lasting injury.

OC Spray - OC spray may be used in situations involving:
- Assaultive subjects; or
- Actively Resistant subjects when:
  1. Verbal commands have failed to bring about compliance; and
  2. Subject has signaled their intentions to actively resist.

OC spray shall not be used on passive resisters who offer **NO** physical resistance.

Striking Techniques - Striking techniques may be used on an assaultive subject to achieve compliance and/or control.

Striking techniques may include the use of issued equipment (e.g., baton, flashlight, PR-24NX), as well as hands, feet, elbows, or knees.

In exigent circumstances, other instrumentalities may be used.

Electronic Control Weapons (ECW) - Department Members are authorized to use ECW in accordance with Department training and UOF-06 *Electronic Control Weapons.*

Continued next page

Subject	Number
Use of Force	**UOF-01**

Lethal Force Authorization

Members are authorized to use lethal force in order to protect themselves or others from an immediate threat of death or serious bodily harm.

Warnings- If feasible, some warning shall be given before any use of force.

Use of Lethal Force: Preventing Escape	Members are authorized to use lethal force to prevent the escape of a suspect when the officer has probable cause to believe that: • The arrest is for a felony; and • The member believes that the force employed creates no substantial risk of injury to innocent persons; and either: 1. The crime for which the arrest is made involved conduct including the use or threatened use of deadly force; or 2. There is a substantial risk that the person to be arrested will cause death or serious bodily harm/serious physical injuries if the suspect's apprehension is delayed. and • If feasible, some warning has been given.
A member <u>may</u> discharge a firearm for:	• The lawful performance of duties; • On or off duty training at a range, specifically designed for that purpose and using only Department authorized ammunition; or • Rendering harmless an animal that represents a threat to public safety or is seriously injured and suffering.
A member **<u>SHALL NOT</u>** discharge a firearm:	• As a warning; • To merely disable a fleeing vehicle; or • At a moving vehicle – **<u>UNLESS</u>**: An occupant uses or threatens to use immediate lethal force directed at the member or another person to cause them serious bodily harm/serious physical injury or death.
Discharge of a Firearm At a Moving Motor Vehicle	Members shall: • As a first course of action, <u>remove themselves</u> from the path of a moving vehicle or position of vulnerability; and • Understand and consider that: 1. Bullets fired at moving vehicles are extremely unlikely to stop or disable the motor vehicle; 2. Bullets fired may miss the intended target or ricochet and cause injury to themselves, other officers, or innocent persons; or 3. If the bullets disable the operator, the vehicle may crash and cause injury to themselves, other officers, or innocent persons.

Continued next page.

Subject	Number
Use of Force	**UOF-01**

Ready Position	When the member reasonably believes that there is a potential threat of serious bodily harm/serious physical injuries or death, the firearm may be placed at the ready position: • Trigger finger is alongside of the frame except when ready to engage; and • In a safe direction, below the line of sight, so as not to impede member's vision.
Use of Force Equipment and Training	The Colonel/Superintendent shall authorize the specific use of force equipment and training to be used by members. Members are responsible for keeping their equipment clean and operational at all times. All members shall have successfully completed training in the specific use of force equipment prior to use.

Investigations/ Reporting

Reporting Use of Force - The policy UOF-03 Reports, shall be adhered to upon any:

- On duty discharge of any weapon outside of a training range specifically designed for that purpose;
- Off duty discharge of a Department weapon outside of a training range specifically designed for that purpose;
- Compliance or striking techniques are used;
- OC Spray is used;
- Department issued Electronic Controlled Weapon (ECW) activation, on or off duty, as defined in UOF-06 Electronic Control Weapons; or
- Use of force caused or is reported to have caused injury or death to another.

References

UOF-03 Use of Force Reports
UOF-06 Electronic Controlled Weapons (ECW)
MPAC: 1.3.1, 1.3.2, 1.3.3, 1.3.4, 1.3.5

Promulgated By:

Department of State Police
General Order

Effective Date	Number
August 1, 2017	**UOF-02**

Subject

Lethal Force - Response

Policy

The Department shall immediately respond to the scene and conduct an investigation when a use of force results in:

- A death;
- Serious bodily injury; and/or
- Any reportable discharge of a firearm per UOF-03 Reports.

Discharge not requiring an investigation:

- Authorized testing in a properly controlled environment (e.g. Armorer, Ballistician); or
- A firearm is discharged at a range, specifically designed for training and using only Department authorized ammunition; or
- Rendering harmless an animal that is seriously injured and suffering.

Officer-Involved Use of Lethal Force Investigation

Fatal

When a Department member is involved in a use of lethal force resulting in a fatality, the District Attorney's Office or SPDU of jurisdiction shall direct the investigation.

Non-Fatal

When a Department member is involved in a use of lethal force **not** resulting in a fatality, the Division of Investigative Services (DIS) Major who oversees the area where the incident occurs shall assign a commissioned officer from DIS to conduct an investigation.

Force Investigation Response and Support Team (FIRST)

The Force Investigation Response and Support Team (FIRST) shall:

- Be comprised of Commissioned Officers designated by the Colonel/Superintendent;
- Be assigned to regional teams; and
- Assist the DIS Commander.

Subject	Number
Lethal Force - Response	**UOF-02**

FIRST Activation

Upon notification of an incident resulting in the use of lethal force, the Communications Section shall notify:

- The DIS Commander or designee; and
- The SPDU Commander of jurisdiction.

The DIS Commander or designee shall dispatch the FIRST.

FIRST Duties

The DIS Commander or designee shall determine the duties of the FIRST which may include:

- Verify that the following has occurred:
    1. The scene is safe and secure;
    2. A perimeter has been established;
    3. Threats have been eliminated; and
    4. Any suspect(s) have been secured.
- Verify that all proper notifications are made, through channels to the Colonel/Superintendent;
- Identify a controlled area for on-scene interviews and conduct interviews where appropriate;
- Verify that individuals are advised of their rights; and
- Coordinate with the assigned DIS investigator to notify next of kin of all law enforcement and/or civilian victims in accordance with ADM-12 Serious Injury/Death of a Member, if necessary.

Weapons Seizure/

The first responding supervisor shall:

- Immediately seize or take custody of involved weapons and magazines (if applicable);
- Transfer custody of the seized weapon to the Firearms Identification Section; and
- Assist the Firearms Identification Section and Crime Scene Services personnel in the processing of evidence.

Crime Scene Services

Crime Scene Services shall:

- Respond to the scene and coordinate all Crime Scene Services activities with the assigned DIS investigator;
- Gather all evidence at the scene in accordance with INV-10 Evidence Collection/Preservation; and
- Map, photograph, and videotape the scene, if necessary.

Firearms Identification Section

If a firearm is involved, a member of the Firearms Identification Section shall:

- Proceed to the scene and take custody of any involved firearms and begin a firearms related investigation; and
- Notify the Armorer when a Departmental firearm is removed from service.

If appropriate, a temporary firearm shall be issued by the Armorer, as specified in ADM-20 Weapons Management.

Interviews

Interviews with involved Department members shall be:

- Conducted by a commissioned officer, as directed by the assigned DIS investigator.

Interviews with civilian witnesses may be:

- Conducted by commissioned and/or non-commissioned officers as directed by the assigned DIS investigator.

Troop/Section Commanders

The Troop/Section Commanders of jurisdiction shall:

- Establish interagency cooperation in conjunction with the assigned DIS investigator.

Members Using Force

A member involved in a use of force incident resulting in death or serious bodily injury shall:

- Surrender use of force equipment **only** to a Department supervisor;
- Absent an injury, incapacitation, or other exigent circumstances:
    1. Submit a detailed written report not less than twenty-four (24) hours, nor more than forty-eight (48) hours after the incident; or
    2. Submit to an interview by a commissioned officer involved in the investigation, in lieu of a written report, subject to all rights under applicable laws and collective bargaining agreements; and
    3. Submit a SP 376 Use of Force Report to the assigned DIS Investigator, within twenty-four (24) hours of the incident.
- Submit to a follow-up interview, if necessary; and
- Be allowed to contact a union representative, if desired.

Temporary Relief from Duty

A member:

- Shall be placed on Administrative Leave with pay for up to five (5) work days, when involved in a shooting or when the member's actions result in a death; or
- May be placed on Administrative Leave with pay in other circumstances, as appropriate.

Medical Evaluations

A member shall undergo a medical evaluation by the State Police Surgeon prior to returning to duty from any period of Administrative Leave following a shooting, or when a member's actions result in a death.

Employee Assistance Unit

Members are strongly encouraged to contact the Employee Assistance Unit (EAU) for additional support and assistance.

Follow-up counseling and assistance shall be provided by the EAU as needed. The EAU shall also assist members in obtaining support resources outside the Department.

Responsibilities and Protocol

Position	Responsibilities
All Members at Scene	• Administer and secure medical aid after any use of force, if necessary; • Protect and secure the scene; • Ensure that the Desk Officer has been notified; • Speak only to Department investigators, unless otherwise ordered by a member of the Command Staff; and • May consult an attorney.
Desk Officer	• Dispatch necessary assistance to the scene; • Notify Troop Duty Officer and Station Commander; • Make appropriate Daily Administrative Journal entries; and • Refer media inquiries to the Media Relations Section or the District Attorney's Office.
Troop Duty Officer	• Dispatch to the scene a supervisor who is at least one rank higher than the involved officer; • Notify Troop Commander; • Notify the appropriate DIS on-call representative; • Notify GHQ Communications Duty Officer; • Make appropriate Daily Administrative Journal entries; and • Refer media inquiries to the Media Relations Section or the District Attorney's Office.
Supervisors	• Determine condition of all members and civilians at the scene and ensure that EMS has been notified; • Ensure the involved weapon(s) have been seized and secured; • Ensure the area has been secured and limit entry to the scene; • Record and document all members present at the scene in the on-scene access control log; • Keep Troop Duty Officer informed; and • Refer media inquiries to the Media Relations Section or the District Attorney's Office.

Continued next page.

Subject	Number
Lethal Force - Response	**UOF-02**

Responsibilities and Protocol (Continued)

Position	Responsibilities
GHQ Communications	• Notify Colonel/Superintendent; • Contact DIS Commander or designee; • Ensure the appropriate DIS on-call representative has been notified; • Notify the Media Relations Section; and • Notify the Employee Assistance Unit.
Lead DIS Investigator	• Assume control of the scene; • Coordinate actions with the Troop Commander and/or DIS Commander or designee; • Before interviewing or requesting written statements, advise the involved member(s) of their rights, if the member is suspected of violating the law; and • Review and submit a SP 376.
Troop Commander of Jurisdiction	• Notify the Division Commander of involved member(s); • Proceed directly to scene in incidents of death or serious bodily injury; and • Assist the media pending arrival of the Media Relations Section.
Division Commander of Member(s) Involved	• Appoint a commissioned officer to conduct an Administrative Review of the final report issued by the assigned DIS supervisor responsible for the investigation. • Note: The Administrative Review is to ensure that members followed Department procedures during the incident.
Colonel/ Superintendent	• Notify the Executive Office of Public Safety and Security (EOPSS).

References

ADM-12 Serious Injury/Death of a Member
ADM-20 Weapons Management
INV-10 Evidence Collection/Preservation
SUP-04 Employee Assistance Unit
SP 376 Use of Force Report

Promulgated By:

Department of State Police
General Order

Effective Date	Number
July 3, 2019	**UOF-03**

Subject

Reports

Policy

All incidents involving the use of force shall be documented.

Definition

Reportable Incident: Any:

- On duty discharge of any weapon outside of a training range specifically designed for that purpose;
- Off duty discharge of a Department weapon outside of a training range specifically designed for that purpose;
- Compliance or striking techniques are used;
- OC Spray is used;
- Department issued Electronic Control Weapon (ECW) activation, on or off duty, as defined in UOF-06 *Electronic Control Weapons*; or
- Use of force caused or is reported to have caused injury or death to another.

Use of Force Reporting

Any reportable incident, as defined above, shall be reported to the Station Desk Officer of jurisdiction and documented within the Daily Administrative Journal.

The involved member(s) shall:

- Submit a SP 376 *Use of Force Report* along with the SP12 or To/From within twenty-four (24) hours of the incident, absent an injury, incapacitation, or other circumstances with approval from Division Commander.
- Ensure that Station/Unit Commander is provided access to ECW for downloading purposes.

Review

Supervisors shall:

- Ensure members submit a SP 376 along with the SP12 or To/From;
- Review every SP 376 and SP12 or To/From ; and
- Forward all reports to the Division Commander, through channels with findings and recommendations as to the necessity of further investigation of the incident.

Continued next page.

Review (Continued)

Station/Unit Commander or Designee Shall:

- Ensure that ECW data is downloaded per manufacturer instructions; and
- Ensure that data from ECW download is consistent with reports submitted by involved member(s).

The Troop Commander and/or Detective Captain of jurisdiction:

- Shall assign a commissioned officer to conduct an administrative review of the use of lethal force; or
- May assign a commissioned officer to conduct an administrative investigation of the use of less lethal force.

Division Commanders shall:

- Forward a copy of all reports, through channels, to the Division of Standards and Training; and
- Forward a copy of all reports to the Use of Force Review Committee.

Division of Standards and Training Commander may:

- Provide a copy of each report involving the discharge of a firearm to the Director of Firearms Training.

Use of Force Review Committee

The Deputy Superintendent shall appoint members of the Use of Force Review Committee. The Use of Force Review Committee shall evaluate each use of force incident and forward their findings and recommendations to the Deputy Superintendent.

Use of Force Review Committee Evaluation

The Committee shall determine that the use of force was:

- Within Department guidelines; or
- Outside Department guidelines.

The Committee's evaluations and recommendations shall include:

- Tactics and training considerations;
- Supervision considerations;
- Department directives; and
- The need for further Department action.

Classifications of weapons discharge include:

- Intentional: deliberate discharge;
- Unintentional: when an officer does in fact depress the trigger and causes the firearm to discharge without consciously or deliberately willing to do so; or
- Accidental: restricted to the description of a mechanical flaw, shortcoming, or breakdown of a firearm that occurs from such causes as excessive wear, corrosion, mechanical design, or a part breakage, which would allow the weapon to discharge without the shooter depressing the trigger; and
- Other findings as necessary.

Subject	Number
Reporting	**UOF-03**

Use of Force Reports Records

The Committee shall maintain in the Deputy Superintendent's Office, a secure file of all Use of Force Reports, investigations, and reviews.

References

UOF-06 *Electronic Control Weapons*
SP 376 *Use of Force Report*

Promulgated By:

Department of State Police
General Order

Effective Date	Number
July 3, 2019	**UOF-04**

Subject

Use of Force-Equipment

Policy

Members on duty shall carry and use only Department issued use of force equipment.

Definition

Use of Force Equipment: All equipment approved by the Colonel/ Superintendent and issued by the Department such as firearms, ammunition, Oleoresin Capsicum (OC) Spray, batons, Electronic Control Weapons (ECW), and/or any other equipment used to effect control and compliance of a subject.

Purchase/ Issuance

Title	Duties
Colonel/Superintendent	• Shall approve all use of force equipment issued and utilized by the Department; and • Shall authorize, in writing, the Division of Administrative Services (DAS) to purchase all use of force equipment issued and utilized by the Department.
Division of Administrative Services (DAS)	• Is solely responsible and solely authorized to purchase any and all use of force equipment issued and utilized by the Department; and • Shall purchase any and all use of force equipment issued and utilized by the Department pursuant to the written authorization of the Colonel/Superintendent or designee.
Armorer	• Shall test and recommend use of force equipment, including ammunition, through channels to the Office of the Superintendent or designee; • Issue and maintain use of force equipment; • Document and retain all records related to use of force equipment; and • Replace use of force equipment as needed.

Subject	Number
Use of Force-Equipment	**UOF-04**

Inspections

All use of force equipment shall be inspected for condition and operational readiness, only by a supervisor trained to inspect such equipment.

Supervisors shall:
- Remove from service any equipment found to be defective; and
- Notify the Armorer when a Department firearm or ECW is removed from service.

Title	Jurisdiction	Occurrence
Commanders/ Supervisors	Direct/conduct an inspection of all use of force equipment of those under their supervision.	Quarterly
Firearms Training Unit	Conduct an inspection of all use of force equipment brought to range.	Pre- and post-training
Staff Inspections	Conduct an inspection of all use of force equipment.	As appropriate

Maintenance

All use of force equipment shall be kept clean and operational at all times.

Issued firearms shall be cleaned promptly after training:
- In a safe location and manner; and
- Prior to leaving any range.

Only the Armorer and personnel authorized by the Armorer shall repair or modify any use of force equipment or parts.

ON DUTY Carry/Security

While on duty:
- Uniformed members shall carry issued sidearms secured in an issued holster; and
- Non-uniformed members shall carry issued sidearms secured in an issued holster, or otherwise authorized holster, as approved by the Colonel/Superintendent.

When carrying issued firearms, members shall do so in a safe and secure manner:
- Sidearms shall be fully loaded with a round in the chamber and the weapon de-cocked, if equipped;
- Desk Officers shall carry their sidearm in their holster on their person;
- Firearms shall not be left unattended in any non-secure location such as a desk drawer or file cabinet; and
- Firearms and ECWs **shall not** be carried on a member's person during the booking process, including (but not limited to) booking, fingerprinting, and the administration of the breath test.

OFF DUTY Carry/Security

When carrying a Department issued firearm off duty, the following items shall be in the member's possession:

- The member's Department's Badge of Office;
- The member's Department's Identification Card; and
- The member's active License to Carry a Firearm.

When issued firearms are not being carried, they shall be secured with the issued firearm lock and/or in a gun safe, inaccessible to children and others.

Members are not required to carry any issued firearm while off duty.

Members are not authorized to carry their Department issued ECW while off duty.

When off duty, members shall secure Department issued ECWs in a manner consistent with the securing of a firearm and in accordance with all applicable Massachusetts Laws. Members must ensure that Department issued ECWs are inaccessible to children and others.

Firearms in Vehicles

Firearms shall not be left unattended in any vehicle, unless the vehicle is a Department issued vehicle for which the Department has authorized a gun safe or other device designed to secure the weapon and the firearm is secured in such a device. When a member stores a firearm in such a device within an unattended Department vehicle, the device shall be locked and secured, the vehicle's windows shall be closed, and the vehicle's doors shall be closed and locked.

Examples of properly secured weapons:

Patrol Rifle:

- The patrol rifle shall be secured in the Department installed gun rack in accordance with the patrol rifle standard operating procedures.

Shotgun:

- The shotgun shall be secured in the Department installed gun rack, in accordance with shotgun standard operating procedures; and
- If equipped, the key lock shall be engaged when the vehicle is unattended.

STOP Team:

- Firearms shall be secured in accordance with STOP Team standard operating procedures.

Vehicle Safe Requests:

Members requesting to install a gun safe within Department vehicles shall:

- Submit a written request for approval to their Division Commander articulating the need for such a device;
- If approved, coordinate with the Fleet Administrator regarding the professional installation of the safe and regarding the location of installation within the vehicle; and
- Agree, in writing, to assume all responsibility for:
  - The loss or theft of the safe; and
  - Any damage caused to the vehicle associated with the installation or removal of the safe.

Continued next page.

Subject	Number
Use of Force-Equipment	**UOF-04**

Firearms in Vehicles (Continued)

The Armorer shall:

- Determine and approve the make and model of all gun safes to be issued by the Department; and
- Advise the Fleet Administrator of the gun safes authorized for purchase.

Division Commanders shall forward all gun safe requests, whether approved or denied, to the Fleet Administrator.

Soft body Armor

Soft body armor shall be issued to members with the intent that it be worn as often as possible, while on duty.

Members who decline to wear the issued soft body armor shall submit a letter to the appropriate Division Commander stating their reasons.

Promulgated By:

Department of State Police
General Order

Effective Date	Number
November 5, 2008	**UOF-05**

Subject

Firearms Qualifications

Policy

The Department shall provide training and instruction to every member in order to become proficient and confident in the use of issued weapons.

All members shall successfully complete appropriate training and shall qualify with weapons and techniques prior to use.

Definition

Specialized Firearms: Any firearm other than the main duty pistol(s).

Training

Safety is of paramount importance. Regardless of a member's rank, Use of Force Instructors shall be in command of all personnel and equipment during training.

Training shall, as closely as possible, reflect the conditions with which members are likely to be confronted. This training shall include comprehensive instruction in:

- Department's use of force directives and applicable standard operating procedures;
- Legal updates;
- Proficiency and safe weapons handling skills; and
- Safety, storage, and maintenance of use of force weapons and equipment.

Failure to Qualify with Firearms

Those members who fail to meet initial qualification and firearms handling standards shall receive immediate remedial assistance. Members may receive two (2) additional opportunities to qualify within the same day; unless the Supervisor of Firearms Training determines that it would be unsafe or impractical to do so.

In the event a member fails to achieve qualification standards after remedial assistance:

- The Division of Standards and Training Commander, or designee, shall immediately notify the Deputy Superintendent.

Subject	Number
Firearms Qualifications	**UOF-05**

Remedial Training

Member(s) failing to initially qualify shall be assigned to the Range for the Remedial Training Program.

The Remedial Training Program shall consist of three phases designed to assist the remedial shooter in attaining firearms qualification standards. The content of the remedial program shall be determined by the Supervisor of Firearms Training.

- Phase 1 Remedial Training shall consist of one (1) training day.
- Phase 2 Remedial Training shall consist of two (2) training days.
- Phase 3 Remedial Training shall consist of two (2) training days.

If a member fails to achieve firearms qualification standards after Phase 1 Remedial Training, the member shall be assigned to the Phase 2 Remedial Training.

If a member fails to achieve firearms qualification standards after the Phase 2 Remedial Training, the member shall be:

- Evaluated by the State Police Surgeon to determine if any physical limitation(s) exist that would prevent them from achieving the firearms qualification standards; and
- Assigned to the Phase 3 Remedial Training at the State Police Academy for more in-depth assistance.

When participating in any phase of the Remedial Training Program, it is mandatory that a member successfully complete two (2) consecutive runs of the qualification course.

If proficiency is not established at the end of the Remedial Training Program:

- The member shall immediately surrender all firearms and cruiser keys to the Supervisor of Firearms Training;
- The Supervisor of Firearms Training shall immediately secure the firearm(s) and cruiser and advise the Division of Standards and Training (DST) Commander or designee; and
- The DST Commander or designee, shall place the member on administrative leave with pay, and shall proceed with an administrative hearing in accordance with Articles 5 and 6 of the Rules and Regulations.

The Three Phase Remedial Training Program shall constitute reasonable efforts by the Department in an attempt to achieve qualification by a member.

Failure to qualify with issued firearms shall result in administrative action, up to and including termination of employment.

Subject	Number
Firearms Qualifications	**UOF-05**

Specialized Firearms- Failure to Qualify

In the event that a member fails to achieve firearms qualification standards with Specialized Firearms after remedial training, the member shall:

- Be required to surrender such specialized firearms to the Supervisor of Firearms Training; and
- Be assigned to a one (1) day Specialized Firearms Remedial Training Program.

If proficiency is not established at the end of the Specialized Firearms Remedial Training Program, the member may:

- Receive additional remedial training at the discretion of the Colonel/Superintendent.

Qualification/ Other Use of Force Weapons

The DST Commander or designee shall establish standards for qualification with other use of force weapons prior to issuance.

Responsibilities

Position	Duties
Supervisor of Firearms Training	• Conduct necessary training and testing; and • Maintain documentation on firearms training.
Division Commander of DST or designee	• Approve instructors; • Recommend training standards; • Maintain program records.
Division Commanders	• Ensure all members are trained as required.
Deputy Superintendent	• Authorize all use of force training prior to implementation.
Colonel/Superintendent	• Establish qualification standards.

Extended Leaves of Absence

Members returning from a leave in excess of ninety (90) days shall comply with any and all training requirements in accordance with ADM-11D Extended Leaves of Absence.

References

Articles 5 and 6 of the Rules and Regulations
ADM-11D Extended Leaves of Absence

Promulgated By:

Department of State Police
General Order

Effective Date	Number
July 3, 2019	**UOF-06**

Subject

Electronic Control Weapons (ECW)

Policy

The Department shall ensure proper guidance and direction on the use of Electronic Control Weapons (ECWs).

Department members shall use, and are authorized to use, only that force which is *objectively reasonable* to:

- Effect an arrest;
- Restrain or subdue an individual resisting a lawful seizure; or
- Protect themselves or others from physical harm.

ECWs may be used by authorized and trained Department members in accordance with this policy and other established Policy and Procedures. Department members shall use reasonable force to control individuals who are violent, exhibiting threatening or potentially violent behavior, or physically resisting arrest or detention.

Members should assess each situation to determine which action shall best bring the incident under control, using only that amount of force that is reasonably necessary.

If deployed, ECW cycles shall be limited to the minimum number of deployments necessary and should last no longer than necessary to bring an individual under control.

Definitions

Electronic Control Weapon (ECW): A weapon that uses electricity to override voluntary motor responses or applies pain in order to gain compliance or overcome resistance. ECWs are designed to incapacitate without causing serious physical injury or death.

ECW Activation: Any time an ECW is turned on, exclusive of training and routine maintenance/readiness checks.

Laser Activation: The ECW is turned on, activating the light and/or laser beam. Laser activation may be utilized as a warning technique if drive stun deployment and/or probe deployment is objectively reasonable.

Spark Display: The ECW is activated and the arc switch is depressed, activating the electrical arc. Spark display may be utilized as a warning technique if drive stun deployment and/or probe deployment is objectively reasonable.

Drive Stun Deployment: In Drive Stun mode, the ECW is a pain-compliance facilitator rather than an electro-muscular disruptor. Drive stun occurs when the ECW is held against the subject, whether or not probes are deployed. Drive stun may be utilized in response to active resistance or assaultive behavior.

Probe Deployment: In Probe Deployment mode, the ECW uses electricity to override voluntary motor responses. Probe Deployment occurs when probes deploy from an ECW, whether or not the probes strike their intended target. This includes follow-up drive stuns when a single probe is attached to an individual. Probe deployment may be utilized in response to assaultive behavior.

ECW Cycle: Occurs when probe deployment delivers energy to an individual.

Objectively Reasonable: This term means that, in determining the necessity for and appropriate level of force, officers shall evaluate each situation in light of the known circumstances, including, but not limited to, the seriousness of the crime, the level of threat or resistance presented by the subject, and the danger to the officer, subject, and/or community. The reasonableness of a particular use of force must be judged from the perspective of a reasonable officer on scene, rather than with the 20/20 vision of hindsight. Determining reasonableness of force must allow for the fact that police officers are forced to make split second judgments in circumstances that are tense, uncertain and rapidly evolving. The force used must be reasonable under the circumstances known to the officer at the time force is used.

Compliant Individual: An individual who is fully cooperative with a Department member.

Passively Resistant Individual: An individual who is uncooperative but does not use physical strength or body movement to resist a Department member.

Actively Resistant Individual: An individual who uses physical strength and/or body movement to resist a Department member. Examples of active resistance include pulling, turning, or walking away from an officer.

Assaultive Individual (Bodily Harm): An individual who attempts to injure a Department member or another person or engages in conduct that has the potential to injure a Department member or another person.

Aggravated Assaultive Individual (Serious Bodily Harm/Death): An individual who engages in conduct that is likely to produce death or serious bodily harm to a member of the Department or another person.

Sensitive Population Groups: Sensitive population groups include those who reasonably appear to be, or are known to be, children, elderly, medically infirm, pregnant, or users of a cardiac pacemaker.

Subject	Number
Electronic Control Weapons	**UOF-06**

Less Lethal Force: Use of force that is not intended to cause serious bodily harm/serious physical injuries or death.

- Members are authorized to use less lethal force in accordance with the law, the contents of General Order UOF-01, and this policy.

Lethal Force: Use of force intended to inflict serious bodily harm/serious physical injuries or death.

- Members are authorized to use lethal force in accordance with the law, the contents of General Order UOF-01, and this policy.

Authorized Users

Only those Department members who have successfully completed the Department's initial ECW training and subsequent in-service ECW training are authorized to use an ECW.

Weapon Readiness

Department members issued and authorized to use a ECW shall:

- Ensure the ECW is carried in an approved holster on the side of the body opposite the service handgun;
  [NOTE: members not assigned to uniformed duty may use other Department-approved holsters and carry the weapon consistent with Department training.]
- Ensure the ECW is fully armed with the safety on in preparation for immediate use;
- Ensure one spare cartridge is available as backup in case of cartridge failure or the need for reactivation;
- Ensure the spare cartridge is stored, carried, and used in a manner consistent with training;
- Ensure cartridges are replaced following the manufacturer's expiration requirements;
- Ensure only manufacturer-approved battery power sources are used for the ECW;
- Prior to each regular tour of duty shift, confirm that the ECW is functioning properly by performing all tests as defined in training; and
- Not make any modifications or repairs on the ECW unless authorized in writing by the Armorer.

Activation

In accordance with the law, the contents of General Order UOF-01, and this policy, and when it is objectively reasonable to do so, Department members are authorized to utilize an ECW to arrest and/or detain an individual that has and/or continues to exhibit behavior that leads the officer to believe the individual is actively resisting or assaultive and will resist being arrested or detained.

Subject	Number
Electronic Control Weapons	**UOF-06**

ECW Use of Force Response Table

If the subject is:	Then the response may include:
Actively Resistant	Laser Activation Spark Display Drive Stun
Assaultive – Bodily Harm	Laser Activation Spark Display Drive Stun Probe Deployment
Aggravated Assaultive – Serious Bodily Harm/Death	Laser Activation Spark Display Drive Stun Probe Deployment NOTE: Department members are not required to use a weapon of less-lethal force if use of lethal force is objectively reasonable.

Situations in which the ECW may be activated in accordance with the above table include but are not limited to:

- When an individual uses force or violence against the member or another person(s);
- When an individual exhibits violent, threatening, or potentially violent behavior;
- When an individual actively resists an arrest or detention;
- When an individual flees in order to avoid arrest or detention in circumstances where the member would pursue on foot and physically effect the arrest or detention;
- When an individual expresses intent and has the means to commit suicide or inflict serious bodily harm to themselves or others and ECW activation does not create additional risk;
- To protect Department members or others against an aggressive animal; and
- In the course of Department-authorized training exercises or demonstrations.

Department members shall:

- Give the individual a warning prior to activating the ECW, unless doing so would place any member or person(s) at risk;
- Adhere to the Department's training regarding warnings, which may include verbal warnings, display of the ECW, laser painting, arcing, spark display, or a combination thereof;
- When feasible, an announcement should be made to other members or personnel on the scene that an ECW is going to be activated;
- Not intentionally activate more than one ECW at a time against an individual; and
- Be aware that an individual subjected to an ECW Cycle may not be able to respond to commands during or immediately following an ECW Cycle exposure.

- ECW cycles should be limited to the least number of exposures and should last no longer than necessary to bring an individual under control. Each 5-second cycle is considered an independent use of force and must be objectively reasonable and be documented in writing.
- Avoid continued ECW use as an attempt to facilitate compliance if circumstances indicate that drive stun deployment is ineffective as a pain-compliance technique.
- Be aware that pain compliance may not be effective against an individual in a mental health crisis state, under the influence of a mind altering substance, or when extremely focused.
- Consider potential risk(s) to third parties or bystanders when activating ECWs.
- Be aware that a subject's heavy clothing may impede the effectiveness of ECWs.
- Aim, to the degree possible, for the following target areas:
  - Lower center mass below the chest
  - Back
  - Legs

  NOTE: Consistent with training and to the extent possible, Department members should avoid sensitive areas such as the eyes, face, head, throat, neck, breasts, groin and genitals.

Department members shall **not** use the ECW:

- On individuals who passively resist as defined within this policy;
- On a handcuffed or secured prisoner;
  EXCEPTION: ECW, in limited situations, may be used on a handcuffed or secured prisoner if an individual exhibits overtly assaultive, self-destructive, or violently resistive behavior that cannot reasonably be controlled by other readily available means.
- In any environment where the member reasonably believes that a flammable, volatile, or explosive material is present, including but not limited to OC spray with volatile propellant, gasoline, natural gas, propane;
- When the individual is located in water;
- In any situation where the member has a reasonable belief that the subject might fall resulting in death or serious physical injury, and the circumstances presented do not justify that risk; or
- On individuals in physical control of a vehicle in motion (e.g., automobiles, trucks, motorcycles, ATVs, bicycles, scooters) unless exigent circumstances exist.

Sensitive Population Group

Department members shall be aware of general concerns when an ECW is used on an individual of a Sensitive Population Group. Department Members are not prohibited from using an ECW on sensitive population individuals, but use is limited to those exceptional circumstances where the potential benefit of using the ECW (i.e., injury reduction) reasonably outweighs the risks and concerns.

Subject	Number
Electronic Control Weapons	**UOF-06**

ECW Post-Activation

After a probe deployment, Department Members shall seek medical attention for the individual and ensure that ECW probes are removed by qualified medical personnel.

In any case of Drive Stun deployment or Probe deployment from an ECW on an individual, members shall:

- Transport the individual to an emergency care facility for evaluation and/or treatment if any of the following apply:
  - The individual requests medical attention or there is an obvious need for medical attention;
  - The ECW was deployed in a sensitive area (e.g., eye, face, head, throat, neck, breasts, groin, genitals);
  - The individual is part of a sensitive population group;
  - More than three ECW cycles were deployed on the individual or the ECW was deployed for continuous cycles amounting to 15 seconds or more; or
  - More than one ECW device has been deployed on an individual.
- Use restraint techniques that minimize risk of impairing a subject's respiration.
- Make reasonable efforts to protect the subject's privacy.

Internal Reporting

Department members who activate an ECW shall:

- Adhere to Policy and Procedure UOF-03 Reports, *Reportable Incident*;
- Report ECW activations to the Station Desk Officer of jurisdiction;
- Ensure ECW activations are documented within the Daily Administrative Journal/Department Records Management System; and
- Ensure that Station/Unit Commander is provided access to ECW for downloading purposes.

The involved member(s) shall:

- Submit a SP 376 Use of Force Report within twenty-four (24) hours of the activation, absent an injury, incapacitation, or other exigent circumstances.

Supervisors shall:

- Ensure members submit a SP 376;
- Review every SP 376; and
- Forward reports to the Division Commander, through channels with findings and recommendations as to the necessity of further investigation of the incident.

Station/Unit Commander or Designee Shall:

- Ensure that ECW data is downloaded as per manufacturer instructions; and
- Ensure that data from ECW download is consistent with reports submitted by involved member(s).

Subject	Number
Electronic Control Weapons	**UOF-06**

External Reporting

The Use of Force Review Committee shall:

- Collect Department information regarding the use of ECW;
- Ensure the Executive Office of Public Safety and Security (EOPSS) *ECW Use Reporting Form* is completed and submitted as required by EOPSS in accordance with M.G.L. c. 140, § 131J and St. 2004, c. 170, s.2;
- Forward a copy of the EOPSS *ECW Use Reporting Form* to the Deputy Superintendent.

Off-Duty Considerations

Members are not authorized to carry their Department issued ECW while off duty.

When off duty, members shall secure Department issued ECWs in a manner consistent with the securing of a firearm and in accordance with all applicable Massachusetts Laws. Members must ensure that Department issued ECWs are inaccessible to children and others.

Training

Department members shall be trained in accordance with the lesson plan provided by the manufacturer approved by EOPSS in accordance with M.G.L. c. 140, § 131J .

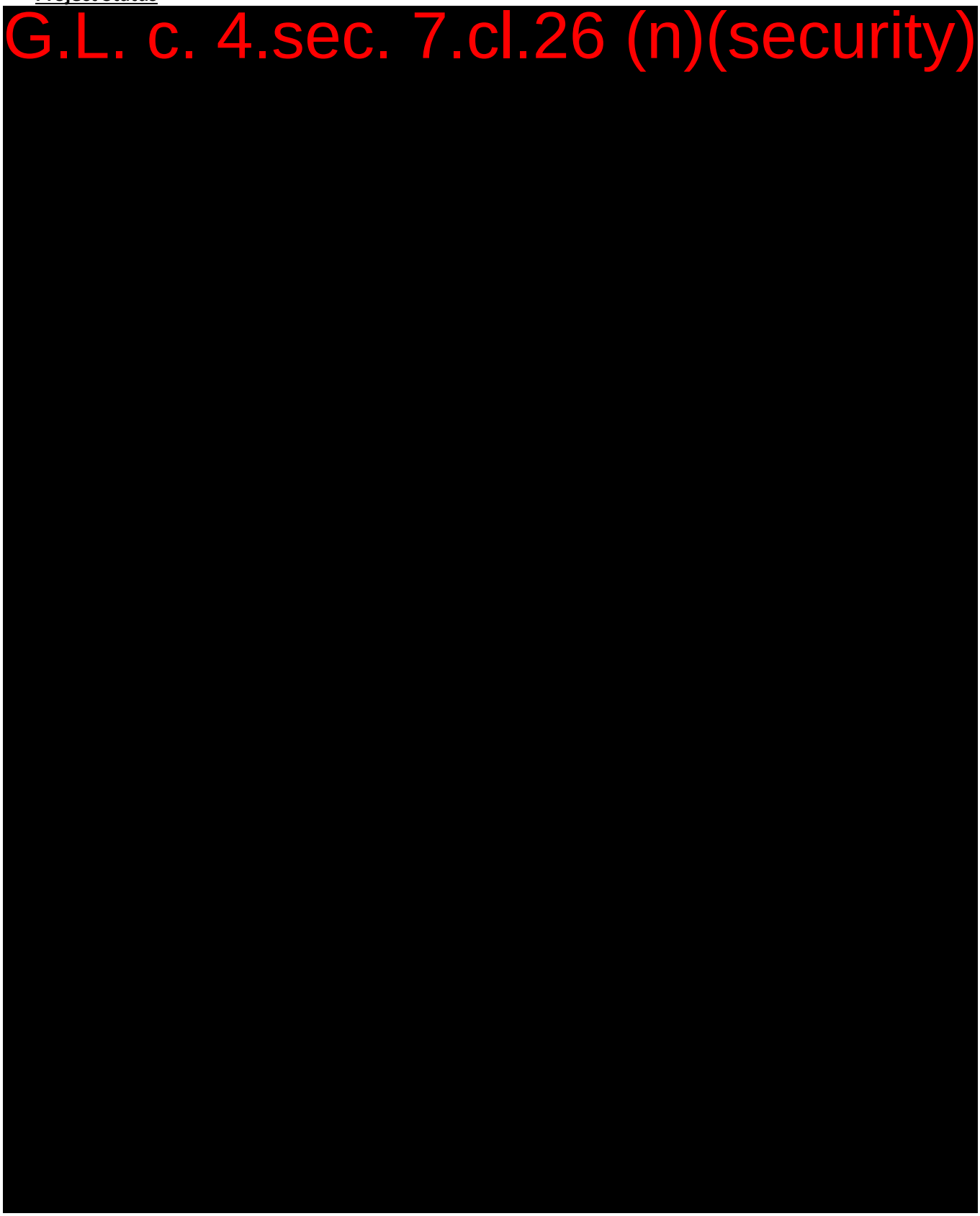
Department members shall be trained in accordance with the law, the contents of General Order UOF-01, and this policy.

References

UOF-01 Use of Force
UOF-04 Use of Force Equipment
International Association of Chiefs of Police (IACP) Electronic Controlled Weapon Model Policy, April 2010
Police Executive Research Forum Electronic Control Weapon Guidelines, 2011
SP 376 Use of Force Report
Electronic Control Weapons in Massachusetts 2014, Executive Office of Public Safety and Security
Executive Office of Public Safety and Security ECW Use Report
Taser® Lesson Plan
501 CMR 8.00 *et seq.*
M.G.L. c. 140, § 131J and St. 2004, c. 170, s. 2.

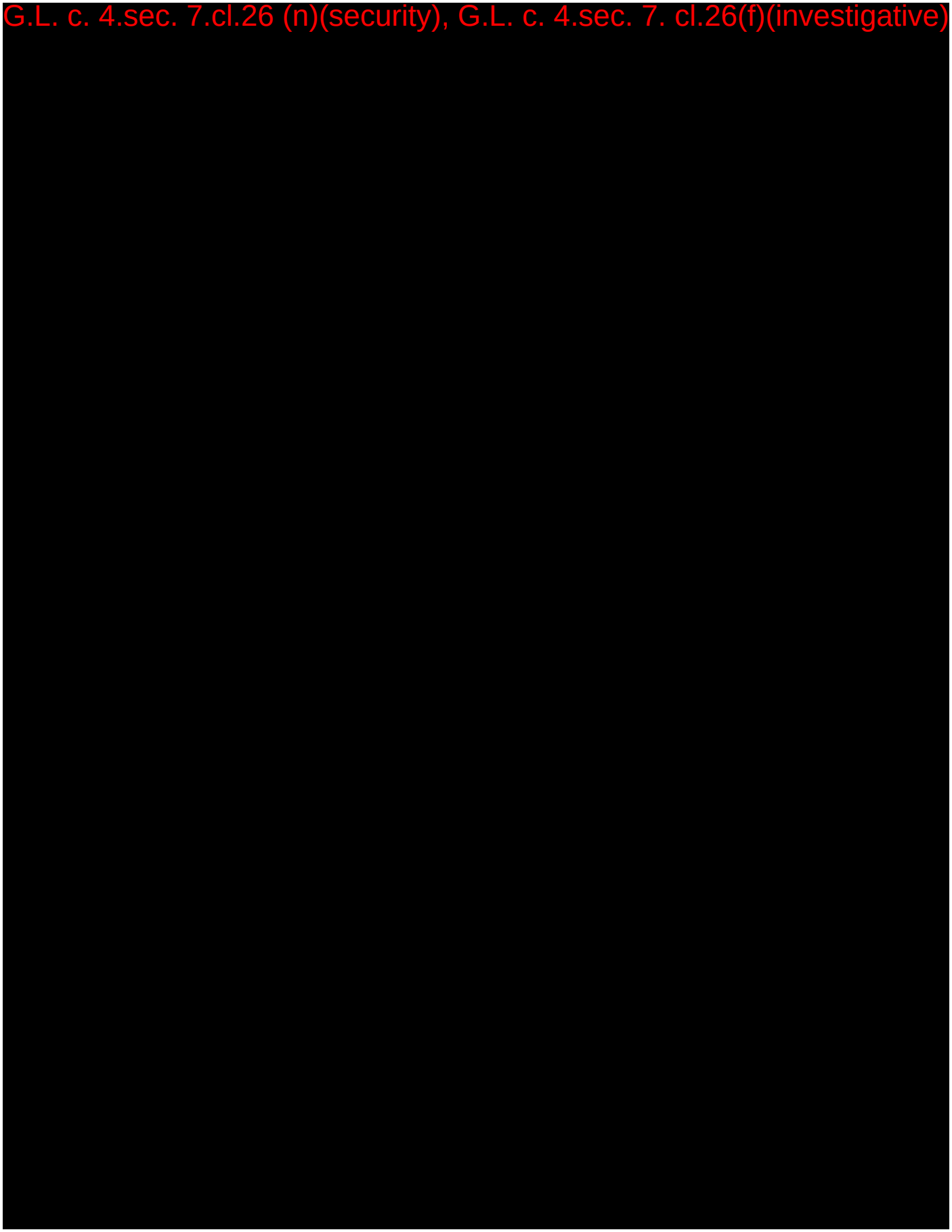
Promulgated By:

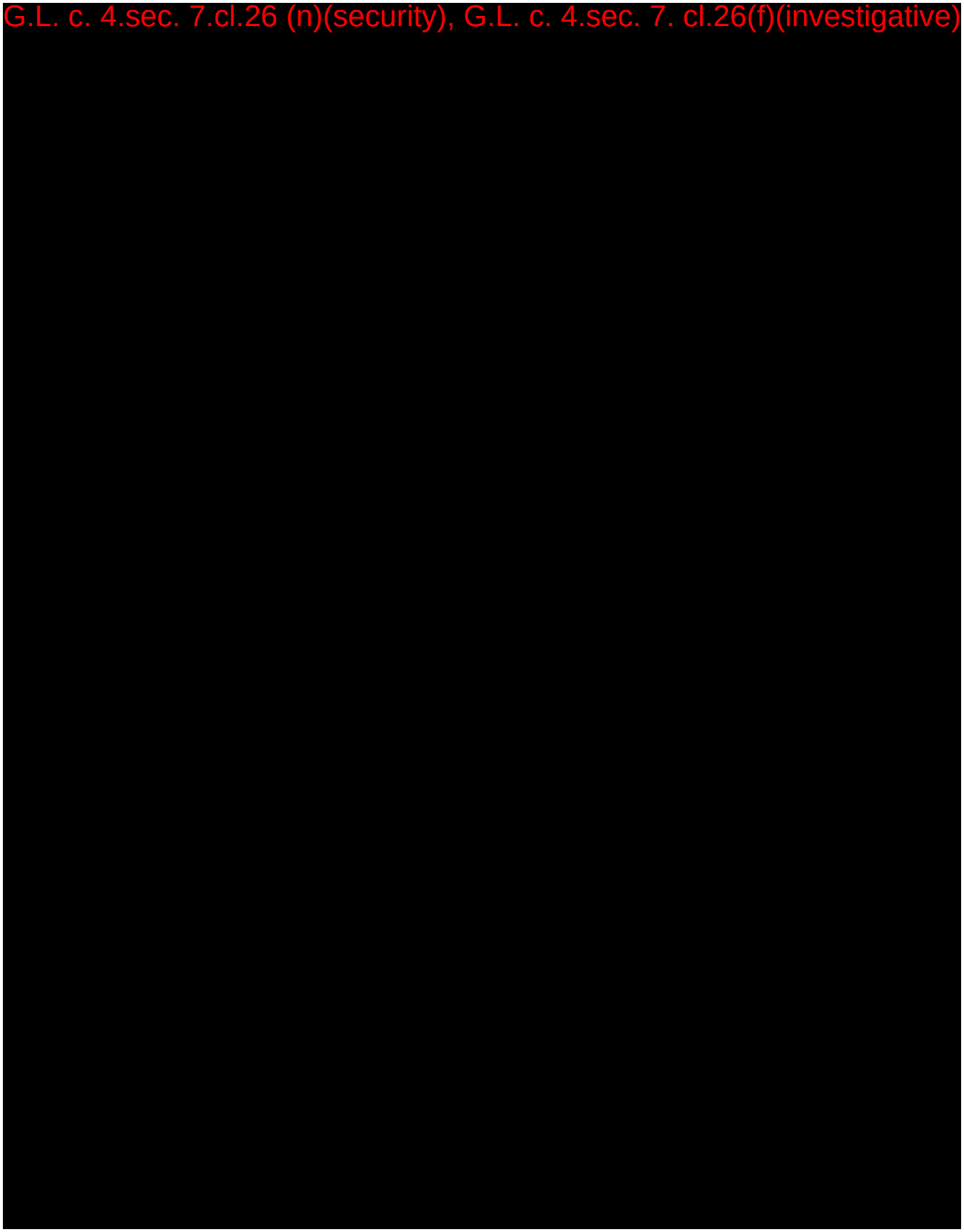
Project Status

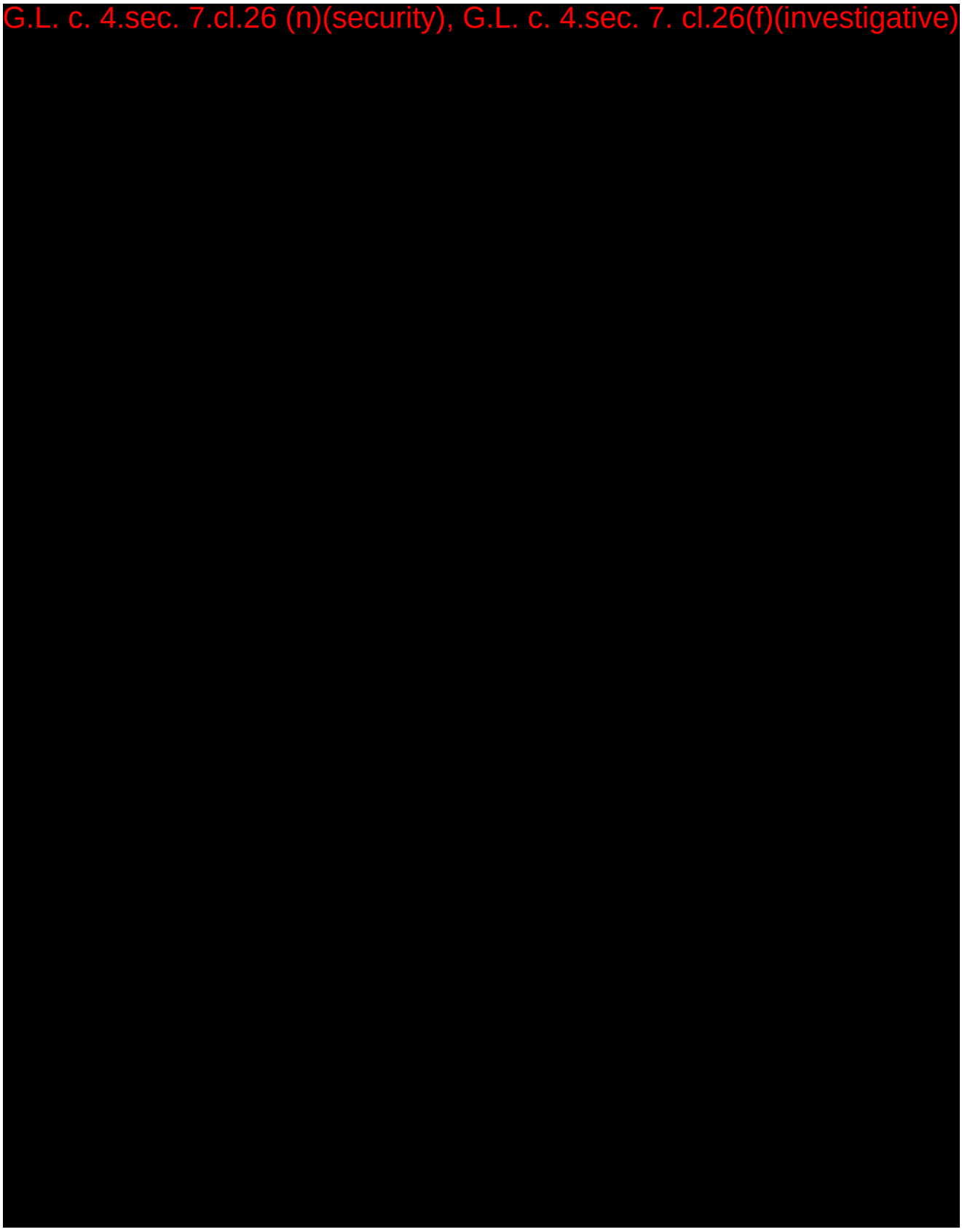


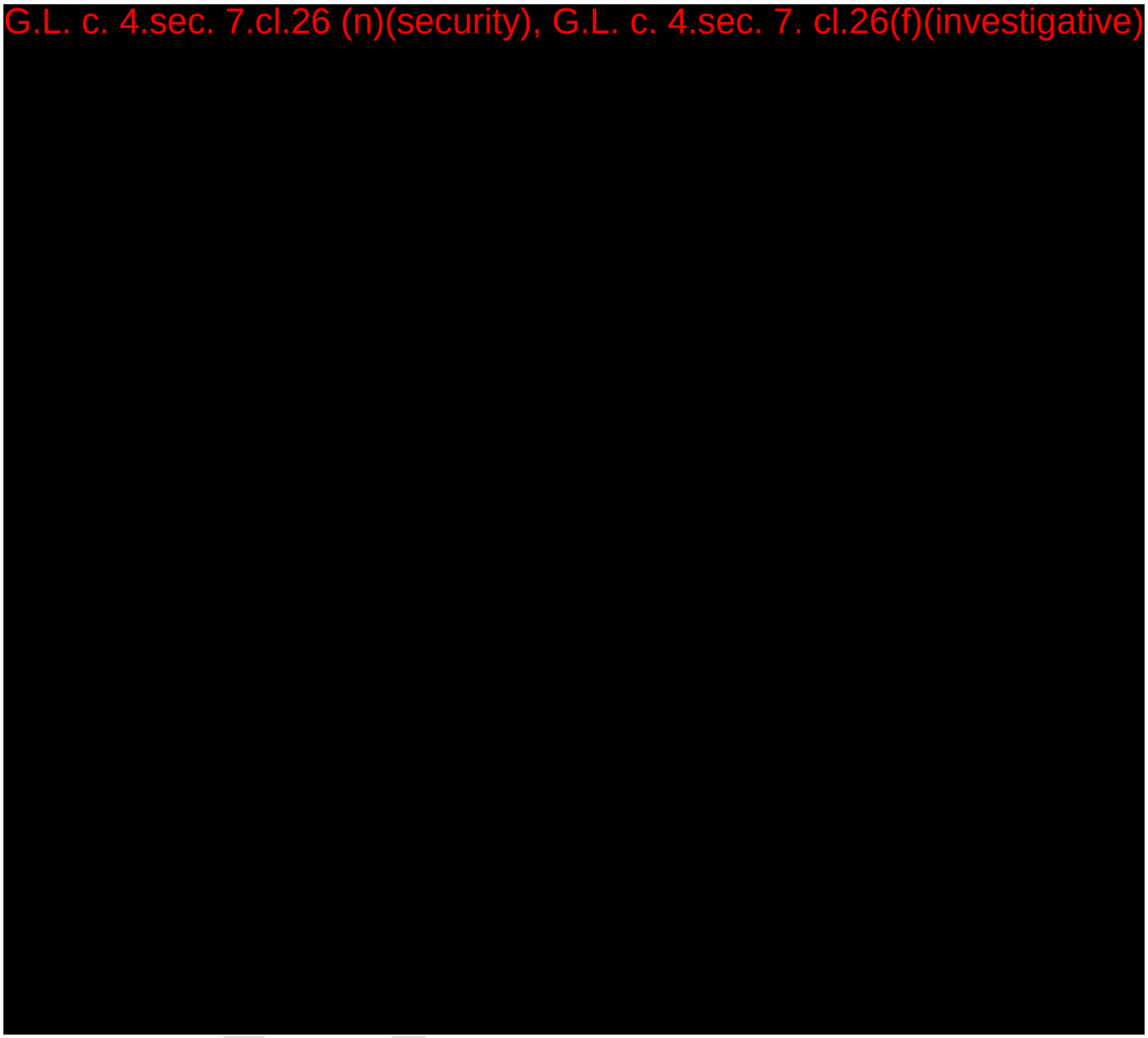
G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

[redacted]


G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)


G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)


G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)


G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

COMMONWEALTH TERMS AND CONDITIONS FOR INFORMATION TECHNOLOGY CONTRACTS

This Commonwealth Terms and Conditions for Information Technology Contracts ("IT Terms and Conditions") form is jointly issued by the Executive Office of Technology Services and Security (EOTSS), the Executive Office for Administration and Finance (ANF), the Office of the Comptroller (CTR) and the Operational Services Division (OSD) for use by all Commonwealth of Massachusetts ("State") Departments and Contractors to govern Contracts subject to the object codes for information technology, as defined by the Office of the Comptroller's Expenditure Classification Handbook, or other Contracts as expressly approved in writing by EOTSS, ANF, OSD, and CTR. Any changes or electronic alterations by either the Department or the Contractor to the official version of this form shall be void. Upon execution of the Standard Contract Form and filing as prescribed by the Office of the Comptroller, these IT Terms and Conditions will be incorporated by reference into any Contract for IT commodities or services executed by the Contractor and any State Department, in the absence of a superseding law or regulation requiring a different Contract form. Performance shall include services rendered, obligations due, costs incurred, commodities and deliverables provided and accepted by the Department, programs provided or other commitments authorized under a Contract. A deliverable shall include any tangible product to be delivered as an element of performance under a Contract. The Commonwealth is entitled to ownership and possession of all deliverables purchased or developed with State funds. The Commonwealth's possession, installation, or use of proprietary IT commodities or services, developed by Contractor for the open market without the use of State funds, shall not transfer title or ownership thereof to the Commonwealth. A "Contract" shall mean, in the following order of priority: (i) these IT Terms and Conditions; (ii) the Standard Contract Form issued jointly by ANF, CTR and OSD, and the Standard Contract Form Instructions and Contractor Certifications; (iii) the Request for Response (RFR) or applicable solicitation document, as it may be amended by the Department; (iv) the Contractor's response to the RFR or applicable solicitation document, as it may be amended by the Department and Contractor, including any negotiated terms and conditions allowable pursuant to law or regulation; (v) a solicitation created by the Department for a particular engagement such as a Request for Quote (RFQ), as it may be amended by the Department; (vi) any negotiated terms and conditions governing a particular engagement, as expressly agreed to in writing between the Department and the Contractor; and (vii) the Contractor's response to the Department's solicitation.

1. *Contract Effective Start Date.* Notwithstanding verbal or other representations by the parties, the effective start date of performance under a Contract shall be the later of the date the Contract was executed by an authorized signatory of the Contractor, the date the Contract was executed by an authorized signatory of the Department, the date specified in the Contract, or the date of any approvals required by law or regulation.

2. *Payments And Compensation.* The Contractor shall only be compensated for performance delivered and accepted by the Department in accordance with the specific terms and conditions of a Contract. The Department may, in its sole discretion, agree to pre-payment for subscription-based IT commodities or services for a term length as specified in the Contract. All Contract payments are subject to appropriation pursuant to M.G.L. c. 29, § 26, or the availability of sufficient non-appropriated funds for the purposes of a Contract, and shall be subject to intercept pursuant to M.G.L. c. 7A, § 3 and 815 CMR 9.00. Overpayments shall be reimbursed by the Contractor or may be offset by the Department from future payments in accordance with state finance law. Acceptance by the Contractor of any payment or partial payment, without any written objection by the Contractor, shall in each instance operate as a release and discharge of the State from all claims, liabilities or other obligations relating to the performance of a Contract.

3. *Contractor Payment Mechanism.* All Contractors will be paid using the Comptroller's payment system unless a different payment mechanism is required. The Contractor shall timely submit invoices and supporting documentation as prescribed in a Contract. The Department shall review and return rejected invoices within fifteen (15) days of receipt with a written explanation for rejection. Payments shall be made in accordance with the bill paying policy issued by the Office of the Comptroller and 815 CMR 4.00, provided that payment periods listed in a Contract of less than forty-five (45) days from the date of receipt of an invoice shall be effective only to enable a Department to take advantage of early payment incentives and shall not subject any payment made within the forty-five (45) day period to a penalty. The Contractor Payroll System shall be used only for Individual Contractors who have been determined to be Contract Employees as a result of the Department's completion of an Internal Revenue Service SS-8 form in accordance with the Omnibus Budget Reconciliation Act (OBRA) of 1990, and shall automatically process all state and federal mandated payroll, tax and retirement deductions.

4. *Contract Termination Or Suspension.* A Contract shall terminate on the date specified in a Contract, unless this date is properly amended in accordance with all applicable laws and regulations prior to this date, or unless terminated or suspended under this Section upon prior written notice to the Contractor. The Department may, without penalty, terminate or suspend a Contract: (i) without cause; (ii) if the Contractor breaches any material term or condition or fails to perform or fulfill any material obligation required by a Contract; (iii) in the event of an elimination of an appropriation or availability of sufficient funds for the purposes of a Contract; or (iv) in the event of an unforeseen public emergency mandating immediate Department action. Upon immediate notification to the other party, neither the Department nor the Contractor shall be deemed to be in breach for failure or delay in performance due to Acts of God or other causes factually beyond their control and without their fault or negligence. Subcontractor failure to perform or price

increases due to market fluctuations or product availability will not be deemed factually beyond the Contractor's control.

5. *Written Notice*. Any notice shall be deemed delivered and received when submitted in writing in person or when delivered by any other appropriate method evidencing actual receipt by the Department or the Contractor. Any written notice of termination or suspension delivered to the Contractor shall state the effective date and period of the notice, the reasons for the termination or suspension, if applicable, any alleged breach or failure to perform, a reasonable period to cure any alleged breach or failure to perform, if applicable, and any instructions or restrictions concerning allowable activities, costs or expenditures by the Contractor during the notice period.

6. *Confidentiality, Privacy, and Protection of Data*. The Contractor shall comply with M.G.L. c. 66A if the Contractor becomes a "holder" of "personal data" and shall comply with M.G.L. c. 93H if the Contractor accesses "personal information." The Contractor shall also protect the physical security and restrict any access to personal or other Department data in the Contractor's possession, or used by the Contractor in the performance of a Contract, which shall include, but is not limited to, the Department's public records, documents, files, software, equipment or systems. See also the Commonwealth's Standard Contract Form and the Enterprise Security Policies and Standards: https://www.mass.gov/handbook/enterprise-information-security-policies-and-standards.

7. *Record-keeping And Retention, Inspection Of Records.* The Contractor shall maintain records, books, files and other data as specified in a Contract and in such detail as shall properly substantiate claims for payment under a Contract, for a minimum retention period of six (6) years beginning on the first day after the final payment under a Contract, or such longer period as is necessary for the resolution of any litigation, claim, negotiation, audit or other inquiry involving a Contract. The Department shall have access, as well as any parties identified under Executive Order 195, during the Contractor's regular business hours and upon reasonable prior notice, to such records, including on-site reviews and reproduction of such records at a reasonable expense.

8. *Assignment.* The Contractor may not assign or delegate, in whole or in part, or otherwise transfer any liability, responsibility, obligation, duty or interest under a Contract, with the exception that the Contractor shall be authorized to assign present and prospective claims for money due to the Contractor pursuant to a Contract in accordance with M.G.L. c. 106, § 9-318. The Contractor must provide sufficient notice of assignment and supporting documentation to enable the Department to verify and implement the assignment. Payments to third party assignees will be processed as if such payments were being made directly to the Contractor and these payments will be subject to intercept, offset, counter claims or any other Department rights which are available to the Department or the State against the Contractor. Upon prompt written notice to the Contractor, the Department may assign or delegate, in whole or in part, or transfer any liability, responsibility, obligation, duty or interest under a Contract, to another Department, provided that the assignee has agreed to take full responsibility of such Contract, liability, responsibility, obligation, duty or interest.

9. *Subcontracting By Contractor.* Any subcontract entered into by the Contractor for the purposes of fulfilling the obligations under a Contract must be in writing, authorized in advance by the Department and shall be consistent with and subject to the provisions of these IT Terms and Conditions and a Contract. Subcontracts will not relieve or discharge the Contractor from any duty, obligation, responsibility or liability arising under a Contract. The Contractor shall be responsible for the acts and omissions of its subcontractors. The Department is entitled to copies of all subcontracts and shall not be bound by any provisions contained in a subcontract to which it is not a party.

10. *Affirmative Action, Non-Discrimination In Hiring And Employment.* The Contractor shall comply with all federal and state laws, rules and regulations promoting fair employment practices or prohibiting employment discrimination and unfair labor practices and shall not discriminate in the hiring of any applicant for employment nor shall any qualified employee be demoted, discharged or otherwise subject to discrimination in the tenure, position, promotional opportunities, wages, benefits or terms and conditions of their employment because of race, color, national origin, ancestry, age, sex, religion, disability, handicap, sexual orientation or for exercising any rights afforded by law. The Contractor commits to purchasing supplies and services from certified minority or women-owned businesses, small businesses or businesses owned by socially or economically disadvantaged persons or persons with disabilities.

11. *Liability.* Unless otherwise exempted by law, and subject to Section 13, the Contractor shall be liable for any and all claims, liabilities, and costs which arise out of the Contractor's performance of a Contract.

12. *Indemnification*. The Contractor shall indemnify and hold harmless the State, including the Department, its agents, officers and employees, against any and all claims, liabilities, and costs for personal injury, property damage, or infringement of intellectual property rights, (each, an "Unlimited Claim"), and all claims, liabilities, and costs, in connection with a security or data breach, or unauthorized disclosure of data, (each, a "Data Breach"), and other claims, liabilities, and costs, which arise out of Contractor's performance of a Contract. After prompt notification by the State, the Contractor shall have an opportunity to participate in the defense of claims and any negotiated settlement agreement or judgment. The State shall not be liable for any costs incurred by the Contractor arising under this Section 12. The Contractor (including its agents, officers, employees or subcontractors) shall at no time be considered an agent or representative of the Department or the State. Any indemnification of the Contractor shall be subject to appropriation and applicable law.

13. *Limitation of Liability*. Absent a higher limitation of liability expressly agreed to in a particular Contract between the Department and the Contractor, the limitation of liability in this

COMMONWEALTH TERMS AND CONDITIONS FOR INFORMATION TECHNOLOGY CONTRACTS

Section 13 shall apply. This Section 13 shall not limit the State's right of recovery for the Contractor's indemnification obligations for an Unlimited Claim under Section 12, nor the State's ability to join the Contractor as a third-party defendant in connection with an Unlimited Claim or Data Breach. The Contractor's liability for any Data Breach shall not exceed the greater of: (i) $250,000; (ii) the amount mandated by applicable State or Federal law; (iii) five times the total value of the Contract (or in the case of subscription-based Contracts, five times the total value of the Contract during the committed subscription term); or (iv) the total coverage provided by Contractor's insurance provider(s) for such Data Breach. The Contractor's liability for any other claim shall not exceed the greater of: (i) $100,000; or (ii) two times the total value of the Contract (or in the case of subscription-based Contracts, two times the total value of the Contract during the committed subscription term). Except for the Contractor's indemnification obligations for an Unlimited Claim or Data Breach under Section 12, the Contractor shall not be liable for incidental or consequential damages, including without limitation, loss of use of equipment, lost revenue, lost savings or lost profits of the State.

14. ***Waivers.*** Forbearance or indulgence in any form or manner by a party shall not be construed as a waiver, nor in any way limit the legal or equitable remedies available to that party. No waiver by either party of any default or breach shall constitute a waiver of any subsequent default or breach.

15. ***Risk Of Loss.*** The Contractor shall bear the risk of loss for any Contractor materials used for a Contract and for all deliverables, Department personal or other data which is in the possession of the Contractor or used by the Contractor in the performance of a Contract until possession, ownership and full legal title to the deliverables are transferred to and accepted by the Department.

16. ***Forum, Choice of Law And Mediation.*** Any actions arising out of a Contract shall be governed by the laws of Massachusetts, and shall be brought and maintained in State court in Massachusetts, unless a federal court in Massachusetts has exclusive jurisdiction thereof. The Department, with the approval of the Office of the Attorney General (AGO), may: (i) consent to the jurisdiction of federal courts outside of Massachusetts; or (ii) agree to voluntary mediation through the Massachusetts Office of Dispute Resolution (MODR) of any Contract dispute and will share the costs of such mediation with the Contractor. No legal or equitable rights of the parties shall be limited by this section.

17. ***Contract Boilerplate Interpretation, Severability, Conflicts With Law, Integration.*** Any amendment or attachment to any Contract which contains conflicting language or has the effect of deleting, replacing or modifying any printed language of these IT Terms and Conditions, as officially published by EOTSS, ANF, CTR and OSD, or any printed language of the Standard Contract Form shall be interpreted as superseded by the official printed language. If any provision of a Contract is found to be superseded by state or federal law or regulation, in whole or in part, then both parties shall be relieved of all obligations under that provision only to the extent necessary to comply with the superseding law, provided however, that the remaining provisions of the Contract, or portions thereof, shall be enforced to the fullest extent permitted by law. All amendments must be executed by the parties in accordance with Section 1 of these IT Terms and Conditions and filed with the original record copy of a Contract as prescribed by CTR. The printed language of the Standard Contract Form, as officially published by ANF, CTR and OSD, which incorporates by reference these IT Terms and Conditions, shall supersede any conflicting verbal or written agreements relating to the performance of a Contract, or attached thereto, including contract forms, purchase orders or invoices of the Contractor.

IN WITNESS WHEREOF, the Contractor certifies under the pains and penalties of perjury that it shall comply with these IT Terms and Conditions for any applicable Contract executed with the Commonwealth as certified by their authorized signatory signing the Standard Contract Form.

LAW ENFORCEMENT EQUIPMENT, SUPPLIES, & SERVICES



SAFEWARE®

SAFEOPS



ACCESSORIES
- B-Square
- Blackinton
- Break-Free
- Hoppe's
- KleenBore
- M-PRO 7
- Smith & Warren
- Speedfeed

AERIAL DRONES
- Aeryon
- DJI
- FLIR

APPAREL
- 5.11 Tactical
- Arc'teryx
- Bulwark
- Elbeco
- Horace Small
- LION
- PROPPER
- Spiewak
- TRU-SPEC

BAGS, CASES & PACKS
- 5.11 Tactical
- BLACKHAWK!
- Crye Precision
- Hatch
- OK-1
- Pelican
- Plano
- R&B Fabrications
- Wolfpack Gear

BALLISTIC SHIELDS
- Hatch
- Paulson Mfg.
- PROTECH Tactical
- United Shield

BATONS
- ASP
- Monadnock

BODY ARMOR & HELMETS
- 3M
- ABA
- Angel Armor
- Armor Express
- Crye Precision
- Custom Armor Group
- FirstSpear
- HESCO
- PROPPER
- PROTECH Tactical
- Second Chance
- Team Wendy
- United Shield

BODY CAMERAS
- Kustom Signals
- HauteSpot Networks

BUNKERS & BARRICADES
- Mitigation Technologies
- Special Ops Bunker

COMMUNICATIONS
- Atlantic Signal
- Con-Space
- LRAD
- NowForce
- Peltor
- Tactical Electronics

CRIME SCENE INVESTIGATION
- DetectaChem
- EVI-PAQ
- Forensics Source
- FoxFury
- Identicator
- Lightning Powder
- Mistral Security
- NIK Public Safety
- ODV
- TacticID by B&W Tek

DECONTAMINATION
- Decon7
- DuPont
- Force1Decon
- Kappler
- Lakeland
- TrueTech

DUTY GEAR
- Bianchi
- BLACKHAWK!
- Boston Leather
- Gould & Goodrich
- Safariland
- Uncle Mike's

EOD
- ADS
- BAHIA 21
- Inert Products
- Lindon Defense
- Med-Eng
- Mistral Security
- Tactical Electronics
- TacticID by B&W Tek
- United Shield

EYEWEAR
- 3M
- Crossfire Safety
- Edge Eyewear
- ESS
- MSA
- Paulson Mfg.
- Pyramex Safety
- Radians
- Revision Military
- Smith Optics
- Wiley X

FIELD TESTING, DRUG & ALCOHOL
- DetectaChem
- Field Forensics
- Intoximeters
- Mistral Security
- TacticID by B&W Tek
- Thermo Fisher
- TrueTech

FIRE SUPPRESSION
- Cold Fire Tactical

FIRST AID & TRAUMA
- Combat Medical Systems
- H&H Medical
- North American Rescue
- Tactical Medical Solutions
- Z-Medica

FLASHLIGHTS & ILLUMINATION
- BLACKHAWK!
- Brite-Strike
- Cyalume
- Eflare
- FoxFury
- Nightstick by Bayco
- Pelican
- Streamlight
- SureFire

FOOTWEAR
- 5.11 Tactical
- Black Diamond
- BLACKHAWK!
- Danner
- HAIX
- Onguard Industries
- Timberland PRO
- Tingley Rubber

GLOVES & ACCESSORIES
- 5.11 Tactical
- Ansell
- Best Glove
- Hatch
- HexArmor
- Honeywell

HANDCUFFS & RESTRAINTS
- CTS Thompson
- Hiatt
- Monadnock

HAZARDOUS ENVIRONMENT APPAREL
- Blauer
- DuPont
- Kappler
- Kimberly-Clark
- Lakeland
- LION
- Radiation Shield Technologies

HAZARDOUS ENVIRONMENT MONITORING
- ADVNT Biotechnologies
- Biosystems
- Bruker Detection Corp.
- BW Technologies
- Chemring
- Draeger
- GFG Instrumentation
- Honeywell
- MSA
- Proengin
- RAE Systems
- Response Biomedical/ RAMP
- Scott Safety

HEAD PROTECTION
- CMC Rescue
- Custom Armor Group
- Hatch
- Revision Military
- Team Wendy
- United Shield

HEARING PROTECTION
- Howard Leight
- MSA
- Peltor

HYDRATION & COOLING
- CamelBak
- TechNiche

K-9
- Castle's K-9
- Vohne Liche Kennels

KNIVES
- Benchmade

LESS LETHAL
- Combined Systems
- Defense Technology
- FNH
- Royal Arms
- Sage Control Ordnance

LICENSE PLATE RECOGNITION
- 3M
- Cintel
- Vigilant Solutions

OPTICS, THERMAL & NIGHT VISION
- Aimpoint
- Argus
- ATN
- Bushnell
- Dueck Defense
- FLIR/Armasight
- Fraser Optics
- Holosun
- ITT Night Vision
- L3-EOTech
- Morovision
- Night Optics USA
- Vortex Optics
- Wilcox

RESPIRATORY
- 3M
- Avon Protection
- Draeger
- Honeywell
- MSA
- North
- Scott Safety

RIOT CONTROL
- Argus
- Armadillo Merino
- Cold Fire Tactical
- Damascus
- DMS
- FirstSpear
- Hatch
- Mehler Law Enforcement
- Original S.W.A.T.
- Yaffy

ROBOTS
- ICOR Technology
- Mistral Security
- Northrop Grumman
- RoboteX
- QinetiQ

SECURITY
- ADANI Systems
- CEIA
- Garrett
- Rapiscan Systems

TOOLS & TACTICAL ENTRY EQUIPMENT
- Armadillo Tactical Gear
- BLACKHAWK!
- Broco
- HURST Jaws Of Life
- J&N Tactical
- Mistral Security
- Osen-Hunter
- Wilcox

TRAFFIC SAFETY & SPEED DETECTION
- Bone Safety Signs
- Eflare
- Harris Industries
- JBC Safety
- Kustom Signals
- ML Kishigo
- MPH Industries
- Stalker Radar
- Wanco

TRAINING EQUIPMENT
- Monadnock
- UTM

TRAINING SERVICES
- Blackthorne Services Group
- Safariland
- Survival Edge Tactical Systems

VEHICLES
- ICS
- LDV
- Lenco
- Nomad
- Polaris

VIDEO & SURVEILLANCE
- AgileMesh
- Camero
- Kustom Signals
- Tactical Electronics

WEAPON ACCESSORIES
- Badger Ordnance
- FirstSpear
- SureFire
- TAB Gear

WEAPON SECURITY
- Auto Vault











TABLE OF CONTENTS

4109

HEAD PROTECTION 6
COMMUNICATIONS 7
RESPIRATORY 8
BODY ARMOR 10
BALLISTICS 10
ACTIVE SHOOTER 11
PUBLIC ORDER 12
- FR BASE LAYER 12
- FR OUTER GARMENT 13
- SCORPION BODY ARMOR 14
- SCORPION BODY ARMOR/VESTS 15
- HEAD PROTECTION 16
- HAND & FOOT PROTECTION 17
- RESPIRATORY PROTECTION 18
- SHIELDS/BATON 19
- FIRE SUPPRESSION 20
- LESS THAN LETHAL 20
- IDENTIFICATION 21
- ACCESSORIES 21

FIRST AID & TRAUMA 22
EXPLOSIVE MITIGATION 24
ROBOTS 26
DRUG DETECTION 27
NIGHT VISION 28
THERMAL IMAGING 28
FLASHLIGHTS & ILLUMINATION 29
VIDEO & SURVEILLANCE 30
TACTICAL ENTRY 31
TRAINING SERVICES 32
K9 32
BODY CAMERA 33
SPEED DETECTION 33
VEHICLES 34
GAS DETECTION 34
RADIATION DETECTION 35
PPE 35
DECONTAMINATION 37
HEARING 38
APPAREL 38
FOOT PROTECTION 39
DUTY GEAR 40

FOR MORE INFORMATION OR TO PLACE AN ORDER:

800.331.6707 | info@safewareinc.com | www.safewareinc.com

UNITED SHIELD ACH/MICH MIL BALLISTIC HELMET

The new US Military design featuring a low profile compact helmet with minimum target area and weight.



- Weight: 2.6-2.8 lbs.
- Features an advanced 7 comfort pad system
- Offers improved head stability with a 4-point adjustable harness, suede covered chip cup and nape strap
- Ballistic performance to NIJ 0106.01 and HP White 0401.01
- Shock absorption - US Army ACH Spec for impact
- Hemi-Anvil, 10ft/sec with less than 150 G's force transmitted to head
- Fragmentation performance to US ACH Mil-Spec

UNITED SHIELD SPEC OPS DELTA GEN II

Made from advanced Aramid composites and provides lightweight robust protection from ballistic and fragmentation projectiles as well as other low energy threats.



- Weight: 2.7 lbs.
- NEW carbon fiber Universal NVG mount with guaranteed no-rattle fit
- NEW USI Rapid Adjustment Dial BOA® retention system with 2-way adjustments
- NEW 4D Combat Pad ultra comfort system with phase change technology
- Industry leading ballistic proprietary thermoplastic aramid composite shell
- Removable suede split chin strap to allow for laundry, replacement or use of gas mask extender
- 4-point adjustment harness, picatinny rails, helmet VELCRO® brand fastener kit and bungees
- NIJ 0106.01 Level IIIA, HP White 0401.01B Level IIIA and exceeds US MIL-SPEC for ACH helmet for 2, 4, 16, 64, 17 grain fragments

REVISION MILITARY BATLSKIN VIPER™ P4 HELMET

The Viper P4 head protection system is the most advanced combat helmet, weighing up to 24% lighter than the legacy U.S. Army ACH system - pushing the boundaries of obtainable weight reduction while maintaining superior ballistic and fragmentation protection.



- Stops NIJ IIIA level threats
- Available with Revision's MSS Liner System for enhanced comfort and stability
- Every helmet meets U.S. Army's strict performance, protection and quality standards
- Foundation for all Batlskin modular protection system components and accessories
- Available in 3 cuts (full, mid and high) and 4 sizes (S-XL)

UNITED SHIELD PASGT BALLISTIC HELMET

The PASGT helmet is manufactured with state of the art advanced high strength multi-layered Aramid composites laminated under heat and pressure.

- Excellent bullet resistance
- Minimal deformation at a weight of approximately 3 lbs.
- Offers improved head stability with a 4-point adjustable harness, suede covered chip cup and nape strap
- Ballistic performance to NIJ 0106.01 and HP White 0401.01B
- Wider cut around ears and collar cut to reduce interference from other equipment



TEAM WENDY EXFIL® BALLISTIC HELMET

With a ballistic rating of NIJ Level III-A, it exceeds current ACH Blunt Impact Protection requirements and offers optimal comfort, fit and stability.

- Hybrid composite shell for increased strength and a unique geometry for ideal fit
- Boltless CAM FIT™ retention utilizes a Boa® Fit System with Cam Lock sliders for one-handed adjustment. Left Eye Dominant (LED) option also available.
- Zorbium® foam liner provides customizable comfort while protecting against blunt impact, and allows for an overhead communications headband
- Lanyard compatible Wilcox® shroud secures any standard NVG mount
- Complete system weight of 2.6 lbs. (size 1) and 2.75 lbs. (size 2) includes the helmet shell, accessory rails, impact liner and retention system





LRAD® 100X

Self-contained, hand-held portable voice broadcast system for on-scene and tactical communications.

- Powerful, intelligible communication up to 600 meters
- 20-30 decibels louder than bullhorns and vehicle P.A. systems
- Focused, directional sound pattern for target-ed communication
- Create instant acoustic standoff perimeter
- 8-hour rechargeable battery
- Simple operator interface
- Water resistant



LRAD® 100X MAG-HS KIT

Rapidly deployable, self-contained voice broadcast system with high-strength magnet mount and wireless operation capability.

- Wireless control up to 300 meters and a high strength, easy on/off magnetic mount system
- Up to 6X louder than systems of comparable size and weight
- Focused, directional sound pattern for targeted communication with unparalleled clarity
- Create instant acoustic standoff perimeter
- High-strength neodymium mount system
- Wireless system batteries operates up to 8 hours
- 8-hour rechargeable battery
- Simple operator interface
- Water resistant



LRAD® 450XL

Low profile, lighter weight and designed for temporary or fixed mounting on tripods, vehicles, and small boats. Generates the audio output of systems almost twice its size and weight.

- Powerful, intelligible communication up to 1,700 meters
- Voice boost for extended coverage
- Safely communicate beyond standoff distances to determine intent
- Clear, long-range directional communication
- All-weather use
- Creates isntant acoustic standoff perimeter



LRAD® 500X-RE

Compact long range communication system designed for mounting on tripods, larger vehicles and boats.

- Fixed or portable mounting
- Powerful, intelligible communication up to 2,000 meters
- Voice boost for extended coverage
- Creates instant acoustic standoff perimeter
- Rugged, military tested construction
- All-weather use
- Low power requirements: 60W w/voice, 260W w/ tone
- Simple operator interface



LRAD® 360XT SOLAR W/ SATELLITE CONTROL

Mobile, self-contained mass notification system on wheels. Broadcasts highly intelligible voice messages and warning sirens with uniform 360° area coverage.

- Integrated with a fully self-contained, ruggedized trailer and features lockable electronics and equipment enclosures containing the amplifier modules and battery pneumatic systems
- Battery bank can be charged using the built-in AC powered battery charger or optional solar panel
- Standard configuration of a 3 stack 360X emitter provides a 1,000 meters radius of clear communication coverage



LRAD® 500X-MMT

Fully self-contained helicopter mounted, air-to-ground communication system featuring rugged mount with fu pan-and-tilt range of motion.

- Powerful, intelligible communication up to 2,000 meters
- Quickly installed and removed from helicopter
- Self-powered for 6+ hours of continuous operation when fully charged
- Supplemental type certificates not required
- Simple operator interface



LRAD® 360XL-MID MOBILE KIT

Rapidly deployable, fully self-contained mass notification and incident management communication system.

- 360° uniform sound coverage
- Powerful, highly intelligible voice communications over 2.0 km2
- Complete mass notification kit (emitter head, power amplifier, control module, push-to-talk microphone)
- Lightweight and compact form factor
- Low power consumption for hours of continuous operation
- Industry-leading voice clarity and intelligibility

LRAD

AVON FM54™ AIR PURIFYING RESPIRATOR

Provides maximum level of protection to the face, eyes, and respiratory tract from CBRN, riot agents, TICs, and toxic industrial materials while maintaining extreme user flexiblity as mission profiles change.

- Functions in both negative and positive pressure modes (APR, SCBA, CCBA, and PAPR)
- Panoramic single lens visor
- Electronic communication port for integrated voice projection and radio communication
- 4 sizes to accommodate all operators
- Low profile brow for superior helmet compatibility
- Interchangeable silicone nosecups for custom fit
- Multiple modes
- Optional VPU provides ability to easily communicate while wearing mask



AVON C50™ MASK ASSEMBLY

Based on the U.S. M50/JSGPM (Joint Services General Purpose Mask) and sharing key technologies, provides maximum operational flexibility to counter multiple threat scenarios, including CBRN agents, TICs and TIMs.

- Offers high protection, outstanding field of vision and superior comfort
- The innovative design features optimize the user's time in the operational area

FOR A NON-CBRN OPTION, ASK ABOUT AVON'S PC50



AVON ST53™ SCBA

Combines Avon's FM53 mask technology with an advanced modular breathing apparatus to provide positive pressure SCBA and/or PAPR capability for specialist operations.

- Utilizes black anodised lightweight components
- Enables a fast response to changing operational conditions in one complete modular system
- A switch between negative (filter) and positive (SCBA) pressure is achieved at the flick of an easy to locate lever on the front of the mask
- Can attach a short or long duration compressed air cylinder and enter a location on filter mode, assess the situation and change to SCBA mode if the need arises



MSA G1 SCBA

Designed solely with your safety and comfort in mind. The G1 SCBA offers integrated and enhanced solutions to exceed your needs today as well as years into the future.

- Facepiece is lightweight and compact (no electronics needed)
- Control module provides dual color LCD and analog displays
- Improved visibility through buddy lights and reflective material
- Heads up display (HUD) shows remaining cylinder pressure in 4 increments via colored LEDs
- Electronic communications are integrated into every unit
- G1 SCBA ergonomics
- Central power system for all electronics
- Available in easily-upgradeable threaded or quick-connect cylinder attachment
- Integrated technology for future expansion
- Customizable



MSA MILLENIUM CBRN GAS MASK

A Hycar version of the reliable military-style gas mask (MCU-2/P Mask, used by the Air Force in Desert Storm). The mask combines high performance, customized fit, comfort, cost efficiency and is ideal for law enforcement and emergency response personnel.

- Flexible, one piece polyurethane lens with wide field of vision, bonded to a durable super-soft Hycar rubber facepiece
- NIOSH approved for protection against CN and CS tear gas
- Effective against, but does not have approval for OC tear gas
- Effective against biological agents and chemical warfare agents
- Dual-canister mount to allow weapon firing from either shoulder
- Canister provides up to 8 hours service time against CN, CS and OC agents
- Drinking tube to allow fluid ingestion in contaminated atmospheres
- Standard equipment includes a speaking diaphragm for clear, short-range communications
- Features a nosecup to reduce lens fogging in low temperatures or high humidity conditions



MSA MILLENIUM CBRN CANISTER





3M™ SCOTT SAFETY AV-3000 W/ SURESEAL FACEPIECE

Combines superior fit with greater comfort and versatility. Holds NIOSH approvals across a wide variety of applications, including CBRN.

- Top down convertibility-single facepiece for APR, PAPR, supplied air and SCBA applications, including CBRN
- Reverse Reflex faceseal for improved comfort and fit
- Deep, low profile seal for easier interface with PPE
- Dual large mechanical voicemitters as well as extensive electronic options for improved communications for every workplace
- Available with Kevlar, Poly or Rubber head harness

3M™ SCOTT SAFETY 40MM CARTRIDGES AND CANISTERS



3M | SCOTT Fire & Safety

3M™ SCOTT SAFETY AIR-PAK™ X3 PRO

The Air-Pak™ X3 Pro SCBA is built on a proven foundation of redundant safety features to help ensure the security and comfort of today's firefighter.



- Easy to remove harness
- New harness materials offer greater resistance to chemical and water absorption to help minimize contamination
- Reflective webbing
- Natural articulation promotes greater range of motion to the firefighter, while transferring weight to the hips for a more balanced load
- Superior breathablity
- Electronic PAR (ePAR) provides wireless, bi-directional communication between the firefighter and incident command to improve fireground accountability and communications
- New buckle design provides firm hold
- Integrated drag rescue loop
- System integrity alarm provides visual and audible alert
- High flow alarm provides visual and audible alert
- No flow alarm provides visual and audible alert
- "Buddy" lights provide a 360° view of the firefighter's air pressure and PASS status

Honeywell

NORTH®

HONEYWELL OPTI-FIT™ TACTICAL GAS MASK

- Superior field of vision offers an unobstructed view
- Full facepiece constructed of soft silicone for excellent comfort, fit and durability
- Choice of headgear - 5-pt. strap or nylon mesh headnet
- Three-position canister mounting adaptable for various applications
- Anti-scratch coated polycarbonate lens
- Lens meets ANSI Z87.1 standard for impact and penetration resistance
- DIN-threaded 40 mm connectors
- Low breathing resistance
- NIOSH approved with the Model 1688 Canister to provide protection against choloracetophenone (CN), chlorobenzylidene malononitrile (CS) and includes a P100 filter for use against particulates such as pepper spray
- NIOSH approval number TC-14G 0264





HONEYWELL NORTH SAF-T-FIT® P100 PARTICULATE RESPIRATOR

NIOSH-approved P100 protection provides 99.97% particulate efficiency against oil and non-oil based particulates.

- Meets OSHA and EPA filtering facepiece requirements for lead abatement
- Full face seal for secure and comfort fit
- Durable and adjustable straps
- Exhalation valve expels warm air
- Molded cup design
- Incorporates humidity-resistant filter media
- Low breathing resistance
- Lightweight design
- Nose clip is color-coded for visible size recognition
- Latex free
- Multiple size options for wide range and improved fit

AIRIUS AND ARAURA LEVEL IIIA ALSO AVAILABLE



UNITED SHIELD AIRIUS LEVEL II VEST

The latest innovation in WEARABLE body armor.

- NIJ 0101.06 certified Level II armor
- Provides the areal density weight and thinness of leading polyethylene vests with the flexibility and softness of leading aramid vests
- Comes standard with SPA carrier with 'Dry Run' moisture management system to wick away mositure from the body
- The SPA features a 12-point adjustment system, hidden plate pockets, full side coverage, recessed closure system and optional tails
- Weight: 0.63 psf
- Thickness: .22'
- Performance: 9mm v50 - 1705 fps/.357 v50 - 1685 fps

UNITED SHIELD ARAURA LEVEL II VEST

- Weight: 0.99 psf
- Thickness: .25'
- Performance: 9mm v50 - 1729 fps/.357 v50 - 1663 fps

BALLISTICS



UNITED SHIELD LITE TACTICAL VEST

Blends the functionality of a tactical carrier with a lightweight design that's geared for high performance. Features an abrasion resistant outer fabric that provides exceptional durability for extreme situations.

- Sturdy 500D Cordura® nylon outershell exterior construction
- Top loading plate pockets
- Additional pocket for one size smaller rifle plate
- MOLLE compatible webbing on the front, back and sides
- Adjustable shoulder straps
- Adjustable cummerbund with hook/loop closure underneath the front flap
- Bungee lace cummerbund adjustment
- Flat Kanagroo magazine pockets on front flap
- "Man-Down" drag strap in the rear
- Internal straps for adjustable groin protector
- Accepts insertion of United Shield concealable panels



UNITED SHIELD GARRISON VEST

Providing high performance ballistic protection, integrated in a fully functional and versatile design to meet the strategic needs of your specific mission.

- Sturdy 500D Cordura® nylon outershell exterior construction
- Top loading plate pockets
- Additional pocket for one size smaller rifle plate
- MOLLE compatibility on front, back and sides
- Adjustable shoulder straps
- Adjustable cummerbund with hook/loop closure underneath the front flap
- Bungee lace cummerbund adjustment
- Flat Kangaroo magazine pockets on front flap
- "Man-Down" drag strap in the rear
- Internal straps for adjustable groin protector



UNITED SHIELD MOLLE CROSSOVER CARRIER

Ideal for law enforcement officers who have occasional equipment-carrying assignments. Can be easily converted into a ballistic protective vest by allowing insertion of United Shield ballistic panels.

- Durable 500D Cordura® nylon exterior fabric
- Spacer mesh interior fabric improves breathability
- Top loading internal front and back plate pockets
- MOLLE webbing compatibiilty in the front of the carrier
- Adjustable front to back side hook/loop closure
- Internal 4" adjustable elastic cummerbund sewn in the back



UNITED SHIELD DELTA +6H BALLISTIC PLATE

Level III+ stand alone single curve ballistic plate. Ergonomically designed using proven technology affording the wearers excellent stand alone protection against a range of high velocity threats.

- NIJ 0101.06 Certified
- 3.1 lbs. | 10" x 12"

DELTA LITE 6H ALSO AVAILABLE

UNITED SHIELD SIGMA 6H BALLISTIC PLATE

Level III+ stand alone multi-curve ballistic plate. Ergonomically designed using proven technology affording the wearers excellent stand alone protection against a range of high velocity threats.

- NIJ 0101.06 Certified
- 5.8 lbs. | 10" x 12"

SIGMA LITE 6H ALSO AVAILABLE

UNITED SHIELD ZETA 6H BALLISTIC PLATE

Level III+ stand alone single curve ballisitic plate. Ergonomically designed using proven technology affording the wearers excellent stand alone protection against a range of high velocity threats.

- NIJ 0101.06 Certified
- 7.6 lbs. | 10" x 12"

ZETA LITE 6H ALSO AVAILABLE



UNITED SHIELD UNIFORM SHIRT CARRIER

Specially designed to be worn over the dress shirt.

- Uniform shirt design
- Durable 600D Cordura® nylon exterior fabric
- Poly/cotton interior fabric
- Hook/loop shoulder adjustment
- Front adjustable side hook/loop closure
- Two front lower pockets with zipper closure
- Internal tablet pocket with zipper closure
- Front chest pockets with hook/loop closure
- Internal cell phone pocket
- Pen openings
- Shoulder mic tabs
- Bottom internal ballistic opening

ACTIVE SHOOTER

UNITED SHIELD LEVEL IV ACTIVE SHOOTER KIT

Includes:

- (1) PST SC650 helmet
- (2) Zeta 6h NIJ06 certified Stand Alone Ballistic Plates and (1) carrier option
- The Level IV plates are ergonomically designed to offer the user NIJ 0101.06 certified stand alone protection
- Bag included





BALACLAVA

- Fire retardant
- Designed to give a specified level of protection against accidental contact with flame and against certain forms of heat transfer
- One Size

DARK NAVY

EA — ARM 21305-15 (SZ)

ARMADILLO MERINO EPIC SOCK

- Over the calf sock
- Extra long so it can be folded down over the top of the boot
- Elastic arch support system
- Elastic above the ankle for a better fit
- Lightweight high-stretch padding up the shin and across the top of the foot
- Reinforced toe and heel
- Smooth toe seam
- 62% wool, 21% polyamide, 9% polypropylene, 8% elastic
- SM-XL

DARK NAVY

PR — ARM 11511-15-1 (SZ)

ARMADILLO MERINO COUGAR SHORT SLEEVE CREW SHIRT

- Crew neck with generous back length
- Seamless underarm for no chaffing and seamless shoulders designed for load carrying
- Extra strong tread in the stitching and a tag free neckline
- Regular fit
- 100% Merino Wool, Jersey Knit
- SM-4X

DARK NAVY

EA — ARM 21001-15-X

ARMADILLO MERINO JOHNNIES 2 LONG JOHN BOTTOMS

- Flattened seams for increased comfort
- Body hugging fit - comfortable under your uniform
- Tag free waist
- Flatlock stitching
- High stretch stitching
- 100% Merino Wool
- Jersey Knit
- SM-4X

DARK NAVY

EA — ARM 21352-15-(SZ)

ARMADILLO MERINO BOOT SOCK

- Over the calf
- 100% wool next-to-skin and elastic support system
- Reinforced toe and heel
- Smooth toe seam
- 65% Merino Wool, 38% Nylon, 11% Elastane
- SM-XL

DARK NAVY

PR — ARM 11606-15 (SZ)

ARMADILLO MERINO PANTHER LONG SLEEVE CREW NECK SHIRT

- Seamless underarm reducing chaffing
- Raglan sleeve with no seams on the shoulders
- Relaxed fit
- Tag free neckline
- Single needle stitching
- High stretch stitching
- 100% Merino Wool
- Jersey Knit
- SM-4X

DARK NAVY

EA — ARM 21011-15-(SZ)

FR PUBLIC ORDER PANT

- Stud fastening waist
- Zip around lower waist to match length of jacket zip
- Drawcord inside waistband
- Side leg pocket
- Knee darts
- Extra patch of outer cloth at knee
- Ankle tabs with stud adjustment
- 3 under studs penetrate only the outer cloth
- Combine with jacket

			DARK NAVY
EA	YAF	460	(SIZE/HEIGHT)

FR PUBLIC ORDER JACKET

- Flap covering
- Velcro fastening throat tab folds back to loop velcro
- Loop pull on front zip
- 6 cm jetted opening under chest flaps on each side
- Left side only zip fastening map pocket with mobile phone and notebook pocket inside
- 5 belt loops
- Back action pleats allowing 7 cm expansion on each side
- Combine with pant
- SM-3X (Short/Regular/Tall/XTall)
- 4X (Short/Regular/Tall/XTall/XXTall)
- 5X (Regular/Tall/XTall/XXTall)

	DARK NAVY
EA	YAF 771 (SIZE/HEIGHT)

PATROLLING SUSPENDERS

- Outside body: 500 D Nylon
- Nylon complies with US MILSPEC MilaCa43734D
- Webbing complies with US MILSPEC MilaWa17337 and MilaWaAA55301
- Mesh complies with US MILSPEC MilaCa8061

	BLACK
EA	FSL 12-0008

GEAR BELT

- Body is sewn with Type 13, 1-23/32" Nylon
- Climbing buckle (A.K.A. Cobra Buckle), 1.75"
- Nylon complies with US MILSPEC MilaCa43734D
- Webbing complies with US MILSPEC MilaWa17337 and MilaWaAA55301
- Mesh complies with US MILSPEC MilaCa8061

	BLACK
EA	FSL 15-0004





CHEST AND BACK PROTECTOR

- Lightweight, ergonomically designed chest and back protection
- Chest protection: From collar bones to waistline
- Back protection: From shoulder blades to waistline
- Outer shell: Super high impact ABS moulded shell. Ridged design gives excellent protection against impact while keeping weight to a minimum.
- Inner foam: Low-density impact absorbing polyethylene moulded foam reduces weight and allows circulation of air around the product
- Fastenings: 4 Velcro adjustable Nylon straps riveted to the body of the guard. One at each shoulder, two at the waist. Ensuring security and comfort.
- Guards should be worn beneath a compatible flame retardant coverall. The outer moulding offers limited flame spread in accordance with UL-94 HB.
- Certification: Meets the requirements of UK Home Office Centre for Applied Science and Technology Standard 20/07
- Sizes SM-LG

BLACK

PR — DMS CH/BCK (SZ)



SHOULDER AND UPPER ARM GUARDS

- Lightweight, ergonomically designed shoulder and upper arm protection
- Area of protection: The clavicle, the top and point of the shoulder and the upper arm to above the elbow
- Outer shell: Super high impact ABS moulded shell. Ridged design gives excellent protection against impact while keeping weight to a minimum.
- Inner foam: Low-density impact absorbing polyethylene moulded foam reduces weight and allows circulation of air around the product
- Fastenings: 2 cotton covered Velcro adjustable Nylon straps riveted to the body of the guard. One attaches around the shoulder strap of body armour, the other fastens around the upper arm.
- Guards should be worn beneath a compatible flame retardant coverall. The outer moulding offers limited flame spread in accordance with UL-94 HB.
- Certification: Tested and approved to UK Home Office Centre for Applied Science and Technology Standard 20/07 rated
- Sizes XS-XL

BLACK

PR — DMS SHP/ARM (SZ)



FOREARM AND ELBOW GUARDS

- Lightweight, ergonomically designed lower arm protection. Fits the curvature of the arm minimising pressure points at the wrist and elbow. Articulated elbow section ensures freedom of movement.
- Area of protection: The forearm from the wrist to above the elbow
- Outer shell: Super high impact ABS moulded shell. Ridged design gives excellent protection against impact while keeping weight to a minimum.
- Inner foam: Low-density impact absorbing polyehtylene moulded foam reduces weight and allows circulation of air around the product
- Fastenings: 3 cotton covered Velcro adjustable Nylon straps riveted to the body of the guard. Ensuring security and comfort.
- Guards should be worn beneath a compatible flame retardant coverall. The outer moulding offers limited flame spread in accordance with UL-94 HB.
- Certification: Tested and approved to UK Home Office Centre for Applied Science and Technology Standard 20/07 rated
- Sizes XS-XL

BLACK

PR — DMS FRM/040 (SZ)

FEMALE GROIN GUARD

- Lightweight, ergonomically designed female groin protection
- Area of protection: Groin and lower abdomen
- Outer shell: High impact lightweight polypropylene moulding contained within a washable polyester cover
- Inner foam: Low-density impact absorbing foam
- Fastenings: Fully adjustable 2" waist strap. 2 x 1" leg straps pass from the bottom of the guard, between the legs to fasten around the waist strap at the back
- Guards should be worn beneath a compatible flame retardant coverall
- Certification: Tested and approved to UK Home Office Centre for Applied Science and Technology Standard 20/07
- Sizes SM-MD

BLACK

EA — DMS FGG/100 (SZ)



MALE GROIN GUARD

- Lightweight, ergonomically designed male groin protection
- Area of protection: Groin and lower abdomen
- Outer shell: High impact lightweight polypropylene moulding contained within a washable polyester cover
- Inner foam: Low-density impact absorbing foam
- Fastenings: Fully adjustable 2" waist strap. 2 x 1" leg straps pass from the bottom of the guard, between the legs to fasten around the waist strap at the back
- Guards should be worn beneath a compatible flame retardant coverall
- Certification: Tested and approved to UK Home Office Centre for Applied Science and Technology Standard 20/07
- Sizes MD-LG

BLACK

EA — DMS MGG/100 (SZ)



THIGH GUARDS

- Lightweight, ergonomically designed thigh protection
- Area of protection: The front and side of the thighs from close to the hip to just above the knee
- Outer shell: Super high impact ABS moulded shell. Ridged design gives excellent protection against impact while keeping weight to a minimum.
- Inner foam: Low-density impact absorbing polyethylene moulded foam reduces weight and allows circulation of air around the product
- Fastenings: 2 cotton covered Velcro adjustable Nylon straps riveted to the body of the guard. One passes around the thigh, the other attaches to the waist belt. Ensuring security and comfort.
- Guards should be worn beneath a compatible flame retardant coverall. The outer moulding offers limited flame spread in accordance with UL-94 HB.
- Certification: Tested and approved to UK Home Office Centre for Applied Science and Technology Standard 20/07 rated
- Sizes XS-XL

BLACK

PR — DMS THG/050 (SZ)



SHIN AND KNEE PROTECTORS

- Lightweight, ergonomically designed lower leg protection. Fits the curvature of the leg minimising pressure points at the knee and ankle. Articulated knee section ensures freedom of movement.
- Area of protection: The knee and shin to the top of the instep
- Outer shell: Super high impact ABS moulded shell. Ridged design gives excellent protection against impact while keeping weight to a minimum.
- Inner foam: Low-density impact absorbing polyethylene moulded foam reduces weight and allows circulation of air around the product
- Fastenings: 3 cotton covered Velcro adjustable Nylon straps riveted to the body of the guard. Ensuring security and comfort.
- Guards should be worn beneath a compatible flame retardant coverall. The outer moulding offers limited flame spread in accordance with UL-94 HB.
- Certification: Tested and approved to UK Home Office Centre for Applied Science and Technology Standard 20/07 rated
- Sizes XS-XL

BLACK

PR — DMS SHN/100 (SZ)



METATARSAL PROTECTOR

- Lightweight, ergonomically designed instep/metatarsal protection
- Area of protection: The top of the foot from the bottom of the shin/knee guard to the toecap of the boot
- Outer shell: Super high impact ABS moulded shell. Ridged design gives excellent protection against impact while keeping weight to a minimum.
- Inner foam: Low-density impact absorbing polyethylene moulded foam reduces weight and allows circulation of air around the product
- Fastenings: A single Velcro fastening leather strap loops around the boot laces to hold firmly in position
- The outer moulding offers limited flame spread in accordance with UL-94 HB.
- Certification: Tested and approved to UK Home Office Centre for Applied Science and Technology Standard 20/07 rated
- Sizes XS-XL

BLACK

PR — DMS FTPM (SZ)

FORTRESS UNIVERSAL TACTICAL VEST

- Provides full protection to the front, back and sides
- Capable of accepting Level II and IIIA ballistic inserts
- Comes with a gusset sewn top-loading plate pocket that accepts 10 x 12 plates and a heavy-duty operator rescue drag handle
- 360° MOLLE webbing, and front gusset sewn map/tool pocket for quick mission access is fully adjustable in girth and length to fit multiple sizes
- Vest adjustments allows standardization of team equipment and has velcro on the front and rear to accept ID patches
- Accessories include neck, throat, bicep and groin armor
- Sizes SM-XL



NAVY

EA — USI FUTV-SZNV

ID PANELS

- Custom identification panels available for helmets and vests
- Customer can select background color and lettering color
- Vest ID panels will have a Velcro backer to apply to vest. Helmet ID panels will come with both sides of the Velcro attached with a glue backing for helmets.





CALL FOR PRICING/ADDITIONAL INFORMATION



FORTRESS UNIVERSAL PLATE CARRIER

- Provides full protection to the front, back and sides
- Capable of accepting Level II and IIIA ballistic inserts
- Comes with a gusset sewn bottom loading plate pocket that accepts 10 x 12 plates and a heavy-duty operator rescue drag handle
- 360° MOLLE webbing, and front gusset sewn map/tool pocket for quick mission access is fully adjustable in girth and length to fit multiple sizes
- Sizes SM-XL

NAVY

EA — USI FUPC-SZNV



017 SERIES PUBLIC ORDER HELMET

- Thermoplastic shell
- Energy absorbing expanded polystyrene line improves impact protection
- High comfort, flame retardant interior with removable cheek pads for easy cleaning, improved hygiene and longer service life
- Headbands, crown pads and sizing pads for easy fit to individual head shapes and sizes
- High-impact polycarbonate visor with option of anti-mist and anti-scratch coating for improved resistance to fogging and surface abrasion
- Replaceable heavy duty neck curtain - padded for extra comfort and optimum protection
- Four metal gauze audio inserts - resistant to liquid penetration
- Adjustable chinstrap with quick release buckle
- Comply fully with PAS 017: 1995 - the first technical performance standard to be dedicated to public order helmets offering a new higher standard of protection for police and prison officers exposed to front line hazards
- Sizes 00-5

	BLACK, NAVY BLUE
EA	ARG 017T/3 (SIZE/COLOR)



APH05 PUBLIC ORDER HELMET

- Choice of thermoplastic or GRP helmet shells incorporating optically correct, high impact resistant polycarbonate visor with optional anti-mist, anti-scratch coating
- Liquid resistant, metal gauze audio apertures enable local commands to be heard
- Compatible with range of CBRN respirators
- Replaceable neck protector and quick release chin strap with chin cup - accepts high dynamic load with minimum extension and helps to maintain helmet stability
- Range of sizes available to provide optimum fit, with combined impact and padded linings to maximize protection and comfort. Internal fitting accepts radio connection.
- Complies with testing requirements of Home Office Scientific Development Branch Standard 2004, incorporating new tests for impact attenuation of whole helmet and solvent resistance of visor
- Thermoplastic (Sizes 00-5)
- GRP (Sizes 00-6)

	THERMOPLASTIC (BLACK, NAVY BLUE)
EA	ARG APH05T/1 (SIZE/COLOR)

	GRP (BLACK, NAVY BLUE, RED, YELLOW, WHITE)
EA	ARG APH05G/1 (SIZE/COLOR)

RIOT CONTROL HEADSET SYSTEM

- Low profile, single sided headset
- Can be mounted inside riot helmet
- Has the ability to adjust the headset's positon close to his/her ear and provide a noise canceling microphone that would cancel crowd noise, focusing only on the clear transmission of the officer's voice
- Push-To-Talk provides the officer with ease of access to activate when needed yet provide a protective shroud to prevent accidental depression

	BLACK
EA	ATL RCH.ERC.47 (HEADSET SYSTEM)
EA	ATL RCH.P01.47 (PUSH TO TALK ASSEMBLY)
EA	RADIO INTERFACE CABLE



AA50 PUBLIC ORDER GLOVE



- Lightweight
- Black leather
- Elasticated mid-length cuff. Gathered wrist with foam padded lining to prevent ingress of liquids. Compatible with commonly used forearm guards and coveralls.
- Outer material: 0.9-1 mm goatskin leather
- Inner lining: 365 gsm Polyester (Heat resistant to EN659:1996 Annex A)
- Intermediate lining: 0.5 mm Low Density Polyethylene Foam
- Thread: Aramid - flame retardant
- Impact protection: 7-8 mm foam rubber to back of hand & 4 mm foam to back of fingers/thumb
- Abrasion protection: Leather reinforcement to high wear areas of palm/fingers
- Blade cut protection: Aramid loaded reinforcement to palm, fingers and back of hand
- Certification: BS7971-6:2003 Type 2 Level 3
- Sizes 6-13

BLACK

PR — DMS AA50 (SZ)

RIOT ControlBY

- Waterproof aniline fireproof cowhide leather according to DIN/EN 407, level 4
- Anti-cut insert lining according to DIN/EN 388, level 5
- Hard shell knuckle and handback protectors
- Shock absorbing protectors (foam and jelly) on fingers, thumb and wrist
- Fireproof stitching thread and fireproof male and female velcro
- Roller buckle closure with leather strap at wrist for secure fit
- Sizes 5-13

BLACK

PR — MLE 13514SW (SZ)



PUBLIC ORDER - FOOT PROTECTION



HAIX® AIRPOWER XR2

- 8" boot
- Climate system
- Reinforced leather pull tab
- Water resistant sun reflect leather
- Rubber/PU outsole
- Anatomically formed TEXON fleece footbed
- Quality insole
- Composite toe cap
- Metal free puncture protection
- Sizes 5-15 (including 1/2 sizes) (Medium, Wide, Extra Wide)

BLACK

PR — HAI 605118 (SZ)

ORIGINAL S.W.A.T. PUBLIC ORDER BOOT

- 9' boot
- Certified to British Standards BS 7971 2016 Part 5 Footwear for protective clothing and equipment for use in violent situations
- Meets EN ISO 20345:2011 for safety boots
- Composite protective toe cap
- 2.2-2.4mm fire resistant full grain leather
- Waterproof membrane for water, liquid and blood borne pathogen resistance
- LENZI® non-metallic anti-penetration board
- 6mm Poron® XRDMA internal metatarsal protector
- 3M™ Defender fluorochemical finish to assist with fluid run off
- Nomex® flame and heat resistant laces
- Additional PORON® XRDMA in lateral ankle area
- Fire and slip resistant rubber outsole tested [redacted]°C
- Salamander Skin™ toe cap resists abrasion, fire, and liquid fuel
- Sizes: D: 4-15 and EEE: 7-16

BLACK

PR — OSB 114031 BLK (SZ)





AVON C50™ MASK ASSEMBLY

- Based on the U.S. M50/JSGPM and sharing key technologies
- Provides maximum operational flexibility to counter multiple threat scenarios, including CBRN agents, TICs and TIMs
- Offers high protection, outstanding field of vision and superior comfort
- The innovative design features optimize the user's time in the operational area
- Sizes SM-LG

	BLACK
EA	AVO 70501-18X



AVON FM53™ MASK ASSEMBLY

- A multi-role Respiratory Protective Equipment (RPE) System that has been developed specifically for specialist applications where the user needs to respond to ever changing operational conditions
- Provides protection against traditional chemical and biological warfare agents and select TIMs
- Offers both positive pressure SCBA, PAPR and negative pressure APR/capability
- All of the capabilities are available from one mask platform without the need to change components
- Right, left or twin port filter configurations available
- Sizes XS-LG

	BLACK
EA	AVO 72601-250-X



AVON OUTSERT ASSEMBLY

CLEAR OUTSERT

- Flexible polycarbonate outsert that simply attaches to 50 series masks to provide additional impact and scratch resistance in extreme environments.

EA	AVO 70501-156

SUNLIGHT OUTSERT

- Additional protection against high level UV light and flash flares. Constructed from flexible polycarbonate providing additional impact and scratch resistance.

EA	AVO 70501-157



MASK BAG

	BLACK
EA	SFW 44014



CBRNCF50 FILTER

- When combined with an appropriate chemical protective mask, the CBRNCF50 filter canister protects the face, eyes and gastrointestinal tract of the wearer against known chemical and biological agents in aerosol, liquid and vapor form

	BLACK
EA	AVO 72602-2



CTCF50 RIOT AGENT FILTER

- Low profile combination filter containing a pleated high-efficiency filter element
- Specifically designed for removal of riot control agents and tear gases including CS, CN and OC pepper spray
- Pack of 4

	BLACK
PK	AVO 72606-3



INTERLOCKING SHIELDS

- Lightweight personal protective shield
- Can be used individually or locked together to form a continuous barrier
- 4 mm thick clear Makralon Polycarbonate. Offers excellent resistance to impacts, thrown objects and liquids while giving the user an excellent field of vision ahead.
- Handles: Forearm hook and double D handle (optional locking folding handles). Aluminum handles with rubber hand grips. Bolted through the blade and backing plate for maximum strength and security

4'	CLEAR
EA	DMS SLD1200INT
6'	CLEAR
EA	DMS SLD1800INT

POLICE OR SHERIFF ID PANEL AVAILABLE

****ID PANEL IS AN OPTION, NOT STANDARD**

PUBLIC ORDER BATON

- One-piece, solid nylon with moulded rubber grip, retaining strap and locating ring
- 31 mm diameter black Nylon 6
- Grip: Moulded rubber textured grip gives excellent security and control
- Lanyard: 5 mm diameter plaited cord
- 24"

	BLACK
EA	DMS BAT610





SOLO SHIELD

- Lightweight (2.0 kg) personal protective shield
- Forearm loop allows the shield to be retained while leaving both hands free to use other equipment
- 4 mm thick clear Makralon Polycarbonate. Offers excellent resistance to impacts, thrown objects and liquids while giving the user an excellent field of vision ahead.
- Handles: Swivelling steel forearm loop and aluminum grab handle. Bolted through the blade and backing plate for maximum strength and security.
- Shield handles are mounted on a foam/aluminum backing plate which significantly reduces transmission of vibration to the forearm and through the handles
- 650 mm diameter x 4 mm thick

	CLEAR
EA	DMS RSHD

POLICE OR SHERIFF ID PANEL AVAILABLE

****ID PANEL IS AN OPTION, NOT STANDARD**

LEATHER BATON HOLDER

	BLACK
EA	BOS7701-1-BLK



PUBLIC ORDER - FIRE SUPPRESSION

AMEREX HALOTRON I "CLEAN AGENT" EXTINGUISHER



- 9 second discharge
- 6-8 foot range
- 10 H x 3.5 W x 2.63 D
- Stored pressure design
- Dependable drawn steel cylinders
- Durable high gloss polyester powder pain
- All metal valve construction
- Temperature range (-40°F to 120°F)
- EPA approved "Clean Agent" for Class A, E and C hazards
- Low GWP
- Low ODP
- Leaves no residue
- User friendly
- 1.4 LBS

	RED
EA	AMX A384T

LEATHER CARRIER

	BLACK
EA	BOS 7702-1-BLK

COLD FIRE™ TACTICAL CANS

- An environmentally friendly fire extinguishing agent that puts out any fire faster, safer, with less water, less damage to property and less risk to personnel
- Completely 'green' and non-toxic
- Instantly cools everything it touches
- Cools 21x faster than water and works to remove heat, therefore preventing re-igniton
- Encapsulates and breaks down hydrocarbons
- Availablity: 12 oz. and 20 oz. Pistol Grip or Loop Handle Spray Cans, 2L and 6L CFT extinguishers, backpack and fleet kit



12OZ. LOOP HANDLE TACTICAL CAN	
EA	CFT CF302-12TL

20OZ. LOOP HANDLE TACTICAL CAN	
EA	CFT CF302-20TL

2 LITER KIT	
EA	CFT CF302-2LTRKIT

PUBLIC ORDER - LESS THAN LETHAL



COMBINED TACTICAL SYSTEMS AEROSOLS

- Advanced solutions with an array of formulations, sizes and delivery including stream, fog, gel, vapor and Omni-Stream™
- Pepper spray
- Crown management, high volume units
- Omni-Stream™ features a bag on valve (BOV) delivery system allowing the operator to hold the can at any orientation and get consistent stream performance



COMBINED TACTICAL SYSTEMS FLASH BANGS AND STING BALL GRENADES

- Flash Bangs are an ATF controlled Class-C explosive device
- Sting-Ball Grenades are explosive "rubber-ball" style grenades that upon initiation eject rubber balls into a radius surrounding the device



COMBINED TACTICAL SYSTEMS 40MM LAUNCHER

- Multi-Launcher 6.2" Cyl Collapsible Stock
- Lightweight and versatile
- Manufactured using 4140 hardened steel, 6061-T6 mil-spec anodized aluminum and DuPont super tough glass filled nylon



SAGE HAND THROWN MUNITIONS

- 40MM Munitions
- 37MM Rifled Munitions
- 37MM Smooth Bore Munitions

SAGE CHASSIS STOCK SYSTEMS

Each SAGE Enhanced Battle Rifle Chassis System is precison CNC machined from a solid billet of high strength aircraft grade aluminum and is finished with mil-spec hard anodizing. The system increases accuracy and reliablity, reduces perceived recoil, provides ambidextrous sling mounts and multiple Picatinny rails for mounting optics and accessories.





V-LITE™

- 0.8 oz.
- A versatile personal lighting/identification marker
- A simple and intuitive alternative to chemical light sticks
- One button to cycle through the preset functions
- Fully encapsulated to ruggedize the electronics, the flexible silicone body not only protects the good stuff inside but also conforms to curved surfaces
- Mounting is made simple with the V-Lite™ sleeve, providing the operator with a velcro-backed attachment system
- An unnoticeable addition to your helmet during routine operations and low-profile enough to reduce snag hazards during airborne operations
- Modes available: On/Off, Blink/Off, On/Blink/Off, Low/High/Off
- One Size

RED, WHITE, BLUE, ORANGE, GREEN, INFRARED

EA — S&S VL-COLOR01XV



LEATHER WATER BOTTLE CARRIER

BLACK

EA — BOS 7703-1-BLK



VTAC® BROKOS HARNESS

- An ideal tactical load bearing solution
- Complements the 5.11® Brokos belt
- Fully adjustable padded shoulder straps
- MOLLE/5.11 SlickStick® shoulder webbing
- Adaptable rear yoke
- 500D Nylon and aerospace mesh
- Low profile adjustment buckle
- Patch tabs at front and rear
- Removable loop ID panel on back
- One size

BLACK

EA — 511 56105 019



EQUIPMENT BAG

- 80 liter storage
- 6 external zipper pockets
- Protective helmet storage pocket
- Heavy duty bottom
- Cordura nylon with reinforced seams and shoulder straps (backpack or shoulder)

BLACK

EA — DMS 80 LTR



VTAC® BROKOS BELT

- Highly versatile load bearing belt
- Wrap-around MOLLE/5.11 SlickStick® web platform
- Polymer inserts for an ergonomic shape
- Durable, weather resistant 500D Nylon
- Aerospace mesh interior
- Lengths: SM-MD (26.5"), L-XL (33"), 2X-3X (42")

BLACK

EA — 511 58642 019 (SZ)

511 58642 019 2XL/3XL

HOOK & LOOP INNER DUTY BELT

- SM (26-30")
- MD (32-36")
- LG (38-42")
- XL (44-48")



BLACK

EA — BLK 44B7SZBK

CALL 800.331.6707
FOR A QUOTE TODAY!



H&H MEDICAL SWAT-T TOURNIQUET (ORANGE)

Allows a more rapid means to control extremity bleeding and allows application higher into the groin and axilla than other tourniquets.

- Ease of application
- Made with a bright safety orange color for easy identification and application
- Instructions for use are printed on the tourniquet along with the trademark pressure application measure showing just how much pressure to apply to reach occlusion



H&H MEDICAL H*VENT LAMINAR VENTED CHEST DRESSING

Designed to work to relieve pressure from an open chest wound due to air in the chest or bodily fluid.

- A unique multi-directional vented dressing (allows the fluids to "drain towards gravity")
- Helps prevent occlusion
- The unique dome membrane design creates a complete seal around the wound area
- Large vent openings on the H*VENT allows for visual monitoring of the wound
- Proven in internal testing to retain a seal during inhalation and to maintain a sustainable negative pressure (below ambient pressure) within the pleural space
- Lowest profile of any vented chest seal and easy to fold



H&H MEDICAL BLEEDING CONTROL BASIC KIT

Provides first responders with a compact and durable individual hemorrhage control kit to treat bleeding from penetrating and other traumatic injuries.

Kit includes:

- SWAT-T tourniquet
- H&H Mini Compression Bandage
- H&H PriMed Compressed Gauze roll
- Nitrile gloves



NORTH AMERICAN RESCUE COMBAT APPLICATION TOURNIQUET (C-A-T)

The C-A-T® utilizes a durable windlass system with a patented free-moving internal band providing true circumferential pressure to the extremity.

- New single routing buckle for faster application, decreased blood loss, effective slack removal, fewer windlass turns, and simplified training with single protocol application standards
- Includes reinforced windlass, stabilization plate, windlass clip and writeable windlass security strap
- Featuring NAR's signature Red Tip Technology® elliptical tab providing added visual clues during application

NORTH AMERICAN RESCUE

NORTH AMERICAN RESCUE RIGID GEN 7 TOURNIQUET CASES W/ SHIRT SHIELD

Designed to provide personnel with the capability of carrying the life-saving C-A-T® Tourniquet on their person by easily mounting it to their duty/patrol/pistol belt, where it is needed most.

- Includes a Shirt Shield complete with mounting hardware to protect your uniform shirt from undue wear caused by the friction from the windlass clip
- Blade-Tech TekLok Belt Attachment fits up to a 2.25" belt
- Injection molded nylon case to stand up to rugged LE/MIL usage





H&H MEDICAL TECC KIT

Designed to hold enough emergency products to respond to a mass casualty situation.

- Contains everything you need to treat the 3 most preventable causes of traumatic death: blood loss, airway occlusion and sucking chest wound
- Meets the basic requirements for Tactical Emergency Casualty Care



NORTH AMERICAN RESCUE M-FAK MINI FIRST AID KIT

Designed to be the most compact, multi-use IFAK for delivering immediate critical care for penetrating, blast or other traumatic injuries.

Kit includes:

- 1 x C-A-T® (Combat Application Tourniquet®) black
- 1 x 4" Flat ETD™
- 1 x S-rolled gauze (4.5" x 4.1 yd)
- 1 x HyFin® Vent Compact Chest Seal, twin pack
- 1 x pair Bear Claw® nitrile trauma gloves, LG
- Super compact, rugged nylon platform that allows attachment both vertically (MOLLE backing) and horizontally (3" belt loop)
- Clam shell configuration utilizes (2) main sleeves that open on both ends for easy access



NORTH AMERICAN RESCUE PATROL VEHICLE TRAUMA KIT

Desinged to provide personnel with an easily accessible, quick to deploy medical kit from your patrol vehicle.

- One side covers all your agency needs to administer basic first aid and community assistance
- Second side offers a first time combination of basic first aid and basic trauma medical items
- Exterior includes MOLLE-style system to accommodate extra equipment as needed





QUIKCLOT® BELT TRAUMA KIT®

A compact, lightweight, wearable holder that fits up to a 2" belt and can be rotated 90° to make room for other gear. Contents can treat up to one injury.

Includes:

- QuikClot Combat gauze® LE
- SWAT-T™ pressure dressing
- Nitrile gloves



QUIKCLOT® BLEEDING CONTROL BAG®

This bag is integral for responding to a range of bleeding situations. Its innovative design allows it to function in a stand-alone capacity or as part of an overall bleeding control program. Contents can treat up to 12 injuries.

Includes:

- QuikClot Combat gauze® LE
- QuikClot® EMS 4x4 dressings
- QuikClot® EMS rolled gauze
- Tourniquets, C-A-T™ , SOF™ TT-W
- Dressing, TacMed Control™ Wrap
- Nitrile gloves
- Shears, EMS-style



ADS XR150 X-RAY SOURCE

Provides the ultimate option in portability for high powered X-ray machines.

- Weighs less than 5 lbs.
- Penetrates up to 1/2" of steel
- Small size makes the unit easy to position in hard to reach places or to maneuver on a robot arm
- Performance - high penetrating capability, durable, lightweight packing, long battery life
- Simplicity - only one variable to control exposure
- Safety - extremely short exposure time and low leakage
- Spectrum - wide spectrum penetrates both high and low density material in same radiograph



ADS MITHIX PRO EOD HOOK AND LINE TEAM KITS

Designed for EOD, bomb squad, and special operations prodedures.

- High quality components
- Stainless steel hooks
- High-strength marine-grade pulleys
- Low-stretch high grade Kevlar rope and other essential tools made specifically for IED, remote movement and remote handling operations



ADS NEX-RAY®

Offers advanced, portable, lightweight x-ray image capture units designed to obtain accurate, near real-time radiographic imaging.

- Patented technology allows NeX-Ray® to dispense with the use of fragile and heavy glass plates integral to most flat panel imagers
- 2 models available (FPX and MMX)
- Can be operated with Windows XP, 7, or 8 laptops or with Android 4.2 (or later) mobile devices
- NeX-Ray® imagers can be operated in standalone, tethered remote, and wireless modes

ADS TITAN

(1) 12" main barrel
(2) Smooth bore extensions
(1) Rifled extenson
(1) Breech cap
(1) Breech plug
(1) Thread protector



NOW WITH TWO NEW CONFIGURABLE OPTIONS

MISTRAL INC.
Member of Mistral Group



MISTRAL SECURITY EXPEN

Ampoule-based technology. Designed for military, EOD, and security personnel primarily for easy carrying and for situations that do not require multiple tests.

- Capabilities: Nitro Aromatic, Nitramines, Ammonium Nitrate, Peroxide, Acetic Anhydride, and much more



MISTRAL SECURITY EXPRAY®

A unique explosive aerosol test technology, Expray®, detects both trace and substance levels of explosives as well as homemade explosive (HME) precursors.

- Capabilities: Nitro Aromatic, Nitro Esters, Nitramines, Inorganic Nitrates and much more



MISTRAL SECURITY TOTAL CONTAINMENT VESSELS (ARC)

Provides full protection against blast and fragmentation with repeated detonation capability.

- Safely contain and transport explosive devices

TACTICAL ELECTRONICS
ELITE TACTICAL CAMERAS & EOD SOLUTIONS





TACTICAL ELECTRONICS 1ST LINE EOD TOOL KIT

Designed to provide EOD operators and bomb technicians with a versatile, lightweight kit that builds upon the capabilities of the Immediate Action Pouch without necessary or wasteful redundancy. Ideal for missions where the user has limited cargo or carry space and where the operator must take weight or dimensions into consideration.

- Small lightweight design
- Can be carried in a cargo pocket or stored in a small compartment
- Ideal for dismounted operations

TACTICAL ELECTRONICS WIRE ATTACK SPECIAL PIERCER PROBES (WASPP) KIT

Specifically designed to allow EOD operators to make non-invasive electrical measurements of wires.

- Includes 10 specialized "bed of nails" piercers with volt meter leads, 10 extensions and 1 roll up carry pouch



TACTICAL ELECTRONICS 2ND LINE EOD TOOL KIT

Customized to equip EOD and bomb technicians with the tools necessary to execute render safe procedures. Allows operators to customize the configuration based on each scenario.

- Comes complete with 6 individually populated tool kits: 1st Line, Immediate Action Pouch, RIP Kit, Detonator Diagnostic Kit, Manual Access Kit and Bit Kit
- All kits fit into one pack with extra room for additional supplies

QINETIQ TALON®

TALON robots are powerful, durable, lightweight tracked vehicles that are widely used for EOD, reconnaissance, communications, sensing, security, defense and rescue. They have all-weather, day/night and amphibious capabilities and can navigate virtually any terrain.

- IOP compliant
- Man-portable, instantly ready for operation
- Fast
- Configurable
- Intuitive
- Outstanding situational awareness: standard 4 color cameras, including night vision, thermal and zoom options
- Withstands repeated decontamination

QINETIQ DRAGON RUNNER® 10

The micro unmanned ground vehicle is lightweight, compact, multi-mission remote platform developed for supporting small unit dismounted operations. When fitted with the Light Weight Modular Arm, it has the ability to investigate and recover or neutralize a potential IED. Day and night sensors allow it to serve as the forward eyes of the team while also delivering remote sensors, emplacing counter-IED charges and more.

- Speed: 4 mph
- Max arm lift: 4.4 lbs.
- Front and rear cameras
- On-board microphone
- Controller: compatible with lightweight radio unit and Gen 2.5 hand controller
- Tough enough to be thrown and survive rough handling and adverse weather

DRAGON RUNNER® 20 ALSO AVAILABLE!"





QINETIQ North America

ICOR MINI-CALIBER®

The lightweight, modular Mini-CALIBER® is a man transport robot for SWAT and EOD operators. Developed for rapid tactical missions, the robot is simple to operate and quick to deploy, providing fast action for searching rooms, hallways, stairwells and confined spaces.

- Includes a manipulator arm on a rotating turret with a 10X zoom camera on the claw and a max arm lift of 15 lbs.
- CBRNE detectors and sensors can be mounted onto the deck of the robot chassis
- Handheld command control unit is portable and intuitive to use
- Clear images are transmitted to the 5.8" LCD daylight readable screen over a wireless RF system

ICOR TECHNOLOGY



ALSO AVAILABLE:



Caliber® T5



Caliber® MK4



MK3 Caliber®



TacticID By. B&W TEK



B&W TEK TACTICID® - GP

A field-ready handheld spectral analysis instrument designed for non-contact forensic analysis. Utilizes proven Raman spectroscopy, allowing users to get real-time actionable identification of unknown chemicals, narcotics, pharmaceutical drugs, explosives and many other substances while reducing operational uncertainty and response time.

- Customized libraries
- Critical component mixture ID
- Indirect contact analysis
- Wi-Fi connectivity
- Touch screen quick notes
- Color-coded result screens
- TacticOne Response™ (24/7/365 emergency support and spectral analysis)

B&W TEK TACTICID® - N

Handheld Raman analyzer for narcotic and pharmaceutical drug identification.

- Comes standard with a comprehensive library of over 1,000 substances
- Critical component mixture ID
- Indirect contact analysis
- Wi-Fi connectivity
- Touch screen quick notes
- Color-coded results screen
- TacticOne Response™ (24/7/365 emergency support and spectral analysis)



MISTRAL SECURITY PDT

A series of individual, presumptive reagent drug tests that help law enforcement officers, drug enforcement agencies and military CID units quickly and easily identify controlled substances while in the field.

- Options: Heroin, LSD, marijuana, cocaine, bath salts and much more



MISTRAL SECURITY PENTEST

An ampoule-based technology that detects trace amounts of drugs as well as bulk amounts.

- Multi-use
- Will not destroy evidence
- Options include: D4D (general screening), Coca, Cannabis, Herosol, LSD, Meth/X, Opiates, and more



MISTRAL INC.
Member of Mistral Group

MISTRAL SECURITY FENTANYL PDT

The only fentanyl test that can distinguish fentanyl from other drugs like meth or amphetamines.

NIGHT VISION



ARMASIGHT PVS7 GEN 3P NIGHT VISION GOGGLES

The most widely recognized and dependable U.S. Military night vision goggle system available.

- Compact, rugged design
- Waterproof
- Ergonomic, simple, easy to operate controls
- Built-in infrared illuminator and flood lens
- Equipped with Automatic Brightness Control (ABC)
- Head or helmet mountable for hands-free usage

AIMPOINT® MICRO T-2

Electronic red dot sighting technology.

- Advanced optical lenses
- Cutting edge lens coatings
- Lightweight sight for extreme conditions
- Excellent night vision compatability



NIGHTOPS TACTICAL PVS-14

A widely recognized monocular night vision device, battle tested by the U.S. Military.

- L-3 Gen 3 Unfilmed technology
- 40 hour runtime
- 1X magnification

THERMAL IMAGING



FLIR BREACH® PTQ136

Thermal imaging monocular. Spots th total darkness.

- Weighing only 7.4 oz. (can be concealed in a pocket or mounted to a helmet with its mini-rail feature)
- On-board recording
- Exceptional vision
- 7 palettes for fast detection of suspects or evidence, day or night
- Digital compass and inclinometer



FLIR THERMOSIGHT® PRO SERII

Thermal imaging weapon sight.

- Exceptional vision
- Built using the new FLIR Boson 1
- Bright, high definition FLCOS display for absolute clarity
- Completely digital for better detection, classification and recovery, day or night
- Powerful and compact hardware is protected by a robust body
- On-board video recording, image capture and storage
- Multiple color palettes
- Digital compass and inclinometer

PELICAN™



PELICAN 7600 TACTICAL FLASHLIGHT WITH WAND KIT

- Performance surpassing 900 lumens
- 3 LED colors (white, red, and green)
- Provides high, strobe, medium and low modes
- Full time battery level indication
- USB rechargeable lithium ion battery
- Type III hard anodized finish
- Ingress protected IPX8 submersible



PELICAN 7100 TACTICAL FLASHLIGHT

Compact/high performance flashlight.

- 5" long
- 700 lumens of light output
- High, strobe, medium and low modes
- Full time battery level indication
- USB Lithium Ion rechargeable
- Ingress protected IPX8 submersible

PELICAN 9490 REMOTE AREA LIGHT

- Up to 6,000 lumens (calculated)
- Up to 24 hours of run time
- Intelligent control (allows for various light output levels)
- Maintenace free LED array with 50,000 hour life expectancy
- Full time battery level indication with low level flashing indicator
- 6' deployable mast with 340° rotation
- Multiple deployment positions
- Quick release/ Hot swappable battery design with 12 volt power supply
- Convenient shoulder strap



STREAMLIGHT

STREAMLIGHT PROTAC HL® USB FLASHLIGHT

USB rechargeable, 850 lumen tactical flashlight.



- Choice of three user selectable programs
- Multi-fuel capability
- Durable, anodized aluminum construction
- Water resistant sliding metal sleeve protects USB port
- Multi-function, push-button tail switch for one-handed operation
- LED technology impervious to shock with a 50,000 hour lifetime
- Anti-roll head
- IPX4 water resistant
- 1m impact resistance tested

STREAMLIGHT TLR-1® GUN LIGHT

Rail-mounted tactical weapon light.



- 300 lumens
- 2.5 hours regulated run time
- 12,000 candela peak beam intensity
- Rail grip clamp system securely attaches/detaches quickly and safely with no tools
- Powered by two 3-volt CR123 lithium batteries
- Mounts directly to handguns with Glock-style rails and to all MIL-STD-1913 (Picatinny) rails
- Machined aluminum sealed construction with black anodized finish
- IPX7 rated design, waterproof to 1m for 30 minutes

STREAMLIGHT TLR-7® GUN LIGHT

Small and mighty 500 lumen tactial weapon light.



- Runs 1.5 hours
- 4,300 candela
- Custom optic produces a concentrated beam with optimum peripheral illumination
- Uses one CR123A lithium battery
- Safe off feature prevents accidental activation
- Rail grip clamp system securely attaches/ detaches quickly and safely with no tools
- Durable, anodized machined aluminum construction
- IPX7 waterproof to 1m for 30 minutes



SUREFIRE X300U-A

1,000 lumens LED handgun light.

- Custom TIR lens creates smooth, far-reaching light with a larger center spot beam
- Integral ambidextrous momentary-and constant-on switching
- Attaches securely to both universal and picatinny accessory rails
- High-strength aerospace aluminum body, mil-spec hard anodized for extreme durability

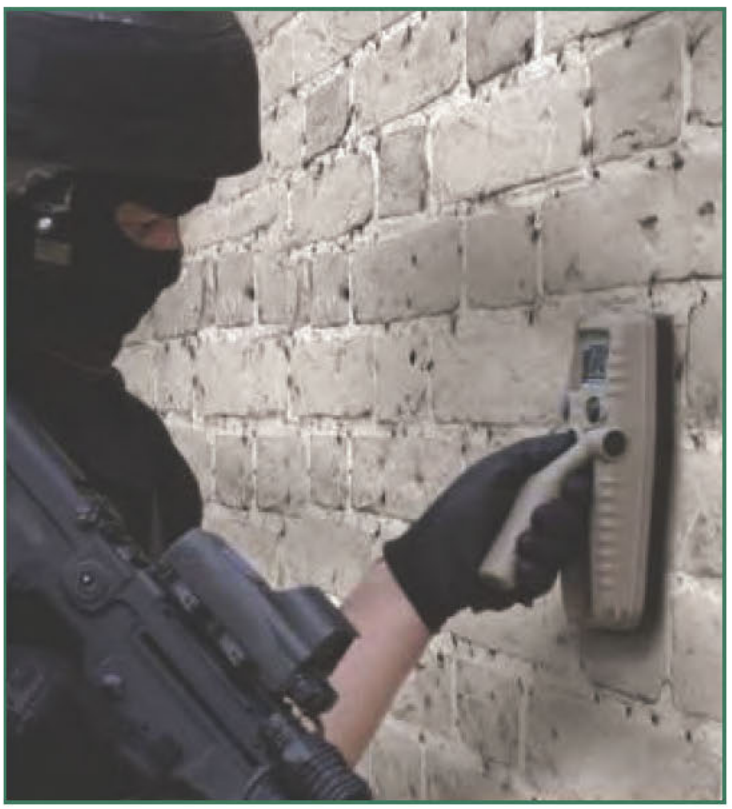


SUREFIRE M600DF-BK

1,500 lumen dual fuel rechargeable LED scout light.

SUREFIRE®

- Virtually indestructible ultra-high-output LED generates 1,200 lumens of blinding light with SF123A batteries and 1,500 lumens with included SF18650A rechargeable lithium ion battery charger kit
- TIR lens shapes versatile beam with enough reach and surround light for close-to longer-range operations
- Mil-Spec hard anodized aluminum body, tempered window and O-ring seals make light rugged, durable, and combat ready
- Activation via Z68 momentary/contant-on push button switching with protective shroud



CAMERO
Step into the known

CAMERO XAVER™ 100

Handheld, tactical through-wall detection system. Provides instant critical situational awareness and target acquisition data.

- Potential uses include: Tactical entry/assault, hostage recovery, search and rescue, breaching and force protection
- Reliable detection of moving and static people behind most common wall materials
- 1d imaging information
- Simple user interface and operation requiring no advanced training

CAMERO XAVER™ 400

Compact, tactical through-wall imaging system. Allows for quick location of people hidden by walls and barriers, enabling tactical teams to step into the known and obtain mission-critical information.

- Compact, light and easy to operate
- Ready to go at the push of a button
- Simple user interface with tracking capabilities for intuitive interpretation
- Simultaneous detection of static and moving objects
- Provides information about room dimensions and major infrastructure elements





CMC RESCUE PERSONAL RAPPEL KIT

Lightweight, durable and low profile. Provides everything needed for rappel access or escape for one tactical officer.

Kit includes:

- Black storage bag
- Stealth rope bag
- 8 Link
- Tactical rappel harness
- Black variable anchor strap
- Large edge guard
- Kong Trapezium Quick-Link
- CMC Lifeline - 75' of black 3/8"
- Prusik cord - 5' of blue 7 mm
- Tubular webbing - 20' of black
- (5) black ProTech™ Screw-Lock carabiners



CMC RESCUE TACTICAL TEAM RAPPEL KIT

Provides rope, harnesses, and hardware for two tactical officers moving in vertical environments, where keeping a low profile is a must.

Kit includes:

- Black storage bag
- #2 black rope bag
- Heavy Rescue Organizer™
- (2) 8 Link
- Black variable anchor strap
- (2) tactical rappel harnesses
- Kong Trapezium Quick-Link
- CMC Lifeline - 150' of black 7/16"
- Tubular webbing - 40' (2 z 12') of black
- Large edge guard
- Prusik cord - 10' (2 x 5') of blue 7 mm
- (7) black ProTech™ Screw-Lock carabiners

TACTICAL ELECTRONICS CORE POLE CAMERA

Extend your vision and tactical inspections.

- High-Definition 1280x720p monochrome video
- Longwave infrared (LWIR) thermal imager
- 4 High-intensity white and LED illumination
- Telescopic pole with locking sections
- Lightweight high density graphite pole
- Omni-directional microphone
- Attaches to POLE Grip, or CORE Grip
- Wireless video transmission - 5 GHz
- AES encryption
- WPA2-PSK authentication
- Graphical LCD for status information
- Hardwire video option
- Backlit push buttons
- MicroSD card video recording (32GB)





TACTICAL ELECTRONICS CORE K-9 CAMERA

Transmits real-time HD video back to the handler.

- High-Definition 1280x720p color video
- Longwave infrared (LWIR) thermal imager
- Adjustable high-intensity IR LED illumination
- Push-to-talk two-way audio
- Wireless video transmission - 2.4 GHz
- AES encryption
- Graphical LCD for status information
- Backlit push buttons
- MicroSD card video recording (32GB)

5.11 BREACHING EQUIPMENT

The Heavy Breaching Kit includes four 5.11 breaching tools desgined to defeat any portal quickly and effectively, along with a steel-reinforced, backpack-style Heavy Kit Bag that keeps your breaching tools organized and ready to roll.

- Size: 37" high
- Includes: MultiBreacher, MultiPry, MiniRam, and EdgeBender, Heavy Kit Bag
- Minimizes breach team exposure time
- Durable steel-framed carry pack
- Padded yoke straps
- 400 lb. quick-release buckles
- Removable hood with hook and loop brand closure



TACTICAL ELECTRONICS CORE UNDER DOOR CAMERA

Gain covert visual inspection into rooms behind closed doors.

- 0.26" insertion panel thickness
- Adjustable high-intensity IR LED illumination
- Attaches to POLE Grip or CORE Grip
- Lightweight high density graphite POLE Grip
- Color eyepiece - AMOLED display (CORE Grip)
- Wireless video transmission - 5 GHz
- AES encryption
- WPA2-PSK authentication
- Graphical LCD for status information
- Hardwire video option
- Backlit push buttons
- MicroSD card video recording (32GB)

TACTICAL ELECTRONICS CORE MONITOR

Presents high-definition video from all CORE cameras over an AES encrypted 5 GHz wireless channel.

- Receives high-definition 1280x720p color video on a 5.0" IPS LCD
- Secure pairing with multiple CORE cameras
- Capacitive touchscreen for setup/ configuration
- 1mm Corning Gorilla Glass screen
- Remote camera control for view selection and illumination/dimming
- WPA2-PSK authentication
- Hardwire video option
- Backlit push buttons





5.11



BSG CBRNE

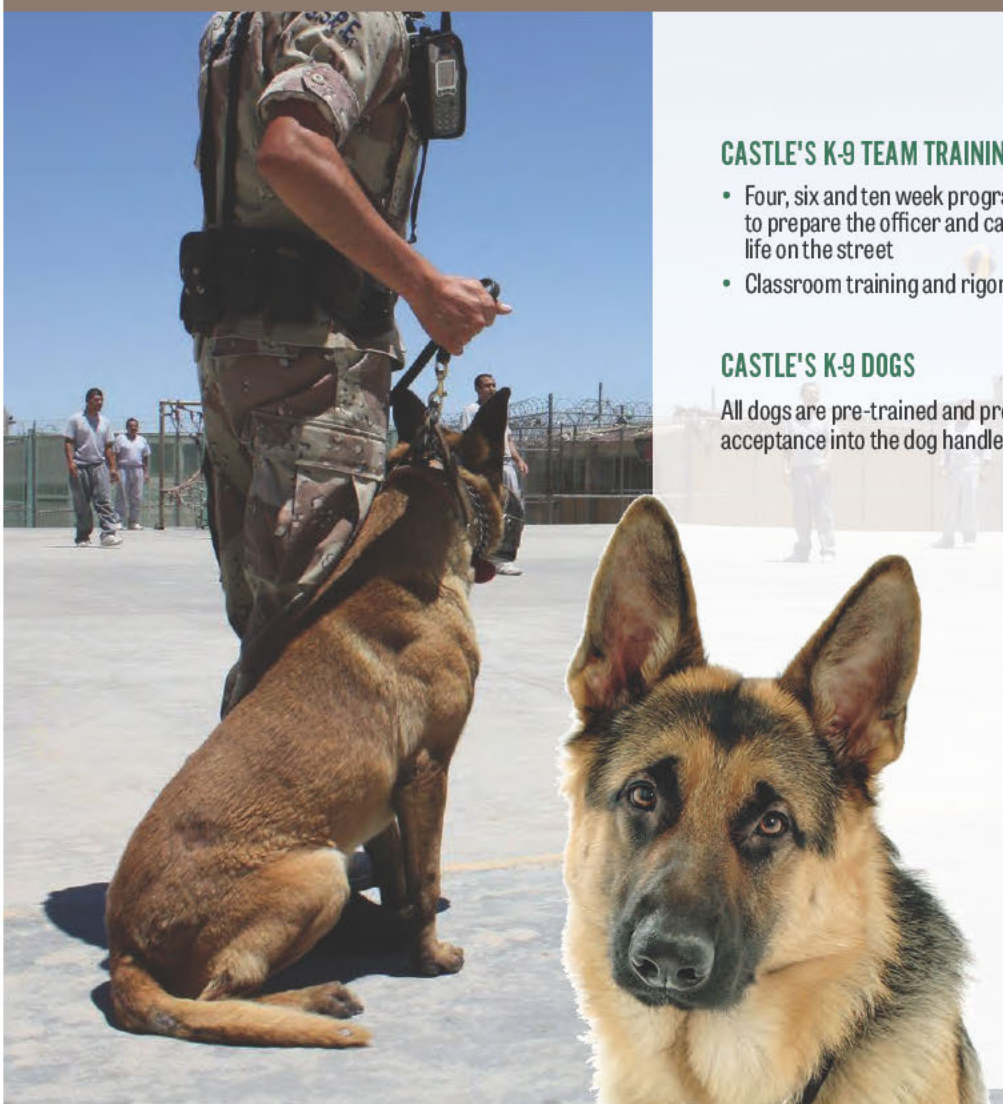
BLACKTHORNE SERVICES GROUP

Provides expertise in CBRNe and related matters. BSG can also branch out to other areas of expertise through their strategic alliances to provide a single point for coordinated consultation on an even larger subject matter.

Training programs include:

- PPE for first responders
- First 100 minutes of RDD, Biological, Chemicals and Explosives response
- Hazardous materials/WMD training
- Illicit and drug lab recognition
- Hazmat rapid intervention teams/fast teams
- Much more!

K9



CASTLE'S K-9 TEAM TRAINING

- Four, six and ten week programs are designed to prepare the officer and canine for everyday life on the street
- Classroom training and rigorous field training

CASTLE'S K-9 DOGS

All dogs are pre-trained and pre-tested before acceptance into the dog handler bonding process

VOHNE LICHE KENNELS

- Selection tested canines
- Narcotic or Explosive trained
- Single or dual purpose

BODY CAMERA

4137

KUSTOM SIGNALS VANTAGE BODY CAMERA

- Flexible data storage solutions (use our cloud or use yours, it is up to you!)
- 30 years of video for law enforcement
- One piece-no cable
- Glove friendly
- Configurable (use only the features you want)
- Rugged design
- IP64 compliant
- 480SD-1080HD capable (and all in between)
- 32GB internal storage
- 120° field of view
- Bookmark button (to mark important events on tape)
- Magnetic mount
- Audio mute

KUSTOM SIGNALS, INC.®



SPEED DETECTION



KUSTOM SIGNALS SMART 650

Speed monitoring awareness radar trailer.

- Kustom Directional RADAR
- 12' high intensity amber LED display
- Flashing overspeed violater alert
- Optional overspeed alerts including 'SLOW', red/blue lightbar, and white LED strobe
- Optional traffic statistics
- 5 year warranty



KUSTOM SIGNALS SMART 850

Speed monitoring awareness radar trailer.

- Kustom Directional RADAR
- 18" high intensity amber LED display
- Flashing overspeed violator alert
- Optional overspeed alerts including "SLOW DOWN", red/blue lightbar, and white LED strobe
- Optional traffic statistics
- Optional solar
- 5 year warranty



KUSTOM SIGNALS VARIABLE MESSAGE SIGN WITH HOMELAND TRAILER

Designed for static and dynamic messages, VMS trailers can be quickly and easily put into place.

- Kustom Directional RADAR
- Amber LED lights provide outstanding visibility
- Hydraulic sign lift
- 4x 2-ton screw leveling jacks
- Removable tongue and 2" ball hitch
- 80W solar panel
- Up to 39 day run time with 6 batteries
- Wi-Fi modem for local wireless programming

3M AUTOMATIC LICENSE PLATE RECOGNITION (ALPR)

3M

ALPR is widely recognized as an effective tool to combat criminal activity, enhance productivity and improve officer safety. Fixed and mobile ALPR systems can help identify certain people and situations:

- Stolen vehicles
- Wanted felons
- Amber alerts
- Sexual predators
- DUI surveillance
- Drug enforcement
- Campus security





GOVERNMENT SECURITY SOLUTIONS

CINTEL ALPR CAMERA

Manufacturer of a full suite of rapidly deployable fixed and mobile ALPR cameras and surveillance products.

CINTEL
Safe. Secure. Simple.





LENCO BEARCAT®

LENCO ARMORED VEHICLES
Protecting Our Nation's Defenders™

Can be used as a SWAT or Military Counter Attack and Rescue vehicle and is often used in hostile Urban Environments.

LDV MOBILE COMMAND CENTERS

LDV

Offers used and new mobile command centers, SWAT trucks and many other specialty vehicle solutions.

GAS DETECTION







MSA ALTAIR® 5X MULTI-GAS DETECTOR

The Altair® 5X is designed with XCell Sensor Technology for faster response and calibration times. XCell Sensors offer superior stability, accuracy and repeatability.

- Easy to use in all applications
- Bluetooth wireless connectivity
- A rugged polycarbonate housing provides unsurpassed durability
- MotionAlert sensor
- InstantAlert feature
- Altair Connect App available on Google Play
- Configurable to meet your needs

MSA
The Safety Company

RAE MULTIRAE WIRELESS, PORTABLE MULTIGAS MONITOR

With the flexibility of up to six gas sensors and the convenience of wireless portability, this multi-gas monitor is versatile and customizable, while delivering real-time access to instrument readings and alarm status from any location. Choose from 25 sensor options including LEL, PID, NDIR, and exotics that can be easily changed in the field. With five built-in alarms, including man down, and wireless connectivity to your command center, MultiRAE delivers vital information for fast incident response.

- Optional integrated wireless
- Dust-tight and waterproof (IP65-rated)
- Onboard gas libraries include 190 VOCs and 55 combustible gases
- Continuous data logging-6 months for 5 sensors 24/7

RAE GAMMARAE II R

A gamma radiation detector and full-range dosimeter in a single instrument. Designed specifically to meet the needs of first responders.

- Two types of sensors for excellent response in high and low dose rate ranges
- Waterproof to IP-67 standards
- Certified for use in Class I, Division 1 hazardous environments
- Top-mounted, invertible display
- Two AA alkaline batteries last up to 600 hours

Honeywell
RAE® SYSTEMS



KROMEK D3S ID

A wearable RIID that gives you the power to make the right decisions about nuclear threats in seconds. A powerful combination of two of Kromek's leading technologies: the non-3He compact thermal neutron detector and its world leading gamma detector, delivering the performance of a RIID in a small, but powerful device, the size of a PRD.

- One of the fastest and most accurate isotope ID devices on the market
- Discreet, wearable, lightweight
- Rapid, visible, audible and tactile alarm settings
- Identifies 17 extra isotopes, 4X faster
- Extensively tested and characterised in multiple DNDO and DARPA programs
- Quick, simple and intuitive to use, no need for specialist training or knowledge
- Built around your operational needs



FLIR®
The World's Sixth Sense®

FLIR IDENTIFINDER® R200

Spectroscopic Personal Radiation Detector (SPRD). Ideal for routine traffic stops or high visibility events and in mass transit or critical infrastructure entry control points.

- Wearable, weighs less than 0.9 lbs.
- Gamma only (R200-G) and gamma/neutron (R200-GN)
- Fully compliant with ANSI N42.32 and N42.48 standards, nuclide identification (≤ 7.5% resolution)
- IP67 and MIL-STD 810G rated enclosure, 1.5m drop-tested on all six sides
- Single-hand operation with 3-button control
- Common user interface with other FLIR raditation detectors
- No consumables or user maintenance



IDENTIFINDER® R300 ALSO AVAILABLE

FLIR IDENTIFINDER® R400

All-Purpose Radionuclide Identification Device (RID)

- Handheld radiation detection and identification
- Intuitive and lightweight (< 3.2 lbs.)
- 3-button interface simplifies operation in high stress situations
- Over 20,000 deployed globally

PPE

DUPONT™ TYCHEM® 2000 SFR

Chemical and secondary flame protection in a lightweight garment. Intended to be worn overy primary flame resistant garments. Also provides an effective barrier against a range of inorganic acids and bases as well as industrial cleaning chemicals and particles.

- Respirator-fit hood lined with Pro-Shield® 6 SFR fabric
- Covered, braided elastic at hood
- Nylon zipper with large metal pull
- Chin flap with double-sided adhesive tape
- Storm flap covers zipper which can be sealed by the wearer with double-sided adhesive strip to prevent intrusion at zipper
- Covered, braided elastic openings at wrist and ankle for tighter fit
- Taped seams

DUPONT®





DUPONT™ TYCHEM® 6000 TF611T

Made of a proprietary barrier film laminated to a Tyvek® substrate. The fabric provides at least 30 minutes of protection against over 180 challenge chemicals including chemical warfare agents and toxic industrial chemicals.

- Strong, durable and lightweight
- Hooded coverall with Elastomeric interface hood for tight fit around respirator
- Rear entry design keeps closure away from direct contact with frontal chemical exposure
- Double storm flap covers zipper which can be secured by the wearer with snaps and hook and loop closure to prevent intrusion at zipper
- Attached dissipative socks with boot flaps
- Attached inner gloves (to be used with appropriate outer gloves)
- Elastic wrist for an optimum fit
- Taped seams provide strong chemical resistance against heavy liquid splashes. A sewn seam is covered with a strip of compatible chemical resistant material through heat sealing

BLAUER RC3® ENSEMBLE

Designed to protect wearers against a broad range of CBRNe threats including liquid and vapor chemicals, radiological and biological particulates, and liquid chemical splash during physically demanding tactical entries, confined space rescue, and US&R missions.

- NFPA 1994 Class 3-R (2018 ed.) certification
- NFPA 1994 Class 4-R (2018 ed.) certification
- NFPA 1992 (2018 ed.) certification
- Breathable GORE CHEMPAK fabric
- Streamlined pattern provides a more tactical fit on the user and better equipment integration
- Durable fabric and seams prevent accidental contamination and provide user confidence
- Ten year shelf life
- Machine washable for multiple uses if not grossly contaminated





Kappler
Know What You're Getting Into.®

KAPPLER DURACHEM® 500

Certified NFPA 1994 protection for both CBRN and Hazmat.

- Includes dual certification to NFPA 1994 for both Class 1 and Class 2
- Provides tactical CBRN protection in non-encapsulating suit
- Rubber gasket fits securely around respirator (eliminates need for taping)
- Rear entry design enhances frontal splash protection



KAPPLER LANTEX® 100

Certified to NFPA 1999 for fentanyl response.

- NFPA 1999 certified Lantex® 100 meets IAB and CDC/NIOSH guidelines for fentanyl protection
- Fabric and seams pass ASTM F1671 blood and viral penetration test
- Breathable protective fabric provides enhanced comfort
- Unique rear entry garment design allows safer doffing, helps prevent cross-contamination
- Soft, flexible rubber gasket around face opening provides secure fit around respirator
- Finger loop features ensures sleeves extend over gloves



LION ERS

LION ready for action

The ERS (Extended Response Suit) protects against lower levels of vapor and liquid concentrations that may be encountered in the Warm Zone when deployed with the proper ensemble. This one piece, front entry suit is breathable for deployment over an extended period of time.

- Durable GORE® CHEMPAK® Selectively Permeable Fabric provides the wearer with protection against TIC's, TIM's, and CWA's below IDLH concentration levels while peforming technical and tactical operations
- Certified to (Warm Zone Operations), NFPA 1994, Class 3 (Toxic Industrial Chemical and Warfare Agent Protection) and NFPA 1992 (Liquid Splash)
- Certifed with variety of face pieces
- Increased mission time and performance due to the breathable selectively permeable membrane
- 24 hour / 3 wash wear life
- Sleek, one-piece, lighweight design with attached hood that easily compacts for storage
- Front-entry design for ease of donning/doffing
- GORE® G9492 inner glove
- Molded face seal that does not require tape and is certified for use with multiple CBRN respirators and masks
- Tapered legs with elasticated cuffs and attached booties for increased funtionality and mobility
- 4 adjustable belt loops to securely wear a duty belt or a PAPR and allow for easy doffing during decontamination



LION MT94™

The MT94™ (Multi-Threat) CBRN ensemble offers first responders advanced protection when facing some of the world's worst chemical and biological threats.

- Limited Hot Zone protection - certified to NFPA 1994, Class 2 and NFPA 1992 for hot zone operations
- GORE® CHEMPAK® Ultra Barrier Fabric provides durable protection against TIC's and CWA's above IDLH concentration levels while also providing improved mobility during tactical and technical operations
- Streamlined design combines durability, mobility and comfort
- Usable for multiple wears and washings, if not exposed or contaminated
- Rugged construction allows you to perform in the most challenging of circumstances
- Certified for use with GORE® G9492™ glove system using GORE® CHEMPAK® Ultra Barrier Fabric





PIP NOMEX HOOD

This NFPA straight cut full face hood is made of 20% Nomex and 80% Lenzing FR, fire resistant 2 ply knit fabrics that are certiifed to NFPA 1971-2007 standard for structural fire fighting.

- 20" in total length with a back gusset that allows it to lay flat around the neck
- Tunneled elastic face opening - 1/2" elastic is encased in fabric to ensure snug and durable fit
- Flatlock seams add strength and extra comfort



APPLICATIONS

- Incident command
- Privacy/scene/evidence protection
- Long-term operations
- Rehab
- Dive rescue

BENEFITS

- 1 person automatic deployment
- Compact storage
- All-weather use
- Pre-installed LED lighting
- Customizable





ZUMRO®
Fast. Simple. Proven.

#1 IN THE INDUSTRY ★

OTHER SIZES & OPTIONS AVAILABLE
PLEASE CALL FOR AN ON-SITE DEMO!



PELTOR®



3M™ PELTOR™ COMTAC™ HEADSETS

Designed to provide warfighters the options needed for successful field hearing protection and combat communications.

- 2-way tactical headset
- Level-dependent surround sound for "talk through"
- Ambidextrous noise-canceling boom mic
- Adjustable sizing

3M™ PELTOR™ TACTICAL 6-S HEADSET

Designed to perceive and localize weak sounds while offering hearing protection in high-noise environments.

- NRR: 19dB
- Small, compact and foldable
- Slim earcup profile
- External earcup microphones help provide situational awareness





ATLANTIC SIGNAL GLADIATOR H TACTICAL HEADSET

Allows an operator to engage and disengage hearing pro at-will while having no impact whatsoever on his ability to RX and TX.

- Earplugs provide up to 23 NRR
- Allows the operator to receive radio communications through his/her facial bones, leaving both ears free to maintain 360° of situational and directional awareness
- Audio transducers are positioned in front of the ears
- Communication systems are customizable

ATLANTIC SIGNAL COMBAT PUSH TO TALK

- Front mounted PTT switch as a secondary actuation switch
- Side mounted switch is quiet and shrouded
- Water resistant

atlantic signal

SAFEWARE IS A PROUD DISTRIBUTOR OF THESE LEADING UNIFORM MANUFACTURERS!

5.11®

elbeco

SPIEWAK® since 1904

TRU-SPEC®





TIMBERLAND PRO® VALOR™ DUTY BOOT

Soft-toe waterproof boots feature outsoles that grip any terrain and lightweight insoles for athletic performance.

- Uppers are black smooth leather and 1200-denier ballistic nylon
- Waterproof membrane
- Mesh lining with antimicrobial treatment for odor control and comfortable feet
- Scotchgard™ protector by 3M for stain resistance
- Bloodborne pathogen-resistant membrane
- Dynamic anti-fatigue technology absorbs shock and returns energy at key zones of the foot for all-day comfort
- Rounded driving moc heel
- Wall-climb toe grip
- Non-marking Timberland PRO® rubber lug outsole is slip-, oil-, and abrasion-resistant



5.11 TACTICAL® A.T.A.C 8" SHIELD CSA/ASTM BOOT

Offers unbeatable puncture, moisture and toe protection for superior safety in the harshest environments. The ATAC Shield Boot keeps you mobile, secure and comfortable at all times.

- Waterproof/breathable BPR membrane
- Side zip functionality
- 5.11 Shock Mitigation System®
- Antibacterial and moisture-wicking lining
- Cushioned insole
- Oil and slip resistant, no-squeak outsole
- Semi-rigid heel and toe reinforcement
- Full grain leather and rugged nylon construction



DANNER ACADIA BOOTS

Made in the USA, the Acadia® features Danner's famous stitchdown construction, providing a more stable platform underfoot and superior durability.

- 8" black
- Waterproof breathable GORE-TEX® lining and a combination upper of 1000 Denier nylon and full-grain leather
- Vibram® Kletterlift outsole provides superior shock absorption and great traction on both wet and dry surfaces

PROPPER® SERIES 100® 8" WATERPROOF SIDE ZIP BOOT

- Polishable full grain leather (black only) with 1000D nylon upper
- Durable, coated, speed lace hardware with 550 paracord lacing
- Fast-rope compatible arch design resists wear from ladders and fast-roping
- Ortholite® sock liner for comfort
- Washable open cell foam inserts contour to your foot for weight distribution and arch support
- Oil- and slip- resistant upper outsole for excellent traction and impact absorption
- Open cell air mesh foam provides full foot air circulation for maximum comfort
- Anti-microbial breathable lining prevents odor and extends the life of the boot
- Triple stitching for durability NATO speed lacing system
- YKK side zipper with zipper guard







HAIX GSG9-S

Developed for and with SRT Teams.

- 8" black
- Waterproof leather
- Footwear liner which will never pull out or wrinkle up over time
- Lightweight foam injected into the sole to provide exceptional shock absorption and superior heat/cold insulation
- Two-zone lacing system

SAFEWARE OFFERS AN EXTENSIVE OFFERING OF DUTY GEAR

GOULD™ &GOODRICH
A PASSION FOR PROTECTION

Including badges, belts, holsters, flashlight holders, magazine cases, radio holders, handcuff holders and much more.



ELSAG Enterprise Operations Center

Welcome **Toya.Adams** [Log Off]

Home | Lists | Data Mining | User Config | System | Monitoring Tools | Help

Reads/Alarms

Map | Date/Time Start 4/29/2020 12:00 AM End 4/30/2020 12:00 AM UTC -04:00 | Rows 50

Plate 1KSC88 Upload Advanced

Apply Reset Select a format Export

Drag a column header and drop it here to group by that column

1 - 7 of 7 items (7 Total Reads)

Overview	Date/Time	Plate	St	GPS	Reader	Status	List	Class	Domain
	4/23/2020 12:30:23 AM UTC-04:00	1KSC88			MDTA-JFK NB	Normal Read			MCAC - MDTA Sharing
	4/23/2020 12:30:21 AM UTC-04:00	1KSC88			MDTA-JFK NB	Normal Read			MCAC - MDTA Sharing
	4/23/2020 12:00:28 AM UTC-04:00	1KSC88			MDTA-FMT NB	Normal Read			MCAC - MDTA Sharing
	4/22/2020 6:49:11 PM UTC-04:00	1KSC88			Fixed MSP-SB 95 Cherry Hill PgCo	Normal Read			Direct Connect - Fixed Sites
	4/22/2020 6:25:52 PM UTC-04:00	1KSC88			MDTA-FMT SB	Normal Read			MCAC - MDTA Sharing
	4/22/2020 6:25:49 PM UTC-04:00	1KSC88			MDTA-FMT SB	Normal Read			MCAC - MDTA Sharing
	4/22/2020 5:53:43 PM UTC-04:00	1KSC88			MDTA-JFK SB	Normal Read			MCAC - MDTA Sharing

1 - 7 of 7 items (7 Total Reads)

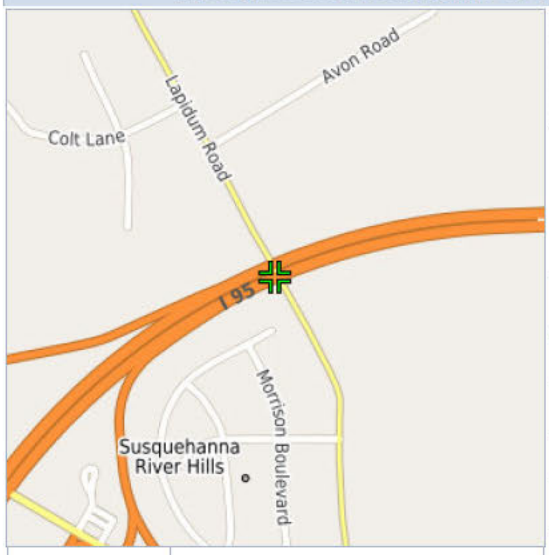
Go Home

EOC 5.6.21020 | culture en-US | uiCulture en-US | Request Server Time 4/29/2020 10:53 AM UTC-04:00

ELSAG

ID: 45d08d64-b4ea-4d3a-be3e-72f5fa8c6b79 Toya.Adams 4/29/2020 10:55:37 AM UTC-04:00

License Plate Number:



Nearest Address	John F. Kennedy Memorial Highway, Susquehanna River Hills, Harford County, Maryland, 21078
Nearest Cross Street	Lapidum Road



Read Info

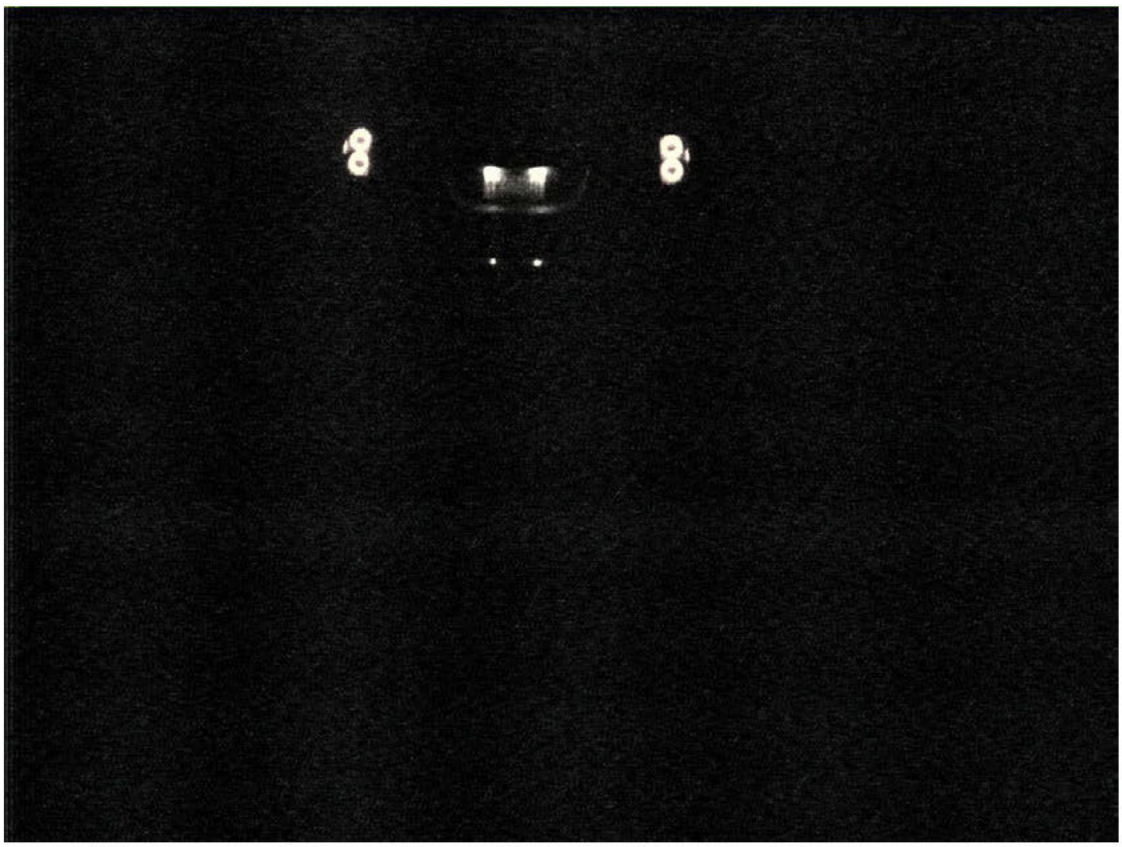
Plate	[redacted]
Date/Time	4/23/2020 12:30:23 AM UTC-04:00
GPS	[redacted]
Reader	MDTA-JFK NB
User	
Camera	JFK-NB-ML-RC
Domain	MCAC - MDTA Sharing
Make	
Model	
Color	
Color 2	
Type	
Tax Class	

ELSAG

ID: 45d08d64-b4ea-4d3a-be3e-72f5fa8c6b79 Toya.Adams 4/29/2020 10:55:37 AM UTC-04:00

License Plate Number: [redacted]1KSC88



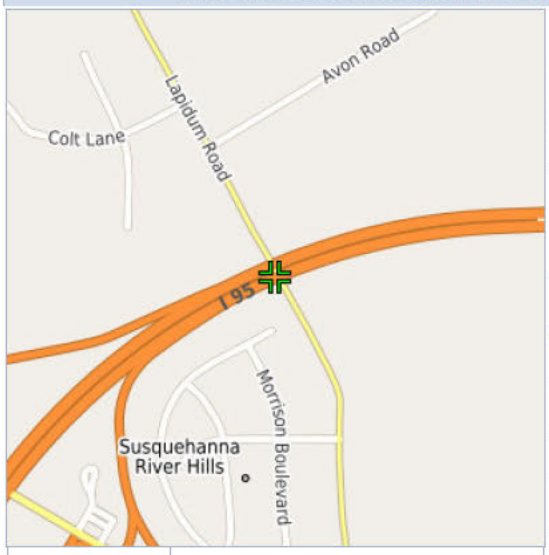


ELSAG

ID: 3a835999-7cc6-42b2-bc00-d489f0912dad

Toya.Adams 4/29/2020 10:55:42 AM UTC-04:00

License Plate Number:



Nearest Address	John F. Kennedy Memorial Highway, Susquehanna River Hills, Harford County, Maryland, 21078
Nearest Cross Street	Lapidum Road

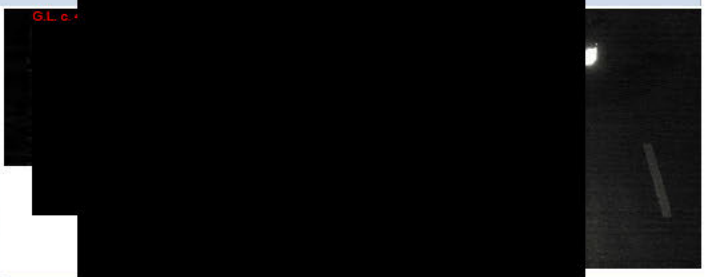
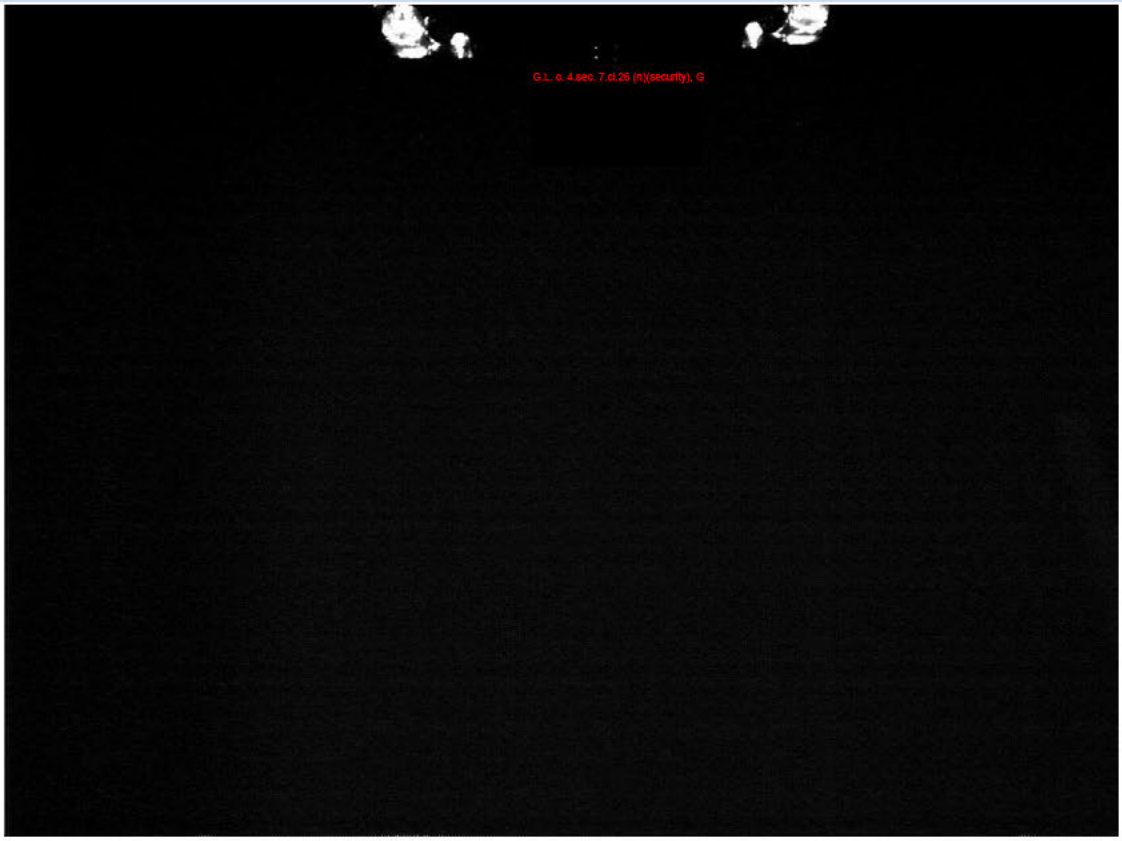


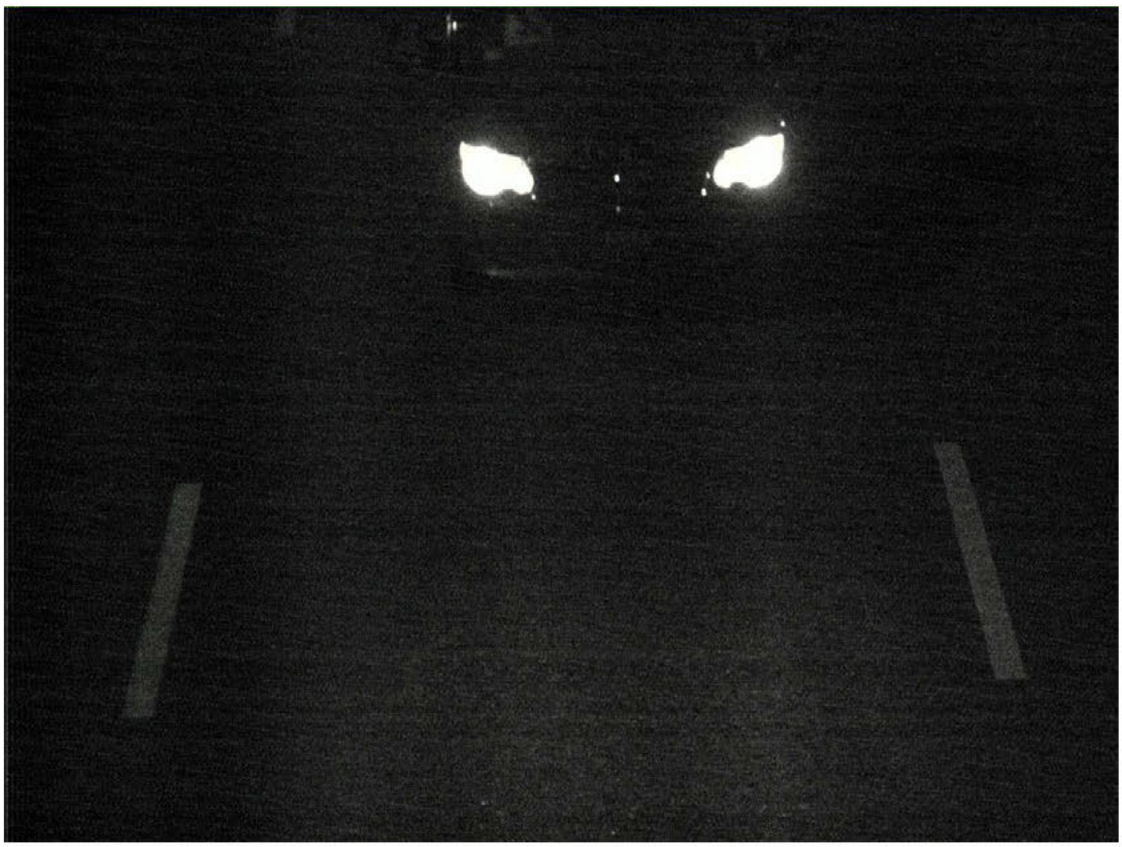
Plate	
Date/T	
GPS	
Reade	
User	
Camer	
Doma	
Make	
Model	
Color	
Color 2	
Type	
Tax Class	

ELSAG

ID: 3a835999-7cc6-42b2-bc00-d489f0912dad Toya.Adams 4/29/2020 10:55:42 AM UTC-04:00

License Plate Number: 1KSC88



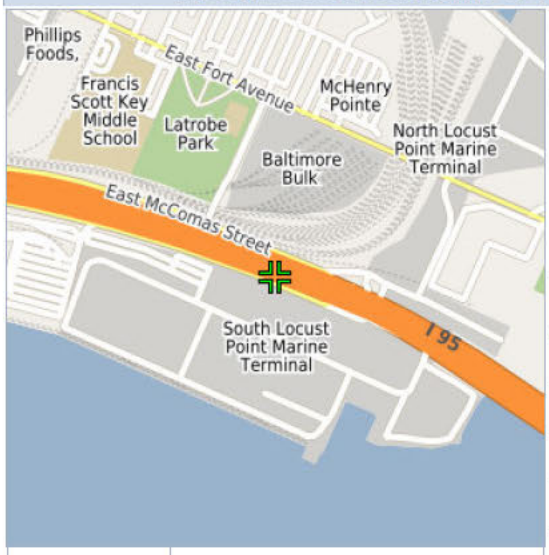


ELSAG

ID: 2f10fb63-e61d-415e-b40b-92322b1592c4 Toya.Adams 4/29/2020 10:55:44 AM UTC-04:00

License Plate Number:

[redacted] G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)



Nearest Address	, , Baltimore, Maryland,
Nearest Cross Street	Fort McHenry Tunnel (Bore 4)

Plate	
Date/Ti	
GPS	
Reader	
User	
Camera	
Domain	
Make	
Model	
Color	
Color 2	
Type	
Tax Class	

ELSAG

ID: 2f10fb63-e61d-415e-b40b-92322b1592c4 Toya.Adams 4/29/2020 10:55:44 AM UTC-04:00

License Plate Number: 1KSC88



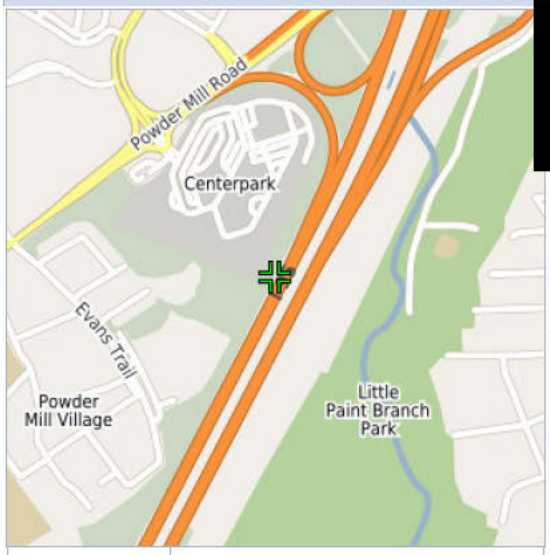


ELSAG

ID: b9916225-c275-4481-8477-55eb3b70ec40 Toya.Adams 4/29/2020 10:55:47 AM UTC-04:00

License Plate Number: [redacted]

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)



Nearest Address	, Beltsville, Prince George's County, Maryland,
Nearest Cross Street	

Pl[redacted]	
Da[redacted]	
GP[redacted]	
Re[redacted]	
Us[redacted]	
Ca[redacted]	
Do[redacted]	
Ma[redacted]	
Model	
Color	
Color 2	
Type	
Tax Class	

ELSAG

ID: b9916225-c275-4481-8477-55eb3b70ec40 Toya.Adams 4/29/2020 10:55:47 AM UTC-04:00

License Plate Number: 1KSC88



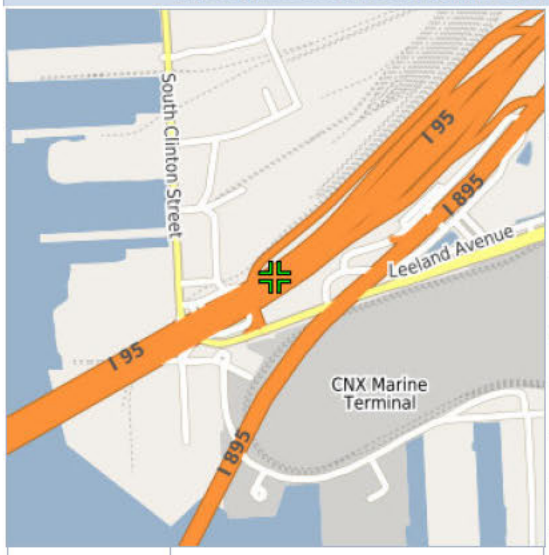


ELSAG

ID: 12bc9c10-8a0e-4f93-b0c5-d7387e0a946a

Toya.Adams 4/29/2020 10:55:50 AM UTC-04:00

License Plate Number:



Nearest Address	, , Baltimore, Maryland,
Nearest Cross Street	

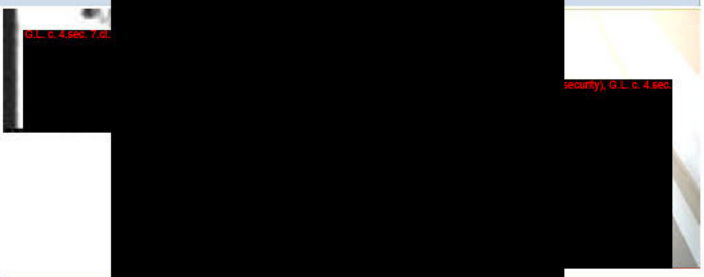


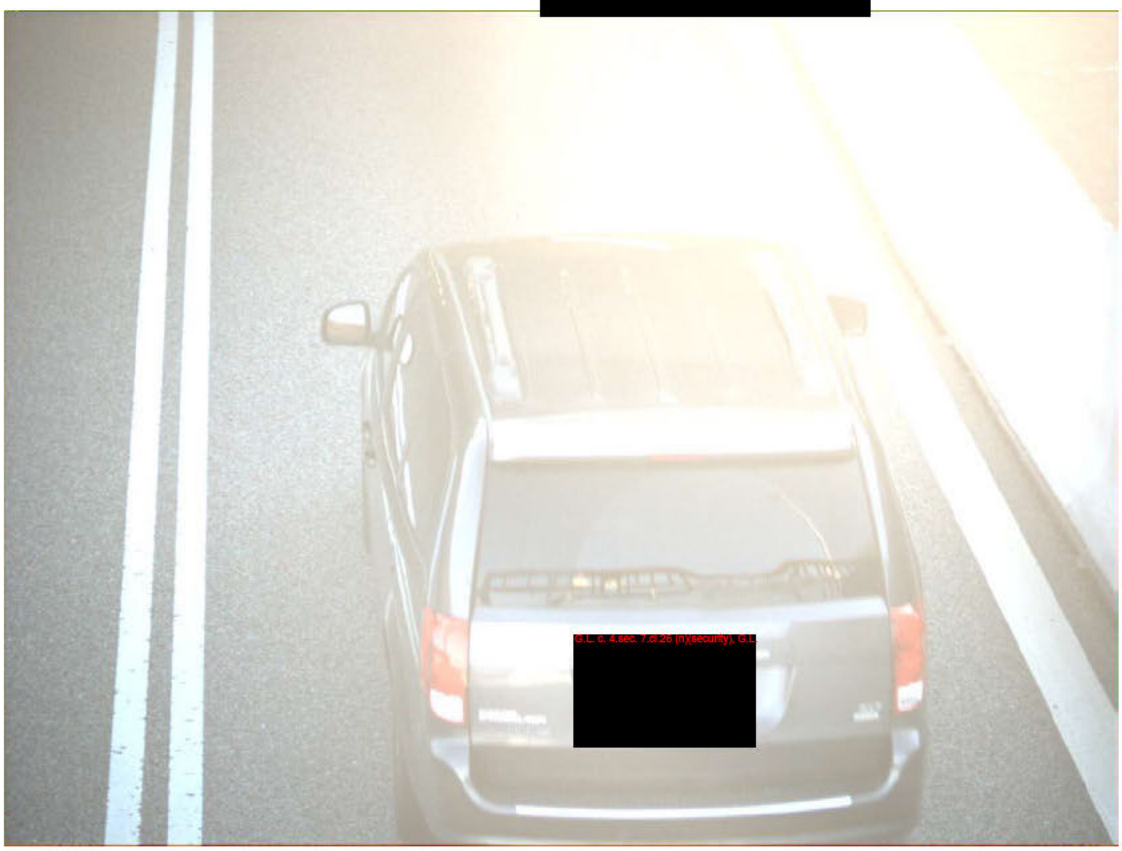
Plate	
Date/Tim	
GPS	
Reader	
User	
Camera	
Domain	
Make	
Model	
Color	
Color 2	
Type	
Tax Class	

ELSAG

ID: 12bc9c10-8a0e-4f93-b0c5-d7387e0a946a Toya.Adams 4/29/2020 10:55:50 AM UTC-04:00

License Plate Number: 1KSC88

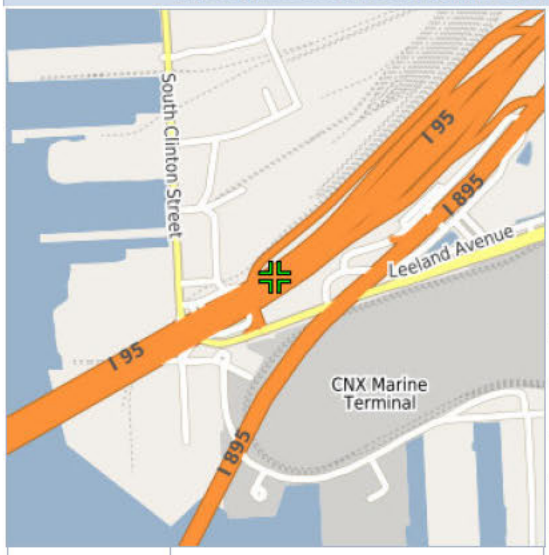




ELSAG

ID: 65fc7695-7c98-449f-9e82-4523daf36320 Toya.Adams 4/29/2020 10:55:53 AM UTC-04:00

License Plate Number: G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)





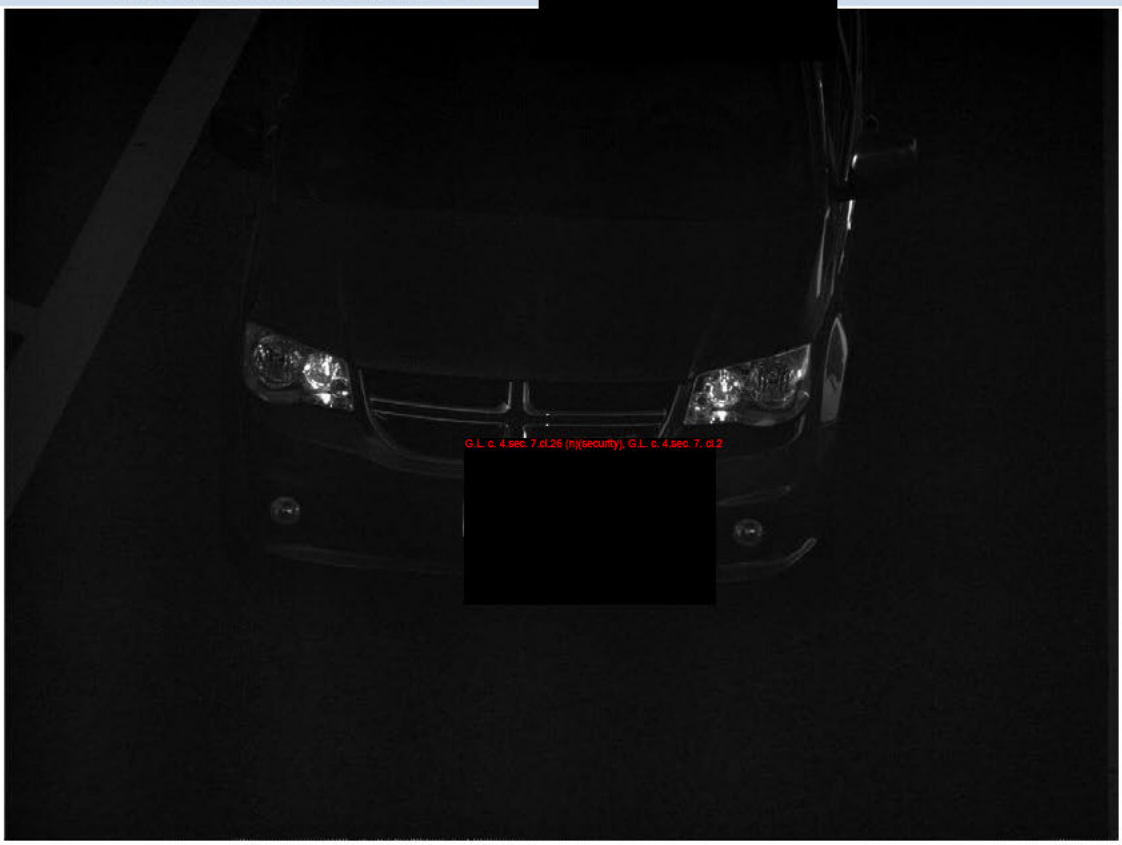
Nearest Address	, , Baltimore, Maryland,
Nearest Cross Street	

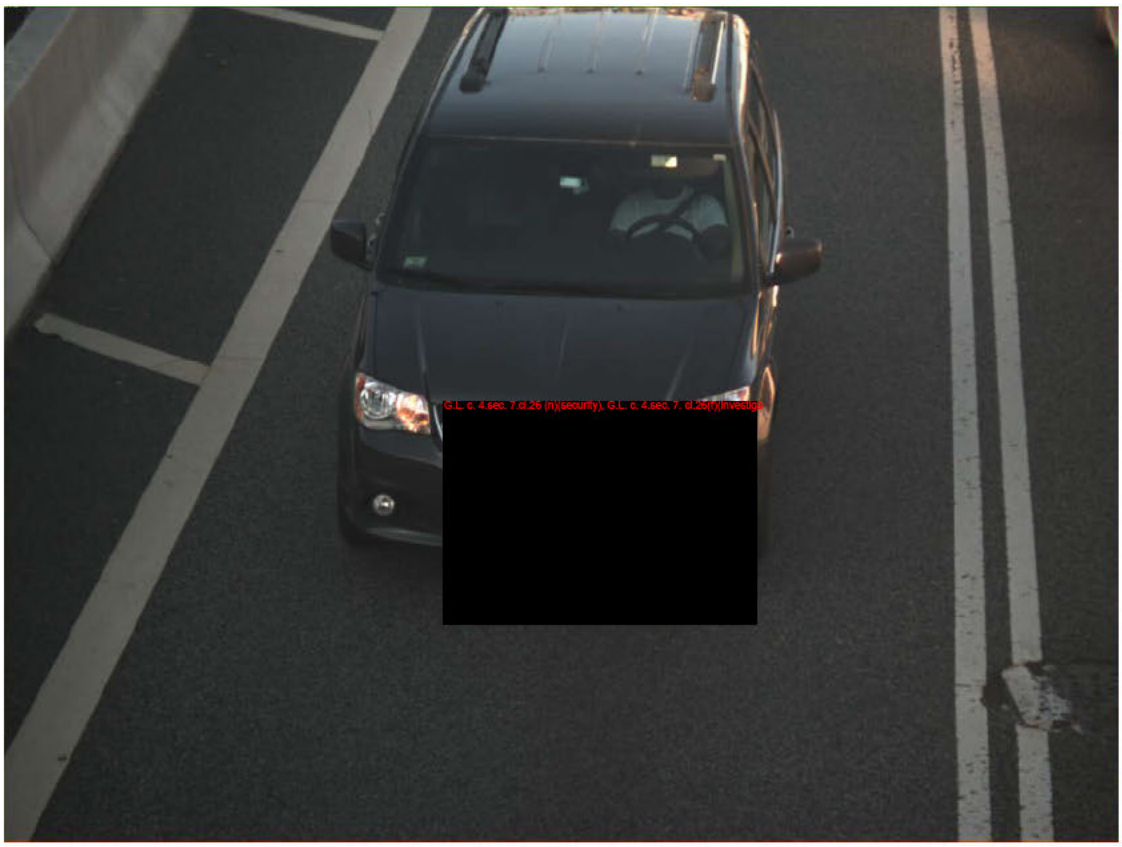
Color	
Color 2	
Type	
Tax Class	

ELSAG

ID: 65fc7695-7c98-449f-9e82-4523daf36320 Toya.Adams 4/29/2020 10:55:53 AM UTC-04:00

License Plate Number: [redacted]



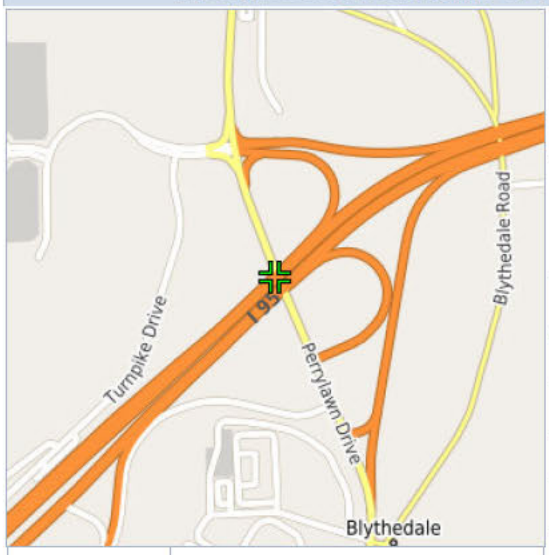


ELSAG

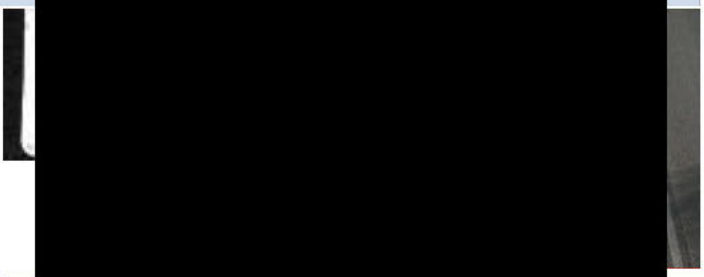
ID: 3f53c988-4b53-4ecb-80ba-792f3054bf49 Toya.Adams 4/29/2020 10:55:55 AM UTC-04:00

License Plate Number:

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)



Nearest Address	, Perryville, Cecil County, Maryland,
Nearest Cross Street	John F. Kennedy Memorial Highway



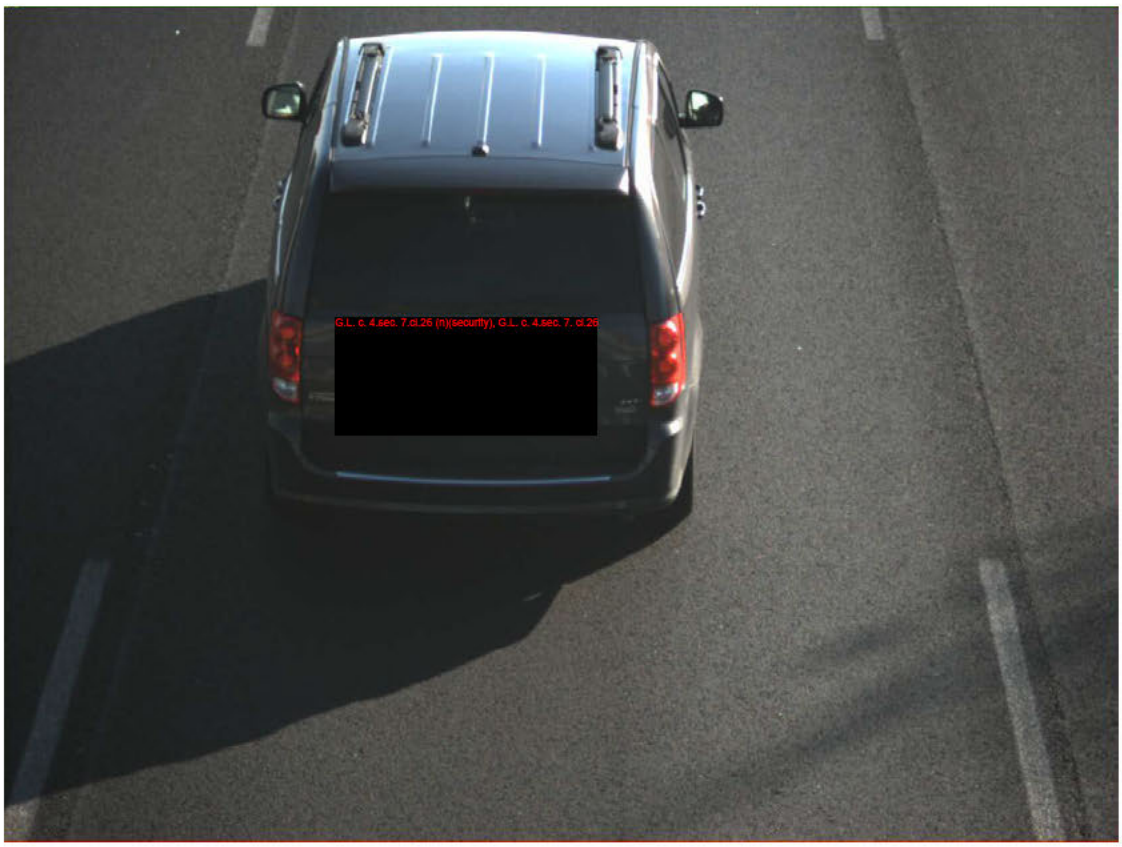
Pl	
Da	
GP	
Re	
Us	
Ca	
Dc	
Ma	
Model	
Color	
Color 2	
Type	
Tax Class	

ELSAG

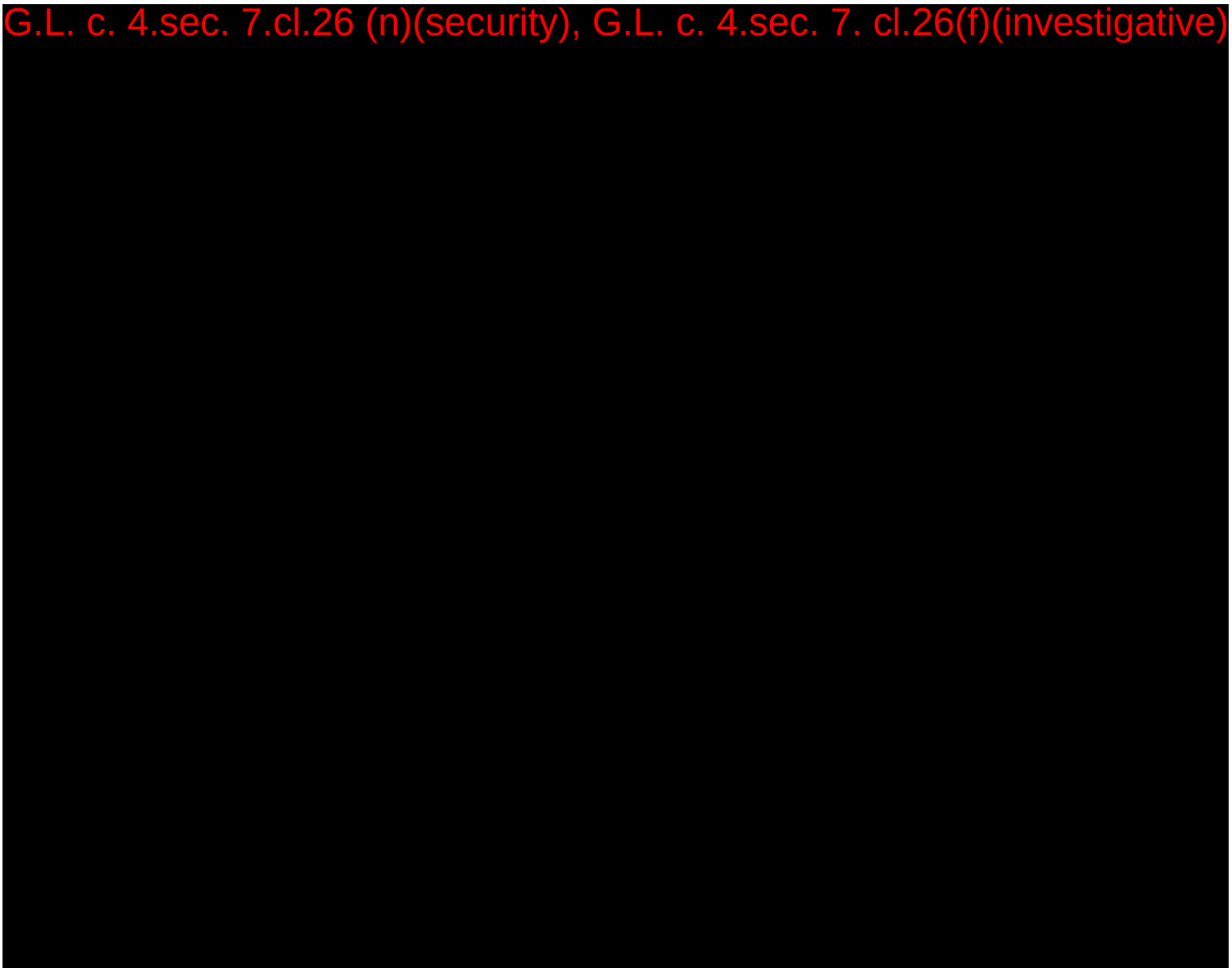
ID: 3f53c988-4b53-4ecb-80ba-792f3054bf49 Toya.Adams 4/29/2020 10:55:55 AM UTC-04:00

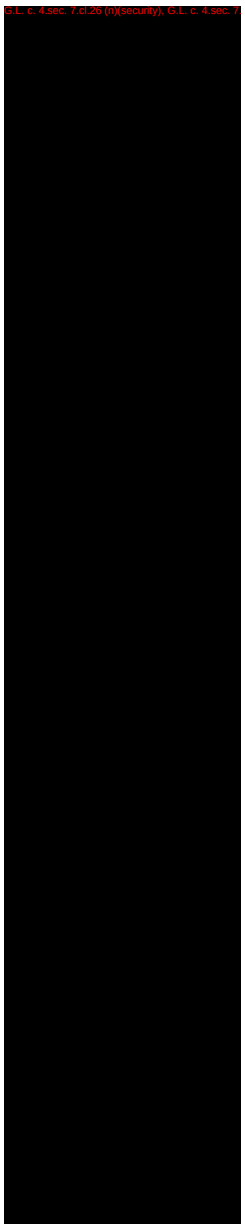
License Plate Number: 1KSC88





Date	Reg	Reader	Name	Action	Trooper	Report




G.L. c. 4,sec. 7,cl.26 (n)(security), G.L. c. 4,sec. 7

Leading the innovation

4162

PIPS TECHNOLOGY
DETECTION INNOVATION

Increase your vision

new mobile solution

mobile camera

&

processor



Extended field of view

- 2 lane coverage
- FOV increased by 42%
- 1280 x 720 @ 60fps
- New sensors for better image quality

Longer Capture Range

- Up to 45ft - 50% increase
- Improved low-light capability

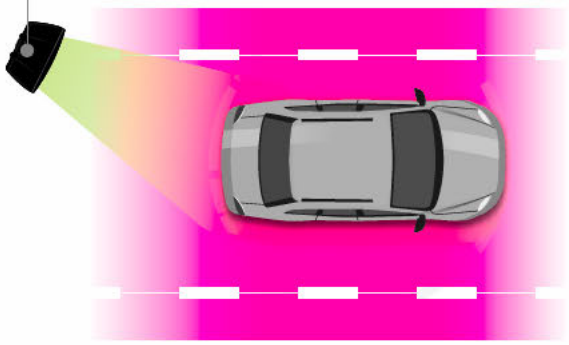
inimal Upgrade Barrier

Same low profile and small footprint
as the P634 mobile camera
Backward compatible with current
IPS™ brackets

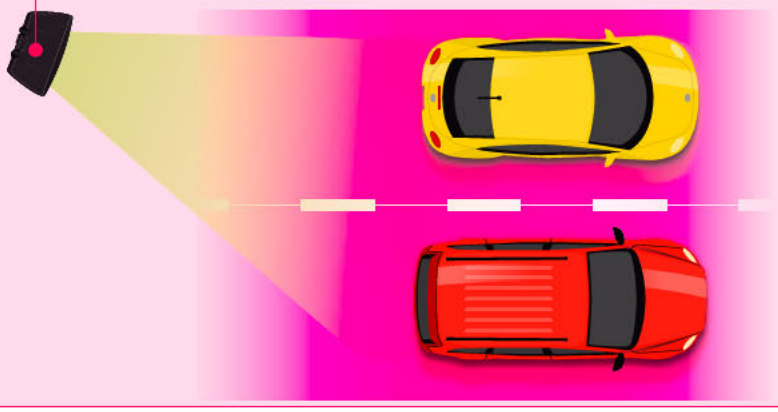
and flexible installation

DE cable available in 15 ft to 100 ft
tal IP67 sealed connectors
7 housing for outdoor operation

P634 camera field of view
(Current)



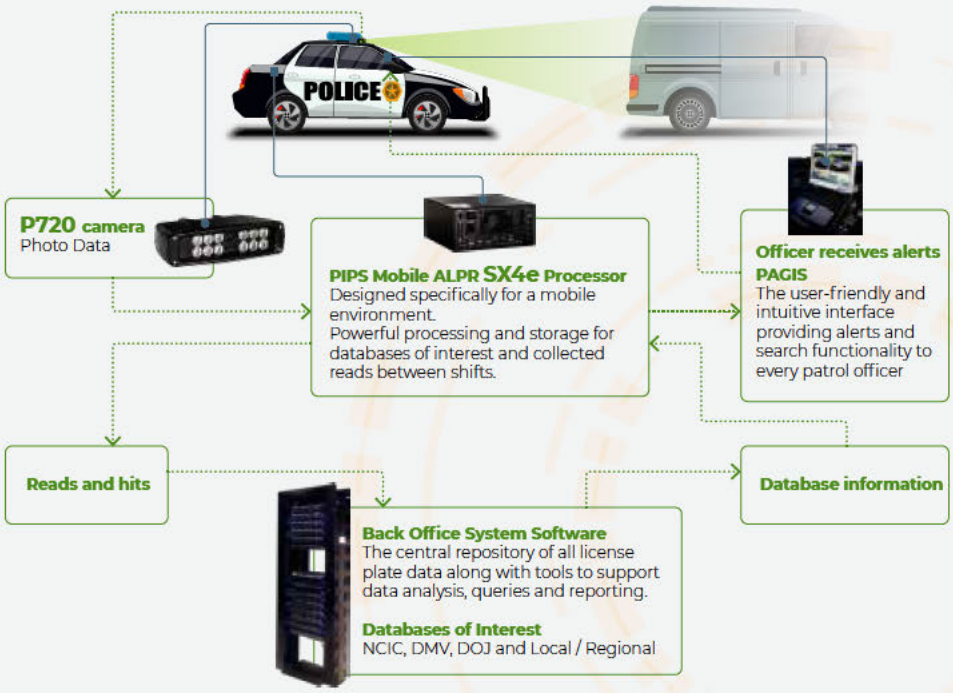
P720 camera field of view



Mobile ALPR Systems

Mobile ALPR Systems assist on-street patrol officers checking for criminal activity by capturing and analyzing license plates against known databases. This compact, rugged system has been IP67 certified and mounts securely below the lightbar for limited visual interference.

PIPS Mobile ALPR Solution is a force multiplier that increases officer productivity and safety with every deployment.



APPLICATIONS

On-street enforcement of:

- Stolen Vehicles
- Amber Alerts
- Unregistered Vehicles
- Wanted Criminals
- Parking Violations
- Be on the Lookout (BOLO)

FEATURES AND BENEFITS:

- Offers high resolution coverage for a full lane of traffic with up to two concurrent vehicles in the field of view.
- Instantly checks captured plates against one or more databases of interest to immediately alert officers of hits.
- Increases spatial awareness for improved officer safety.
- Enhances proactive, preventative enforcement by enabling more intelligent investigations and data sharing across jurisdictions.
- Back Office System Software (BOSS) stores all collected data in a central location to support data analysis, data queries and reporting for law enforcement investigations (in accordance with each jurisdiction's data retention policy).

PIPS TECHNOLOGY DETECTION INNOVATION
is a trademark of Neology Inc., and either registered or pending registration in several jurisdictions.

For additional information, assistance or maintenance questions please contact Neology ALPR/ANPR support at:

PHONE: **833-PIPS-LPR (833-747-7577)**

- Option 1 for sales
- Option 2 for support

For the **U.S/Can and all other areas**:
Sales Enquiry Email: sales@pipstechnology.com
Support Request Email: support@pipstechnology.com

For **Europe, Middle East and Africa**:
Sales Enquiry Email: sales@pipstechnology.co.uk
Support Request Email: support@pipstechnology.co.uk

A NEOLOGY MOBILITY TECHNOLOGIES bussiness.

Neology Headquarters San Diego
Address: 13520 Evening Creek Drive Suite 460. San Diego, CA 92128

Neology UK Ltd.
Address: Form 1 Bartley Wood Business Park Hook Hampshire RG27 9XA

Neology Mexico
Plaza Carso II, Lago Zurich No.219-piso 10 C.P. 11529 Ciudad de Mexico



PIPS TECHNOLOGY™
DETECTION INNOVATION



PAGIS Administrator's Manual

Version 2.14

Updated 7/16/2020

NEOLOGY MOBILITY TECHNOLOGIES

Table of Contents

Table of Contents 2

NOTICES 4

Technical Support 4

Design Changes 4

Trademarks 4

Copyright 4

Version 4

INTRODUCTION 5

1.1 Dual Lens Color and Infrared Camera 5

1.1.1 Available Products 5

1.2 Using This Manual 6

SCREEN REFERENCE 7

2.1 The PAGIS Software Login Screen 7

2.1.1 Logging on with the Default Administrative Account 7

2.2 Main Screen - Live View 8

2.2.1 Getting Started in PAGIS 8

2.3 The PAGIS Navigation Buttons 9

2.3.1 Camera Control Buttons 9

2.3.2 GPS Indicators 10

2.3.3 Camera Firmware Update (Restricted Users) 10

2.3.4 Day/Night Mode 10

2.4 Begin Shift 11

2.4.1 Sync via USB Thumb drive (or Local Source) 11

2.4.2 Sync via Wireless Network 11

2.4.3 PAGIS Auto-Sync Settings 11

2.4.4 Begin Shift – Additional Information 11

2.5 End Shift 11

2.5.1 Sync to BOSS 11

2.6 Cam Mode Button 12

2.6.1 Camera Modes 12

2.7 Taking a Picture 12

2.8 Search Entry Screen 13

2.8.1 Searching Synchronized Hotlists for License Plates 13

2.8.2 Searching Locally Stored Reads and Hits 13

2.8.2.1 Searching for a Match 14

2.8.3 Wild Card Symbols 14

2.8.4 Manually Adding a Plate to PAGIS 15

2.8.4.1 ADD VLP Query 15

2.8.4.2 ADD VRM Report Screen 15

2.9 The Review Screen 16

2.9.1 Summary Review Section 16

2.9.2 Review Navigation Buttons 16

2.9.3 Reads 17

2.9.3.1 Reads Result Screen Navigation Buttons 17

2.9.3.2 Interactive Buttons – Reads Screen 17

2.9.4 Hits 18

2.9.4.1 Hit Screen Attributes 18

2.9.4.2 Hit Screen Function Buttons 19

2.9.4.3 Interactive Buttons – Hits Screen 19

2.9.4.4 Set Disposition – Additional Detail 19

2.9.4.5 Add Intel – Additional Detail 20

2.9.5 Misreads 20

2.9.5.1 Marking a Record as a Misread: 21

2.9.6 Audits 22

2.9.7 Targets 22

2.9.7.1 The Targets Screen 23

2.9.7.2 Targets Screen Navigation Buttons 23

2.9.8 Databases 24

2.9.8.1 Databases Screen Functions 24

2.9.8.2 Databases Screen Navigation Buttons 24

2.9.8.3 Databases Edit- “Manual Reports” 25

ADMIN SETTINGS 26

3.1 Sync Options Screen 26

3.1.1 Synchronization Types 26

3.1.1.1 Synchronization to Disk (Local Storage) 27

3.1.1.2 Synchronization with BOSS 27

3.1.1.3 Sync to “Instation” (Formerly BOF2 and BOF3) 28

3.1.2 Global Sync Options 29

3.2 PAGIS Privacy Settings (Local Data Retention) 30

3.3 Language 31

3.4 Location 31

3.5 Users 32

3.5.1 User Privileges ____ 32
3.6 Sound ____ 33
3.6.1 Configuration Buttons ____ 33
3.7 System ____ 34
3.8 Rules ____ 35
3.8.1 Rules – Additional Clarifications ____ 35
3.9 OCR ____ 36
3.10 External ____ 37
3.10.1 XML Datastream Ports ____ 37
3.11 Cameras ____ 38
3.11.1 Checking the Connection ____ 38
3.11.2 Troubleshooting Camera Connections ____ 38
3.11.3 Configuring the Cameras in PAGIS ____ 39
3.12 Cam Setup ____ 40
3.12.1 Cam Setup Navigation Buttons ____ 40
3.13 Configs (Camera View Modes) ____ 41
3.13.1 Configs Navigation Buttons ____ 41
3.13.2 Reviewing and Modifying Existing Modes ____ 42
3.13.3 Adding a New Camera Mode ____ 43
3.14 Info ____ 44
3.15 Camera Firmware Update, (Admin) ____ 44
PAGIS INSTALLATION GUIDE ____ 45
4.1 PAGIS System Requirements ____ 45
4.2 PAGIS Prerequisites ____ 45
4.2.2 PAGIS Software Installation (MDC) ____ 46
4.2.3 PAGIS Software Installation (Mobile Processor) ____ 47
TROUBLESHOOTING TIPS ____ 48
5.1 Troubleshooting & Tips ____ 48
5.1.1 PAGIS with NetMotion VPN ____ 48
5.1.2 Cisco VPN Client: ____ 48
5.1.3 Microsoft .NET 3.5 Installation ____ 48
5.1.4 Firewall Settings for Client-Server Installations ____ 48
PAGIS/BOSS3 CONFIGURATION ____ 49
6.1 Creating a New Device in BOSS3 ____ 49
6.2 Enabling a New Mobile System in BOSS3 ____ 49
6.3 Assigning Ownership to a Device in BOSS3 ____ 49
6.4 Assigning Hotlists to a Device in BOSS3 ____ 50
PAGIS/BOSS4 CONFIGURATION ____ 50
7.1 Creating a New Device in BOSS4 ____ 50
7.2 Enabling a New Mobile System in BOSS4 ____ 50
7.3 Assigning Ownership to a Device in BOSS4 ____ 51
7.4 Assigning Hotlists to a Device in BOSS4 ____ 51
APPENDIX A: THE GLOSSARY ____ 52
APPENDIX B: PAGIS SOFTWARE DATABASE FILE ____ 53
APPENDIX C: FAQ ____ 55
APPENDIX D: XML DATASTREAM ____ 60

4166

NOTICES

The information within this manual is authorized for distribution to customers, authorized service center personnel, and distributors of Neology. Every effort has been made to supply correct information. However, Neology assumes neither responsibility for its use, nor for any infringements of patents or other rights of third parties, which may result from its use. No license is granted by the manufacturer under any patent or patent rights. Neology reserves the right to modify and update the equipment at any time without prior notice. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means to a third party without the prior consent of the copyright holder. The manufacturer's warranty will be invalidated if untrained personnel operate the equipment or if any attempt is made to service the equipment by unauthorized personnel.

This manual contains confidential and proprietary information and should not be redistributed except as needed for proper use and maintenance of the agency's Mobile ALPR system.

Technical Support

Service of this equipment by replacement of parts, on-site repair, routine maintenance inspection, and scheduled remote support session is available. Please contact PIPS Technology's ALPR Technical Support.
Phone: 833-PIPS-LPR (833-747-7577), Option 2
Support Team Email: Support@PIPSTechnology.com
For Customers in Europe, Middle East and Africa: Support@PIPSTechnology.co.uk
Web: www.pipstechnology.com
Fax: 858-391-0264
Corporate Office: 13520 Evening Creek Drive Suite 460. San Diego, CA 92128

Design Changes

Neology reserves the right to change the design of any product from time to time without notice and with no obligation to make corresponding changes in products previously manufactured.

Trademarks

PIPS Technology™ is a trademark of Neology Inc., and either registered or pending registrations in several jurisdictions. Windows, Windows 7, Windows 8, Window 10, and .NET are all trademarks of the Microsoft Corporation. Other trademarks and registered trademarks are the property of their respective owners.

Copyright

The Neology / PIPS Technology PAGIS Software is copyright of Neology. All rights reserved. This product contains confidential and trade secret information of Neology and is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portions of it, may result in civil and criminal penalties.

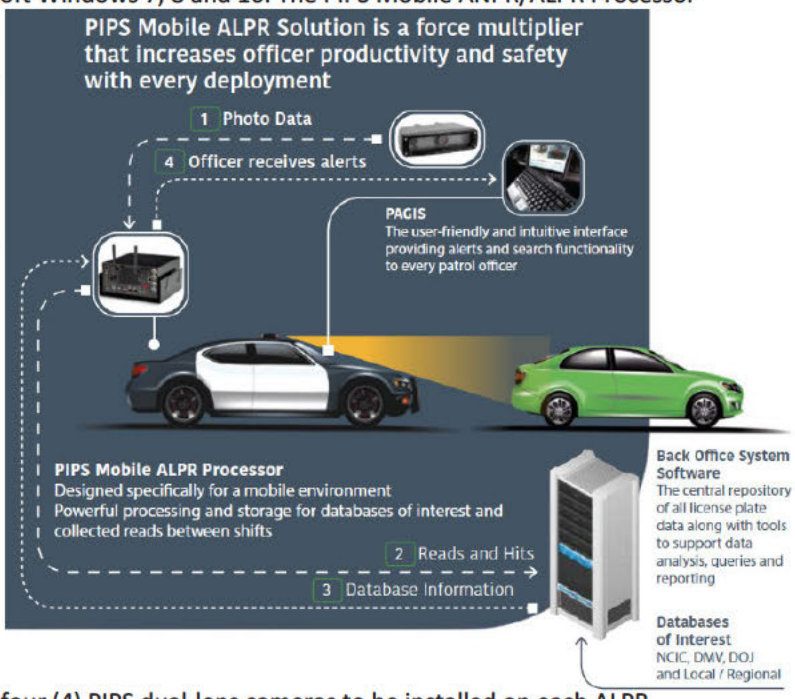
Version

This manual demonstrates the attributes of the Neology / PIPS Technology PAGIS Software Version 2.14 and was last updated in March 2020.

INTRODUCTION

PIPS Technology's Automated License Plate Recognition (ALPR) software solution called PAGIS utilizes dual-channel, dual-lens, cameras to "read" plates. Our software is optimized to run on the Mobile Processor itself or in conjunction with a mobile data computer (MDC). Our mobile software is compatible with Microsoft Windows 7, 8 and 10. The PIPS Mobile ANPR/ALPR Processor comes equipped with Microsoft Windows 7 Embedded.

The PAGIS Software processes the infrared plate image provided by any of the cameras and then interprets the plate number through Optical Character Recognition (OCR) via the mobile processor. The PAGIS application then searches for any matches of the plate with those listed in the databases, or "hotlists," distributed from the PIPS Back Office System Software (BOSS) or other external sources.



WARNING: To reduce the risks associated with impact, which if not avoided, could result in serious injury or death: Do Not interact with the ALPR system while driving in hazardous situations. The PIPS mobile camera series and License Plate Capture Software are not intended for use in hazardous environments, so that the User and/or others are not put at risk for personal injury and/or property damage.

1.1 Dual Lens Color and Infrared Camera

The PIPS Technology Mobile ALPR System allows for a maximum of four (4) PIPS dual-lens cameras to be installed on each ALPR vehicle provided that the vehicle supports the additional mounting equipment.

Each dual-lens mobile camera uses visible light to take color overview pictures of the vehicle and uses infrared (IR) illumination to capture the license plate's alphanumeric characters. IR illumination offers the best capture performance of reflective license plate characters for the following reasons:

- State issued license plates are designed to be highly reflective to IR light.
- Cameras using IR capture technology do not depend on the presence of visible light to function.
- Cameras using IR capture technology are not negatively impacted by the effects of headlights, solar glare, or total darkness.
- IR light penetrates rain and fog better than visible light.
- Due to these attributes, the system can be used 24 hours a day, seven days a week.

1.1.1 Available Products

Additional information about this and other PIPS Technology applications, cameras, and solutions are available on the PIPS web site: http://www.pipstechnology.com

1.2 Using This Manual

4169

The section overview of this software manual is as follows:

Section 1: The Introduction and Basics

Section 2: PAGIS User's Section: Explains screen function and User Operations in the PAGIS Software

Section 3: Troubleshooting Tips

Section 4: Software Administrator's Guide: Explains how to install and configure the PAGIS Software

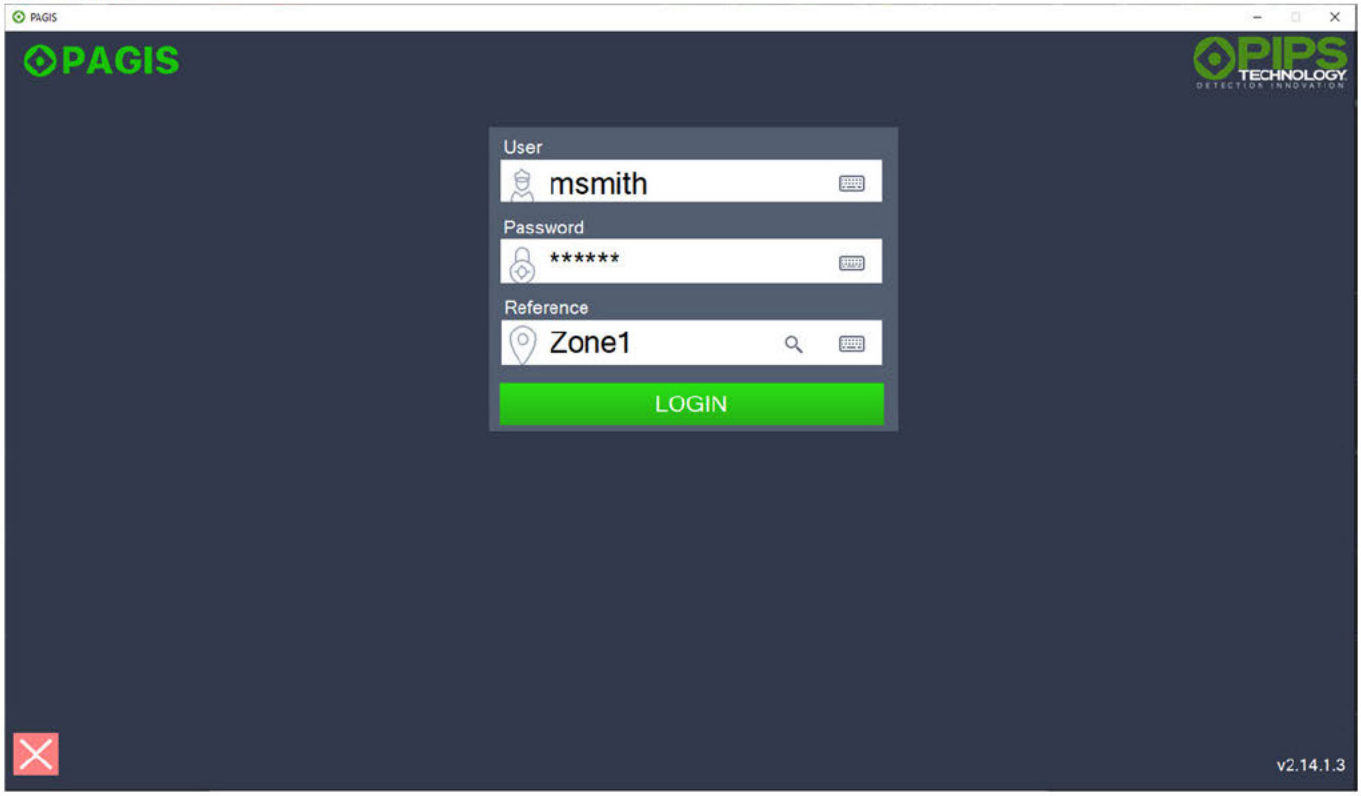
Section 5: Additional Information and Troubleshooting Tips

Section 6: Initial BOSS configuration for new PAGIS devices (MDCs)

Appendices: Additional features and details

SCREEN REFERENCE

This section guides the user through the PAGIS Software screens and the available options. Screens are grouped according to function. When a button is grayed out or missing, the option is not available, or no information has been accrued to activate it.



2.1 The PAGIS Software Login Screen

The PAGIS Software allows users with various access privileges to use the same MDC. For users with touch screen monitors, the Keypad button immediately to the right of any text box gives the user access to an on-screen keyboard for data entry.

User Field: The alphanumeric string assigned to identify the user. Usernames are not case sensitive.
Password Field: Password of the assigned user logging in. Passwords are case sensitive.
Reference Field: This is an optional field utilized to fit a number of use cases. A user can manually enter a reference at logon, leave the field blank, or select list of unique tags that will be associated with all data captured while logged in. If the Administrator has configured a default reference tags, that information will be displayed automatically. Otherwise, it will be blank.
Login Button: Submits the username and password to attempt a login.
Exit Button: By clicking the X icon in the lower left-hand corner, the user can exit/close the PAGIS Software.

2.1.1 Logging on with the Default Administrative Account

The PAGIS Software includes a default administrative account that can be used for the initial configuration. To do so, simply click the **Login** button with the User and Password fields blank.

NOTE: System Administrators are strongly encouraged to configure users for PAGIS just before, or soon after the installation and setup. PAGIS users accounts are created and maintained in BOSS. Once Users are established by the BOSS System Administrator, the default user account is automatically disabled. Best practices are to be certain at least one User account has administrative privileges.

2.2 Main Screen - Live View

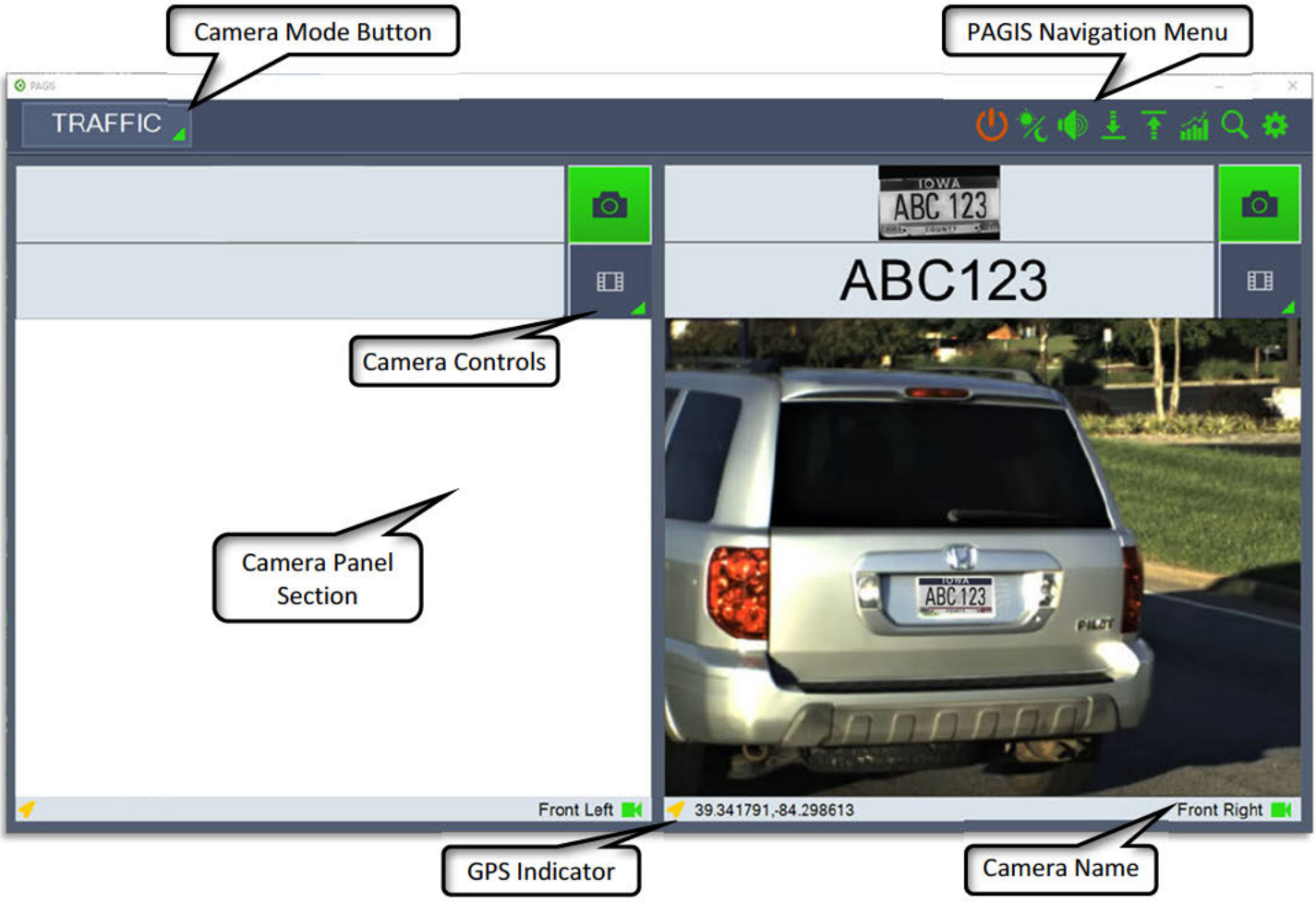
Upon a successful login, the user will see the Main screen (Live View). This is the default view and starting place of all PAGIS Software features. (NOTE: Access to features is based on user group rights established in BOSS.)

The Main Screen is also the place users will monitor read images and ALPR "hits". At the initial startup of the system it is normal to see only a blank/grey screen for a few seconds. Once a connection has been established with the mobile cameras, white boxes will be displayed showing the live-feed camera panels. At this point, the system is ready to capture reads/plates.

2.2.1 Getting Started in PAGIS

By default, PAGIS loads into a static view. This means live video will not automatically appear in the camera panels (white boxes) until a plate has be captured or the user selects one of the live feed options.

Once a plate is "seen" by a camera assigned to the current viewing mode (Traffic vs Parking), it will display the captured information in the corresponding camera panel. Each plate capture is also accompanied by a short "Beep" to audibly alert the user a read has taken place. (NOTE: If the user is in the Traffic Mode at the time a parking camera reads a plate, there will be a sound effect, but no plate image will be displayed on screen unless that plate is on a synchronized Hotlist or until the user switches to Parking Mode.)



2.3 The PAGIS Navigation Buttons

4172

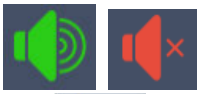
This section provides a quick reference guide to the available navigation buttons of the Live View screen.



The Camera Mode button is located in the upper left corner and is used to switch between the configured camera modes. Once configured, the name will change to a selected mode. The default values are “ALL”, “Traffic” and “Parking”.



The Logoff button is located in the upper right of the window. When selected, the user will be logged out of PAGIS and return to the login screen.



The Sound button is located to the right of the Logoff button. When selected, this button with toggle the PAGIS system sounds On and Off.



Day/Nite mode switches PAGIS between day & night mode screen skins.



The Begin Shift Synchronization button is located to the right of the Sound button. When selected, this will reach out to the BOSS server to download users, hotlists, and other system settings.



The End Shift Synchronization button is located to the right of the Begin Shift Button. When selected, this will upload any previously unsent reads, images, and audits to the BOSS server.



The Statistics/Review button is located to the right of the End Shift Button. When selected the user is able to review Databases/Hotlists, Reads, Targets, and other PAGIS information.



The Search button is located to the right of the Review Button. When selected the user can search his/her reads as well as manually add a license plate to a temporary hotlist.



The Admin/Settings button is located in the upper right corner of the screen. This button is only viewable to Admin level users and allows for system configuration changes and setup.



Firmware update icon will atomically appear when PAGIS detects a new firmware is available for the P720 mobile cameras. All user types are notified, but only Admins can apply the update.

2.3.1 Camera Control Buttons

The dual-lens cameras can capture both color and an infrared image. Formerly, there were a total of three buttons that allowed the user to view the IR and color feed as well as capture a picture directly from PAGIS. Now there is a toggle button to switch between color and IR views and a separate button to take a picture. These buttons are displayed on the main Live Screen as shown below:



The Camera View Selector button: This is the default state at login showing the Static View. (**NOTE**: PAGIS does not automatically display a life feed.)



Color View: by clicking on the Camera View Selector button once, the user will switch to the Color View Mode. This displays the current view of the color camera and will time out after 60 seconds.



IR View: by clicking on the Camera View Selector button twice, the user will switch to the Infrared (IR) View Mode. This displays the current view of the IR camera and will time out after 60 seconds.



The Take Pic button: Just above the Camera View Selector button is the “Take Pic” button. This button allows the user to quickly take a picture from the camera currently viewed.

2.3.2 GPS Indicators

4173

GPS is stamped on each read and hit as capture events take place by the system. The signal strength and location indicators are located underneath the camera panels at the bottom of the Live Screen.

39.341788,-84.298518 Shows an example of the Location Indicator displaying the Lat/Long on the most recent read

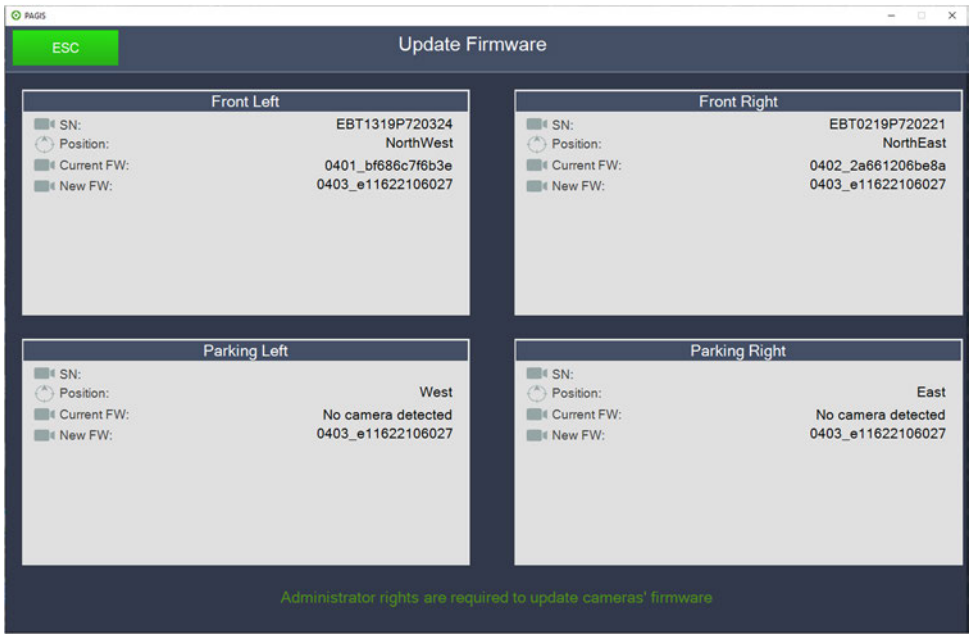
A green or yellow indicator shows a strong or medium strength GPS lock.

A red indicator shows there is no available GPS information.

2.3.3 Camera Firmware Update (Restricted Users)

Camera firmware update provides a means for PIPS to update the camera software to enhance and or correct camera performance. The frimware icon will only apper when update is avialable.

- The firmware update process only updates camera that are attached and function on the mobile processor.
- Restricted PAGIS users are only notified and displayed update information, only a PAGIS administrator can apply the FW update.

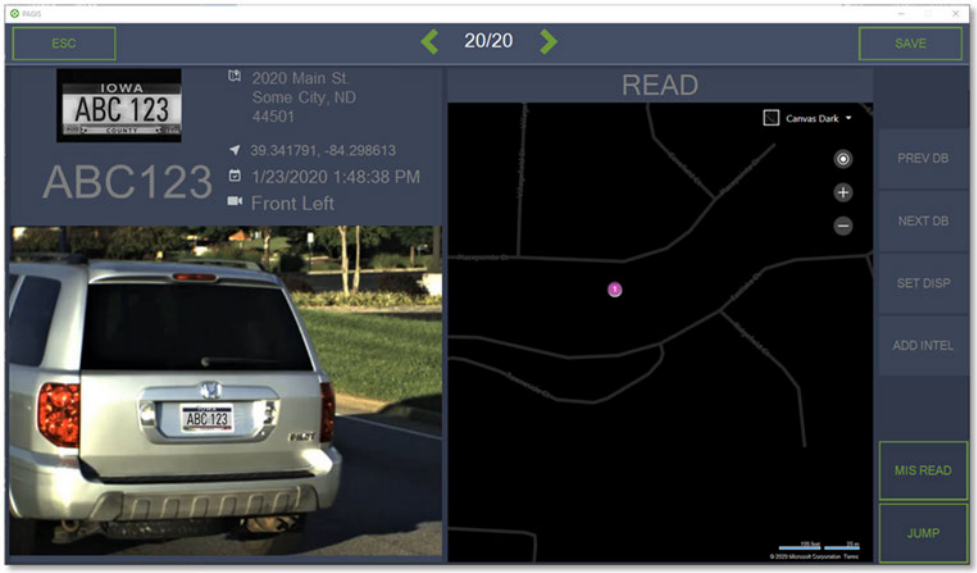


Firmware Updater Window List.

- Title “Camera Name”.
- Camera serial number.
- Position.
- Current FW version.
- New FW version available.

2.3.4 Day/Night Mode

Day/Night mode changes PAGIS user interface skins to a darker appearance to reduce illuminating the vehicle interior.



2.4 Begin Shift

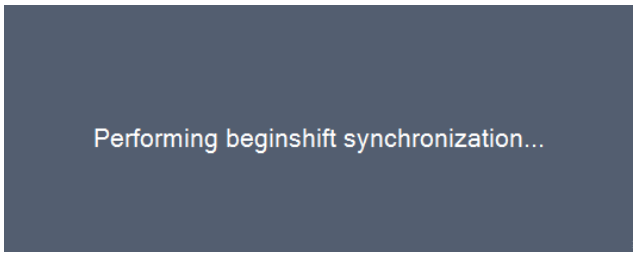
Begin Shift is thought of as the first step for all PAGIS users. From the Live View Screen, the PAGIS user must click the Begin Shift button twice. Once to select the function and once more to launch the Sync. With most agencies, this action utilizes a wireless network to import all the necessary data used during a shift (Hotlists, Dispositions, and Targets) directly from the BOSS Server. However, agencies can also configure their systems to perform this function via Thumb drive or a local source file.

2.4.1 Sync via USB Thumb drive (or Local Source)

Depending on the agency network, some alter the default PAGIS/BOSS configuration mode to use a USB Thumb drive or locally stored file on the MDC/Laptop instead of the wireless Sync. In order to synchronize effectively, the user must first confirm he/she has access to the source location before initiating Begin Shift. **NOTE**: All synchronizations using this method must be performed manually. To learn more about this process, refer to the "Client Tools" section of the BOSS Manual.

2.4.2 Sync via Wireless Network

Synchronizations over a wireless network provide the agency with additional automated features. Best practices recommend the user manually launch Begin Shift from the Live View Screen at the beginning of every patrol shift. However, it is possible for users to allow PAGIS to synchronize via its auto-sync settings. When a manual Begin Shift is launched, the Main View Screen removes the camera feeds and displays a status window of the Sync process. Once the Begin Shift operation is complete, PAGIS will return to the normal Main View Screen.





2.4.3 PAGIS Auto-Sync Settings

PAGIS auto-sync settings are best thought of as how PAGIS receives additional updates and maintains the downloaded ALPR data throughout the entire patrol shift. This prevents the need for the officer to manually perform Begin Shift functions multiple times a day. The auto-sync occurs every 30 seconds and receives data in small batches. The batches are not to exceed 1MB in size for every minute of download. In addition to receiving data, the auto-sync function also uploads a copy of data collected by PAGIS and sends it to BOSS for reporting/processing.

2.4.4 Begin Shift – Additional Information

By default, the synchronizations in PAGIS receive only what has been changed to the ALPR data since the last Sync. Meaning, if some plates have been removed from a Hotlist and others have been added, the system will only transfer that data instead of downloading the entire Hotlist each time the Begin Shift is launched. This helps to reduce the amount of data transferred over the agency's network. **NOTE**: Begin and End Shift synchronization, as well as all auto-sync features, are dependent upon stable communication to the BOSS server via an active data connection.

2.5 End Shift

End Shift in PAGIS is the process in which all the collected ALPR data (Reads, Hits, and Images) from the recent shift is uploaded to the BOSS server and cleared from the local cache. As with Begin Shift, the agency has two options. They can choose to Sync via USB Thumb drive or via wireless connection. Best practices recommend users perform an End Shift Sync at the end of every patrol.

2.5.1 Sync to BOSS

At the end of every shift, the accrued ALPR data should be exported to BOSS. Just like with Begin Shift, the user must click the button twice to launch it (once to select it and once more to execute the Sync). During the Sync, PAGIS uploads any Reads, Hits, and Images not already synchronized to BOSS and purges these items from the local cache on the MDC's hard drive. Completing an End Shift also removes any VLP entries manually added to PAGIS during the shift.

2.6 Cam Mode Button

Clicking the Cam Mode button in the upper left corner of the Live View Screen allows the user to cycle through the different camera modes configured by the PAGIS Administrator. Changing the camera mode changes which cameras are displayed on the Main Screen.

2.6.1 Camera Modes

By default, PAGIS provides "Parking" and "Traffic" as the two configuration modes. Users often switch these modes to suit their current use-case. For example, an officer in a parking lot will often switch the mode to "Parking" so s/he can see the parking cameras on the Live View Screen. They can then switch back to "Traffic" when monitoring city streets.

2.7 Taking a Picture

The PAGIS software has ability to quickly take a picture from one of the currently displayed ALPR cameras on the Live Screen. The user only needs to click on the Take Pic button.



To Take a Picture:

1. From the Live View Screen, press the Take Pic button from the desired camera
2. The image taken will be displayed
3. Enter a description of the picture in the text field at the bottom of the screen
4. Press Save to save the picture or Escape to cancel. Either action will return you to Live View.

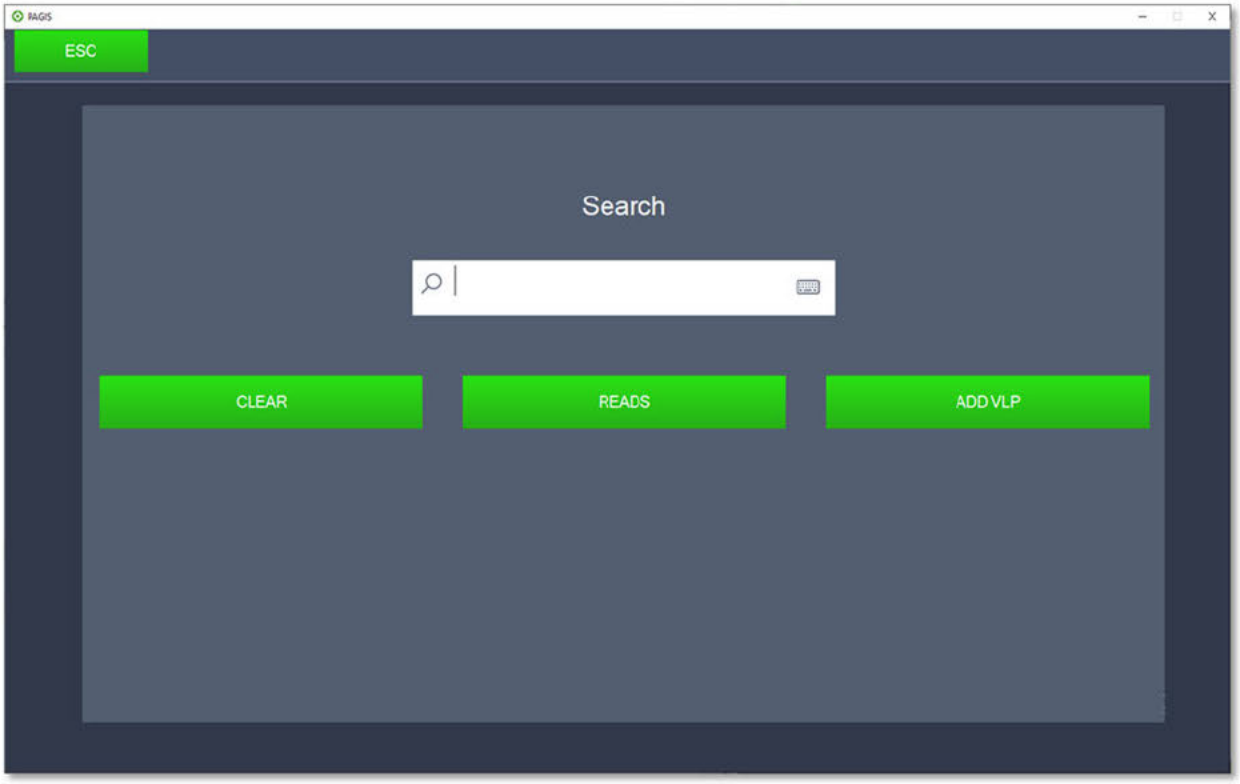
NOTE: The picture will Not be saved if a description/note is not entered in the text box.

To View the Saved Images:

1. Navigate to the Review menu in PAGIS
2. Select Audits
3. The user will be able to see a thumbnail of the image and the saved text/note
4. In order to review the saved images at a later time, the user will need to run the Audit Report from BOSS.

2.8 Search Entry Screen

Pressing the Search button icon from the Live View screen or SEARCH from the Databases window allows the user to search all manually entered plates as well as all BOSS synchronized databases (Hotlists) for license plate and target information. Users can also search all locally stored reads/images accrued since the last End Shift by clicking the Reads button instead of pressing the Enter key.



2.8.1 Searching Synchronized Hotlists for License Plates

By entering a vehicle license plate number (VLP) and pressing the Enter key or the ADD VLP button, the user can quickly search all the stored plate information locally collected as well as the information from all synchronized hotlists distributed from the BOSS server. **NOTE**: Hotlists can only be searched by entering complete VLPs. Wildcards and partial plate numbers will not return results.

Search Box: The text field used to enter the desired plate search via alphanumeric characters and/or wild card symbols.

Clear Button: Clears the contents of the search box.

Driver's License Info: The search field can also check the Hotlists for any DL information stored (Not available all countries).

Reads Button: This button searches for a match from all the reads/hits locally stored on the MDC/Laptop.

ADD VLP: Searches all locally stored hotlists for the plate and if there's no match, allows the user to add the plate to the "Manual Reports" alert list for use in the field. **NOTE**: All manual entries are cleared with each End Shift

ESC: The Escape button allows the user to exit to the Main/ Live View screen.

2.8.2 Searching Locally Stored Reads and Hits

As mentioned previously, this search function allows users to find reads and hits directly from their recent patrols using the search field and the Reads button. These searches pull only the reads and hits locally gathered/stored since the last time the user completed an End Shift. **NOTE**: The search results are specific to each Windows User Profile and do NOT pull images from the BOSS server.

2.8.2.1 Searching for a Match

4177

- From the Search field, users may enter a plate (or partial plate with wildcards) and then click the **READS** button.
- Results are displayed with the data gathered at the time the read was taken (See example below).
- Each result should display the infrared (IR) image of the plate as well as the color overlay of the vehicle for review.
- Each result shows the GPS data, Closest address point, Time and Date, and the Camera that read the plate.
- If there are multiple results, the user can cycle through them by clicking the left and right navigation arrows.



2.8.3 Wild Card Symbols

The use of wild card symbols in the Search box allows greater flexibility for the user, but may return a larger set of results.

- Wild card searches performed using the asterisk (*) designates an unknown number of characters.
- Wild card searches performed using the underscore (_) indicates a single missing or unknown character.
- Searches can be performed using one, both or no wild card symbols.

Example: The officer received an alert from Dispatch looking for a vehicle plate containing the letter J and the number 8 separated by one character. Because the officer doesn't know how many characters there are before or after the J and 8, he enters *J_8* in the search box to review all possible matches of J and 8 separated by only one digit.

2.8.4 Manually Adding a Plate to PAGIS

PAGIS allows users to manually add a plate of interest directly into the software as needed. Once saved, these entries are stored as part of the Manual Reports alert list and work just like any other Hotlist synchronized from the BOSS server.
NOTE: These additions are designed to be temporary and are cleared from the software with each End Shift.

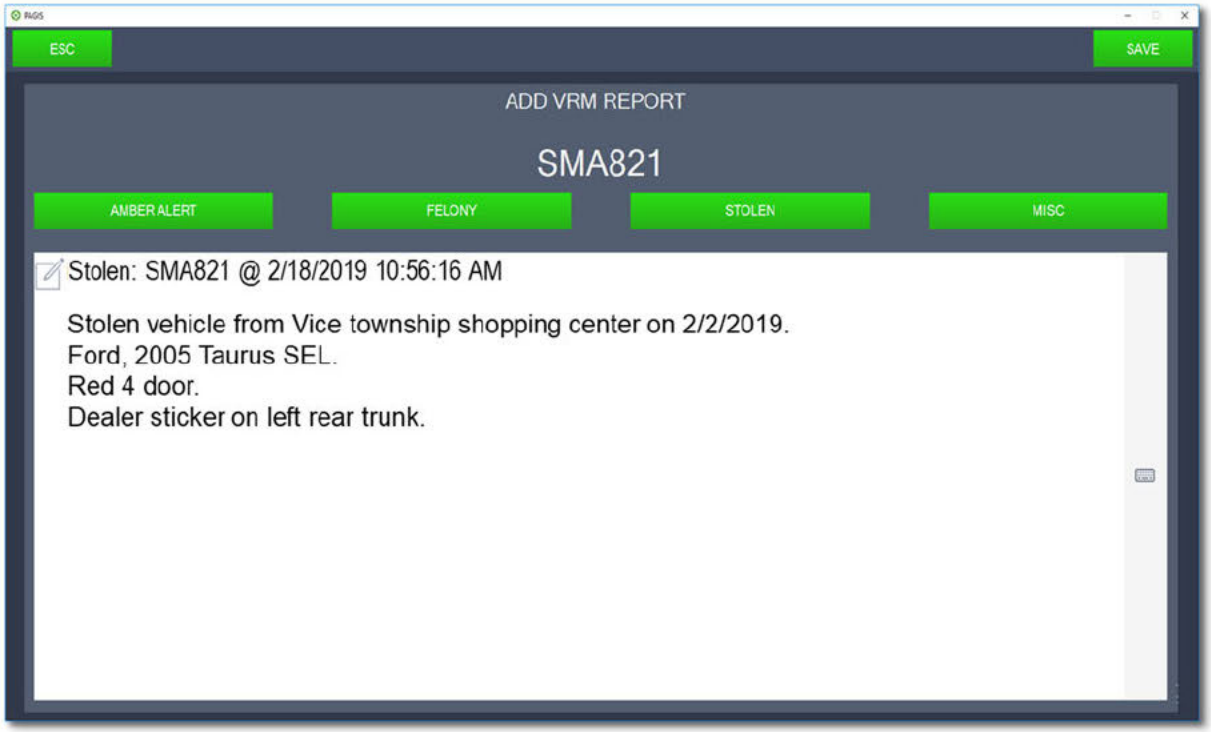
2.8.4.1 ADD VLP Query

Before an entry is added to the Manual Reports Hotlist in PAGIS, the software searches all stored databases for a match. If a match occurs, a message will display under the search box showing which Hotlist(s) it has been found in. If the VLP query does not return a match, the "ADD VRM REPORT" screen appears.



2.8.4.2 ADD VRM Report Screen

If the desired plate does not already reside in another Hotlist, the ADD VRM Report Screen becomes accessible to the user.



1. From the Search Entry Screen, enter the desired plate to add.
2. Click the ADD VLP button. If no match is found on any other hotlist, the "Add VRM Report" screen will appear.
3. Click to select the applicable alert type (AMBER ALERT , FELONY , STOLEN , or MISC)
4. Either leave the default information or add additional detail.
5. Click Save at the top right to add the plate to the Manual Entries Hotlist

2.9 The Review Screen

4179

PAGIS allows users to review all locally stored data from one easy location. Clicking the Review icon from the Main Screen launches Review. This screen is divided into the Summary View Chart and sub-section navigation buttons to the right.



2.9.1 Summary Review Section

The Summary View Chart is divided into five categories and allows a user to review the information collected during their shift at a glance.

Total Reads: Shows the total number of Reads/Hits synced to BOSS and the total number of reads captured during the shift.
Reads: Shows the total number of reads synced to BOSS and the total number of reads captured during the shift.
Hits: Shows the total number of hits synced to BOSS and the total number captured during the shift.
Misreads: Shows the total number of reads marked as a "misread" synced to BOSS and the total marked during the shift.
Audits: Shows the total number of audits synced to BOSS and the total number of audits during the shift.
Targets: Shows only the number of targets downloaded from BOSS.
(NOTE: The Sync value will always be zero for customers using Disk Sync mode/Client Tools.)

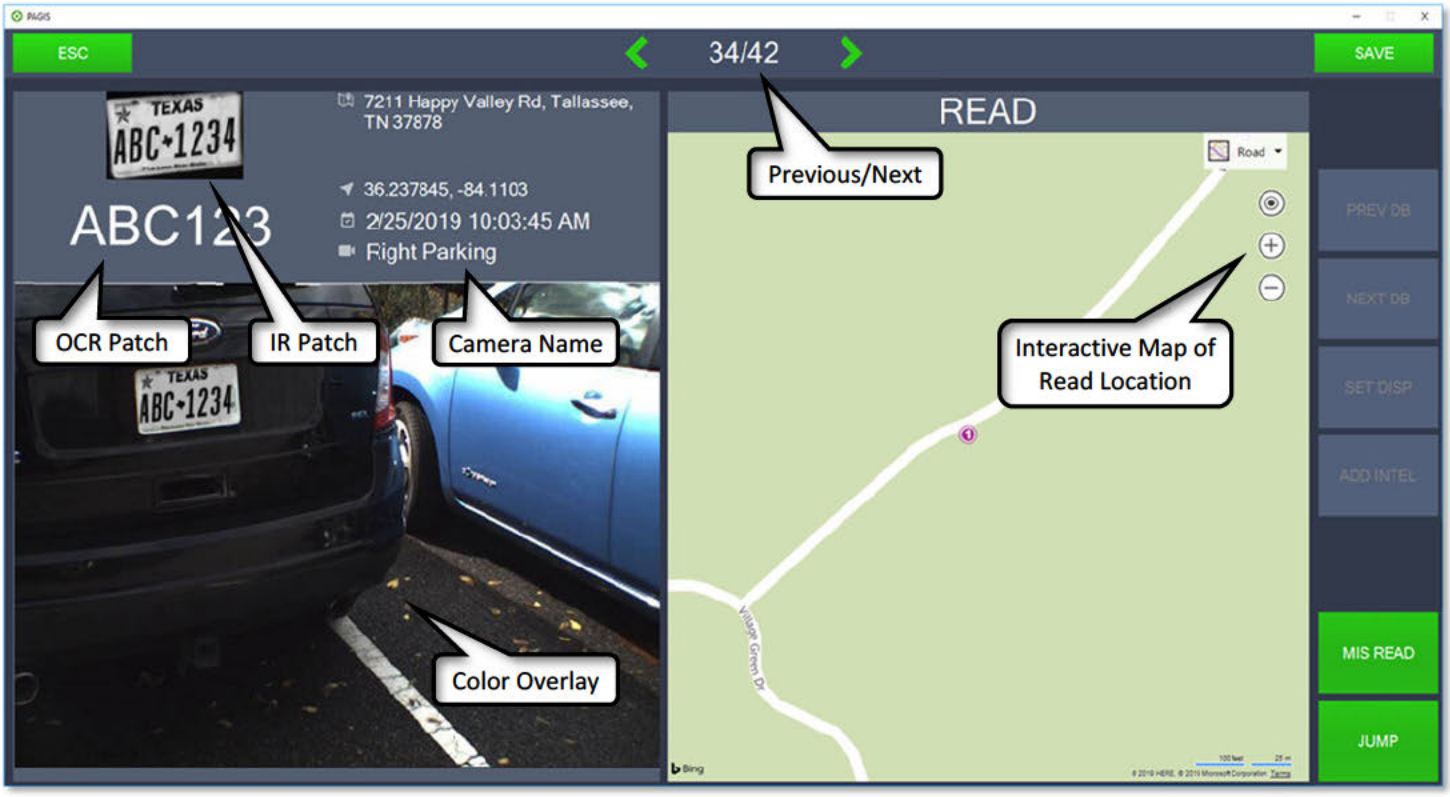
2.9.2 Review Navigation Buttons

The navigation buttons allow the user to review specific sets of information gathered during the shift.

Reads: Review all plate detections that have occurred since the last End Shift synchronization.
Hits: Review the hit alerts for Vehicle License Plate (VLP) reads that matched a Hotlist.
Misreads: Review reads and/or hits that have been manually flagged during the shift as misreads, where the plate number in the image does not match the OCR interpretation of the plate (e.g., a letter O misread as a Q or zero).
Audits: Review failed and successful logons, any manual data entered during the shift, pictures taken and all manual license plate searches.
Targets: Review targets that have been synchronized/downloaded from Boss.
Databases: Review all the Hotlists currently distributed to this PAGIS laptop/MDC.
Esc: Returns the user to the previous screen.

2.9.3 Reads

From the Main Screen, the user can review his or her accumulated Reads (those gathered since the last End Shift was completed) by clicking on the Review icon and then selecting the Reads Navigation button. The Read Review Screen is divided into two main sections. The left side displays the information gathered at the time of the read and the right side displays an interactive map of the GPS location.



NOTE: Buttons that are greyed out indicate options that are not available in the current view. For example, the Reads and Hits review screens share the same layout but different on-screen options.

2.9.3.1 Reads Result Screen Navigation Buttons



Read Count: The left number is the current record. The right number is the total available for review.

Next/Previous button: The arrows on either side of the read count allow the user to navigate back and forth to review reads/results.



MisRead button: When the button is green it indicates the record has NOT been edited as a Misread by a user. Once a Misread is saved, this button will turn grey and the record title will update.



Jump button: Allows the user to "jump" to a specific record without the need to navigate one record at a time using the Next/Previous buttons.



Save button: Apply any changes/edits and return to the Main Screen.



Escape button: Returns the user to the Main Screen.

2.9.3.2 Interactive Buttons – Reads Screen

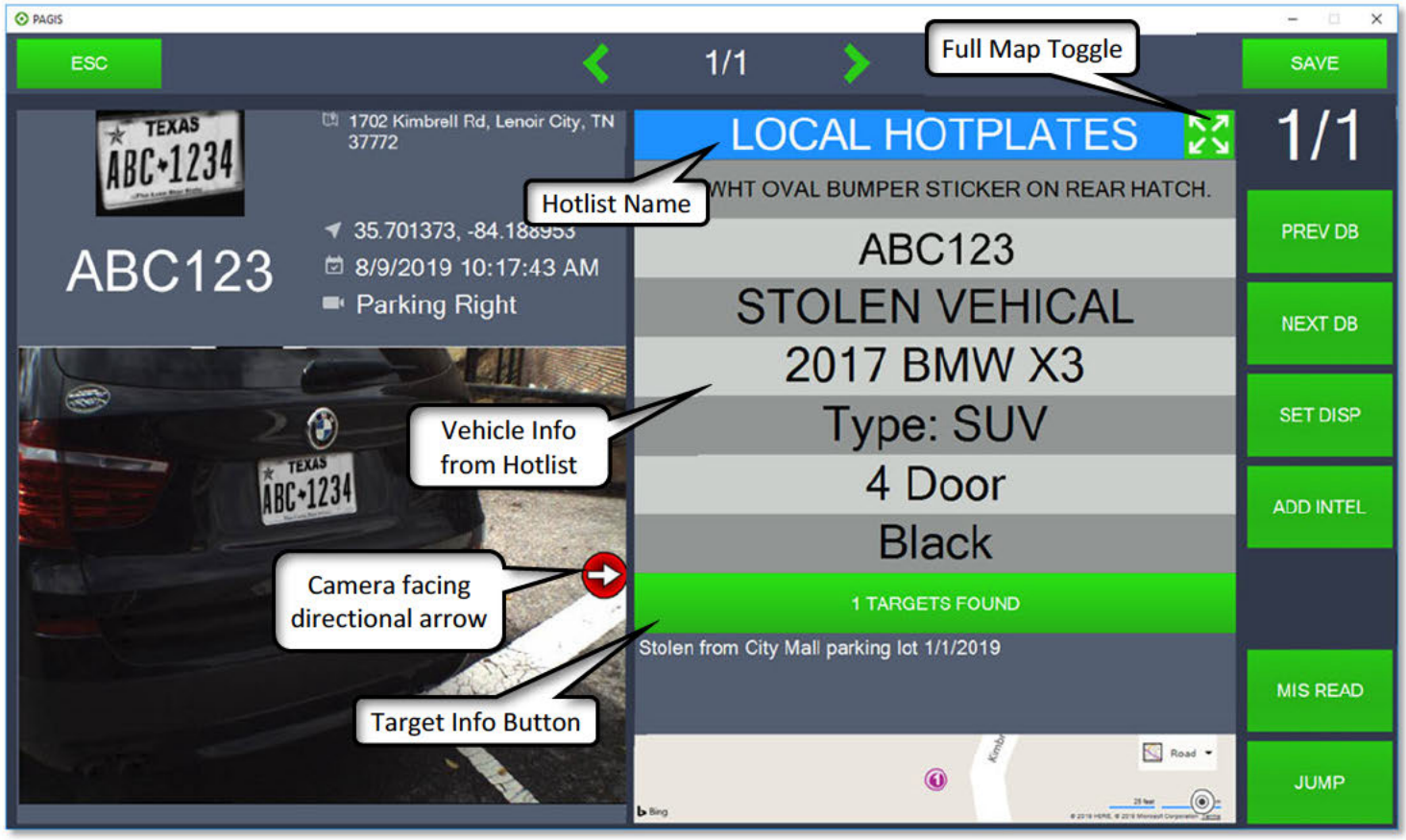
From the Reads Review, the user can interact with the following:

- IR Patch: The user can click on the IR "Patch" plate image to open a full-screen view.
- OCR Patch: The user can click on the OCR "Patch" image to edit the license plate number if necessary/Misread.
- Color OV Image: The user can click on the color image to open a full-screen view.
- Map: The user can manipulate the interactive map of the read location (Map Type, Scroll, and Zoom).

2.9.4 Hits

Users can manually access the Hits Section by first selecting the Review icon from the Live View Screen and then clicking the Hits Button. The Hits Screen is also divided into two main sections. The left side displays the information gathered from the ALPR equipment during the read. And the right side displays the information provided by the associated alert list.

NOTE: Each time a VLP matches a Database value (a license plate read by the system matches a Hotlist entry), PAGIS plays an audible tone and automatically displays the Hit Screen to alert the user.



2.9.4.1 Hit Screen Attributes

Hit Count and Navigation Buttons: Displays the total Hit count as well as the Next/Previous navigation buttons.
IR Patch Image: A thumbnail image of the license plate from the IR camera.
OCR Text: The character string the OCR engine generated from the current plate.
GPS Location: The GPS coordinates at the time of the hit. (If a GPS device is not attached, the Lat/Long is displayed as 0,0).
Date and Timestamp: The date and time when the read/hit was captured.
Overview Image: The overview image of the vehicle from the Color Camera. (**NOTE**: Color images require visible light)
Camera Name: The name of the camera that captured the read ("Right Parking" in the screenshot).
Hotlist Name: This is the name of the Hotlist or "Database" where the plate was matched.
Target Button: When available, this indicates a person of interest is associated with the Hit and opens the Targets Screen.
Vehicle Information: The area of grey bars will display the related vehicle information from the Hotlist. Any information added manually by the user will appear in the Text Box near the bottom of the screen.
Interactive Map: Shows the location the Hit took place. Users can access full-screen view by clicking the map or the toggle .

2.9.4.2 Hit Screen Function Buttons



The Hit Count Indicator: shows how many Hotlists the current Hit has registered against.



Previous DB button: This button moves the user to the previous Database/Hotlist that produced a Hit.



Next DB button: Pressing this button moves the user to the next Database/Hotlist that produced a Hit.



The Set Disposition button: prompts the user to report the disposition of the hit by selecting one of the approved codes assigned in BOSS by the Administrator.



The Add Intel button: allows the user to add additional information regarding the current Hit.



The Misread button: allows the user to flag the Hit as a misread.



The Jump button: Allows the user to "jump" to a specific Hit instead of navigating one at a time.

2.9.4.3 Interactive Buttons – Hits Screen

- IR Patch: The user can click on the IR "Patch" image to open a full-screen view.
- OCR Patch: The user can click on the OCR "Patch" image to edit the license plate number if necessary/Misread.
- Target Button: Shows associated person(s) of interest and opens the Targets Screen.
- Color OV Image: The user can click on the color image to open a full-screen view.
- Map: The user can manipulate the interactive map of the read location (Map Type, Scroll, and Zoom).

2.9.4.4 Set Disposition – Additional Detail



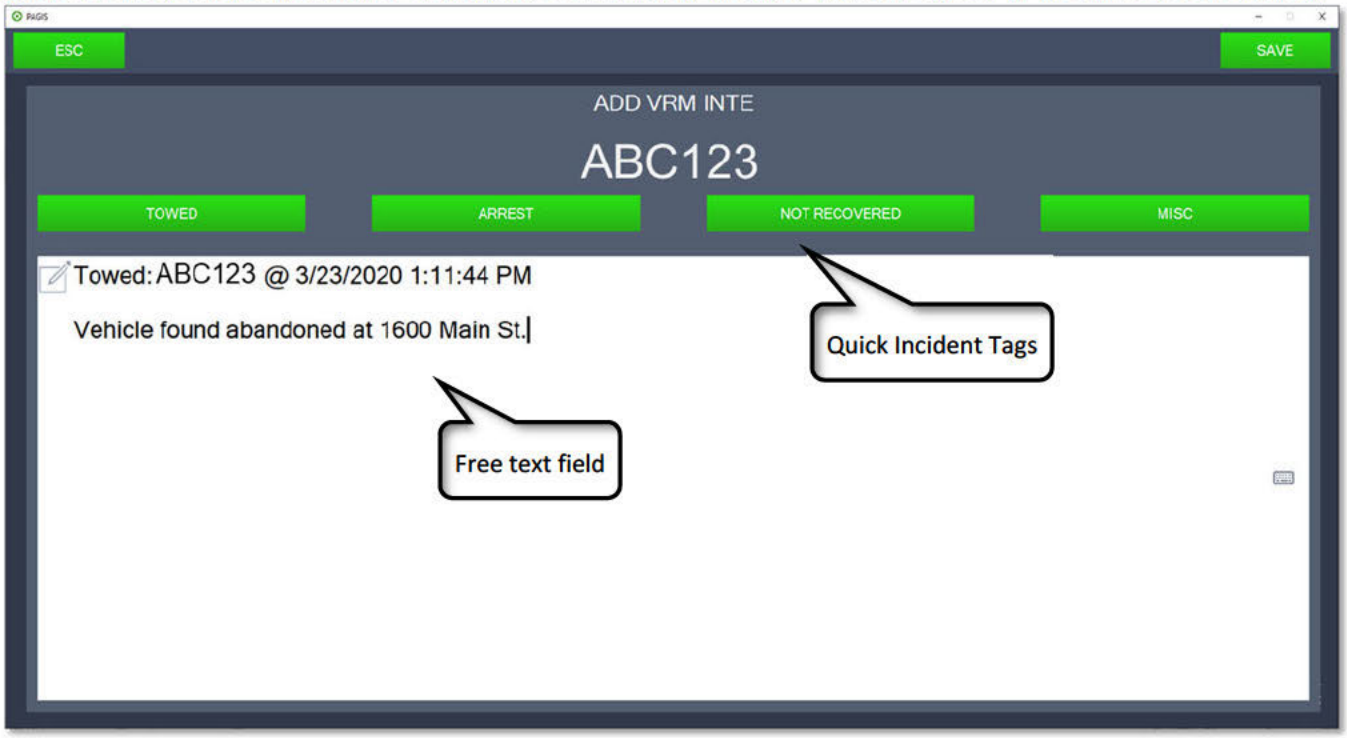
PAGIS allows for additional information to be added to a record in the form of a Disposition. Once Hits are flagged with a disposition code, the Agency is capable of running a "Reads Statistics by Disposition Report" in BOSS. Thus, providing valuable metrics and understanding to leadership in regard to their ALPR Enterprise.

When the "Set Disp" button is selected, the user is prompted to choose from a list of predefined values set by the Agency/BOSS Administrator. Once a disposition is selected and Saved, the disposition is reported to BOSS and will also show up in the Hits Review Screen text box in PAGIS on the next alert notification.

2.9.4.5 Add Intel – Additional Detail

4183

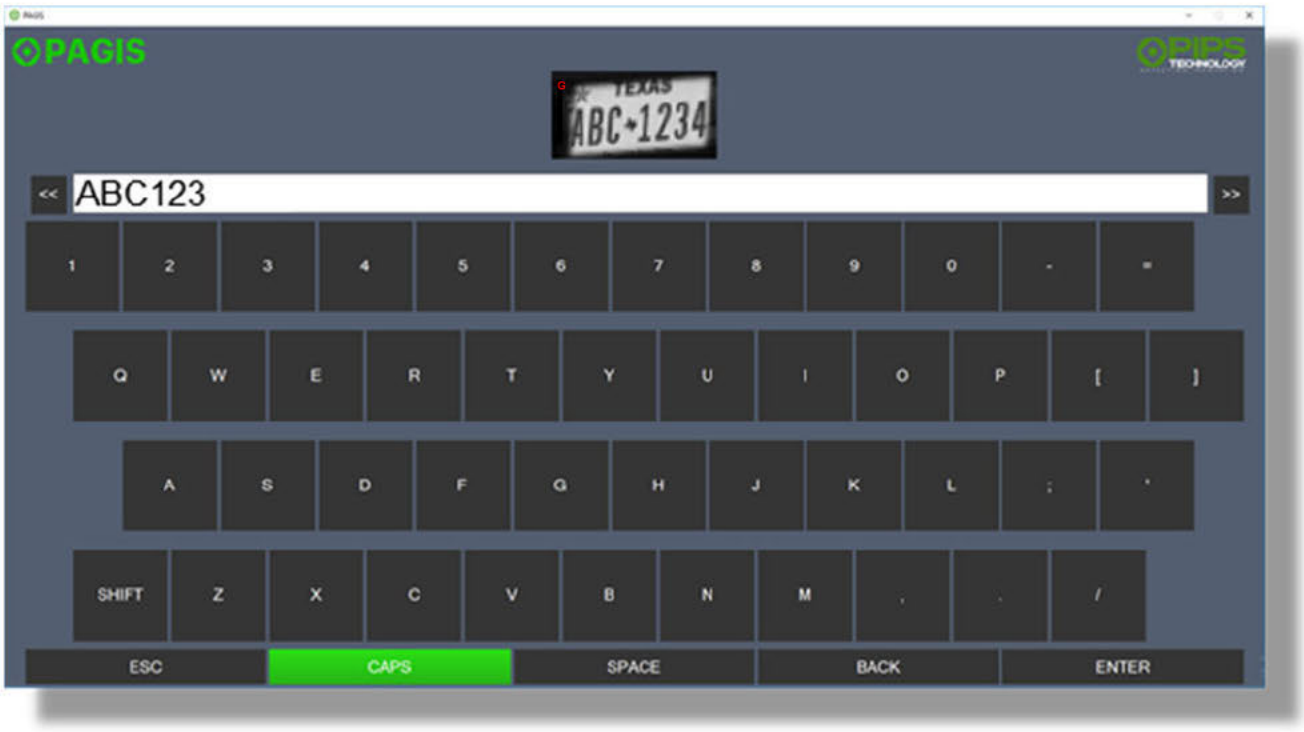
The Add Intel button launches the Intel screen. The user is prompted to assign one of four values: Towed, Arrest, Not Recovered, and Misc. by clicking the associated button at the top of the screen. The user may also enter additional detail regarding the license plate/vehicle. After clicking the Save button, the intel will now appear in the Hits Screen text box.



2.9.5 Misreads

PAGIS allows the user to mark Reads and Hits with incorrect OCR translations as a Misread. This is most commonly done by Agencies for Hits only as users typically don't have time to review every single Read from their shift. Once an errant Hit is corrected, the system updates the record to show it as a Misread and thus improves Agency Hit Reporting.

Correcting a plate read can be accomplished by clicking on the "OCR Patch" in either the Hits or Reads review screen. When the user clicks on the OCR Patch, the OCR Edit Screen opens and allows the user to update the Vehicle License Plate (VLP) data.



2.9.5.1 Marking a Record as a Misread:

The user can mark a record as a Misread from both Reads or Hits Review Screen. Each user can either simply flag the record as a Misread or update the OCR Patch information. **NOTE**: This ability is only available until the user has performed an End Shift function.

Manually Flagging a Read or Hit as a Misread:

1. Navigate to either the Reads or Hits Review Screen
2. Click on the Misread button on the Right
3. Click Save
4. Take note that the record title has now changed from “Read” to “Misread”

Updating the Read/Hit OCR Patch:

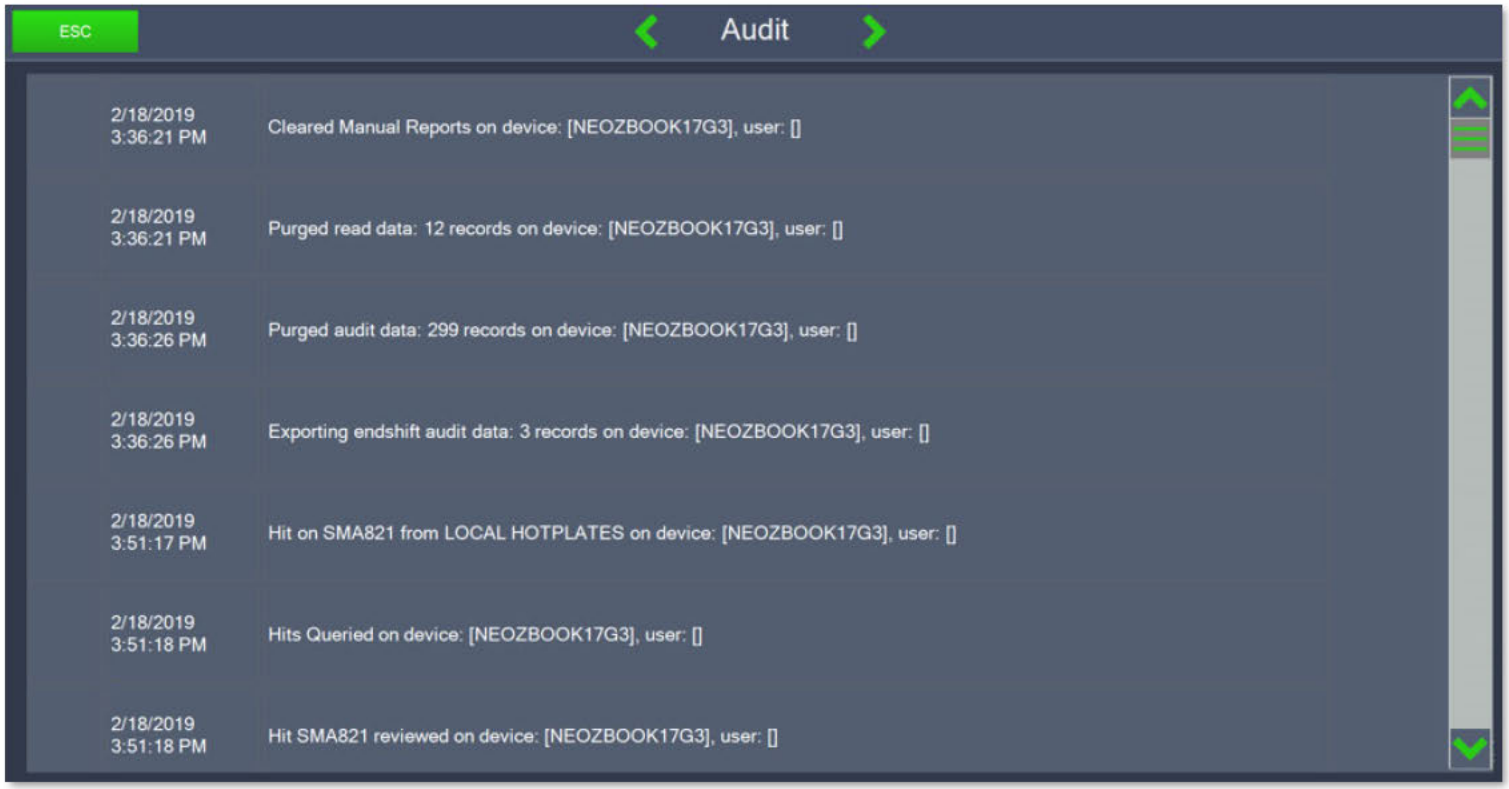
1. Navigate to either the Reads or Hits Review Screen
2. Click on the OCR Patch (Text just under the IR Plate Image)
3. Use the keyboard or on-screen keypad to update the Vehicle License Plate Number
4. Click the Enter Button to Save the changes (and exit back to the Review Screen)
5. When the user saves the changes to the OCR Patch, the record (Read/Hit) is automatically flagged as a Misread

2.9.6 Audits

4185

PAGIS logs both user and key system activity during each use of the software. The audit log captures various information like Read searches, synchronizations, hits, and user login attempts. The Audit Report is viewed in PAGIS by navigating to the Review section and selecting “AUDITS”.

NOTE: Performing an End Shift or syncing the database clears the current log.



2.9.7 Targets

PAGIS has the ability to display information regarding Persons of Interest in response to a Hit alert. Targets are created by BOSS/Hotlist Administrators, and typically provide detailed information about owners of a registered vehicles. When configured, Target data is always linked to unique VLP data (a specific License Plate). If PAGIS registers a Hit on a Plate with a target ID, the Target Information Button is displayed in the Hit Alert window and allows the user to access the Target Screen.



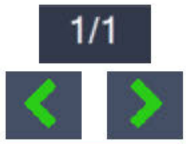
2.9.7.1 The Targets Screen

When a PAGIS user clicks the Target Information Button from a Hit Alert, the Targets Screen opens. This screen displays the information from the BOSS server about the Person(s) of Interest matched to the Hit (license plate).



2.9.7.2 Targets Screen Navigation Buttons

If a Hit alert has more than one Target associated with it, the PAGIS user can navigate all Target information with the buttons described below:



Target Count: The left number is the current record. The right number is the total available for review.

Next/Previous button: Arrows on either side of the target count allow the user to navigate back and forth to review the various targets.



Jump button: Allows the user to "jump" to a specific record without the need to navigate one record at a time using the Next/Previous buttons.

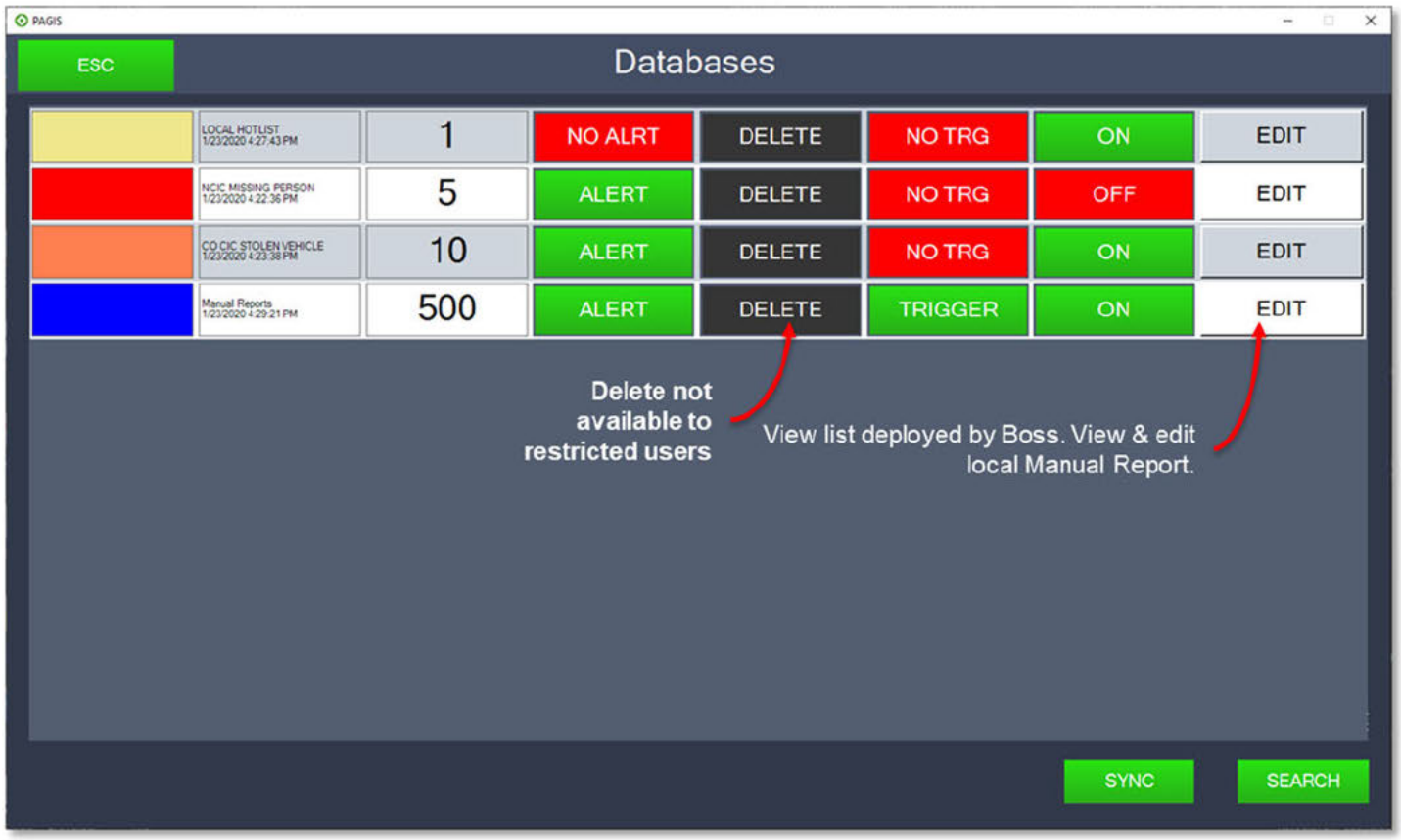


Close button: Returns the user to the previous screen.

2.9.8 Databases

Users can review Hotlists in PAGIS by navigating to the Review section and selecting "DATABASES" on the right. From the Databases Screen, users can toggle Hotlists functions On and Off based on their rights.

NOTE: User rights and Hotlist attributes are configured in BOSS.



2.9.8.1 Databases Screen Functions

Hotlist Color Code: The color attributed to each Hotlist by the BOSS Administrator.

Hotlist Name: The name of the Hotlist given by the BOSS Administrator. Also shows the time/date of the last synchronization.

Hotlist Priority: The priority of the Hotlist assigned by the BOSS Administrator. The lower the number between 1 and 999, the higher the priority. If a plate resides on multiple Hotlists, the list with the higher priority will be displayed first.

Alert Button: Toggles audible alerts On and Off for each Hotlist until the next synchronization.

Delete Button: Based on user rights, allows the user to temporarily delete a Hotlist from PAGIS until the next synchronization. To delete a hotlist, the user must click the button twice (it turns green and then deletes the list).

Trigger Button: Toggles external triggers On and Off. An example of an external trigger is a light bar.

On/Off Button: Disables and enables each Hotlist (each Hotlist is set to On by default).

Edit: View and edit localy created hotplates with a given hotlist, Hotlist/Hotplates deployed via BOSS can only be viewed.

NOTE: Hotlist settings altered in PAGIS will be reset to their default configuration during the next Sync or End Shift. The default configurations are assigned by the BOSS Server/Administrator.

2.9.8.2 Databases Screen Navigation Buttons

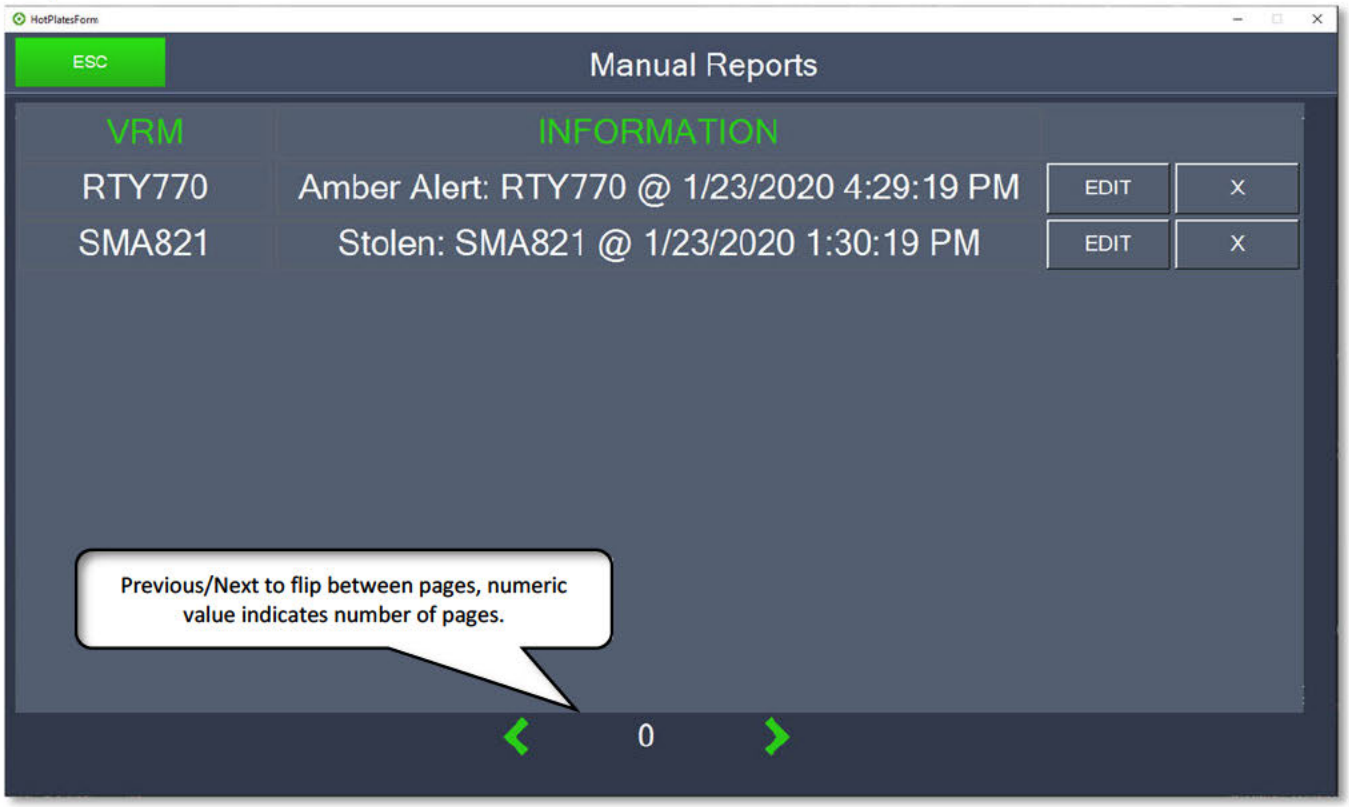
SYNC — **Sync button**: Synchronizes PAGIS with the BOSS server in order to update the Hotlists.

SEARCH — **Search button**: Open the Search Entry Screen (See section 2.8 for more information).

2.9.8.3 Databases Edit- “Manual Reports”

Editing Hotlist has two function based on origin of hotlist.

- Hotlist deployed to PAGIS via BOSS cannot be edited, only the hotplates list can be viewed. Editing/updates are indented to be managed via BOSS.
- Hotlist created in PAGIS, i.e. “Manual Reports” can be managed by PAGIS users, allowing for changes or deletion of the hotplates contained within the hotlist.



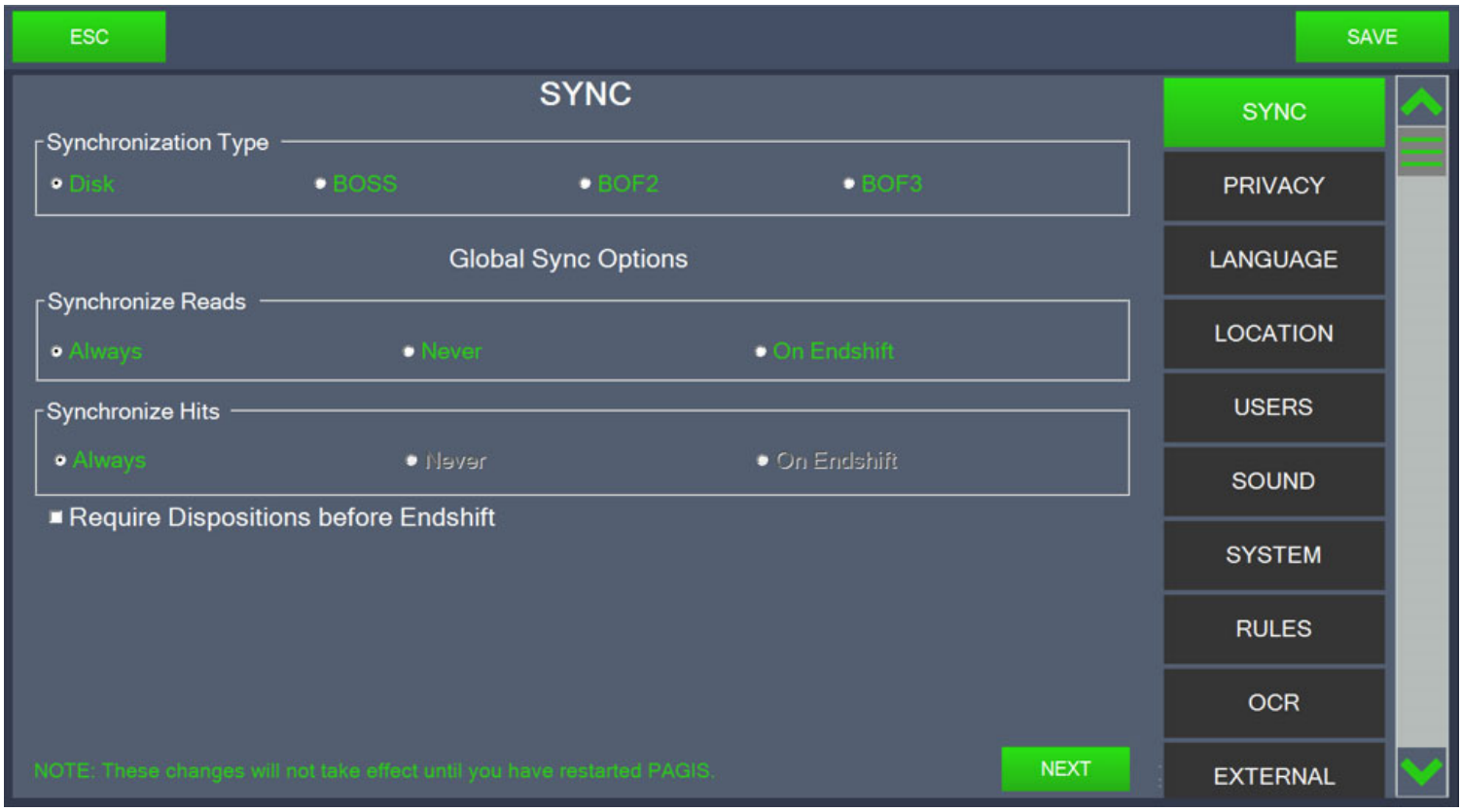
EDIT Button: Make changes to the indicustly hotplate information including licanse plate nuamber.
X Button: Remove indivualy hotlist from hotlist.
Previous/Next Button: Scroll thought lising of hotplates contaned within the hotlist. The numeric value indicates the number of pages.

ADMIN SETTINGS

The Settings Menu is the central location for configuring PAGIS Software functions endpoint by endpoint. Users with Admin level rights in PAGIS can see and click on the Settings Button from the Live View Screen. Launching Settings opens the menu to the Sync Options Screen by default. **NOTE**: Users without Admin level access will not see this icon on the Live View Screen.

3.1 Sync Options Screen

As mentioned previously in sections 2.4 and 2.5, PAGIS uses various sync options to store, update, and synchronize ALPR data to and from the BOSS server. On the Sync Screen, Administrators configure the synchronization method and options.
NOTE: Configuration changes will not take effect until they are saved and the PAGIS Software has been restarted.



3.1.1 Synchronization Types

- **Disk**: Uses local storage of Sync files in conjuction with a USB flashdrive to manually Sync to and from BOSS.
- **BOSS**: Uses a wireless data network to Sync files to and from the BOSS server.
- **BOF2**: Used predominantly in Europe (see regional guide for support).
- **BOF3**: Used predominantly in Europe (see regional guide for support).

3.1.1.1 Synchronization to Disk (Local Storage)

4190

Sync to Disk is a manual two-part process most commonly used with a USB Thumb drive. To use Begin Shift, the user accesses a centralized terminal (Ex. Patrol Room PC) to download the files from BOSS and then inserts the Thumb drive in the laptop to perform Begin Shift. At the end of the day, the user then Performs End Shift from the laptop/MDC connected to the Thumb drive and uploads those files to BOSS via the central terminal (See the "Client Tools" section of the BOSS Manual).
NOTE: From the Sync Menu, select "Disk" and click the Next button at the bottom to configure the drive location.

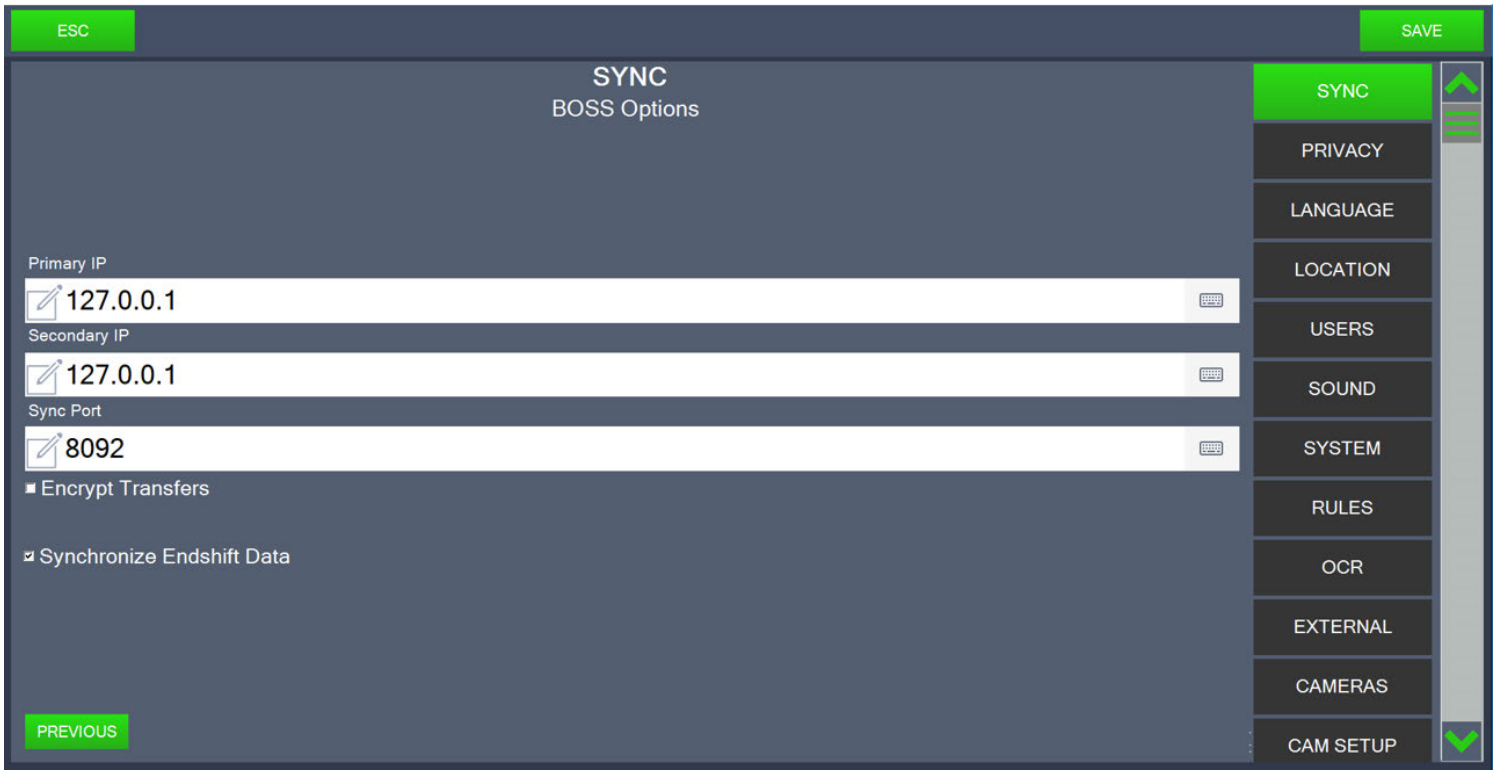


- **Delete Beginshift Data on Sync**: The sync folder on the Flash Drive is deleted once all Begin Shift data has been imported to PAGIS. This is on by default to help prevent false alerts.
- **Encrypt Endshift Data**: All uploaded End Shift data created in PAGIS is encrypted. This is off by default.
- **Copy Endshift Data on Sync**: If unchecked, no End Shift data will be transferred from PAGIS to the Drive location.
- **Keep Only Updated Databases**: Removes any Hotlists from PAGIS that were not updated during Begin Shift as "outdated". This is off by default.

Sync to Disk Setup:
In the text box, enter the drive path or letter to be used with Disk Sync. Folder name is not required as PAGIS creates the required folder(s). Once entered, select the desired options and then click the Previous button. Click Save to retain the settings.

3.1.1.2 Synchronization with BOSS

Sync to BOSS is a streamlined method for updating ALPR data to the field units and the server. Additionally, selecting this option enables the PAGIS auto-sync features that synchronize data throughout the shift without user involvement. However, this does require a stable data connection as well as some network configuration before it can be utilized.



Sync to BOSS Screen:

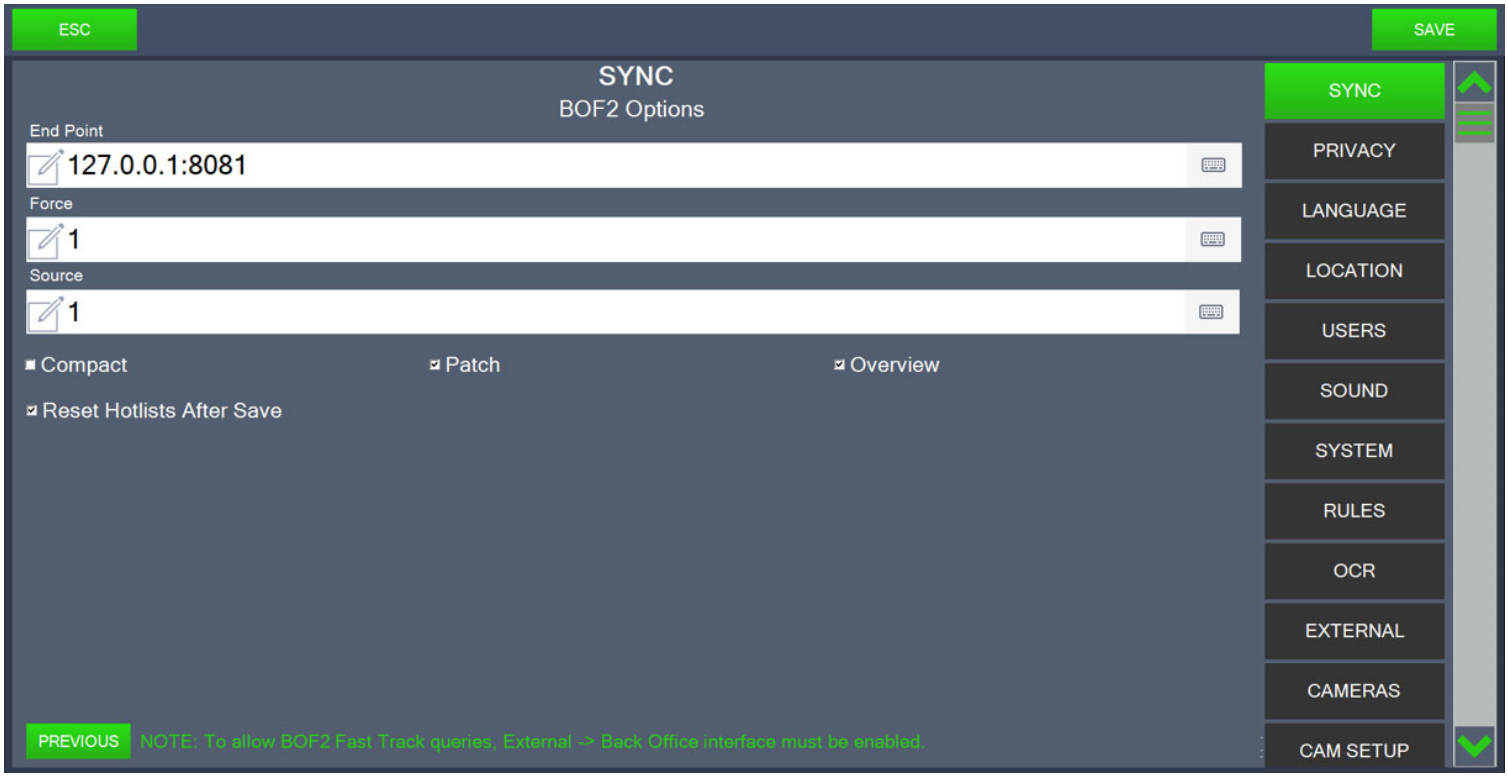
- **Primary IP**: The IP address of the BOSS server. This can also be the DNS name (**NOTE**: using DNS adds an additional failure point via the Domain Controllers and is not recommended as the best option).
- **Secondary IP**: Used for a secondary IP in cases where users switch from a cellular network to a Domain APN thus routing to BOSS from either an internal or external IP. This field can be left blank or with the primary IP as well.
- **Encrypt Transfers**: When enabled, data transfers to BOSS will be encrypted.
- **Synchronize Endshift Data**: On by default, this enables PAGIS to sync to BOSS when End Shift is performed by the user.

Sync to BOSS Prerequisites:
To establish the wireless sync to BOSS, the Agency Network Administrator will need to open TCP 8092 to the BOSS server as well as define the internal and/or external IP address(es).

Sync to BOSS Setup:
From the Sync Settings Menu, the Admin must select the BOSS option and click the Next button. Then s/he will update the Primary and Secondary IP fields as necessary and de/select any options. Once configured, click the Previous button and then click Save to retain the changes. (For more information on PAGIS Auto-Sync settings, refer to section 2.4.3)
NOTE: After synchronizing to BOSS, data is flagged in the database to prevent duplicate values on future synchronizations.

3.1.1.3 Sync to "Instation" (Formerly BOF2 and BOF3)

The Instation software was formerly known as BOF2 & BOF3 and was developed by Anite PLC. It is a web-based Back Office software suite used in European markets to provide similar features as the PIPS BOSS server and UI Client.
NOTE: These options are NOT used in the Domestic United States.

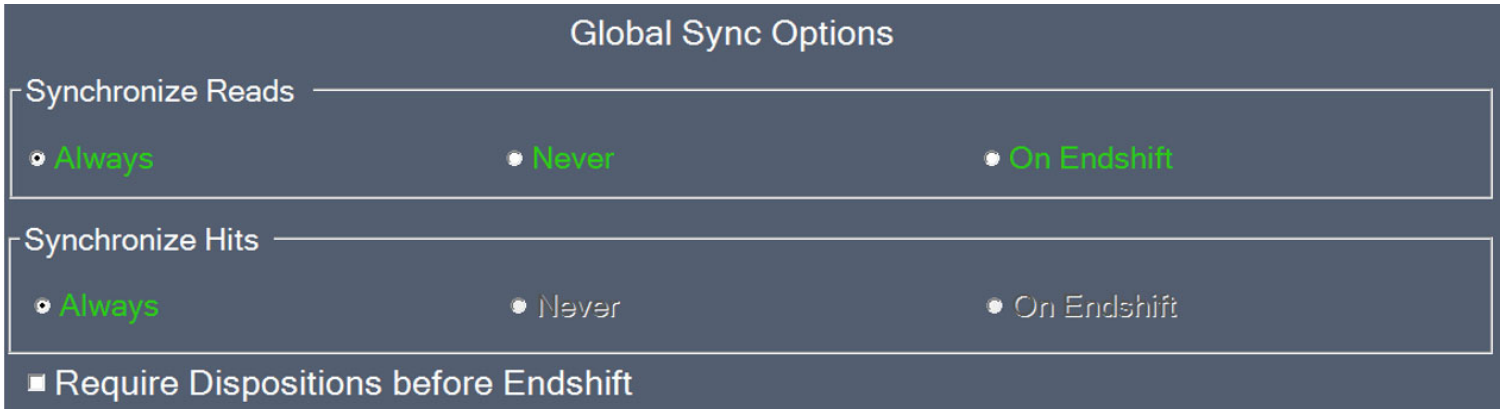


- **End Point**: The IP Address of the Instaion website. Format must be [IP Address:Port]
- **Force/Source**: Unique codes assigned to each police force.
- **Compact**: This option minimizes data transfer to Instation. Images will be deselected by default when in use.
- **Patch**: Refers to the image of the plate pulled from the read. This is on by default.
- **Overview**: Refers to the color overlay image from the read. This is on by default.
- **Reset Hotlists After Save**: When the software syncs to Instation, this will reset the hotlist tracking.

3.1.2 Global Sync Options

4192

Global Sync settings control how PAGIS synchronizes ALPR data during Begin and End Shift cycles and applies to both manually launched synchronizations as well as Auto-Sync functions. The two sections are Synchronize Reads and Synchronize Hits.



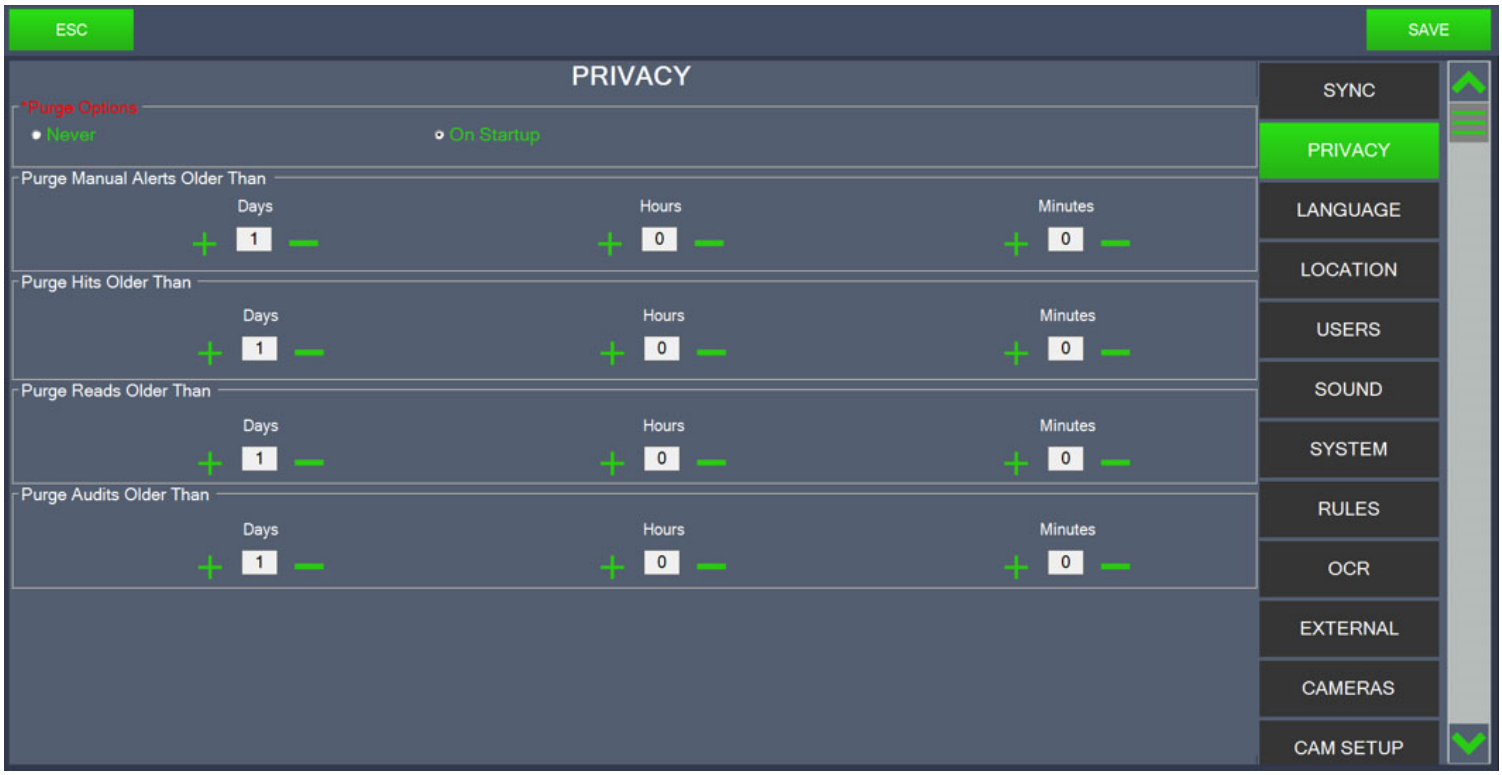
NOTE: All Hits are Reads, but not all Reads are Hits. A "hit" is a read that coincides with an Alert List. Due to this, the Options selected in the "Synchronize Reads" section dictate what options are available in the "Synchronize Hits" section. Unavailable options are greyed out.

- **Always**: Reads and Hits are synchronized to BOSS as close to real-time as the data network and PC processing allow.
- **Never:** The information gathered during the shift will be "sanitized" with each launch of End Shift. The corresponding data and images will NOT be sent to the BOSS server.
- **On End Shift**: Synchronization to BOSS will only occur when the user manually launches End Shift.
- **Require Dispositions before Endshift**: Requires the user to select a disposition code for each Hit registered in the PAGIS software since the last End Shift was completed before the Synchronization is processed.

3.2 PAGIS Privacy Settings (Local Data Retention)

4193

Although most commonly configured in BOSS, the PAGIS Software allows the Admin to configure the data retention settings for the local endpoint by minutes, hours, or days. This feature ensures the data captured/stored on the MDC is sanitized by the software itself (this is important for customers without BOSS). **NOTE**: To enable the Privacy settings, the Admin must select the "On Startup" purge option and then set at least one value in each row. Rows left with all Zero will not be sanitized or purged.



- **Never**: Selected by default, this option disables the PAGIS privacy settings and uses only those set in BOSS.
- **On Startup**: This option must be selected in order to enable the PAGIS privacy settings. Once enabled, PAGIS looks to purge/sanitize the system each time it's launched or restarted.
- **Purge Manual Alerts Older Than**: Controls how frequently all of the Databases/Hotlists in PAGIS are purged. The purge rate is calculated from the timestamp of the Hotlist. Once the retention value is surpassed, the Hotlist is deleted. Hotlists distributed from BOSS will be re-downloaded on the next Sync.
- **Purge Hits Older Than**: Controls how frequently all Hits in PAGIS are purged. The purge rate is calculated from the timestamp of read. Once the retention value is surpassed, the Hit is removed the next time PAGIS is restarted.
- **Purge Reads Older Than**: Controls how frequently all Reads in PAGIS are purged. The purge rate is calculated from the timestamp of read. Once the retention value is surpassed, the Read is removed the next time PAGIS is restarted.
- **Purge Audits Older Than**: Controls how frequently all Audits in PAGIS are purged. The purge rate is calculated from the timestamp of audit. Once the retention value is surpassed, the audit is removed the next time PAGIS is restarted.

NOTE: Once the hits, reads, databases, or audits have been purged, they can no loner be viewed in the PAGIS software.

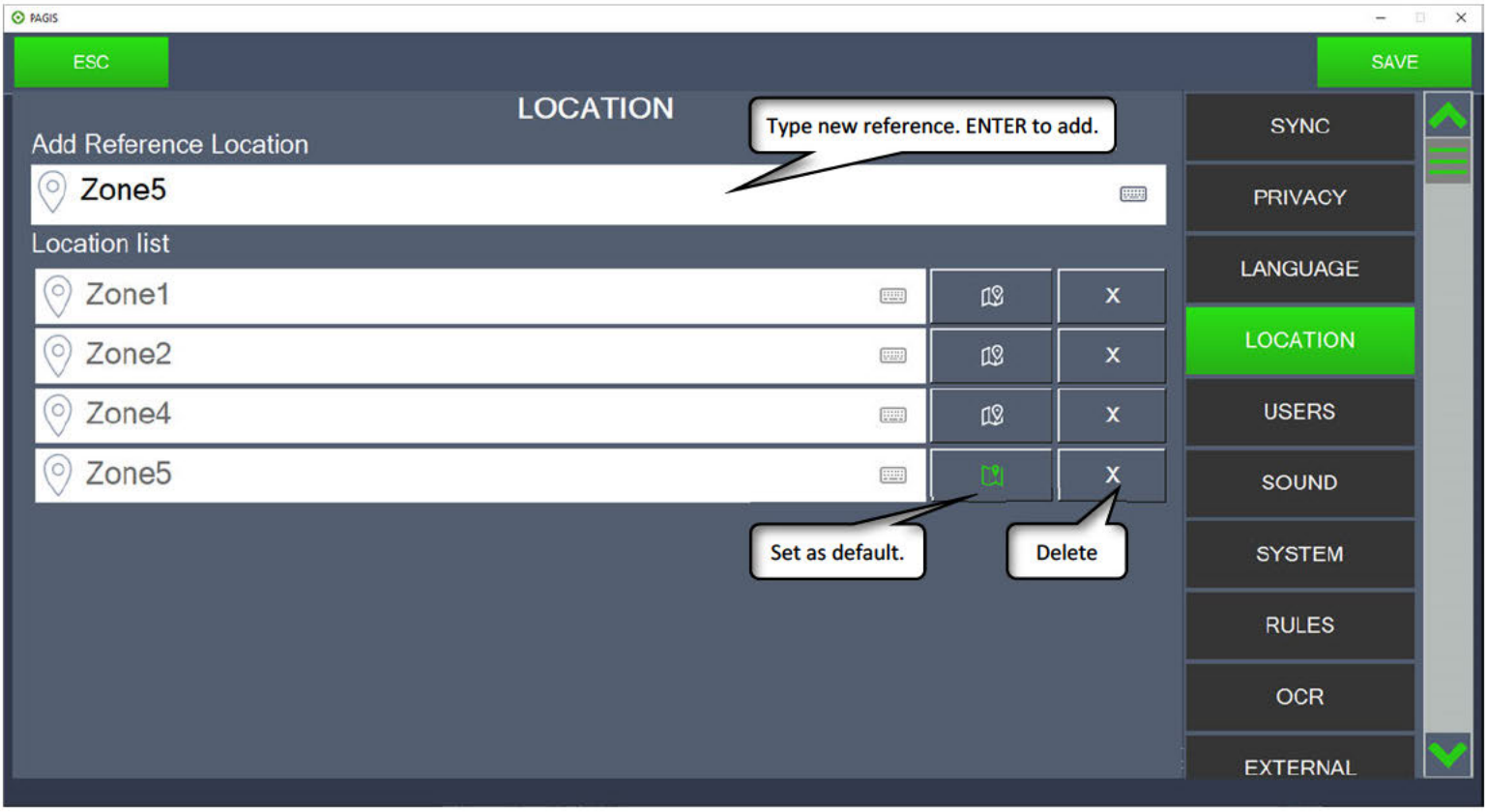
3.3 Language

4194

The Language screen allows the Admin to change the language assignment used in the PAGIS Software. Available languages are listed in the drop-down list and are added during the installation process.

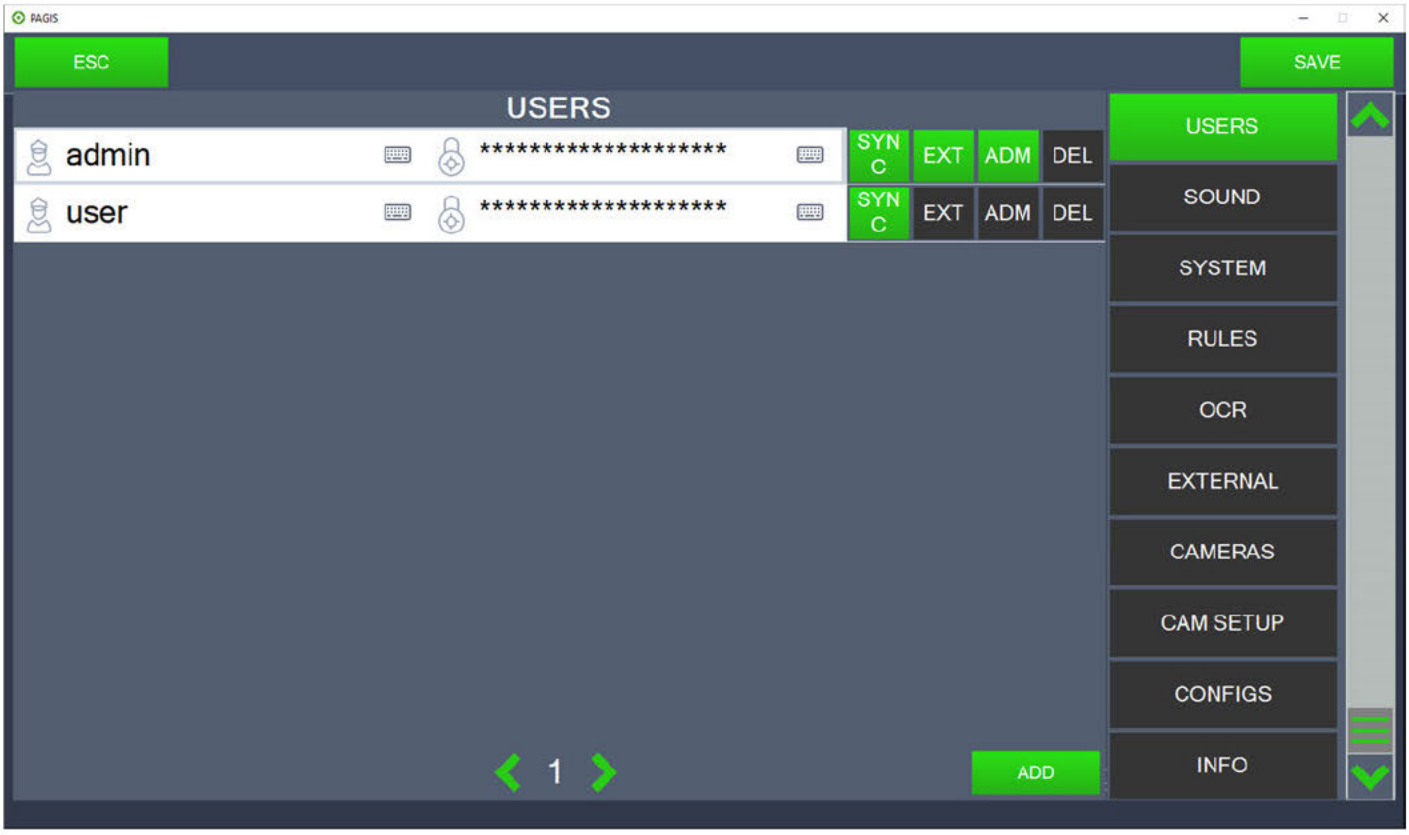
3.4 Location

Updates to the location field will auto-fill the “Reference” section of the PAGIS Login Screen. These are often used to specify a patrol region (Examples: “North Patrol” or “A2”). Once designated all reads/hits will show this designation. Muiltiple “Referance” location can be added, the available list can then be selected from the login screen.



3.5 Users

User accounts, credentials, and rights are generally administered from BOSS and then distributed to the MDC. However, PAGIS does allow for Administrators to add and delete users as well as set their privileges directly from PAGIS.



NOTE: Adding user directly in PAGIS should be limited to customers not utilizing a BOSS server. User accounts created directly in PAGIS by customers with BOSS will be overwritten/removed during the next sync.

Adding a User in PAGIS:

1. From the Admin Screen, select the Users Button on the Right
2. Click the Add Button ADD
3. Enter the case sensitive username in the Username Field (max of 15 alphanumeric characters)
4. Enter the case sensitive password in the Password Field (max of 15 alphanumeric characters)
5. Select the User's privileges
6. Click the Save Button SAVE

3.5.1 User Privileges

These are the "rights" the new user will have in the PAGIS software (When selected, each button turns green).

SYNC — **Sync:** Allows users to synchronize data.

EXT — **External**: Allows the user to access external databases.

ADM — **Admin**: Provides the user Admin rights and allows him/her to configure the PAGIS Software.

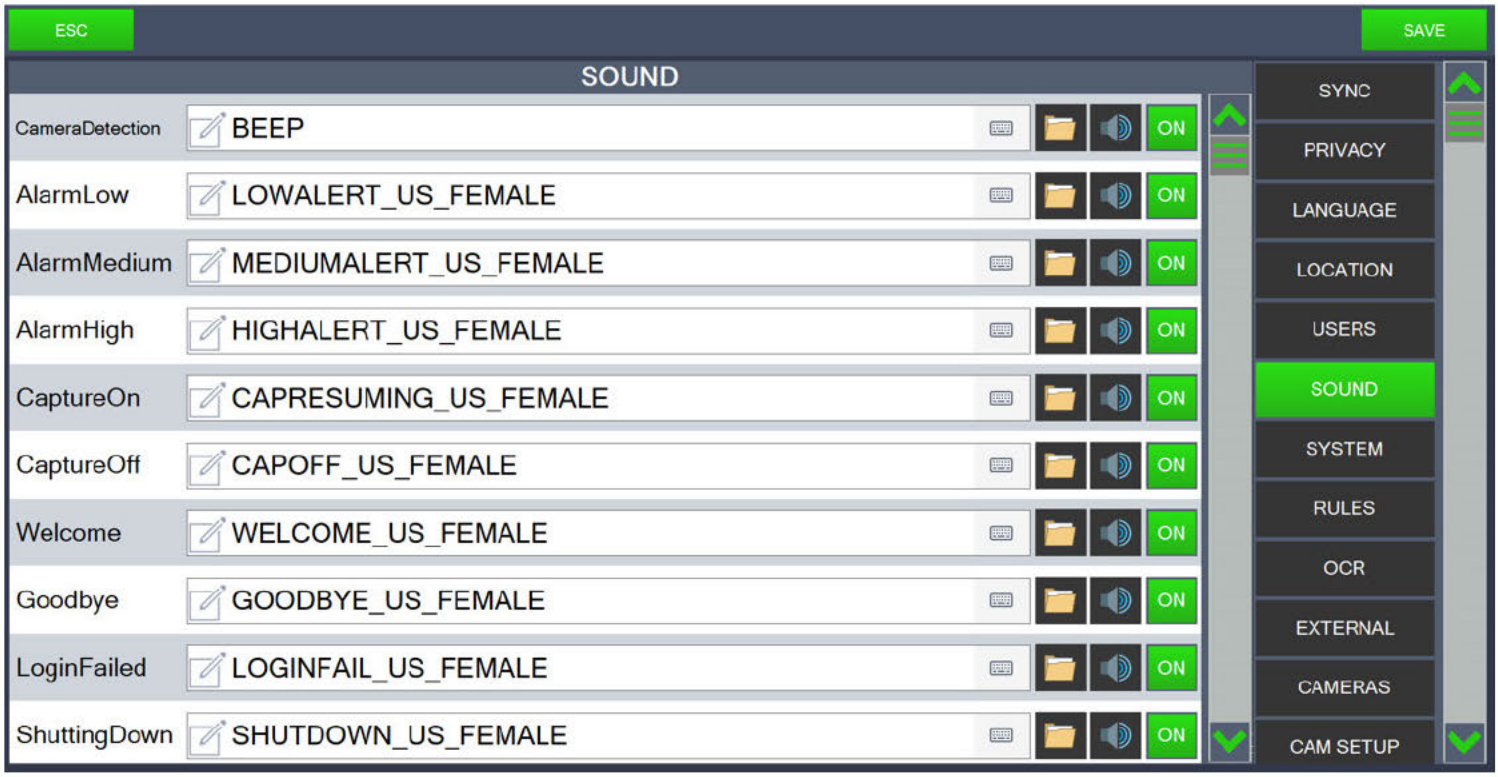
DEL — **Delete**: Allows the Admin to delete a User from the list. Click once to select and the save button to delete.

NOTE: Creating a new user in PAGIS automatically deactivates the default user account settings (Section 2.1.1).

3.6 Sound

4196

Sounds in PAGIS mirror the user or software activity (Ex. Login, Audible alert from a "Hit", and Logout) and are On by default. PAGIS Administrators can adjust the sounds from the available presets and/or load unique .wav files onto each MDC for custom use. **NOTE**: The default storage path is C:\Program Files (x86)\PIPS Technology, Inc\PAGIS2\sounds



3.6.1 Configuration Buttons

The sounds listed on the configuration screen can be altered or updated by PAGIS administrators using the buttons below. **NOTE**: Changes to any sounds must be saved before they can be played in PAGIS.



Click to browse to the sounds folder. This is used to select a new sound file.



Click to Test/Play the selected sound.



Shows the status of that sound. Click to turn each sound Off.

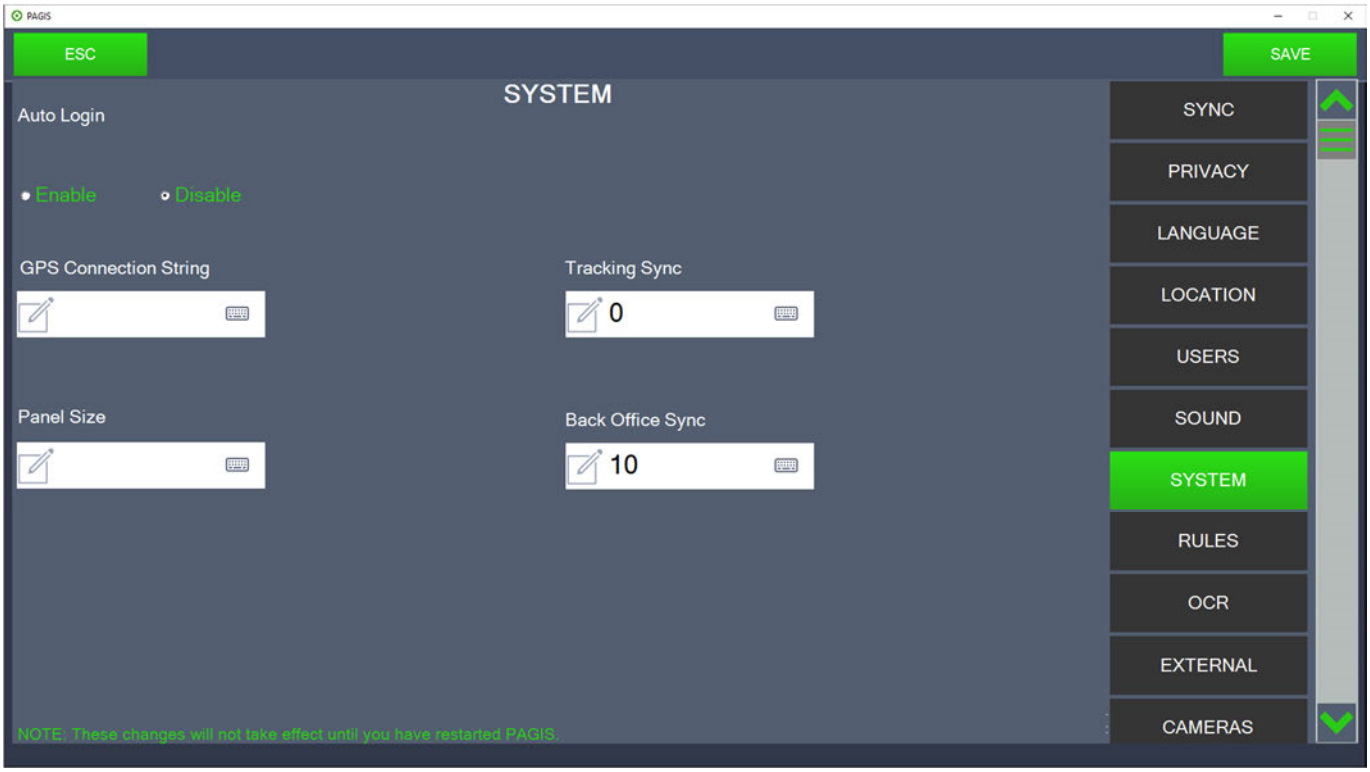


Shows the status of that sound. Click to turn each sound On.

3.7 System

4197

The System screen determines external system connections. The primary external connection is the GPS antenna. The GPS connection string will accept TCP/IP ports or COM port designations. This section also contains control of the PAGIS "Auto Login" feature (which is set to Off by default).

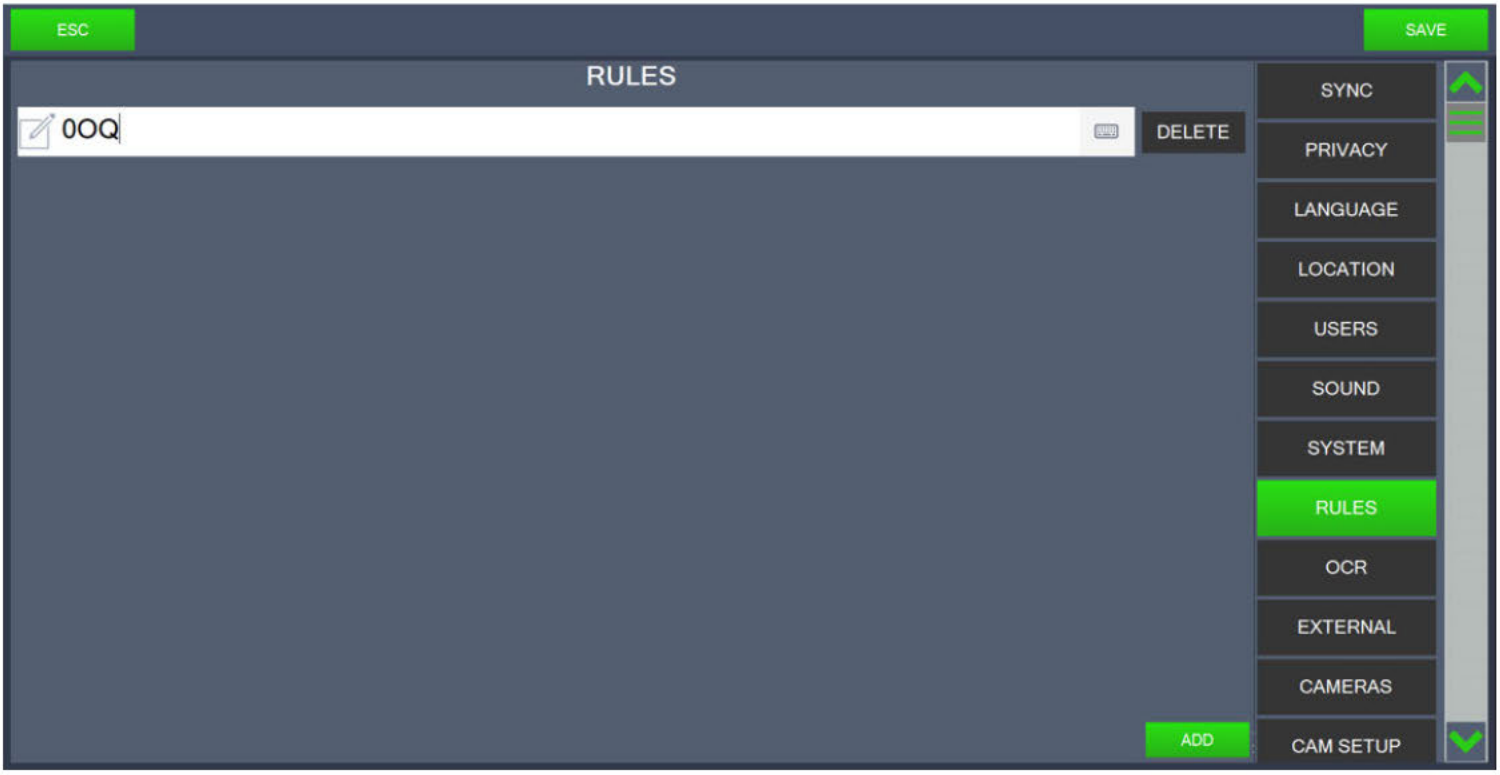


- **Auto Login**: Enabling this feature will ignore existing user account information and login to PAGIS as the Admin. This feature is recommended only for unattended use (Speed-Trailer applications and Covert Drop and Go deployments).
- **GPS Connection String**: This value is utilized by PAGIS to acquire the GPS feed from its source. The default is traditionally either blank (no entry) or 6.
- **Tracking Sync**: Controls the sync intervals in (Sec.) that PAGIS communicates with BOSS4 to update tracking status. Default off=Zero, values can range from 1-9999. BOSS4 Back Office Software requiered for this feature.
- **Panel Size**: Controls the resolution of the color image displayed on the Live View Screen. By default this is blank as PAGIS controls the aspect ratio. However a PAGIS Admin can assign custom resolutions in WxL format (720x1024) to assist with non-standard dispalys.
- **Back Office Sync**: This setting controls the sync timing that PAGIS sends data back to BOSS3/BOSS4, Timing is in (Sec.), default is 10sec, values can range from 0-9999.

NOTE: All changes must be saved and will not take effect until PAGIS is restarted.

3.8 Rules

Rules in PAGIS allow Administrators to force the software to process plate reads in specific ways. For example, in states that allow for both O and 0 (zero) on their license plates, a rule can be set to read any zero as an O and any O as a zero. This provides PAGIS greater flexibility to the standard OCR functions.



Adding a Rule to PAGIS:

1. Click the Add Button ADD
2. Enter the desired alphanumeric characters (Ex. 0 and O) into the text field
3. Click the Save Button SAVE at the top right of the screen

Deleting a Rule:

1. Locate the rule to be removed from PAGIS
2. Click the Delete Button DELETE to the right of the rule (It will turn green when selected)
3. Click the Save Button to complete the removal

3.8.1 Rules – Additional Clarifications

1. Rules are processed based on the first character entered. So in order to read any O as a zero, the Admin will need to add rule "O0". And in order to read any zero as an O, a second rule must be entered as "0O".
2. Rules are NOT designed to overhaul OCR function. Any consistently misread values should first be brought the attention of PIPS Support for review. And only those cases where further adjustments to the OCR software are impossible would rules be recommended.
3. Adding rules to PAGIS will make it less likely to miss a Hit Alert. However, it will increase the number of Hit Notifications that require the Officer to visually confirm the OCR read ("IR Patch") and the Hotlist Alert match.

3.9 OCR

The OCR Section in PAGIS provides Administrators some additional options on how they would like PAGIS to process plate reads.



- **JPEG Images**: On by default, this forces PAGIS to use compressed .JPG images instead of the full resolution Bitmap images each time a read is taken. This settings minimizes data storage requirements and preserves MDC drive space.
- **Inverse Plates**: Off by default, this setting is only used in States where plates with light color lettering over a dark background are prevalent. Enabling this option increases processing load and should remian disabled unless required.
- **Square Plates**: Off by default, this setting adjusts the read area plates that are square instead of retangular.
- **Disable Duplicate Read**: On by default, this setting helps PAGIS prevent duplicate plate reads. If a VLP is read by more than one camera within a short period, the duplicate read is ignored. This minimizes data storage requirements and improves overall system metrics related to numbers of Hits and Reads.

NOTE: Once changes are made, the Admin must click the Save Button SAVE button in the upper right corner to retain them.

3.10 External

The External Screen allows the Admin to connect PAGIS to an external database or device via XML Datastream. This feature is Off by default and any changes must be saved before they will be available.



Enabling the Datastream:

1. Click the Off Button OFF to toggle to On ON
2. Click the Save button in the upper right corner
3. Close and reopen PAGIS

NOTE: Enabling this feature will reduce the overall performance of the PAGIS Software.

3.10.1 XML Datastream Ports

Administrators will need to configure their external device or database to utilize two specific TCP ports:

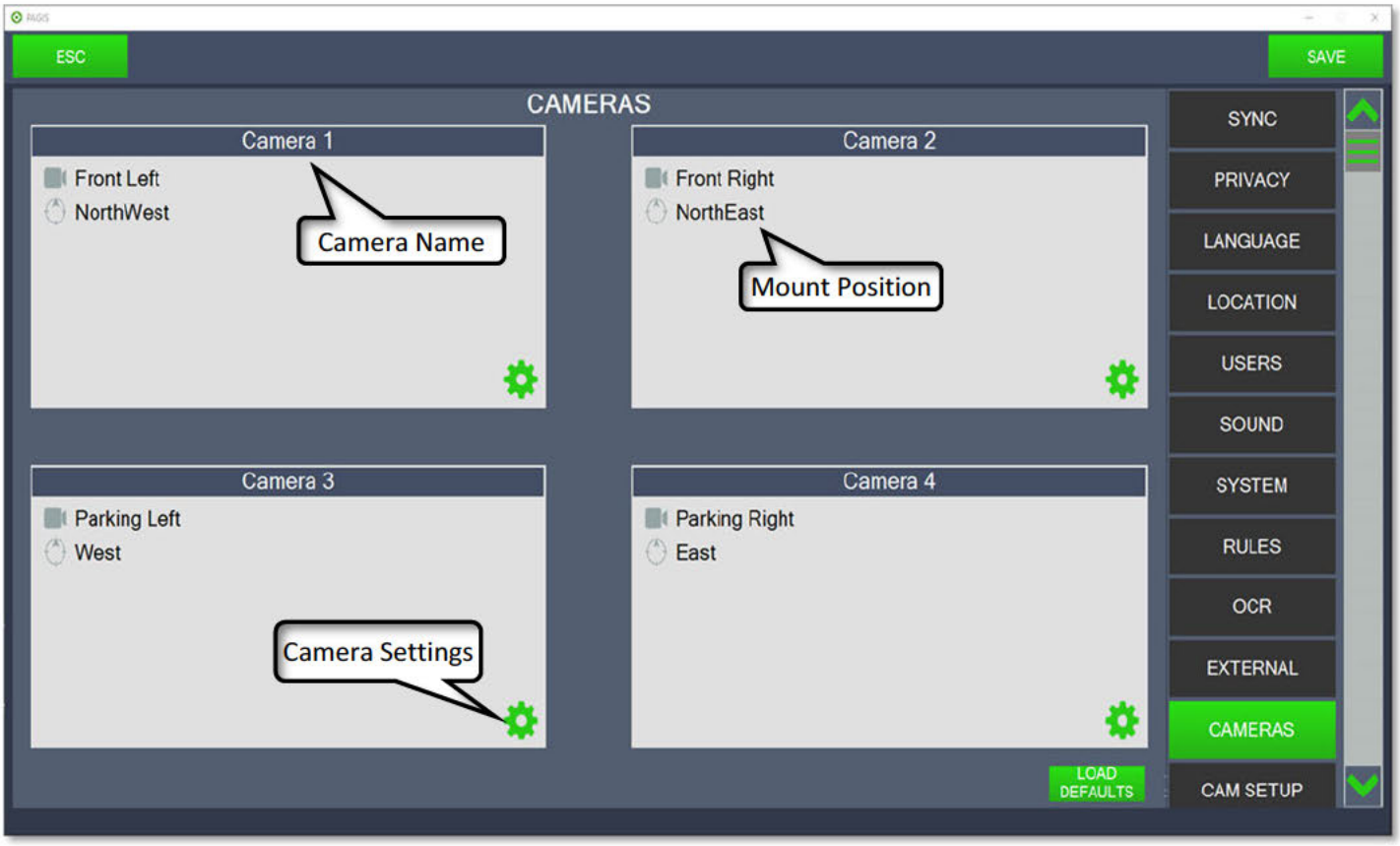
1. Query Port: TCP 7000
2. XML Datastream/Heartbeat: TCP 10100

NOTE: Greater detail on the XML Datastream can be found in Appendix D

3.11 Cameras

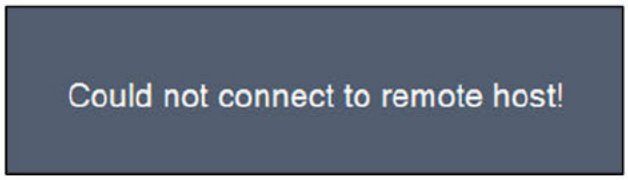
The Cameras Section provides the Administrator the means to add/delete, identify, and configure the ALPR cameras. Although the PAGIS Software comes preloaded with a default layout, best practices advise the Admin to fully review, and completely configure at least one MDC by hand in order to tailor the setup for the Agency's unique attributes.

IMPORTANT: The configuration steps completed here will dictate the available camera mode options in the Configs Section.



3.11.1 Checking the Connection

In order to configure the cameras, the PAGIS Software and the SX Processor (Black Box) must be able to communicate. If they cannot, the Administrator will receive the error message below as soon as he or she clicks on the Cameras Button CAMERAS indicating that PAGIS cannot "see" the cameras.



3.11.2 Troubleshooting Camera Connections

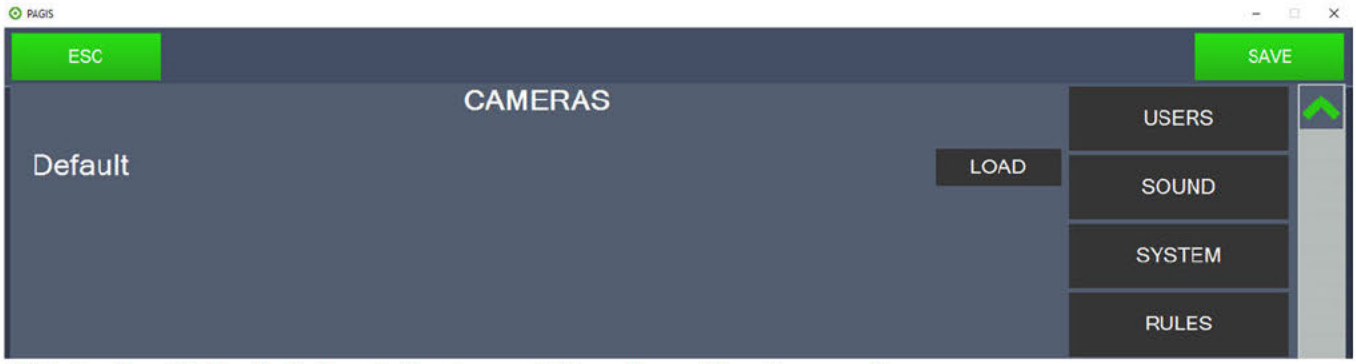
The most common troubleshooting steps have been included below for convenience. If these don't resovle the issue, please contact PIPS Support for additional assistance. **NOTE**: For more information see Appendix C – The Mobile FAQ

1. Start the vehicle and confirm power to the Processor. Confirm the SX switch, and any added in-line switch, is set to On.
2. Confirm the network adapter settings on the laptop match the proper Static IP scheme for the SX Processor in use.
3. Disable the local Windows Firewall, VPN software, and any real-time monitoring software one at a time.
4. Use a different network cable ensuring it's properly seating in NIC port on the SX as well as the MDC or Docking Station.
5. Docking Stations can also impede communication. Test by removing the laptop from thhe dock, directly connect the network cord to the laptop, and then reconfigure the network adapter settings as needed.

3.11.3 Configuring the Cameras in PAGIS

This section will assist with the general configuration of the cameras. Administrators can begin by selecting the Settings Icon to edit each of the existing cameras or by selecting the Load Defaults Button LOAD DEFAULTS. This manual will start with Load Defaults.

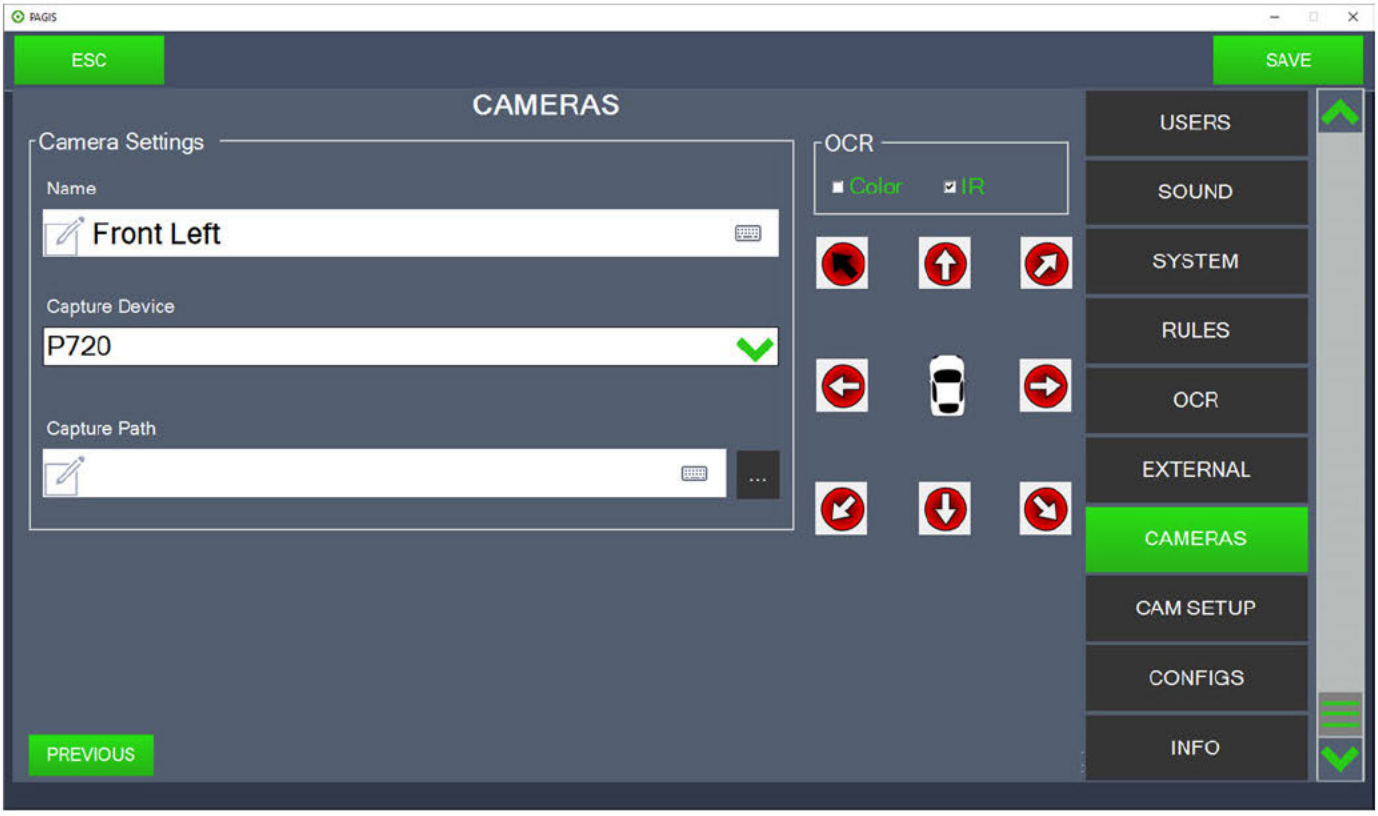
Gettings Started – Load Defaults:



1. Click the Load Defaults Button in the lower right portion of the Cameras Screen
2. Locate "Default" and click the Load Button LOAD
3. Once it's selected (and turned Green), click the Save Button (This returns the Admin to the Cameras Screen)
4. Click the Settings Icon to inspect and configure each camera one at a time

The Camera Settings (Edit) Screen:

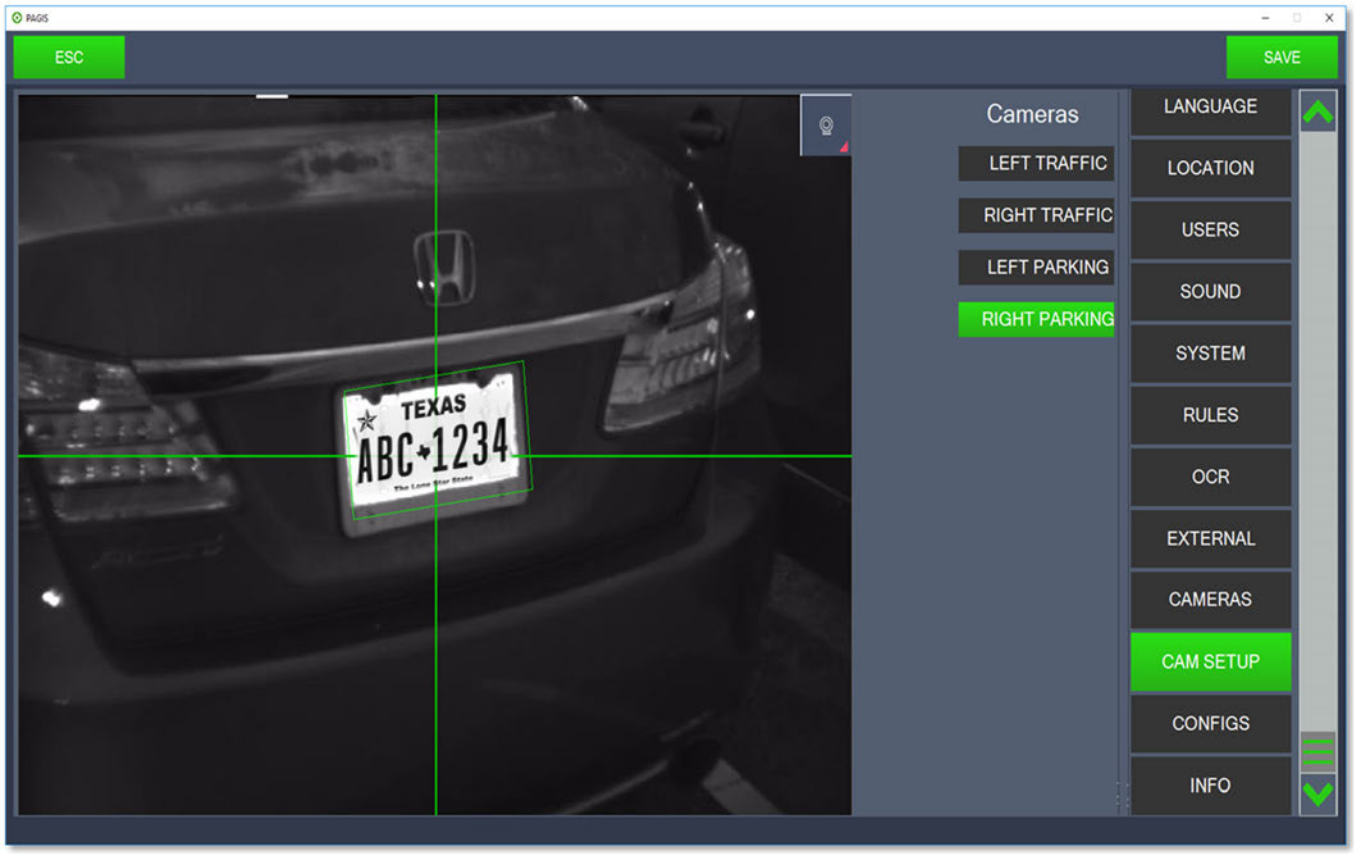
This provides the Admin a single screen to edit the name, confirm the capture device, assign camera position, and confirm OCR.



1. Confirm/Update the Camera Name **NOTE**: Use Camera Names with 11 characters or less to avoid various UI anomalies
2. Confirm the "Capture Device" field was auto-detected. If not, use the drop down to select the only Pxxx value on the list
3. Leave "Capture Path" blank (This is an optional field)
4. Select the camera mount position indicating the direction the camera is facing. The arrows turn black when selected
5. Ensure the OCR is set to IR. The color camera is used for OCR in only rare situations and will increase system load as well as the likelihood of false alerts. Use this setting with caution
6. Click the Save Button to retain the changes

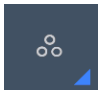
3.12 Cam Setup

The Cam Setup Screen presents Administrators with a live preview of the configured cameras. This section also allows the Admin to switch view modes from Color to IR to ensure the system is functioning properly. **NOTE**: This screen can also be utilized as a means to align newly mounted cameras when RDP access to the SX Processor is limited or unknown.



3.12.1 Cam Setup Navigation Buttons

The Admin may view the output of each camera by clicking on the camera name. When a camera is selected, the button will turn green to indicate it has been selected. In order to switch view modes, the Admin must use the following buttons:



Color View: The Color View Mode is the default view when the Admin first enters Cam Setup. This displays a live preview of the color camera.

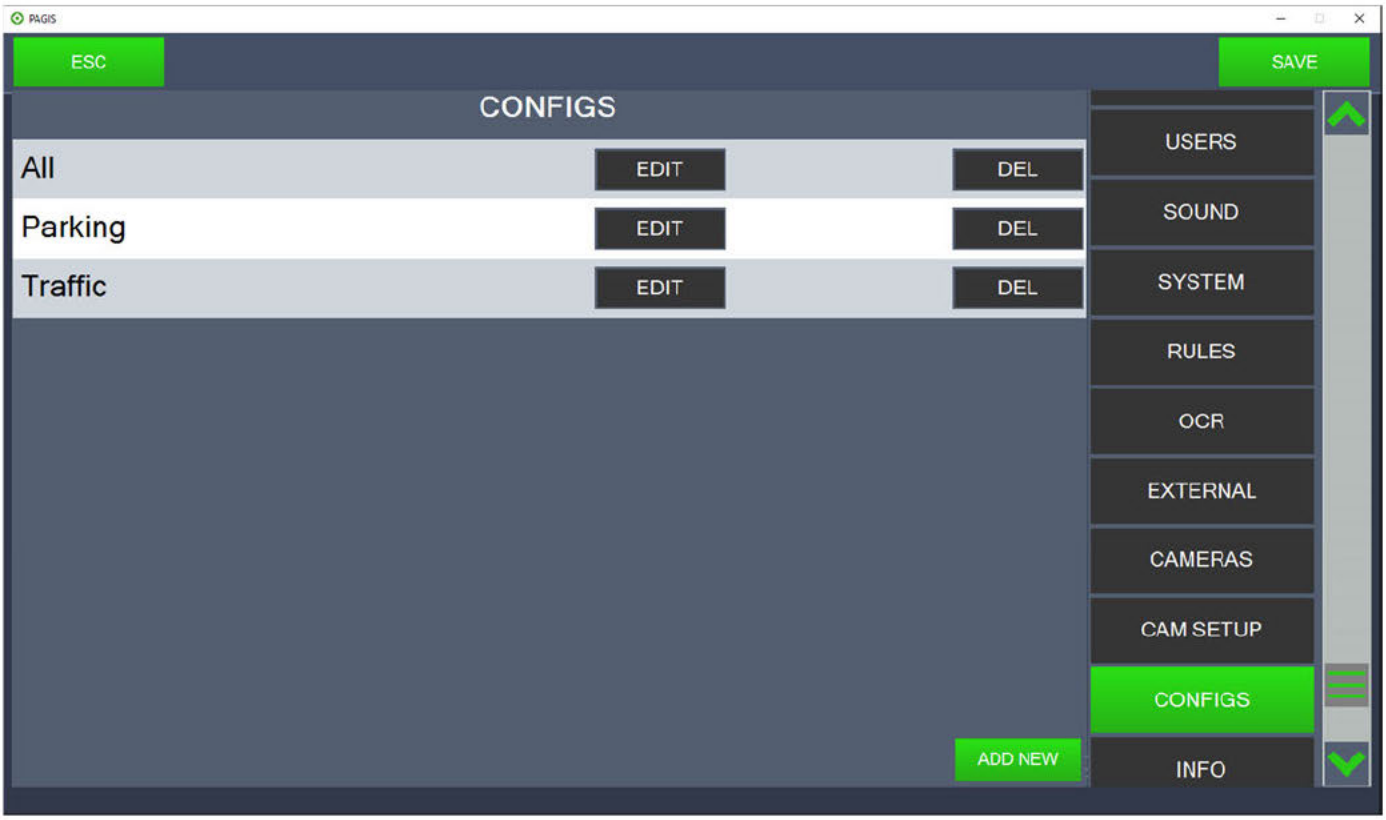


IR View: By clicking on the Camera View Selector button, the Admin will switch to the Infrared (IR) View Mode. This displays a live preview of the IR camera.

NOTE: Unlike the main Live View Screen, the camera feed shown on the Cam Setup page will not time out when in use. This feature makes it easier for the Administrator to review and align the mobile cameras.

3.13 Configs (Camera View Modes)

The Configs Screen allows the Admin to construct how the cameras will be displayed on the Live View Screen for the user. This section also allows agencies to create multiple viewing configurations to meet specific environmental needs or to add greater functionality to the software. By default, the Configs layout provides the agency with three camera modes, “ALL”, “Traffic” and “Parking”. All mode dipalys the front two cameras and rear two are activated, Traffic mode only displays the front two cameras and rear cameras are off, Parking mode only displays rear two cameras and front cameras are off.



3.13.1 Configs Navigation Buttons

To properly configure the camera modes used in PAGIS, the Admin will navigate this section with the following:



To delete a config/camera mode, click the DEL button to select it (turns Green) and then click Save



To review, edit, or modify a camera mode, click the EDIT button



To preserve changes or finalize a deletion, click the SAVE button

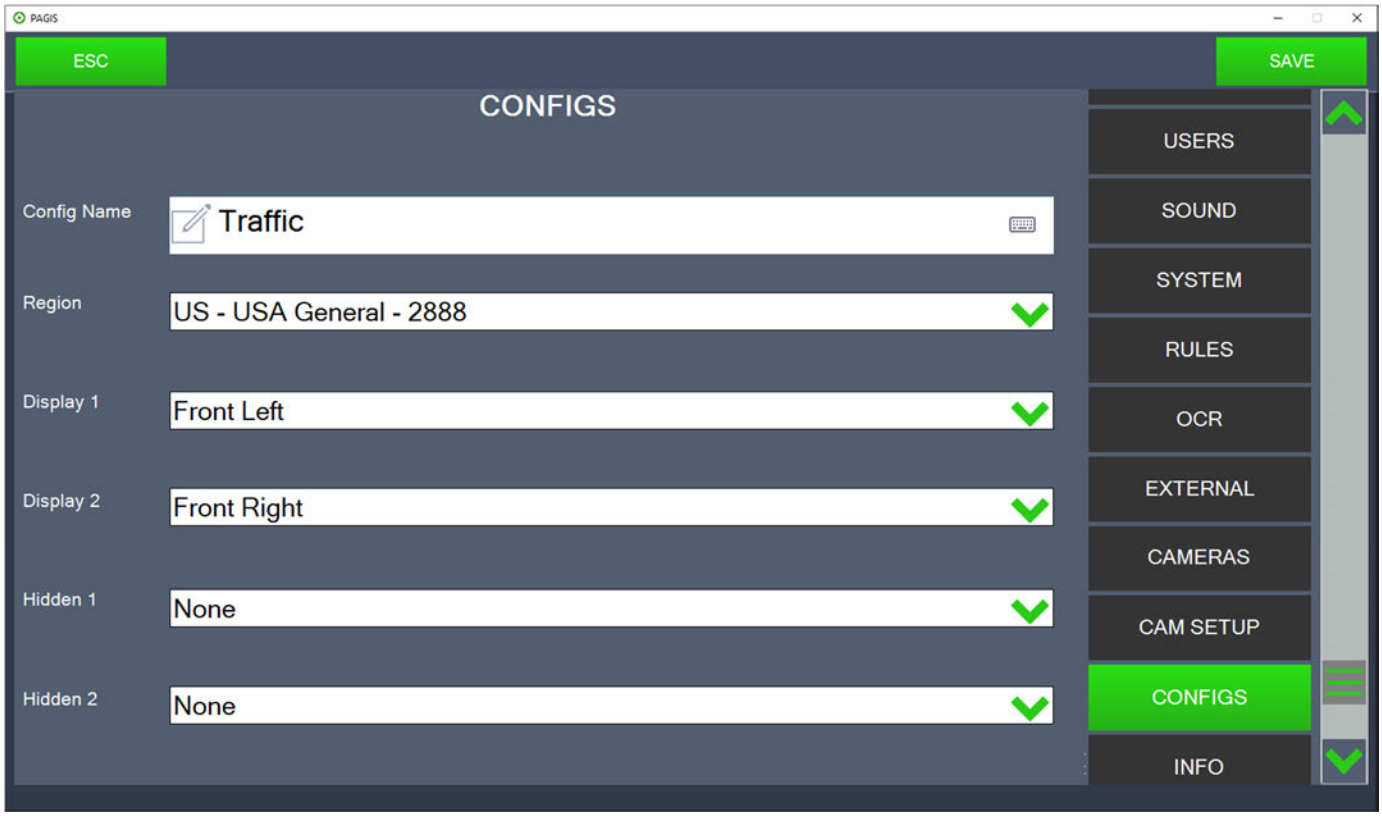


To add a new camera mode, click the ADD NEW button

NOTE: The number of Configs equals the number of Camera Modes available to the user from the Live View Screen. Each camera mode untilizes the Config name established in this section. Users cycle through the modes on the Live View Screen by clicking the Mode Selection Button in the upper left corner.

3.13.2 Reviewing and Modifying Existing Modes

When getting started, most Administrators will begin by simply modifying the existing camera modes or “configs”. The following example will demonstrate the standard configuration of a four-camera mobile unit.

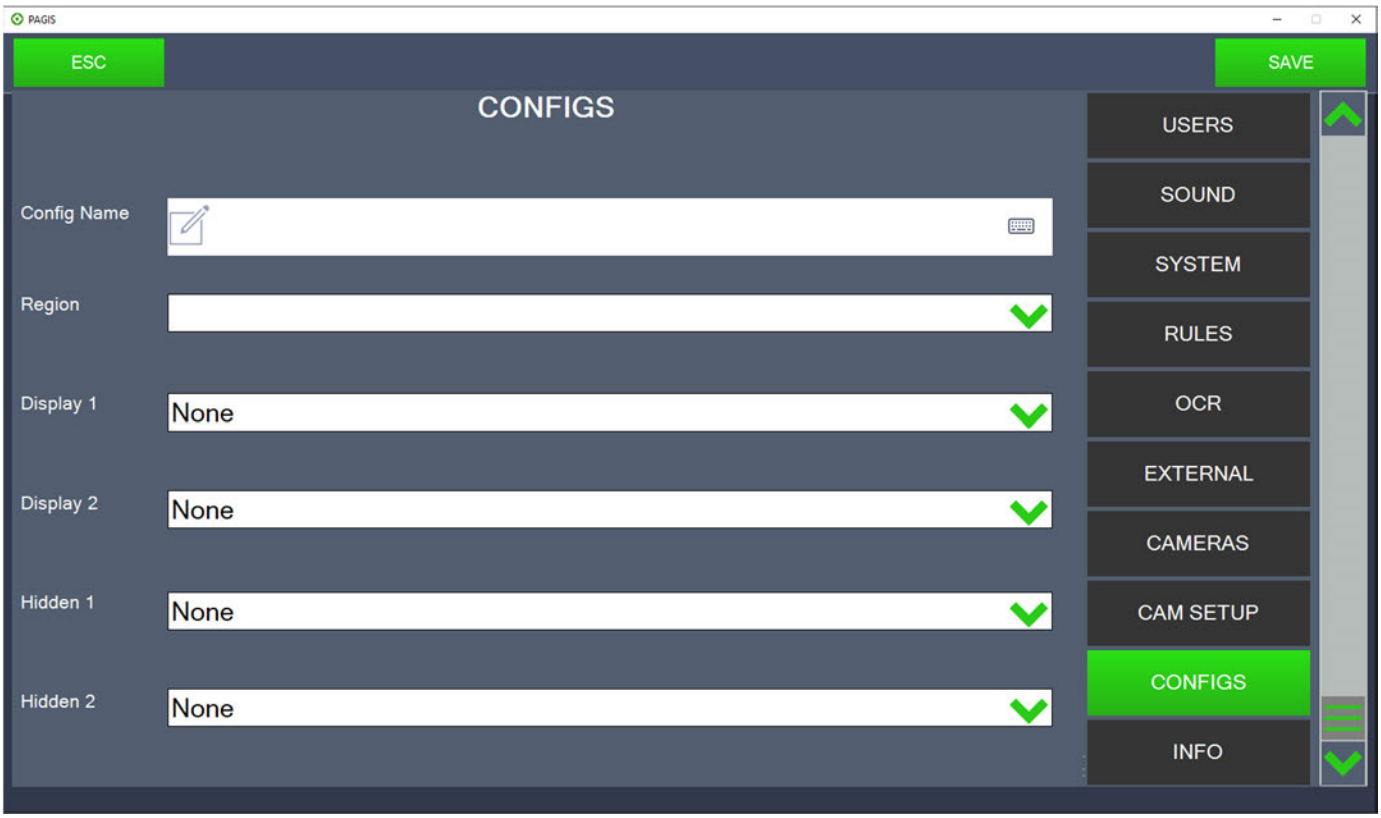


1. Click the EDIT Button EDIT from the main Configs Screen to modify a mode
2. Review/Update the name of the Mode **NOTE**: The name should be intuitive for all users as this becomes the label of the mode selection button on the Live View Screen
3. Click the drop down arrow on the Region field to select the best local option (Adds additional accuracy to OCR)
4. Confirm the camera listed in the Display 1 field. This camera will be displayed on the left side of the Live View Screen
5. Confirm the camera listed in the Display 2 field. This camera will be displayed on the right side of the Live View Screen
6. Confirm the Hidden 1 field shows one of the other cameras not listed in the Display fields
7. Confirm the Hidden 2 field shows the last available camera not yet listed (Leave field as “NONE” for 3-cam systems)
8. Click the Save button to retain the changes
9. Click the Configs Button from the menu to access the other Mode(s)
10. Perform steps 1-8 for all Configs/Camera Modes available

NOTE: Cameras listed in the Hidden fields will function, perform OCR, and capture plate reads, but they will not be displayed to the user while in the named camera mode (unless a Hit is detected opening the Alert Screen). For ALPR units with more than two cameras, best practices dictate the Admin utilize these fields.

3.13.3 Adding a New Camera Mode

When the two default modes provided in the PAGIS software do not offer the agency all the functionality desired, the Administrator can use the Configs Screen to add additional camera modes. For example, if officers request a mode to view only the cameras on the left side of the vehicle while stopped on the side of the road, the PAGIS Adminstrator can build that functionality from this screen.



1. Enter a name for the new Mode (Ex. “Left Side”)
2. Click the drop down arrow on the Region field to select the best local option (Adds additional accuracy to OCR)
3. Confirm the camera listed in the Display 1 field. This camera will be displayed on the left side of the Live View Screen
4. Confirm the camera listed in the Display 2 field. This camera will be displayed on the right side of the Live View Screen
5. Confirm the Hidden 1 field shows one of the other cameras not listed in the Display fields
6. Confirm the Hidden 2 field shows the last available camera not yet listed (Leave field as “NONE” for 3-cam systems)
7. Click the Save button to retain the changes

3.14 Info

4207

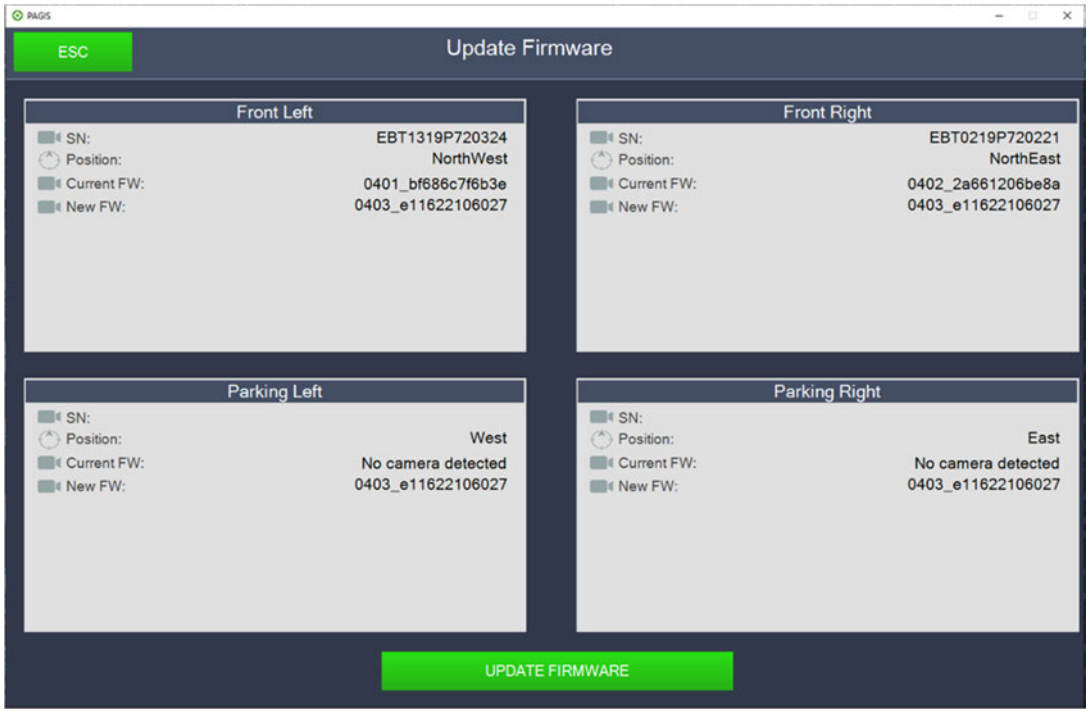
The Info screen displays additional information including the version number of the current installation. This information is helpful when contacting Technical Support.



3.15 Camera Firmware Update, (Admin)

Camera firmware update provides a means for PIPS to update the camera software to enhance and or correct camera performance. The frimware icon  will only apper when a update is avialable.

- The firmware update process only updates camera that are attached and function on the mobile processor.
- Administrator must log into PAGIS and apply the FW update. The update process takes around 4min and should not be interrupted or risk permanently damaging the cameras, PAGIS will return to normal opertaion after update.
- Once the "UPDATE FIRMWARE" button is clicked PAGIS will switch to full gray screen with message indicating "Camera Firmware is Updating", during this process you'll will notice small command windows opening on top of PAGIS, these windows represent the firmware being applied to each active camera so you may notice one or server depending. Once completed a message will appear "Firmware Updated Successfully" then PAGIS will return to normal operation.
- After FW completion and return to "Live View", its requiered to cycle thought the "Cam Mods" to refresh cameras.



Firmware Updater Window List.

- Title "Camera Name".
- Camera serial number.
- Position.
- Current FW version.
- New FW version available.

4.1 PAGIS System Requirements

The PAGIS Software requires the following minimum system requirements for the mobile data computer:

- Intel I3 CPU at 2.0 GHz or higher.
- Windows Operating System (Win7-Win10).
- Microsoft .NET Framework 3.5.
- 8 GB of RAM.
- At least 1 GB of free disk space.
- SVGA display with a minimum resolution of 800 x 600 pixels.
- Available 10/100 Ethernet port.
- Keyboard and mouse, or a touch screen monitor.
- Internet access needed for mapping and Firmware update.

4.2 PAGIS Prerequisites

Prerequisites:

1. Ability to install software.
2. Ability to configure the network adapter.
3. PAGIS 2.12 and above are only compatible with SX4 and SX4e Processors.

Network Adapter Settings:

The PIPS mobile processor operates based on a static IP and is preassigned the IP address of 192.168.200.201. When connecting laptop/MDC to the PIPS mobile processor your computer must be on the same IP network as the mobile processor, in fact the connecting compute must adopt one octet lower than the assigned IP of the PIPS processor in order for MDC installed PAGIS to connect to the mobile processor and receive data from the ALPR cameras. Below are the steps to configure your computer.

1. Navigate to Adapter Options in Windows and right click on the adapter and select properties.
2. Click to select IPv4 and click Properties
3. Click the radio button “Use the following IP Address” to set the Static IP address.
4. Enter 192.168.200.200 in “IP address” section.
5. Enter 255.255.255.0 in “Subnet mask” section.
6. Either leave the “Default gateway” blank or enter 192.168.200.201.
7. Click OK to save changes.

NOTE: The Mobile processor is pre-configured to relay its camera data connection to the 192.168.200.200 IP address, using alternative IP’s on MDC/Laptop will result in the software’s failure to communicate with the cameras when using VPRelay mode.

Alternative IP Network:

It is possible to configure the PIPS mobile processor to utilize a different IP network in conjunction with MDC/Laptop. Typical scenario would be when PIPS mobile processor and MDC/Laptop are connected through an onboard modem that has an Ethernet switch with available ports. Below are the general steps to changing IP network.

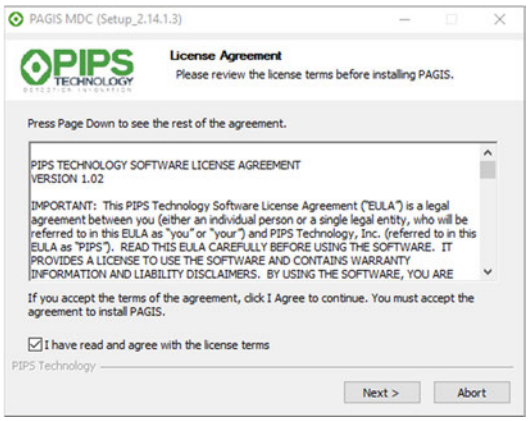
1. Follow the step above to connected to PIPS mobile processor.
2. Remote desktop to PIPS mobile processor and login using credentials provided in SX4 or SX4e manual.
3. In Windows “Services” find and stop the “PIPS VPRELAY” service.
4. Navigate to “C:\PIPSTechnology\VPRelay” and located file “anpr2.ini and open in notepad.
5. Alter “Address=192.168.200.102” to the IP your MDC/Laptop will assume after change to new network, save and close. The “PIPS VPRELAY” service will use this IP address to send camera data to PAGIS running on MDC/Laptop.
6. Alter PIPS mobile processors “Ethernet adapter 1” to new IP, refer to SX4 or SX4e manual for instruction on disabling the “WFManager” so change made to Ethernet are permanently saved.
7. Reboot PIPS mobile processor and enable “WFManager”.
8. Reassign IP on MDC/Laptop.
9. Start PAGIS on MDC/Laptop and confirm camera connectivity, if issues refer to FAQ’s in this manual for troubleshooting tips.

4.2.2 PAGIS Software Installation (MDC)

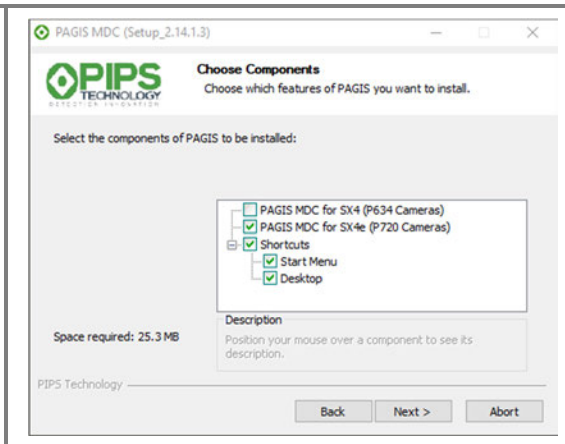
1. If PAGIS exist on your computer, it must be version 2.9 or 2.12 for installer to update. If your version of PAGIS is older it is recommended you “EndShift” any existing data, then uninstall PAGIS.
2. It is recommended you “EndShift” any existing data if upgrading a previous version of PAGIS.
3. Prior to software installation, take the time to figure out what version of PIPS mobile processor you have as the software installation requires you to select options so it can properly configure the camera settings based on processor type. PAGIS version 2.14 supports processor versions SX4 & SX4e only, you can either look at the product tag located on the processor or look at the camera IO ports on the back of the processor. If the 4 camera IO ports are vertically arranged RJ45’s then it’s a **SX4e(P720)**, if they are vertically arranged circular shaped “LEMO” connectors then it’s a **SX4(P634)**. Horizonal arranged circular shaped “LEMO” connectors is a SX3 and is not compatible with PAGIS 2.14.
4. Upgrading to PAGIS V2.14.x.x also requires that the PIPS mobile processor be updated to same version in order to take advantage of the Firmware updater feature.



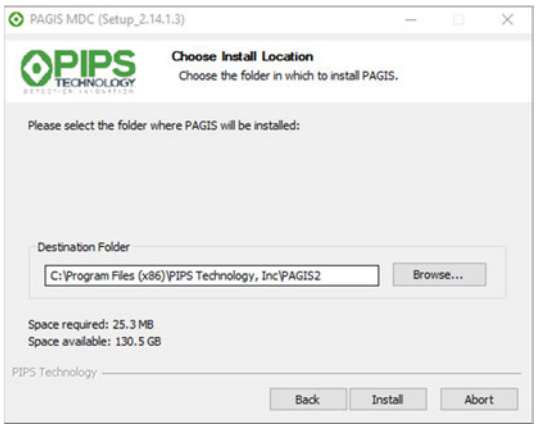
5. Place the PAGIS installer on your computer’s desktop, “PAGIS_Setup_MDC_2.14.x.x.exe”.
6. Right click the PAGIS installer executable and select “Run as administrator”.



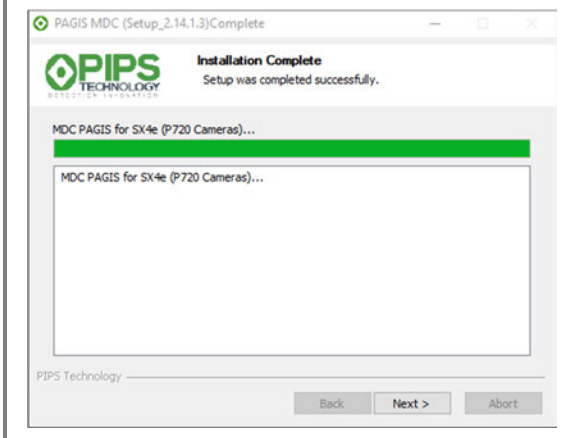
7. Check the license agreement box, then click Next.



8. Select the mobile processor type and alter “Shortcuts” if needed. Next to continue.



9. Confirm path if upgrading, click Install to proceed.



10. Installation Compete, Next to proceed.
11. Click Finish.
12. Click Yes to reboot if you would like to test PAGIS auto start at login if selected during installation, otherwise click No as its not required for PAGIS to run.

Note: See Appendix A for terminology definitions.

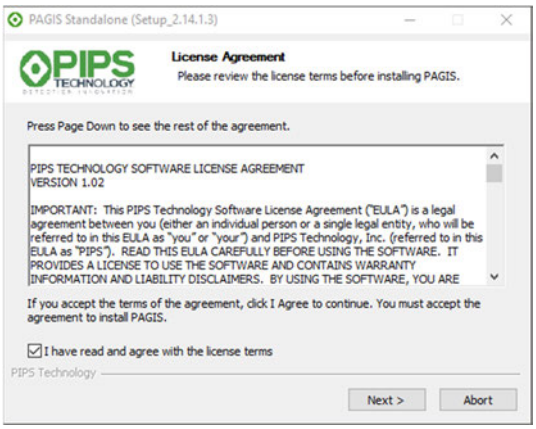
4.2.3 PAGIS Software Installation (Mobile Processor)

1. PAGIS v2.14.x.x updater is only compatible with PIPS mobile processors SX4 & SX4e.
2. The PAGIS updater only updates existing versions of PAGIS on mobile processor, version 2.9 and newer.
3. Update required for both “Standalone” & “Service/VPRelay” to support some of the newer features.
4. The processor must be in its respective mode to update that option as the folder path are hidden when not active, see “Change Mode” in SX4 or SX4e manual.

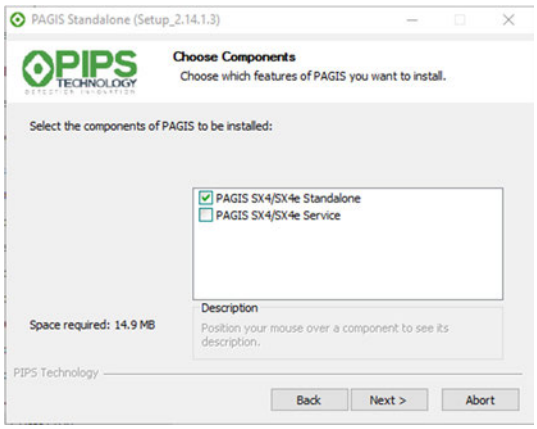
NOTE: If processor is in Service/VPRelay mode you MUST stop the “PIPS VPRELAY” service before running the updater.



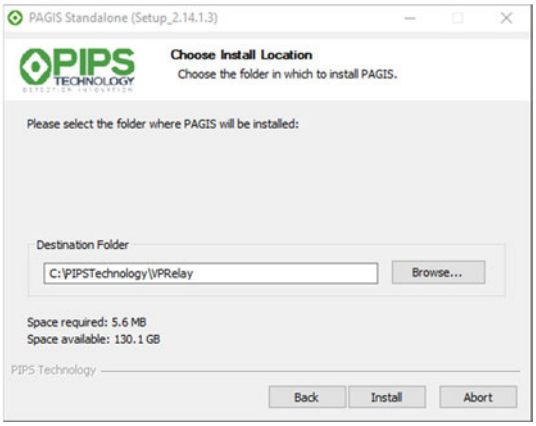
5. Remote desktop into processor or utilize attached monitor/keyboard.
6. Place the updater in C:\PIPSTechnology folder on the PIPS mobile processor.
7. Execute PAGIS Updater.



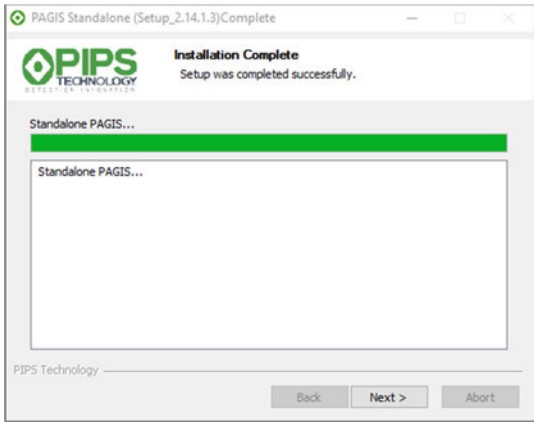
8. Check the license agreement box, then click Next.



9. Select option to update, next to continue.
   - Standalone= PAGIS login from Processor.
   - Service= PAGIS login from connected Laptop.



10. Change the default path presented by updater, see below.
    - For “Service” C:\PIPSTechnology\VPRelay.
    - For “Standalone” C:\PIPSTechnology\Standalone.



11. Installation Compete, Next to proceed.
12. Click Finish.
13. Click Yes to reboot.

Note: See Appendix A for terminology definitions.

TROUBLESHOOTING TIPS

This section provides some basic troubleshooting tips and information

5.1 Troubleshooting & Tips

- The first login to PAGIS after the new install of an unconfigured version does not require a username or password. Simply click Login to be granted Admin access to the software.
- A good means to test the communication from the MDC to BOSS is ping or telnet (over TCP 8092) through the command prompt.
- A good means to test the communication from the MDC to the SX Processor is ping or telnet (over TCP 9000) via command prompt.
- For many other troubleshooting tips, see Appendix C – Frequently Asked Questions

5.1.1 PAGIS with NetMotion VPN

Agencies utilizing NetMotion VPN software on the MDC will need to apply the following passthrough steps:

1. Login to the NetMotion server as administrator
2. Click Settings > Then select Client > Select Global Client Settings > Then select Passthrough List
3. Click the “Add…” button on the right > Select “Network Address”
4. Enter the following settings (as shown):
    A. IP address:192.168.200.0 (the zero is correct, it's an IP address “range”) Subnet Mask: 255.255.255.0.
    B. Keep all other settings default (as shown) and click OK.
5. The MDC must then disconnect from NetMotion and reconnect again for the settings to be applied locally.

5.1.2 Cisco VPN Client:

Make sure Stateful Firewall is unchecked and "Allow Local LAN".

5.1.3 Microsoft .NET 3.5 Installation

The PAGIS Software requires Microsoft .NET Framework 3.5 specifically. If the MDC doesn’t have .NET, it can be downloaded from the Microsoft website.

5.1.4 Firewall Settings for Client-Server Installations

For client-server installations, the Windows Firewall needs to allow the SX Processor and the MDC to communicate. If the MDC is maintained by a Network Administrator, he or she should be contacted before making changes to the firewall. The command prompt commands for the exceptions are below

Option 1: Allow Microsoft Windows Version 8 or newer to auto-detect the launch of the PAGIS.exe application and use the wizard to add the PAGIS.EXE to the exception list (making note of Public or Private Network settings as necessary).

Option 2: Add PAGIS to the exception list manually by browsing to the install path of PAGIS. The default is below for reference: C:\Program Files (x86)\PIPS Technology, Inc\PAGIS2\PAGIS.exe

Option 3: Add the communication ports manually:
TCP in/out 8092 = Pagis sync port to BOSS back office software.
TCP in/out 9000 = Mobile processor camera feed port.
TCP in/out 9001 = Mobile processor camera snapshot port.
TCP in/out 32023 = Mobile processor camera setup port.
TCP in/out 10000 = Mobile processor data capture port.
NOTE: XML Datastream uses TCP 10100 and TCP 7000

PAGIS/BOSS3 CONFIGURATION 4212

In order for the PAGIS software to function properly, the device must be built, enabled, and configured in BOSS3 before being deployed for service in the field.

6.1 Creating a New Device in BOSS3

Once network communication to BOSS3 has been established from the vehicle, the new device must be "built" or added to the Device List in BOSS3 before it can be used. The approved way to do this, is to simply perform a Begin Shift from the PAGIS software. **NOTE**: The computer name is what will be displayed in BOSS as device name.

1. At the PAGIS Live View Screen, click the Begin Shift button once to select it, and then click again to launch the sync.
2. If the laptop has previously been setup to communicate with BOSS and is already enabled, the sync transfer window should appear in the middle of the Live View Screen.
3. If this is a new/disabled device, a message indicating "HttpStatusCode" will be displayed.
4. This indicates the BOSS3 server has received the sync request but has rejected it due to device status.
5. Once the BOSS Admin has enabled the device, the Status Code error will not appear again, and syncs should complete as configured in BOSS3.

6.2 Enabling a New Mobile System in BOSS3

Installing PAGIS and configuring the network settings is only the first step in making the ALPR unit operational. Once PAGIS is configured to work with or on the SX Processor and the mobile cameras, it must then be enabled in BOSS3 before synchronizations can take place. **NOTE**: By default, every new device recognized by the BOSS3 server is disabled until the Admin enables it. This is done for security.

1. Log into the BOSS3 UI Client Software with Admin privileges.
2. Click the Admin button on the left to expand the options.
3. Click the Devices button. The new device should now be listed to the right.
4. Click the name of the Device to select it. (This will open the device details screen)
5. Click the Edit button at the bottom of the window.
6. Click the Enable button from the Edit window.
7. This will enable the device and return the Admin to the Device List.

NOTE: If desired, the Admin can re-enter the Edit window to assign an alternate name in BOSS3 for the new device. The Admin will need to update the "Description" field and then click the Save button. Agencies commonly use this field to signify the Unit number, Car name, or Patrol Shift. The "Name" field is the device/host name and cannot be edited in BOSS3.

NOTE: Once the Device is enabled the Admin needs to assign ownership and hotlist distribution.

6.3 Assigning Ownership to a Device in BOSS3

Every new device added to BOSS3 allows for Admin level access into PAGIS without the use of a username or password. In order to password protect the PAGIS software, the BOSS Administrator must assign "Owners" to the device in BOSS3.
NOTE: For more detail on Users, User Groups, Sites, and Roles, refer to the BOSS3 manual.

1. Login to the BOSS3 UI with Admin credentials.
2. Click the Admin button on the Left to expand the options.
3. Click Devices to review the list.
4. Click on the Device Name to open the device details screen.
5. Click on the Edit button.
6. Locate the "Owners" field. Click the Select button to the right.
7. Check the box(es) for the appropriate Site(s)/User Group(s). **NOTE**: This tells BOSS3 which sets of users will have rights to login to PAGIS from this specific device.
8. Notice the Select button has changed to a Save button. Click Save to retain changes.
9. Confirm the changes show in the Owners Field.
10. Click the Save button at the top left of the Edit window.

6.4 Assigning Hotlists to a Device in BOSS3

In order for the PAGIS users to receive alerts, one or more of the stored hotlists in BOSS3 must be distributed to the new device. **NOTE**: For more information on building and configuring Hotlists, refer to the BOSS3 manual.

1. Login to the BOSS3 UI with Admin credentials.
2. Click the Admin button on the Left to expand the options.
3. Click the “Hotlists” button to review the list of configured alert lists.
4. Click the Hotlist Name to select the first alert list. This will open the Details screen.
5. Click the Edit button at the bottom of the window.
6. Locate the “Deployment” field. Then click the Select button to the right.
7. Check the box next to the name of the new device.
8. Notice the Select button has changed to a Save button. Click Save to retain the changes.
9. Confirm the changes show in the Deployment Field.
10. Click the Save button at the top left of the Edit window.
11. Perform these steps again for all remaining Hotlists necessary for this device.

PAGIS/BOSS4 CONFIGURATION

In order for the PAGIS software to function properly, the device must be built, enabled, and configured in BOSS4 before being deployed for service in the field.

7.1 Creating a New Device in BOSS4

Once network communication to BOSS4 has been established from the vehicle, the new device must be “built” or added to the Device List in BOSS4 before it can be used. The approved way to do this, is to simply perform a Begin Shift from the PAGIS software. **NOTE**: The computer name is what will be displayed in BOSS as device name.

1. At the PAGIS Live View Screen, click the Begin Shift button once to select it, and then click again to launch the sync.
2. If the computer has previously been setup to communicate with BOSS and is already enabled, the sync transfer window should appear in the middle of the Live View Screen.
3. If this is a new/disabled device, a message indicating “HttpStatusCode” will be displayed.
4. This indicates the BOSS4 server has received the sync request but has rejected it due to device status.
5. Once the BOSS Admin has enabled the device, the Status Code error will not appear again, and syncs should complete as configured in BOSS4.

7.2 Enabling a New Mobile System in BOSS4

Installing PAGIS and configuring the network settings is only the first step in making the ALPR unit operational. Once PAGIS is configured to work with or on the SX Processor and the mobile cameras, it must then be enabled in BOSS4 before synchronizations can take place. **NOTE**: By default, every new device recognized by the BOSS4 server is disabled until the Admin enables it. This is done for security.

1. Log into the BOSS4 URL with Admin privileges.
2. Navigate to the Resources pulldown menu.
3. Select Devices from the menu options. The new device should now be listed.
4. Click the name of the Device to select it. (This will open the device details windows on the left)
5. Click the Enable slide toggle to enable device, located in upper right of device edit window then click save.
6. This will enable the device, synchronization between BOSS4 and PAGIS is allowed.

NOTE: Once the Device is enabled the Admin needs to assign ownership and hotlist distribution.

7.3 Assigning Ownership to a Device in BOSS4

Every new device added to BOSS4 allows for Admin level access into PAGIS without the use of a username or password. In order to password protect the PAGIS software, the BOSS Administrator must assign “Owners” to the device in BOSS4.

NOTE: For more detail on Users, User Groups, Sites, and Roles, refer to the BOSS4 manual.

1. Login to the BOSS4 URL with Admin credentials.
2. Navigate to the Resources pulldown menu.
3. Select Devices from the menu options. The new device should now be listed.
4. Click the name of the Device to select it. (This will open the device details windows on the left)
5. Locate the “Owner” field. Click in the Owner filed, and a list of all available Groups will appear.
6. Select group by clicking on it, it will then automatically be added to owners, see list below “Owner”.
7. To add mode groups, repeat step 15.
8. Confirm the changes show in the Owner Field.
9. Click the Save button at the bottom right of the Edit window.

7.4 Assigning Hotlists to a Device in BOSS4

In order for the PAGIS users to receive alerts, one or more of the stored hotlists in BOSS4 must be distributed to the new device.

NOTE: For more information on building and configuring Hotlists, refer to the BOSS4 manual.

1. Login to the BOSS4 URL with Admin credentials.
2. Navigate to the System pulldown menu.
3. Select Hotlists from the menu options
4. Click the Hotlist Name to select the first alert list. This will open the Details screen.
5. Locate the “Deployment” field.
6. Check the box next to the name of the new device listed.
7. Click the Save button at the bottom right of the Edit window.
8. Perform these steps again for all remaining Hotlists necessary for this device.

APPENDIX A: THE GLOSSARY

4215

ALPR/ANPR	"Automatic License Plate Recognition/Automatic Number Plate Recognition".
BOSS	"Back Office System Software". This is the ALPR server.
GPS	"Global Positioning System".
GUI	"Graphical User Interface".
Hotlist	A database or list that contains vehicle license plates of interest ("alert list").
IR	Infrared light.
License Plate	Also called a tag or number plate.
MDC	"Mobile Data Computer". This is the tablet or laptop in the vehicle.
OCR	"Optical Character Recognition" (also referred to as a "cardet").
OS	"Operating System".
PAGIS	This is the License Plate Capture Software most commonly used in an ALPR vehicle.
Service	Operation mode of the PAGIS software. Service or "VPRelay" is used to refer to PAGIS instance that is running directly on the PIPS mobile processor without a GUI interface, this mode is intended to run in conjunction with MDC version of PAGIS installed on laptop connected via Ethernet.
Standalone	Operation mode of the PAGIS software. Standalone is used to refer to PAGIS instance that is running directly on the PIPS mobile processor with a GUI interface. Same a "Service"
SX	SX is a short notation referencing PIPS's mobile processor, commonly the SX is followed by the generation number of the processor, i.e. SX3, SX4 & SX4e.
UI	A "User Interface" is the means in which the user can access and navigate the software.
USB Flash Drive	Also called a thumb drive or memory stick.
VLP	"Vehicle License Plate".
VPN	"Virtually Protected Network".
VPRelay	Operation mode of the PAGIS software. VPRelay or "Service" is used to refer to PAGIS instance that is running directly on the PIPS mobile processor without a GUI interface, this mode is intended to run in conjunction with MDC versions of PAGIS installed on laptop connected via Ethernet.
Whitelist	Opposite of a standard BOSS Hotlist. This is a list of license plates that should not trigger an alert.

APPENDIX B: PAGIS SOFTWARE DATABASE FILE

This section is used to configure the PAGIS Software when it's not being used with the Back Office System Software (BOSS). Comma-separated value (CSV) format is the only format the PAGIS Software supports for importing data into the vehicles for the purpose of matching against the captured license plate data. PAGIS will support CSV files with any number of columns, called "fields", as long as the first field is the VLP (Vehicle License Plate). **NOTE**: The CSV format is standard ASCII.

Example CSV Files:

1. *ABC123, Red, Ford, Explorer, 1996, WANTED XYZ456, Blue, Audi, A4, 2001, MURDER*
2. *45ABC234, Vehicle wanted in associated with a kidnapping on 12/5/2005 995BD233, Vehicle reported stolen from Liz's Lounge at 6am on 12/1/2005*
3. *UIO223 ABC123*

General Function:

PAGIS calls/utilizes files in pairs. Each database in PAGIS is created using two files; a CSV file, and an INI configuration file. Without both of these files, the database will not load and PAGIS will not "see" it. Each CSV file/hotlist must have the exact same name as the INI configuration file. Example: Stolen.ini and Stolen.csv will work. Stolen.ini and Plates.csv will not.

Reading an INI Configuration File

Lines that appear in brackets [] are called "Headings". The labels that appear inside the headings, are called "values". Values will always contain an equal sign (=). If a line starts with a semicolon, it is considered to be a comment and is not read by the software. There is no limit to the number of comments in the INI file.

The [SETTINGS] Heading

The values in the Settings heading are: NumFiles, DbName, DbColor, Priority, Covert, Alarm, and NumFields.

- NumFiles: Determines how many database files the system should split the specified hotlist into. Generally, this value is set to 1. But for larger hotlists (200,000+ lines), a number of 2-5 may be more desirable.
- DbName: Tells the PAGIS Software what the displayed name of the hotlist should be.
- DbColor: Sets the display color of the hotlist. This is merely an esthetic setting and not a functional setting. The right-hand side of the equal sign is the HEX value representing the ARGB values for the color. If this value is unknown, the Admin should simply leave this line out of the file.
- Priority: Designates the priority of this hotlist in relation to other hotlists in the system. The highest priority database is 1 and the lowest is 999. **NOTE**: if a plate resides on multiple lists the higher priority will be alerted first.
- Covert: Determines whether standard PAGIS Software users are alerted when a hit is made from the database. Covert database can be used for hotlists that are included for information-gathering purposes rather than eliciting user intervention. The system can also be configured to notify via email or SMS message when a hit is made from a covert hotlist.
- Alarm: Sets the audible alert to be played in PAGIS when a hit is made from the hotlist. Values for Alarm are LOW, MED, HIGH
- NumFields: Indicates how many fields (columns) are in the CSV file. If this value is less than the actual number of fields in a file, then the additional fields are placed in the general information area. This value also determines the number of headings of the [Field x] present in the file. For example, if NumFields=2 then there will be two additional headings, [Field 0] and [Field 1]. **NOTE**: Adding "Creation =" will place the timestamp the hotlist was added to the Begin Shift file.

The [FIELD X] Heading

Under the Field heading, there are two configurable values, “Name” and “PAGIS”.

- Name: Tells the system what the name of this field is. If no name is specified, then no name given to the field. The format is Name = <field>
- PAGIS: Specifies how to display the field in the GUI/PAGIS Software.
  - If no value is defined, the field is placed as general information.
  - Values 1-5 represent special fields for the PAGIS Software that translate to the information being displayed in a box of its own when a hit is processed.
  - A value of 6 represents an ID number to cross reference the vehicle from the hotlist with a person from the wanted list.
  - A value of 7 is identical to leaving the value undefined.

Sample INI Configuration File

[Settings] NumFiles=1
DbName=Stolen Vehicles DbColor=ffffff00 Priority=5 Covert=False Alarm=MED NumFields=8
;PAGIS Values
;0 is VRM / VLP (Not User Definable, always Field 0)
;1 is Special Field 1
;2 is Special Field 2
;3 is Special Field 3
;4 is Special Field 4
;5 is Special Field 5
;6 is ID Number (PNC ID, Driver’s License, Social Security Number, etc.)
;7 is General Info (Default for all undefined fields) [Field 0]
PAGIS=VRM

Sample INI Configuration File

[Field 0] Name=VRM
[Field 1] Name=Color
PAGIS=3 [Field 2]
Name=Make PAGIS=1
[Field 3] Name=Model
PAGIS=2 [Field 4]
Name=Action PAGIS=4
[Field 5] Name=Warning
PAGIS=5 [Field 6]
Name=PNCID PAGIS=6
[Field 7] Name=Intelligence PAGIS=7

To deploy a locally created hotlist to PAGIS without BOSS.

1. Create a folder called “beginshift” (Without Quotes) on the root drive of whatever drive media your using that PAGIS has access to, remember only on root drive, no subdirectory’s. Example C:\beginshift.
2. Place the .CSV & .INI in the newly created beginshift folder.
3. Log into PAGIS and configure Sync to access the drive where your file/files are located. When setting disk drive letter in PAGIS no need to indicate folder path as PAGIS assumes by default that “beginshift” exist on the root drive your selecting, refer to section 3.1 in this manual.
4. Go back to main screen and do beginshift.

APPENDIX C: FAQ

Q: **HOW DO I ENTER A SUPPORT CASE?**
A: We have a webform you can use here, you can email our Support Team at Support@PIPSTechnology.com, or you can call us on the phone Monday-Friday 8am to 4pm Central Time (9am-5pm Eastern) at (833) 747-7577 Option 2.

Q: **HOW DO WE CREATE USERS IN PAGIS?**
A: The agency BOSS Administrator creates all users, both for BOSS and for PAGIS. Once the user is created in BOSS, the Admin would click the user's name to select/edit the user. Then click the Advanced button and update the PAGIS specific password. Please note that the username and password fields are both case sensitive and the PAGIS users need to be added to a group with the Role that allows them to use PAGIS/LPCS.

If you have any further questions, please feel free to enter a request for support here.

Q: **WHERE DO USERS CHANGE THEIR LOGIN PASSWORD IN PAGIS?**
A: User passwords are created and updated in BOSS via the UI client software. For the majority of our customers using both the PAGIS Software and BOSS, any user accounts or passwords created in the PAGIS Software itself will be overwritten by the user information defined in BOSS during the next sync.

If you have any further questions, please feel free to enter a request for support here.

Q: **HOW DO WE REQUEST AN RMA REPAIR?**
A: To assist with this, please navigate here to review our RMA procedure as well as to download the request form. Please keep in mind that once submitted, all repairs are reviewed for age of equipment and warranty status before final processing takes place. Additionally, incomplete forms and those without much detail often result in processing delays.

If you have any further questions, please feel free to enter a request for support here.

Q: **WE GOT NEW MDC LAPTOPS IN THE PATROL CARS, HOW DO WE ADD THOSE DEVICES TO BOSS?**
Q: **HOW DO WE EDIT THE DEVICE NAMES IN BOSS?**
A: The initial device template/skeleton is automatically created in BOSS the first time the device attempts to Sync from the field. Devices should NEVER be created manually. For PAGIS laptops, this is done after PAGIS is installed and configured and Begin Shift is launched. However, if the agency would like to organize the device list by updating the "Device Name" field, those steps are below:
1. Login to the BOSS UI with Admin rights
2. Navigate to Admin > Devices
3. Click on a device name to select it > Click Edit
4. Update the name of the device in the "Description" field (Name field cannot be altered)
5. Click Save > This will take you back to the Device Summary List. The "Device Name" field should show the new name

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **WE HAVE A NEW MOBILE COMPUTER/MDC THAT'S NOT SYNCING WITH BOSS.**
Q: **WE KEEP SEEING AN HTTP_STATUS_CODE ERROR WHEN RUNNING BEGIN SHIFT.**
A: This error most commonly means that a new device in the field (laptop/tablet) can "see" the BOSS server, but that it hasn't been enabled yet to "talk" with it. Follow the general steps below to address this issue:
1. The agency BOSS Administrator will need to login to the BOSS UI client and Select Admin
2. Then select Devices and from there, left click on the device/computer name of that MDC to edit it
3. Once in the Edit screen, Enable the device. This will take you back to the Device List.
4. Click the name to edit the device again. Now assign users/Owners and save.
NOTE: The Select button becomes a Save button when selecting which Groups/Users should have access to login to this device

5. Once that is done, navigate to Admin > Hotlists
6. From here, click on each hotlist one at a time to distribute them to the new device being sure to Save the changes next to the Distribution field. Note again that the Select button becomes a Save button. And there's another Save button at the top left of the edit window.
7. After this is complete, perform Begin Shift from the field unit/MDC and confirm there are no further errors.

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **NEW PAGIS USER CAN'T LOGIN BUT OTHERS CAN.**
Q: **USERS CAN LOGIN TO PAGIS WITH NO CREDENTIALS AT ALL.**
A: Entry or login to the PAGIS software in the field is partially controlled by the Device settings in BOSS. The users themselves must also be properly setup with an LPCS/PAGIS password. To check the current device settings/ access, perform the following steps:
1. Login to BOSS UI (with Administrator rights)
2. Select the Admin Section
3. Select Devices and then Select the Device in question by PC name
4. Once selected click on the Edit button near the bottom
5. Locate and inspect the "Owners" Field (this is a list of users/groups that have access to login to the device)
NOTE: If this field is blank, the device is in an open configuration mode allowing admin level access simply by clicking login (any credentials would also be accepted).
6. To update the device owners, click the "Select" button next to the Owners field (notice it changes to a Save button)
7. Check which Users/Groups of Users should be able to login to PAGIS from this device
8. Click the Save button next to the field
9. And then click Save in the upper left portion of the Edit window
10. Have a previous user or Admin login to PAGIS and perform Begin Shift to sync the new data
11. A PAGIS Admin can confirm by navigating to Admin, Admin, and then Users to review the list
12. Another test would be to have the new user attempt to login

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **WHEN USERS LOGIN TO PAGIS, THEY ONLY SEE A GREY SCREEN.**
Q: **CAMERAS AREN'T SHOWING UP IN PAGIS ANYMORE.**
SEE ALSO: "THE LINK LIGHTS ON OUR ALPR COMPUTER/MDC WON'T TURN ON OR FLASH"
A: Below are some basic troubleshooting steps you'll want to follow before creating a support ticket.
1. Doublecheck the physical power switch on the black box/Processor is On. In many vehicles, there is also an in-line switch in the front of the vehicle that needs to be switched On. When the units are properly powered and on, you should see lights and hear fans running.
2. Confirm that the network adapter settings on the laptop match the proper Static IP scheme for the SX Processor in use. The older scheme is 192.200… and the newer scheme is 192.168…. NOTE: the adapter status in Windows should say "unidentified network". If it says "cable unplugged" the laptop can't "see" the SX.
3. If the power and Static IP settings are good and things still aren't working, test further by disabling the three main software related culprits. Turn off/bypass the local Windows firewall, antivirus, and VPN software one at a time.
4. If you're still not able to see the camera feed after that, you may want to use a different network cable as those can get damaged over time and then confirm that the cord is properly plugged into the ports.
5. If the network cord from the SX Processor is routed through a docking station, then it's possible the dock is preventing the traffic. You should contact the dock's manufacturer for the most recent firmware. To test for this, remove the laptop from the dock, directly connect the network cord to the laptop, and then reconfigure the network adapter settings (remove the static settings from the dock's adapter/ and assign the static IP to the laptop's NIC adapter).

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.
Q: **THE LEFT FRONT CAMERA ON OUR ALPR VEHICLE IS NO LONGER SHOWING IN PAGIS**?
Q: **HOW DO WE TROUBLESHOOT MOBILE CAMERAS**?
A: Below are the main troubleshooting steps to test the camera(s) and cable(s) on a system where only one or two cameras are

no longer displaying images.
Step 1: Confirm MDC/SX communication - steps shown in section “Cameras aren’t showing up in PAGIS anymore.” 4220
Step 2: Access the SX Processor – RDP or directly connect a monitor, keyboard, and mouse to the SX. Contact PIPS Support for help with RDP if the credentials are unknown to the agency.
Step 3: Confirm camera activity – Launch Tools. Then open P6Utility or Mobile Toolkit. Check the camera feeds/function by switching the Input menu to the camera(s) in question
Step 4: Unplug and Reattach the Camera Cables – Note, the cables DO NOT TWIST. The metal locking nut on the cable slides back about a millimeter and the cable comes straight out. Do this at the SX Processor and the Camera. You may need to remove the camera from the mount in order to unplug the cable successfully (most brackets use a #3.5 Hex/Allen Wrench)
Step 5: Swap Port on SX Processor – At the SX Processor, swap the camera cables from the non-working camera to a port with a working port (Take care to note the swap so the cables get back to their original ports). If the camera outage stays at the port site, the issue is most likely the capture card on the SX Processor and will require RMA (Example: working Left cam is swapped to port of non-working Right cam and no longer functions. AND the previous non-working Right cam starts working once it’s plugged into the Left cam’s port). If the fault/error stays with the camera regardless of SX port, continue to Step 6.
Step 6: Physically Swap Camera Locations – Once all other items are checked, move the camera itself to a working position in order to test the cable. (Example: physically move Left cam to the Right cam position on the top of the vehicle) Connect the cable at the new position and test feed in Tools > P6Utility/Mobile Toolkit. If the camera works at the new location, the issue is most likely a bad cable. If the camera still does not work, the issue is most likely a faulty camera in need of repair/RMA.

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **WE’RE NO LONGER GETTING GPS IN PAGIS.**
Q: **WE’RE NOT SEEING GPS DATA FROM SOME OF OUR FIELD UNITS IN BOSS.**
A: Below are the basic troubleshooting steps for checking the GPS of field units:
1. Login to PAGIS (as Admin)
2. Navigate to Admin section, then click the Admin button
3. Select “System” on the left pane
4. Confirm/Set the button at top to “Default”
5. Remove any value(s) stored in the GPS Connection String field. Leave ‘5’ in the Computer String.
6. Click the Save button to retain changes made.
7. Close PAGIS fully and relaunch and log back in to test (Note: GPS will only show with test reads/hits)
8. For versions of PAGIS 2.9 and up, test with a GPS Connection String of 6 if the blank field doesn’t work. Save the changes. Log out. Close the software and then relaunch to test.

Please be advised, that some GPS issues can be caused by local or domain firewall settings, antivirus software, or any other software package monitoring/transmitting network data. To test these, disable or bypass those software options on the MDC and retest.

If these initial troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **HOW DO I INSTALL THE PAGIS SOFTWARE?**
Q: **I JUST LOADED PAGIS ON A MACHINE AND IT CRASHES WITH A .DLL ERROR WHEN I TRY TO LAUNCH IT.**
A: The most common installation of PAGIS is Client/Server or “VPRelay Mode”. The .dll error is caused by the installer not being run from the HDD and/or the wrong install option being selected (Example: SupeRex instead of MDC). The best practices for the installation are below. (Note, this does not cover MDC or PAGIS configuration, only the act of installation)
1. Always copy the installer over to the HDD/Desktop of the MDC. Never run it from a thumb-drive or network share
2. Regardless of how you're logged in to Windows, right click the installer and select "run as Admin" or "run with elevated privileges"
3. Continue through the message/error about OS compatibility
4. Click next on the wizard and then be sure to select the MDC option (to use with VPRelay)
5. After that, it's next, next, next, finish the reboot is not necessary

If these steps did not resolve the issue, please feel free to enter a request for support here.

Q: **USERS ARE GETTING HITS/ALERTS ON PREVIOUSLY RECOVERED STOLEN PLATES.**
Q: **USERS AREN'T GETTING HITS FROM KNOWN ACTIVE PLATES.**
Q: **THE HOTLISTS IN PAGIS DON'T SHOW TODAY'S DATE.**
Q: **THE HOTLISTS AREN'T SYNCING WITH BEGIN/END SHIFT.**
A: Whether it's from data latency or just use over time, the local file structure can get some minor corruption and will need to be refreshed. The steps below show the best practices:
1. Login to Windows with Admin rights (ability to uninstall/delete software)
2. Login to PAGIS and perform an End Shift
3. When complete without error, Logout of PAGIS and then Exit/Close the program
NOTE: If the End Shift fails or displays an error, contact Support for additional assistance.
4. If there were no errors, locate the PAGIS icon on the desktop.
5. Right click on the icon and select "Open File Location" (This should open a window where the program was installed)
6. Scroll up and locate the folder labeled "data". Double-click it to open it
7. Select and delete everything in here EXCEPT for "Attributes.db"
8. Once that's complete, Login to the PAGIS software again
9. Perform a Begin Shift. This will pull down fresh data from the server
NOTE: Once complete, the files in the data subfolder as well as the Databases section of PAGIS should be restored.

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **IS PAGIS COMPATIBLE WITH OUR NEW WINDOWS 10 LAPTOPS?**
A: Although there's a warning about compatibility during the install of PAGIS on any Windows OS after XP, it is compatible with all them. However, we have seen errors occur when agencies copy and paste folder structures from previous installations. This of course is not recommended.

Q: **THE LINK LIGHTS ON OUR ALPR COMPUTER/MDC WON'T TURN ON OR FLASH.**
Q: **OUR WINDOWS 10 MDC WAS WORKING BUT HAS STOPPED COMMUNICATING TO THE SX PROCESSOR.**
A: There are many variables with troubleshooting any network connection. And the connection from the ALPR computer to the SX Processor is no different. The following troubleshooting list highlights the most common:
1. The physical network cord is bad/damaged.
A: Test with a different cable and confirm that it is plugged in fully

2. The network adapters are not configured or have incorrect static IPs
A: Confirm the Static IP scheme in use and properly configure the network adapters

3. Local and/or Domain Firewall rules have prevented the flow of communication
A: Disable or bypass these and test again

4. VPN, Anti-Spyware, Antivirus, or other monitoring software has blocked communication
A: Disable or bypass these one at a time and test after each to find the culprit(s)

5. Docking Station Firmware can be incompatible with some newer computers or become corrupt
A: Test by running the network cord straight to the MDC and then configuring the network adapters (NOTE: It would also be a good idea to contact station manufacturer to see what the latest firmware version is and upgrade as necessary)

6. The NIC Drivers have become corrupt
A: Update the specific Networking drivers in use on the MDC through the Device Manager in Windows

7. Turn off all power saving settings of the Ethernet Adapter in the device manager
A: Uncheck "Allow the computer to turn off this device to save power"

8. Check for Windows 10 update 1709 and 1803 as this update will not allow the NIC and Cellular Aircard to run simultaneously

A: Settings > Update and Security > Windows Update > “Update History” link – if there, see the steps in the FAQ 4222

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **AS SOON AS WE DOCK OUR MDC, WE LOSE CONNECTION TO THE WIRELESS.**
Q: **OUR WINDOWS 10 LAPTOP LOSES CONNECTION TO THE INTERNET WHEN THE NETWORK CABLE IS PLUGGED IN.**
Q: **OUR MDC HAS MICROSOFT VERSION 1709 OR 1803 AND CAN’T CONNECT TO WIFI WHEN DOCKED.**
A: Microsoft Updates (1709 and 1803) prevent the Wireless connection as soon as a Network cable is plugged into the device. This also occurs for MDCs/laptops that are docked (where the Network cable from the SX Processor is run through the docking station). As of January 2019, the steps to correct this are below.
WIN10 version 1803
1. Open Regedit
2. Expand HKEY_LOCAL_MACHINE
3. Navigate to Software > Policies > Microsoft > WcmSvc > Local
4. Right click on Local > Hover over New > Select “DWORD (32-bit)”
5. Name the new value “fMinimizeConnections”
6. Right click the on the new name > select Modify > Set value data to 1 (leave base Hex) > Click OK
7. Reboot Windows and test

WIN10 version 1709 - Microsoft fixed this with Update KB 4284822. But if you still have issues, the registry steps are below:
1. Open Regedit
2. Navigate to HKEY_LOCAL_MACHINE > Software > Policies > Microsoft > WcmSvc > Local
3. Right click on Local > Hover over New > Select “DWORD (32-bit)”
4. Name the new value “fMinimizeConnections”
5. Right click the on the new name > select Modify > Set value data to 0 (leave base Hex) > Click OK
6. Then Navigate to HKEY_LOCAL_MACHINE\Software\Microsoft\Wcmsvc
7. Right click on Wcmsvc > Hover over New > Select DWORD (32-bit)
8. Name the value “IgnoreNonRoutableEthernet”
9. Right click on the new value > Modify > Set value data to 1 (leave base in Hex) > OK
10. Reboot Win10 and test

If the steps above did not resolve the issue, you may need to address this with Microsoft. Their support site is here.

APPENDIX D: XML DATASTREAM

Overview

The XML Datastream can be used to push the current data from a running PAGIS system to another application. The data available via the Datastream includes reads, hits and current images. The connection to the Datastream is a TCP/IP socket (default port: 10100). When initially connecting, an XML packet is passed to the PAGIS Software to subscribe to the Datastream. The data connection is configured as "push only" and doesn't allow receipt of additional external data. The current image stream is pushed periodically whereas reads and hits are passed as close to real-time as possible.

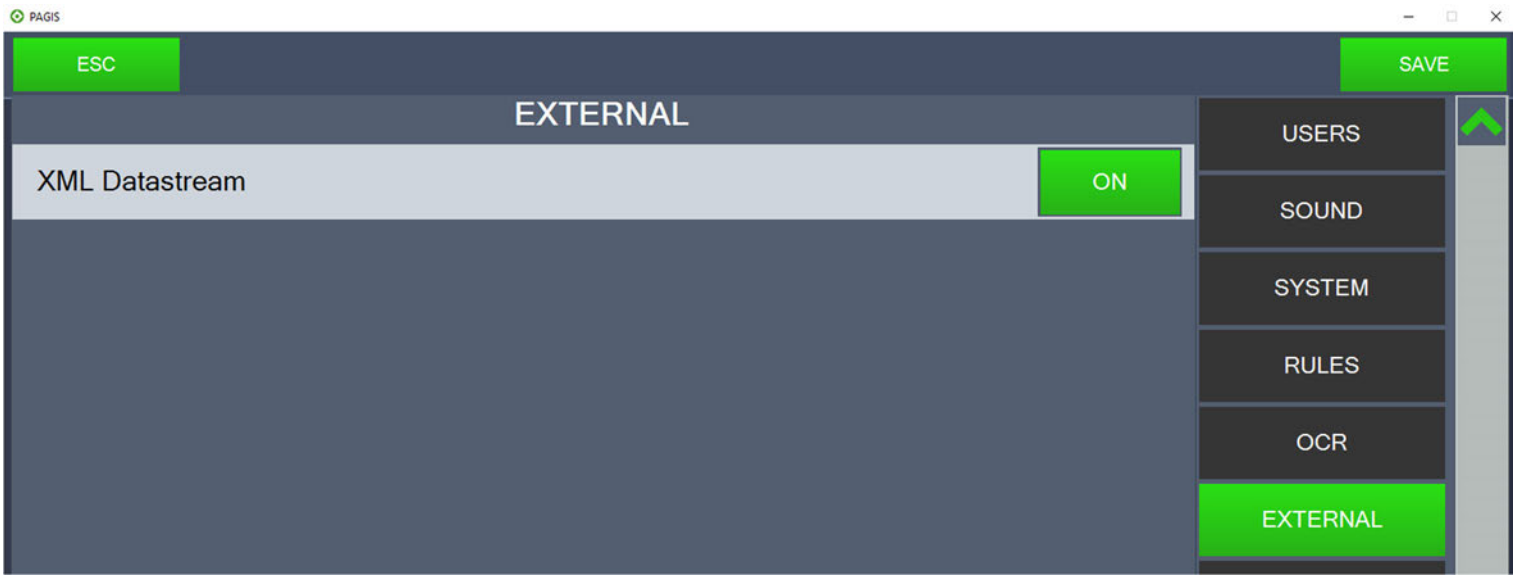
PAGIS Port

By default, the PAGIS.exe.config file has a key for defining the port number for the XML Datastream. The default value is 10100. This setting does not need to be changed unless the default port is unavailable.
The key has the following format:

```
<!--XML Datastream Settings/-->
<add key="XML.Datastream.Port" value="10100"/>
```

PAGIS Admin Setting

To utilize this feature, the XML Datastream needs to be enabled in PAGIS. To do this, navigate to Settings > Admin > External. The "XML Datastream" option should be turned on as shown in the image below and then saved.



XML Subscription

When initially connecting to PAGIS, the Datastream subscriber will receive only a Heartbeat XML packet (see example below) until PAGIS receives a subscription packet from the subscriber. The properly formed subscription packet defines the specific data that the subscriber wishes to receive.

Heartbeat XML Packet

The Heartbeat Packet is sent once every 10 seconds. The purpose of the heartbeat packet is to let the subscriber know that the communications channel is working between PAGIS and the subscriber. The timestamp is sent in the format of "`YYYY-MM-DDThh:mm:ss`".

Sample of the Subscription XML Packet

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-heartbeat>
  <timestamp>2011-10-13T09:41:56Z</timestamp>
</pips-datastream-heartbeat>
```

Subscription XML Packet

A properly formed subscription packet will have all of the data being requested from PAGIS. To receive a specific datatype, a tag must be added to the subscription to define the desired datatype. The valid entries for datatype are: Reads, Hits, and CurrentImage.

- Subscribing to Reads will send all plates that are detected by PAGIS regardless of whether or not it has an associated hit.
- Subscribing to Hits will send all plates detected by PAGIS that are on a hotlist and the associated Read data for that Hit.
- Subscribing to the CurrentImage Datastream offers two additional attributes that may be passed as well. The "camera" attribute can be set to determine which camera the image is coming from. If no value is passed for "camera" the value defaults to zero. The "milliseconds" attribute determines how long the system waits between sending the current image. The default value for milliseconds is 1000. If a value of zero is sent, the system will send a single snapshot.

Sample of the Subscription XML Packet

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-subscription>
  <datatype>Reads</datatype>
  <datatype>Hits</datatype>
  <datatype>HitTrigger</datatype>
  <datatype camera="0" milliseconds="1000">CurrentImage</datatype>
</pips-datastream-subscription>
```

HitTrigger

The HitTrigger packet is used to alert other systems that a hit has occurred on the PAGIS system. The packet is greatly simplified from the Reads/Hits XML packet and only contains the license plate text, timestamp and a description of the hit. The description will contain the name of the hotlist that originated the hit and may be used to send additional information.

Sample of the HitTrigger XML Packet

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-hittrigger>
  <timestamp>2011-10-13T09:41:56Z</timestamp>
  <vrm>SBX989</vrm>
  <hotList name='Alpha'>
    <field1><![CDATA[This is Alpha Field 1]]></field1>
    <field2><![CDATA[This is Alpha Field 2]]></field2>
    <field3><![CDATA[This is Alpha Field 3]]></field3>
    <field4><![CDATA[This is Alpha Field 4]]></field4>
    <field5><![CDATA[This is Alpha Field 5]]></field5>
  </hotList>
</pips-datastream-hittrigger>
```

Reads/Hits XML Packet

The Reads/Hits packet contains information about the plate that was detected. This information includes:

- Source – The device that detected the plate
- Camera – The camera on the device that detected the plate
- Read – The Information about the plate that was captured
- VRM – The plate translated to text
- Timestamp – When the read occurred
- GPS – The location coordinates where the read took place
- ImagesPatch – The image of plate in infrared (IR)
- Overview – The image of scene/car in Color
- Hits – The associated hotlist(s) data

Sample of the Current Image XML Packet

NOTE: The Current/Live Image XML Packet contains the current image from the camera. It is sent every 5 seconds.

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-currentimage>
  <timestamp>2011-10-13T09:41:56</timestamp>
  <data>(Image data here)</data>
</pips-datastream-currentimage>
```

Sample Read with Hits XML

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-reads>
  <reads>
    <source>
      <name>PAGIS_90210</name>
      <software name="PAGIS" version="2.6.8" />
      <camera name="Front Left">
        <read>
          <state>TN</state>
          <vrm>SBX989</vrm>
          <confidence>97.5</confidence>
          <timestamp>2011-09-30T09:30:10Z</timestamp>
          <username><![CDATA[shronski]]></username>
          <gps>
            <latitude>-87.4567</latitude>
            <longitude>98.7654</longitude>
          </gps>
          <images>
            <image name='Patch'>
              <type>IR</type>
              <data>

<![CDATA[/9j/4AAQSkZJRgABAQAAAQABA.....................................................................
.....................................................................................................
..... /9k=]]>
              </data>
            </image>
            <image name='Overview'>
              <type>Color</type>
              <data>

<![CDATA[/9j/4AAQSkZJRgABAQAAAQABAAD.....................................................................
.....................................................................................................
.... //2Q==]]>
              </data>
            </image>
          </images>
          <misread>0</misread>
          <manual>0</manual>
          <hits>
            <hotList name='Alpha'>
              <field1><![CDATA[This is Alpha Field 1]]></field1>
              <field2><![CDATA[This is Alpha Field 2]]></field2>
              <field3><![CDATA[This is Alpha Field 3]]></field3>
              <field4><![CDATA[This is Alpha Field 4]]></field4>
              <field5><![CDATA[This is Alpha Field 5]]></field5>
            </hotList>
            <hotList name='Beta'>
              <field1><![CDATA[This is Beta Field 1]]></field1>
              <field2><![CDATA[This is Beta Field 2]]></field2>
              <field3><![CDATA[This is Beta Field 3]]></field3>
              <field4><![CDATA[This is Beta Field 4]]></field4>
              <field5><![CDATA[This is Beta Field 5]]></field5>
            </hotList>
          </hits>
        </read>
      </camera>
    </source>
  </reads>
</pips-datastream-reads>
```



PIPS TECHNOLOGY™
DETECTION INNOVATION



PAGIS Administrator's Manual

Version 2.14

Updated 4/10/2020

NEOLOGY MOBILITY TECHNOLOGIES

Table of Contents

Table of Contents 2

NOTICES 4

Technical Support 4

Design Changes 4

Trademarks 4

Copyright 4

Version 4

INTRODUCTION 5

1.1 Dual Lens Color and Infrared Camera 5

1.1.1 Available Products 5

1.2 Using This Manual 6

SCREEN REFERENCE 7

2.1 The PAGIS Software Login Screen 7

2.1.1 Logging on with the Default Administrative Account 7

2.2 Main Screen - Live View 8

2.2.1 Getting Started in PAGIS 8

2.3 The PAGIS Navigation Buttons 9

2.3.1 Camera Control Buttons 9

2.3.2 GPS Indicators 10

2.3.3 Camera Firmware Update (Restricted Users) 10

2.3.4 Day/Night Mode 10

2.4 Begin Shift 11

2.4.1 Sync via USB Thumb drive (or Local Source) 11

2.4.2 Sync via Wireless Network 11

2.4.3 PAGIS Auto-Sync Settings 11

2.4.4 Begin Shift – Additional Information 11

2.5 End Shift 11

2.5.1 Sync to BOSS 11

2.6 Cam Mode Button 12

2.6.1 Camera Modes 12

2.7 Taking a Picture 12

2.8 Search Entry Screen 13

2.8.1 Searching Synchronized Hotlists for License Plates 13

2.8.2 Searching Locally Stored Reads and Hits 13

2.8.2.1 Searching for a Match 14

2.8.3 Wild Card Symbols 14

2.8.4 Manually Adding a Plate to PAGIS 15

2.8.4.1 ADD VLP Query 15

2.8.4.2 ADD VRM Report Screen 15

2.9 The Review Screen 16

2.9.1 Summary Review Section 16

2.9.2 Review Navigation Buttons 16

2.9.3 Reads 17

2.9.3.1 Reads Result Screen Navigation Buttons 17

2.9.3.2 Interactive Buttons – Reads Screen 17

2.9.4 Hits 18

2.9.4.1 Hit Screen Attributes 18

2.9.4.2 Hit Screen Function Buttons 19

2.9.4.3 Interactive Buttons – Hits Screen 19

2.9.4.4 Set Disposition – Additional Detail 19

2.9.4.5 Add Intel – Additional Detail 20

2.9.5 Misreads 20

2.9.5.1 Marking a Record as a Misread: 21

2.9.6 Audits 22

2.9.7 Targets 22

2.9.7.1 The Targets Screen 23

2.9.7.2 Targets Screen Navigation Buttons 23

2.9.8 Databases 24

2.9.8.1 Databases Screen Functions 24

2.9.8.2 Databases Screen Navigation Buttons 24

2.9.8.3 Databases Edit- “Manual Reports” 25

ADMIN SETTINGS 26

3.1 Sync Options Screen 26

3.1.1 Synchronization Types 26

3.1.1.1 Synchronization to Disk (Local Storage) 27

3.1.1.2 Synchronization with BOSS 27

3.1.1.3 Sync to “Instation” (Formerly BOF2 and BOF3) 28

3.1.2 Global Sync Options 29

3.2 PAGIS Privacy Settings (Local Data Retention) 30

3.3 Language 31

3.4 Location 31

3.5 Users 32

3.5.1 User Privileges ____ 32
3.6 Sound ____ 33
3.6.1 Configuration Buttons ____ 33
3.7 System ____ 34
3.8 Rules ____ 35
3.8.1 Rules – Additional Clarifications ____ 35
3.9 OCR ____ 36
3.10 External ____ 37
3.10.1 XML Datastream Ports ____ 37
3.11 Cameras ____ 38
3.11.1 Checking the Connection ____ 38
3.11.2 Troubleshooting Camera Connections ____ 38
3.11.3 Configuring the Cameras in PAGIS ____ 39
3.12 Cam Setup ____ 40
3.12.1 Cam Setup Navigation Buttons ____ 40
3.13 Configs (Camera View Modes) ____ 41
3.13.1 Configs Navigation Buttons ____ 41
3.13.2 Reviewing and Modifying Existing Modes ____ 42
3.13.3 Adding a New Camera Mode ____ 43
3.14 Info ____ 44
3.15 Camera Firmware Update, (Admin) ____ 44
PAGIS INSTALLATION GUIDE ____ 45
4.1 PAGIS System Requirements ____ 45
4.2 PAGIS Prerequisites ____ 45
4.2.2 PAGIS Software Installation (MDC) ____ 46
4.2.3 PAGIS Software Installation (Mobile Processor) ____ 47
TROUBLESHOOTING TIPS ____ 48
5.1 Troubleshooting & Tips ____ 48
5.1.1 PAGIS with NetMotion VPN ____ 48
5.1.2 Cisco VPN Client: ____ 48
5.1.3 Microsoft .NET 3.5 Installation ____ 48
5.1.4 Firewall Settings for Client-Server Installations ____ 48
PAGIS/BOSS3 CONFIGURATION ____ 49
6.1 Creating a New Device in BOSS3 ____ 49
6.2 Enabling a New Mobile System in BOSS3 ____ 49
6.3 Assigning Ownership to a Device in BOSS3 ____ 49
6.4 Assigning Hotlists to a Device in BOSS3 ____ 50
PAGIS/BOSS4 CONFIGURATION ____ 50
7.1 Creating a New Device in BOSS4 ____ 50
7.2 Enabling a New Mobile System in BOSS4 ____ 50
7.3 Assigning Ownership to a Device in BOSS4 ____ 51
7.4 Assigning Hotlists to a Device in BOSS4 ____ 51
APPENDIX A: THE GLOSSARY ____ 52
APPENDIX B: PAGIS SOFTWARE DATABASE FILE ____ 53
APPENDIX C: FAQ ____ 55
APPENDIX D: XML DATASTREAM ____ 60

4228

NOTICES

The information within this manual is authorized for distribution to customers, authorized service center personnel, and distributors of Neology. Every effort has been made to supply correct information. However, Neology assumes neither responsibility for its use, nor for any infringements of patents or other rights of third parties, which may result from its use. No license is granted by the manufacturer under any patent or patent rights. Neology reserves the right to modify and update the equipment at any time without prior notice. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means to a third party without the prior consent of the copyright holder. The manufacturer's warranty will be invalidated if untrained personnel operate the equipment or if any attempt is made to service the equipment by unauthorized personnel.

This manual contains confidential and proprietary information and should not be redistributed except as needed for proper use and maintenance of the agency's Mobile ALPR system.

Technical Support

Service of this equipment by replacement of parts, on-site repair, routine maintenance inspection, and scheduled remote support session is available. Please contact PIPS Technology's ALPR Technical Support.
Phone: 833-PIPS-LPR (833-747-7577), Option 2
Support Team Email: Support@PIPSTechnology.com
For Customers in Europe, Middle East and Africa: Support@PIPSTechnology.co.uk
Web: www.pipstechnology.com
Fax: 858-391-0264
Corporate Office: 13520 Evening Creek Drive Suite 460. San Diego, CA 92128

Design Changes

Neology reserves the right to change the design of any product from time to time without notice and with no obligation to make corresponding changes in products previously manufactured.

Trademarks

PIPS Technology™ is a trademark of Neology Inc., and either registered or pending registrations in several jurisdictions. Windows, Windows 7, Windows 8, Window 10, and .NET are all trademarks of the Microsoft Corporation. Other trademarks and registered trademarks are the property of their respective owners.

Copyright

The Neology / PIPS Technology PAGIS Software is copyright of Neology. All rights reserved. This product contains confidential and trade secret information of Neology and is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portions of it, may result in civil and criminal penalties.

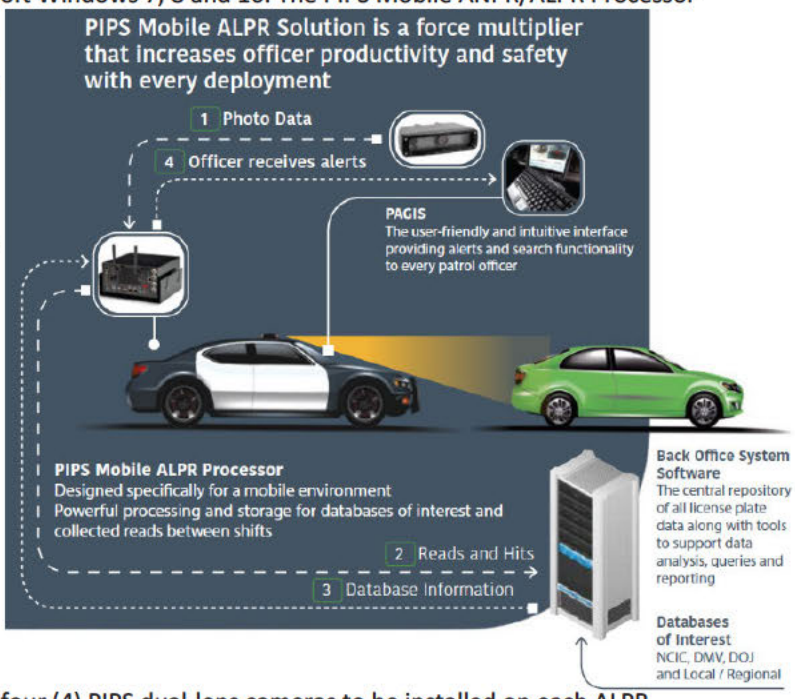
Version

This manual demonstrates the attributes of the Neology / PIPS Technology PAGIS Software Version 2.14 and was last updated in March 2020.

INTRODUCTION

PIPS Technology's Automated License Plate Recognition (ALPR) software solution called PAGIS utilizes dual-channel, dual-lens, cameras to "read" plates. Our software is optimized to run on the Mobile Processor itself or in conjunction with a mobile data computer (MDC). Our mobile software is compatible with Microsoft Windows 7, 8 and 10. The PIPS Mobile ANPR/ALPR Processor comes equipped with Microsoft Windows 7 Embedded.

The PAGIS Software processes the infrared plate image provided by any of the cameras and then interprets the plate number through Optical Character Recognition (OCR) via the mobile processor. The PAGIS application then searches for any matches of the plate with those listed in the databases, or "hotlists," distributed from the PIPS Back Office System Software (BOSS) or other external sources.



WARNING: To reduce the risks associated with impact, which if not avoided, could result in serious injury or death: Do Not interact with the ALPR system while driving in hazardous situations. The PIPS mobile camera series and License Plate Capture Software are not intended for use in hazardous environments, so that the User and/or others are not put at risk for personal injury and/or property damage.

1.1 Dual Lens Color and Infrared Camera

The PIPS Technology Mobile ALPR System allows for a maximum of four (4) PIPS dual-lens cameras to be installed on each ALPR vehicle provided that the vehicle supports the additional mounting equipment.

Each dual-lens mobile camera uses visible light to take color overview pictures of the vehicle and uses infrared (IR) illumination to capture the license plate's alphanumeric characters. IR illumination offers the best capture performance of reflective license plate characters for the following reasons:

- State issued license plates are designed to be highly reflective to IR light.
- Cameras using IR capture technology do not depend on the presence of visible light to function.
- Cameras using IR capture technology are not negatively impacted by the effects of headlights, solar glare, or total darkness.
- IR light penetrates rain and fog better than visible light.
- Due to these attributes, the system can be used 24 hours a day, seven days a week.

1.1.1 Available Products

Additional information about this and other PIPS Technology applications, cameras, and solutions are available on the PIPS web site: http://www.pipstechnology.com

1.2 Using This Manual

The section overview of this software manual is as follows:

Section 1: The Introduction and Basics

Section 2: PAGIS User's Section: Explains screen function and User Operations in the PAGIS Software

Section 3: Troubleshooting Tips

Section 4: Software Administrator's Guide: Explains how to install and configure the PAGIS Software

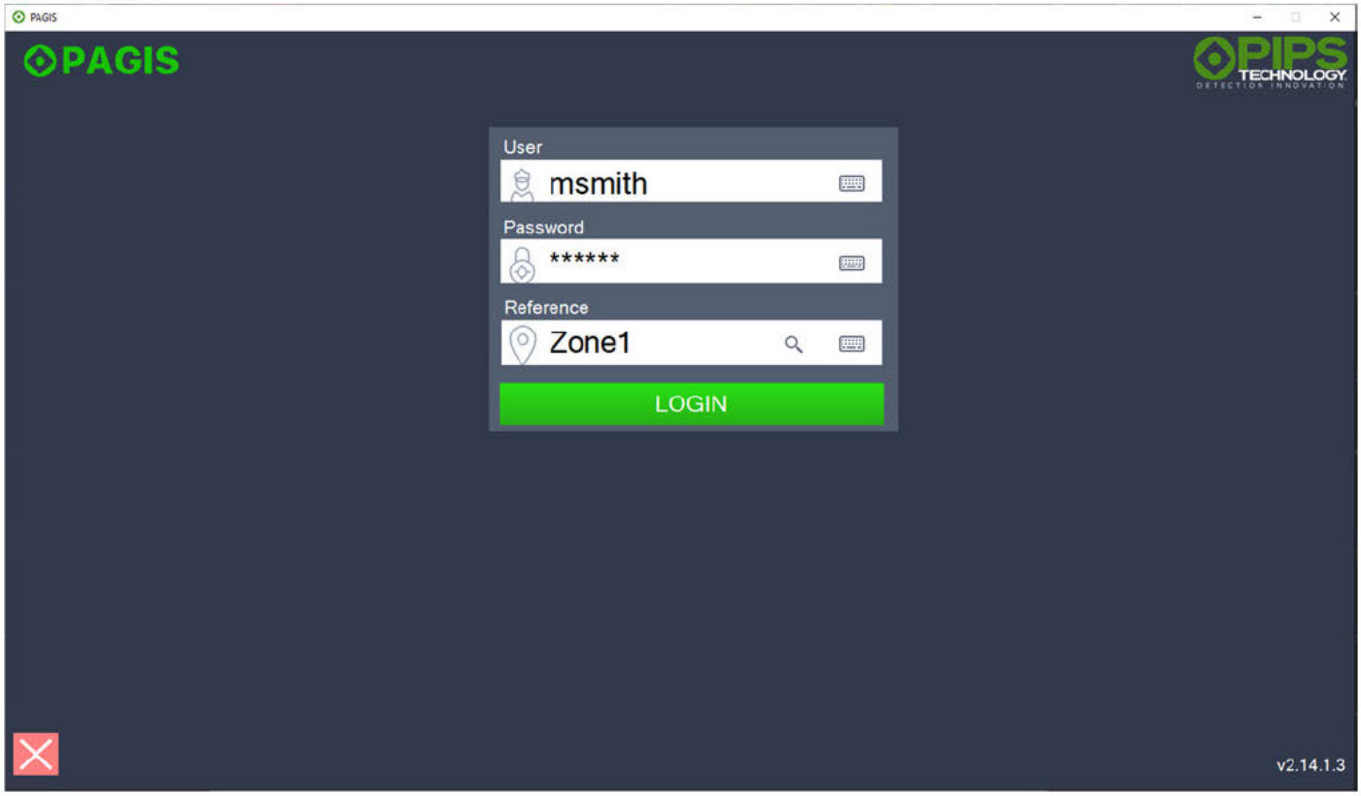
Section 5: Additional Information and Troubleshooting Tips

Section 6: Initial BOSS configuration for new PAGIS devices (MDCs)

Appendices: Additional features and details

SCREEN REFERENCE

This section guides the user through the PAGIS Software screens and the available options. Screens are grouped according to function. When a button is grayed out or missing, the option is not available, or no information has been accrued to activate it.



2.1 The PAGIS Software Login Screen

The PAGIS Software allows users with various access privileges to use the same MDC. For users with touch screen monitors, the Keypad button immediately to the right of any text box gives the user access to an on-screen keyboard for data entry.

User Field: The alphanumeric string assigned to identify the user. Usernames are not case sensitive.
Password Field: Password of the assigned user logging in. Passwords are case sensitive.
Reference Field: This is an optional field utilized to fit a number of use cases. A user can manually enter a reference at logon, leave the field blank, or select list of unique tags that will be associated with all data captured while logged in. If the Administrator has configured a default reference tags, that information will be displayed automatically. Otherwise, it will be blank.
Login Button: Submits the username and password to attempt a login.
Exit Button: By clicking the X icon in the lower left-hand corner, the user can exit/close the PAGIS Software.

2.1.1 Logging on with the Default Administrative Account

The PAGIS Software includes a default administrative account that can be used for the initial configuration. To do so, simply click the **Login** button with the User and Password fields blank.

NOTE: System Administrators are strongly encouraged to configure users for PAGIS just before, or soon after the installation and setup. PAGIS users accounts are created and maintained in BOSS. Once Users are established by the BOSS System Administrator, the default user account is automatically disabled. Best practices are to be certain at least one User account has administrative privileges.

2.2 Main Screen - Live View

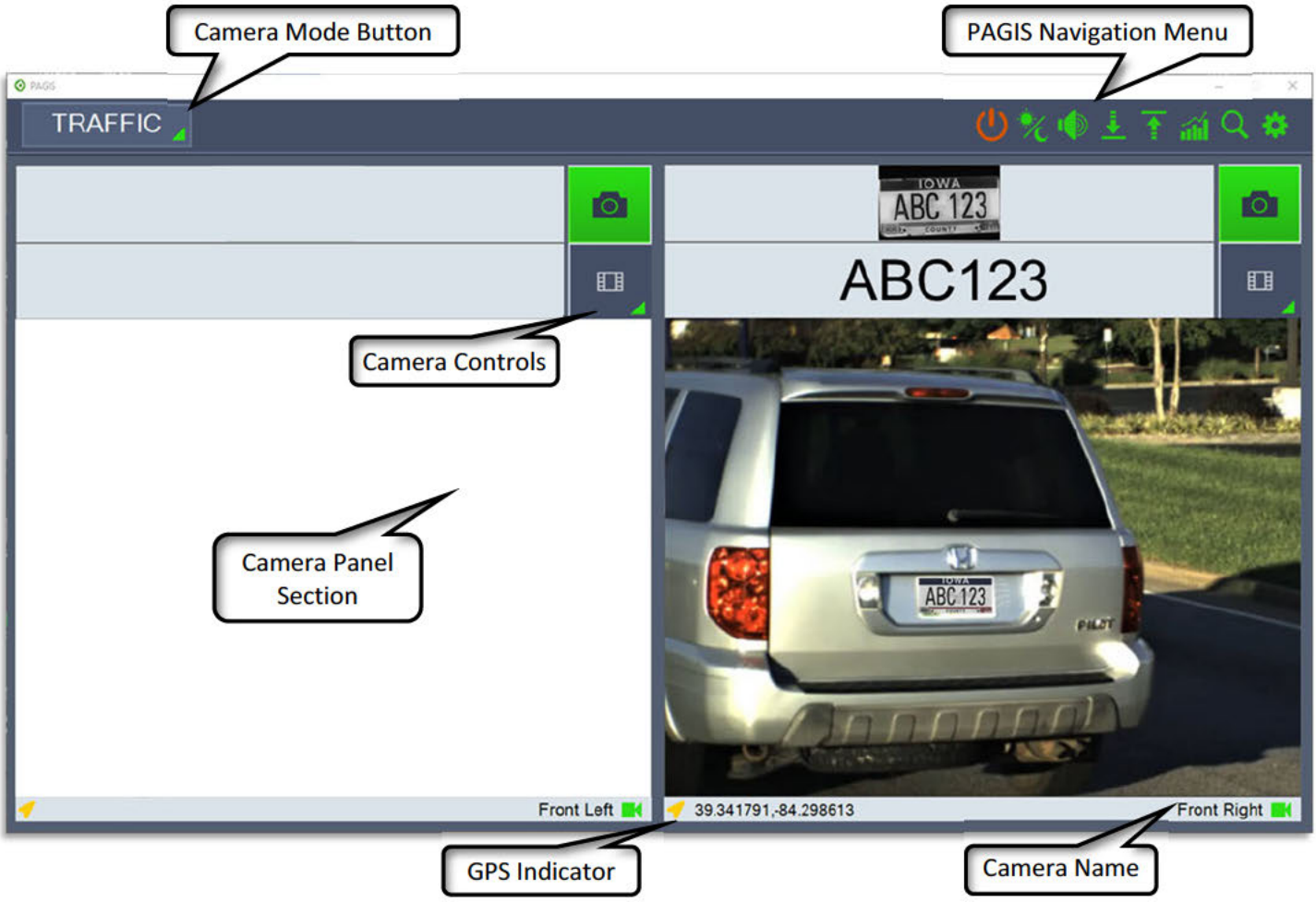
Upon a successful login, the user will see the Main screen (Live View). This is the default view and starting place of all PAGIS Software features. (NOTE: Access to features is based on user group rights established in BOSS.)

The Main Screen is also the place users will monitor read images and ALPR "hits". At the initial startup of the system it is normal to see only a blank/grey screen for a few seconds. Once a connection has been established with the mobile cameras, white boxes will be displayed showing the live-feed camera panels. At this point, the system is ready to capture reads/plates.

2.2.1 Getting Started in PAGIS

By default, PAGIS loads into a static view. This means live video will not automatically appear in the camera panels (white boxes) until a plate has be captured or the user selects one of the live feed options.

Once a plate is "seen" by a camera assigned to the current viewing mode (Traffic vs Parking), it will display the captured information in the corresponding camera panel. Each plate capture is also accompanied by a short "Beep" to audibly alert the user a read has taken place. (NOTE: If the user is in the Traffic Mode at the time a parking camera reads a plate, there will be a sound effect, but no plate image will be displayed on screen unless that plate is on a synchronized Hotlist or until the user switches to Parking Mode.)



2.3 The PAGIS Navigation Buttons

4234

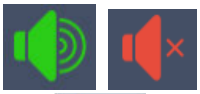
This section provides a quick reference guide to the available navigation buttons of the Live View screen.



The Camera Mode button is located in the upper left corner and is used to switch between the configured camera modes. Once configured, the name will change to a selected mode. The default values are “ALL”, “Traffic” and “Parking”.



The Logoff button is located in the upper right of the window. When selected, the user will be logged out of PAGIS and return to the login screen.



The Sound button is located to the right of the Logoff button. When selected, this button with toggle the PAGIS system sounds On and Off.



Day/Nite mode switches PAGIS between day & night mode screen skins.



The Begin Shift Synchronization button is located to the right of the Sound button. When selected, this will reach out to the BOSS server to download users, hotlists, and other system settings.



The End Shift Synchronization button is located to the right of the Begin Shift Button. When selected, this will upload any previously unsent reads, images, and audits to the BOSS server.



The Statistics/Review button is located to the right of the End Shift Button. When selected the user is able to review Databases/Hotlists, Reads, Targets, and other PAGIS information.



The Search button is located to the right of the Review Button. When selected the user can search his/her reads as well as manually add a license plate to a temporary hotlist.



The Admin/Settings button is located in the upper right corner of the screen. This button is only viewable to Admin level users and allows for system configuration changes and setup.



Firmware update icon will atomically appear when PAGIS detects a new firmware is available for the P720 mobile cameras. All user types are notified, but only Admins can apply the update.

2.3.1 Camera Control Buttons

The dual-lens cameras can capture both color and an infrared image. Formerly, there were a total of three buttons that allowed the user to view the IR and color feed as well as capture a picture directly from PAGIS. Now there is a toggle button to switch between color and IR views and a separate button to take a picture. These buttons are displayed on the main Live Screen as shown below:



The Camera View Selector button: This is the default state at login showing the Static View. (**NOTE**: PAGIS does not automatically display a life feed.)



Color View: by clicking on the Camera View Selector button once, the user will switch to the Color View Mode. This displays the current view of the color camera and will time out after 60 seconds.



IR View: by clicking on the Camera View Selector button twice, the user will switch to the Infrared (IR) View Mode. This displays the current view of the IR camera and will time out after 60 seconds.



The Take Pic button: Just above the Camera View Selector button is the “Take Pic” button. This button allows the user to quickly take a picture from the camera currently viewed.

2.3.2 GPS Indicators

GPS is stamped on each read and hit as capture events take place by the system. The signal strength and location indicators are located underneath the camera panels at the bottom of the Live Screen.

39.341788,-84.298518 Shows an example of the Location Indicator displaying the Lat/Long on the most recent read

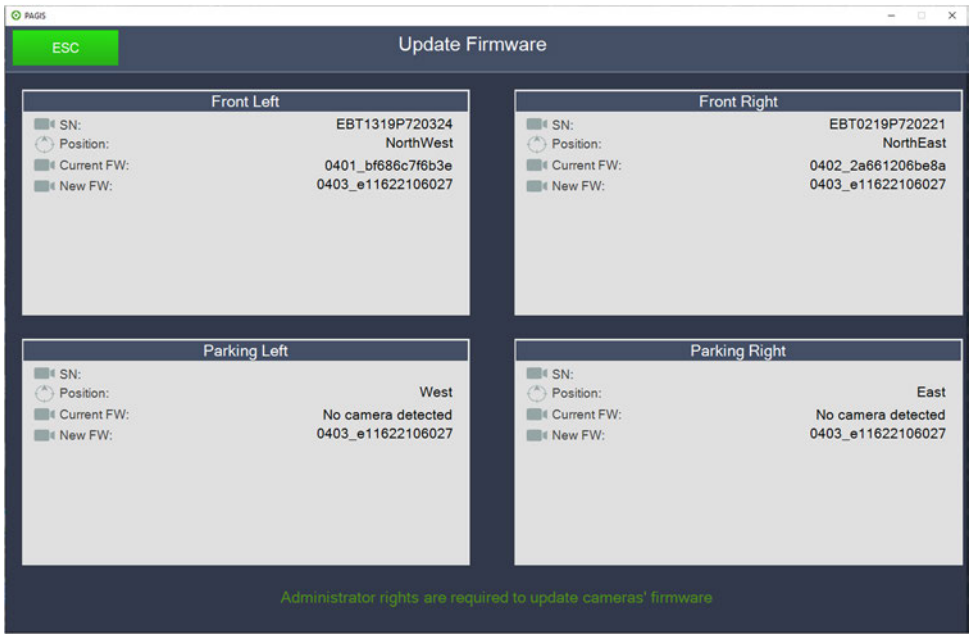
A green or yellow indicator shows a strong or medium strength GPS lock.

A red indicator shows there is no available GPS information.

2.3.3 Camera Firmware Update (Restricted Users)

Camera firmware update provides a means for PIPS to update the camera software to enhance and or correct camera performance. The frimware icon will only apper when update is avialable.

- The firmware update process only updates camera that are attached and function on the mobile processor.
- Restricted PAGIS users are only notified and displayed update information, only a PAGIS administrator can apply the FW update.

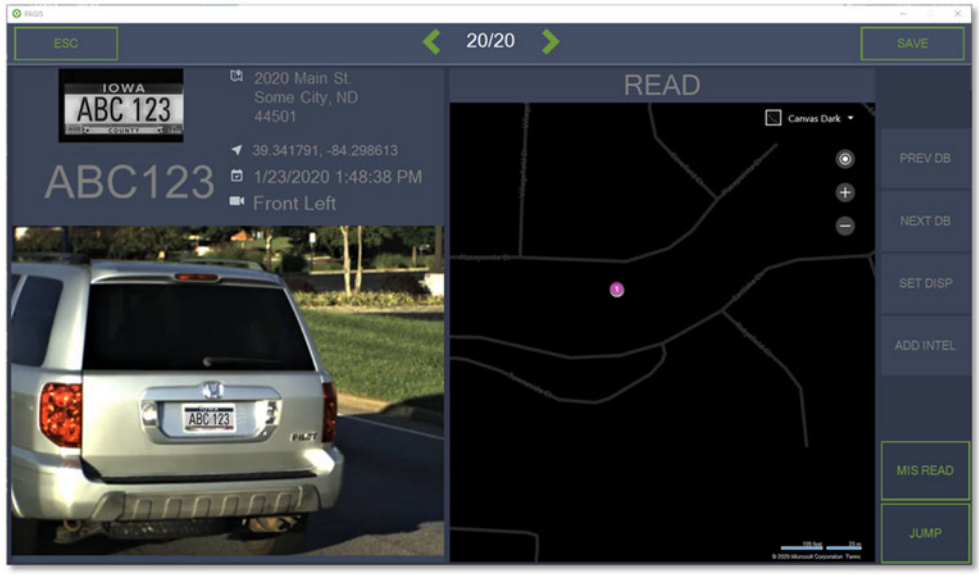


Firmware Updater Window List.

- Title “Camera Name”.
- Camera serial number.
- Position.
- Current FW version.
- New FW version available.

2.3.4 Day/Night Mode

Day/Night mode changes PAGIS user interface skins to a darker appearance to reduce illuminating the vehicle interior.



2.4 Begin Shift

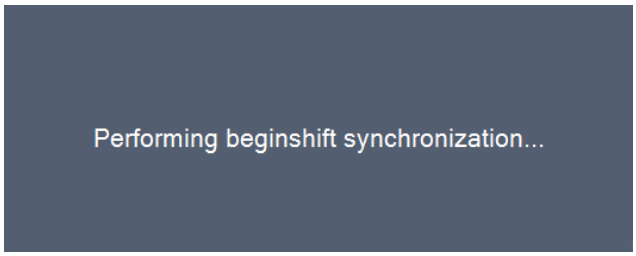
Begin Shift is thought of as the first step for all PAGIS users. From the Live View Screen, the PAGIS user must click the Begin Shift button twice. Once to select the function and once more to launch the Sync. With most agencies, this action utilizes a wireless network to import all the necessary data used during a shift (Hotlists, Dispositions, and Targets) directly from the BOSS Server. However, agencies can also configure their systems to perform this function via Thumb drive or a local source file.

2.4.1 Sync via USB Thumb drive (or Local Source)

Depending on the agency network, some alter the default PAGIS/BOSS configuration mode to use a USB Thumb drive or locally stored file on the MDC/Laptop instead of the wireless Sync. In order to synchronize effectively, the user must first confirm he/she has access to the source location before initiating Begin Shift. **NOTE**: All synchronizations using this method must be performed manually. To learn more about this process, refer to the "Client Tools" section of the BOSS Manual.

2.4.2 Sync via Wireless Network

Synchronizations over a wireless network provide the agency with additional automated features. Best practices recommend the user manually launch Begin Shift from the Live View Screen at the beginning of every patrol shift. However, it is possible for users to allow PAGIS to synchronize via its auto-sync settings. When a manual Begin Shift is launched, the Main View Screen removes the camera feeds and displays a status window of the Sync process. Once the Begin Shift operation is complete, PAGIS will return to the normal Main View Screen.





2.4.3 PAGIS Auto-Sync Settings

PAGIS auto-sync settings are best thought of as how PAGIS receives additional updates and maintains the downloaded ALPR data throughout the entire patrol shift. This prevents the need for the officer to manually perform Begin Shift functions multiple times a day. The auto-sync occurs every 30 seconds and receives data in small batches. The batches are not to exceed 1MB in size for every minute of download. In addition to receiving data, the auto-sync function also uploads a copy of data collected by PAGIS and sends it to BOSS for reporting/processing.

2.4.4 Begin Shift – Additional Information

By default, the synchronizations in PAGIS receive only what has been changed to the ALPR data since the last Sync. Meaning, if some plates have been removed from a Hotlist and others have been added, the system will only transfer that data instead of downloading the entire Hotlist each time the Begin Shift is launched. This helps to reduce the amount of data transferred over the agency's network. **NOTE**: Begin and End Shift synchronization, as well as all auto-sync features, are dependent upon stable communication to the BOSS server via an active data connection.

2.5 End Shift

End Shift in PAGIS is the process in which all the collected ALPR data (Reads, Hits, and Images) from the recent shift is uploaded to the BOSS server and cleared from the local cache. As with Begin Shift, the agency has two options. They can choose to Sync via USB Thumb drive or via wireless connection. Best practices recommend users perform an End Shift Sync at the end of every patrol.

2.5.1 Sync to BOSS

At the end of every shift, the accrued ALPR data should be exported to BOSS. Just like with Begin Shift, the user must click the button twice to launch it (once to select it and once more to execute the Sync). During the Sync, PAGIS uploads any Reads, Hits, and Images not already synchronized to BOSS and purges these items from the local cache on the MDC's hard drive. Completing an End Shift also removes any VLP entries manually added to PAGIS during the shift.

2.6 Cam Mode Button

Clicking the Cam Mode button in the upper left corner of the Live View Screen allows the user to cycle through the different camera modes configured by the PAGIS Administrator. Changing the camera mode changes which cameras are displayed on the Main Screen.

2.6.1 Camera Modes

By default, PAGIS provides "Parking" and "Traffic" as the two configuration modes. Users often switch these modes to suit their current use-case. For example, an officer in a parking lot will often switch the mode to "Parking" so s/he can see the parking cameras on the Live View Screen. They can then switch back to "Traffic" when monitoring city streets.

2.7 Taking a Picture

The PAGIS software has ability to quickly take a picture from one of the currently displayed ALPR cameras on the Live Screen. The user only needs to click on the Take Pic button.



To Take a Picture:

1. From the Live View Screen, press the Take Pic button from the desired camera
2. The image taken will be displayed
3. Enter a description of the picture in the text field at the bottom of the screen
4. Press Save to save the picture or Escape to cancel. Either action will return you to Live View.

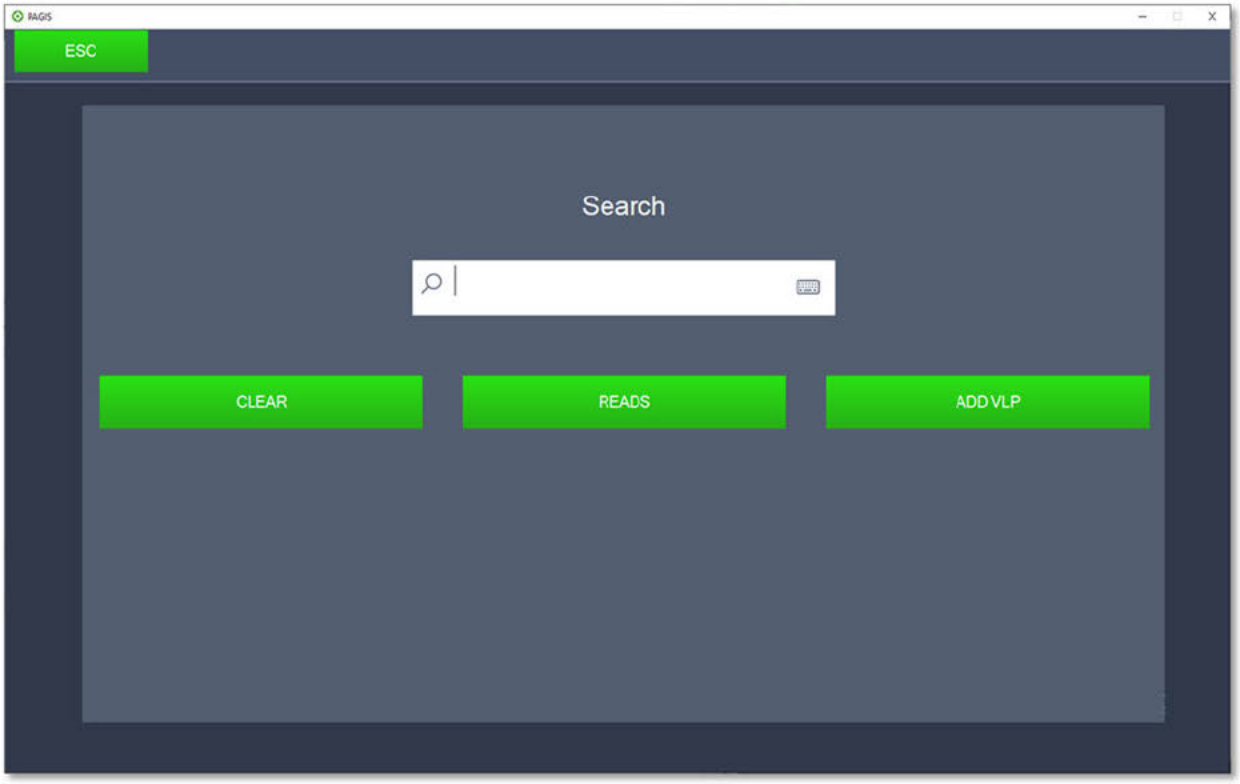
NOTE: The picture will Not be saved if a description/note is not entered in the text box.

To View the Saved Images:

1. Navigate to the Review menu in PAGIS
2. Select Audits
3. The user will be able to see a thumbnail of the image and the saved text/note
4. In order to review the saved images at a later time, the user will need to run the Audit Report from BOSS.

2.8 Search Entry Screen

Pressing the Search button icon from the Live View screen or SEARCH from the Databases window allows the user to search all manually entered plates as well as all BOSS synchronized databases (Hotlists) for license plate and target information. Users can also search all locally stored reads/images accrued since the last End Shift by clicking the Reads button instead of pressing the Enter key.



2.8.1 Searching Synchronized Hotlists for License Plates

By entering a vehicle license plate number (VLP) and pressing the Enter key or the ADD VLP button, the user can quickly search all the stored plate information locally collected as well as the information from all synchronized hotlists distributed from the BOSS server. **NOTE**: Hotlists can only be searched by entering complete VLPs. Wildcards and partial plate numbers will not return results.

Search Box: The text field used to enter the desired plate search via alphanumeric characters and/or wild card symbols.

Clear Button: Clears the contents of the search box.

Driver's License Info: The search field can also check the Hotlists for any DL information stored (Not available all countries).

Reads Button: This button searches for a match from all the reads/hits locally stored on the MDC/Laptop.

ADD VLP: Searches all locally stored hotlists for the plate and if there's no match, allows the user to add the plate to the "Manual Reports" alert list for use in the field. **NOTE**: All manual entries are cleared with each End Shift

ESC: The Escape button allows the user to exit to the Main/ Live View screen.

2.8.2 Searching Locally Stored Reads and Hits

As mentioned previously, this search function allows users to find reads and hits directly from their recent patrols using the search field and the Reads button. These searches pull only the reads and hits locally gathered/stored since the last time the user completed an End Shift. **NOTE**: The search results are specific to each Windows User Profile and do NOT pull images from the BOSS server.

2.8.2.1 Searching for a Match

4239

- From the Search field, users may enter a plate (or partial plate with wildcards) and then click the **READS** button.
- Results are displayed with the data gathered at the time the read was taken (See example below).
- Each result should display the infrared (IR) image of the plate as well as the color overlay of the vehicle for review.
- Each result shows the GPS data, Closest address point, Time and Date, and the Camera that read the plate.
- If there are multiple results, the user can cycle through them by clicking the left and right navigation arrows.



2.8.3 Wild Card Symbols

The use of wild card symbols in the Search box allows greater flexibility for the user, but may return a larger set of results.

- Wild card searches performed using the asterisk (*) designates an unknown number of characters.
- Wild card searches performed using the underscore (_) indicates a single missing or unknown character.
- Searches can be performed using one, both or no wild card symbols.

Example: The officer received an alert from Dispatch looking for a vehicle plate containing the letter J and the number 8 separated by one character. Because the officer doesn't know how many characters there are before or after the J and 8, he enters *J_8* in the search box to review all possible matches of J and 8 separated by only one digit.

2.8.4 Manually Adding a Plate to PAGIS

PAGIS allows users to manually add a plate of interest directly into the software as needed. Once saved, these entries are stored as part of the Manual Reports alert list and work just like any other Hotlist synchronized from the BOSS server.
NOTE: These additions are designed to be temporary and are cleared from the software with each End Shift.

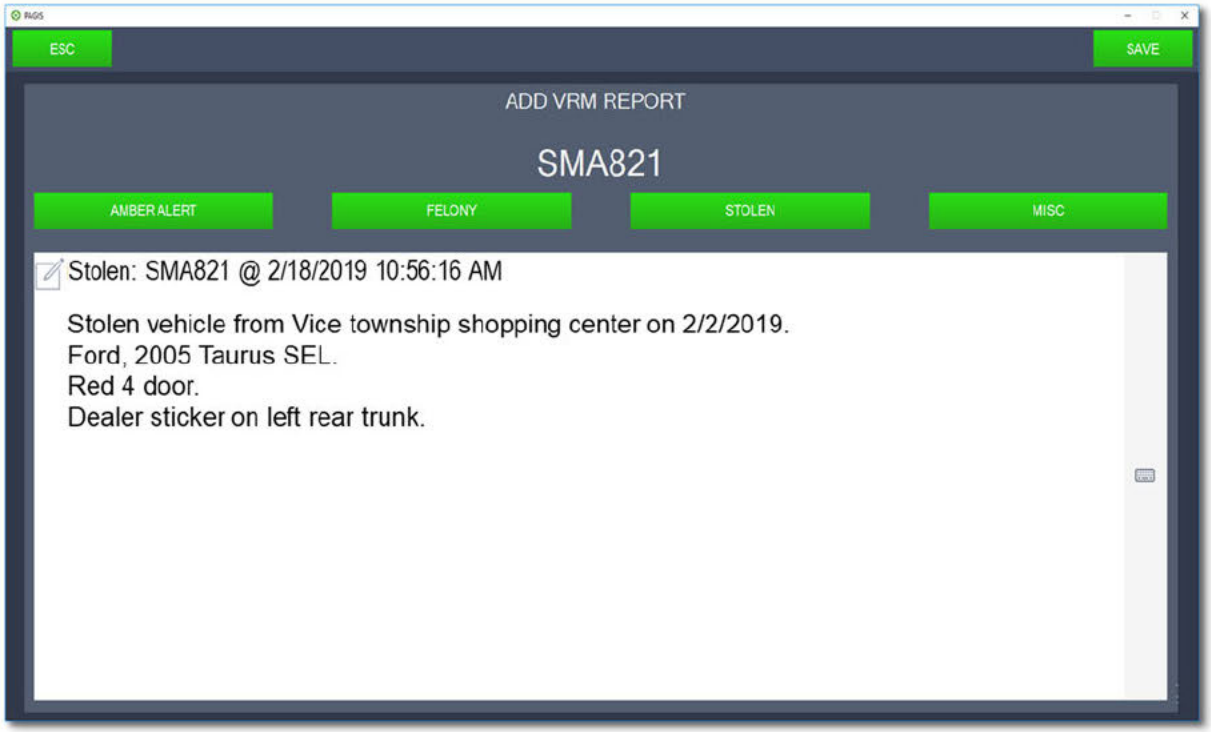
2.8.4.1 ADD VLP Query

Before an entry is added to the Manual Reports Hotlist in PAGIS, the software searches all stored databases for a match. If a match occurs, a message will display under the search box showing which Hotlist(s) it has been found in. If the VLP query does not return a match, the "ADD VRM REPORT" screen appears.



2.8.4.2 ADD VRM Report Screen

If the desired plate does not already reside in another Hotlist, the ADD VRM Report Screen becomes accessible to the user.



1. From the Search Entry Screen, enter the desired plate to add.
2. Click the ADD VLP button. If no match is found on any other hotlist, the "Add VRM Report" screen will appear.
3. Click to select the applicable alert type (AMBER ALERT , FELONY , STOLEN , or MISC)
4. Either leave the default information or add additional detail.
5. Click Save at the top right to add the plate to the Manual Entries Hotlist

2.9 The Review Screen

4241

PAGIS allows users to review all locally stored data from one easy location. Clicking the Review icon from the Main Screen launches Review. This screen is divided into the Summary View Chart and sub-section navigation buttons to the right.



2.9.1 Summary Review Section

The Summary View Chart is divided into five categories and allows a user to review the information collected during their shift at a glance.

Total Reads: Shows the total number of Reads/Hits synced to BOSS and the total number of reads captured during the shift.
Reads: Shows the total number of reads synced to BOSS and the total number of reads captured during the shift.
Hits: Shows the total number of hits synced to BOSS and the total number captured during the shift.
Misreads: Shows the total number of reads marked as a "misread" synced to BOSS and the total marked during the shift.
Audits: Shows the total number of audits synced to BOSS and the total number of audits during the shift.
Targets: Shows only the number of targets downloaded from BOSS.
(NOTE: The Sync value will always be zero for customers using Disk Sync mode/Client Tools.)

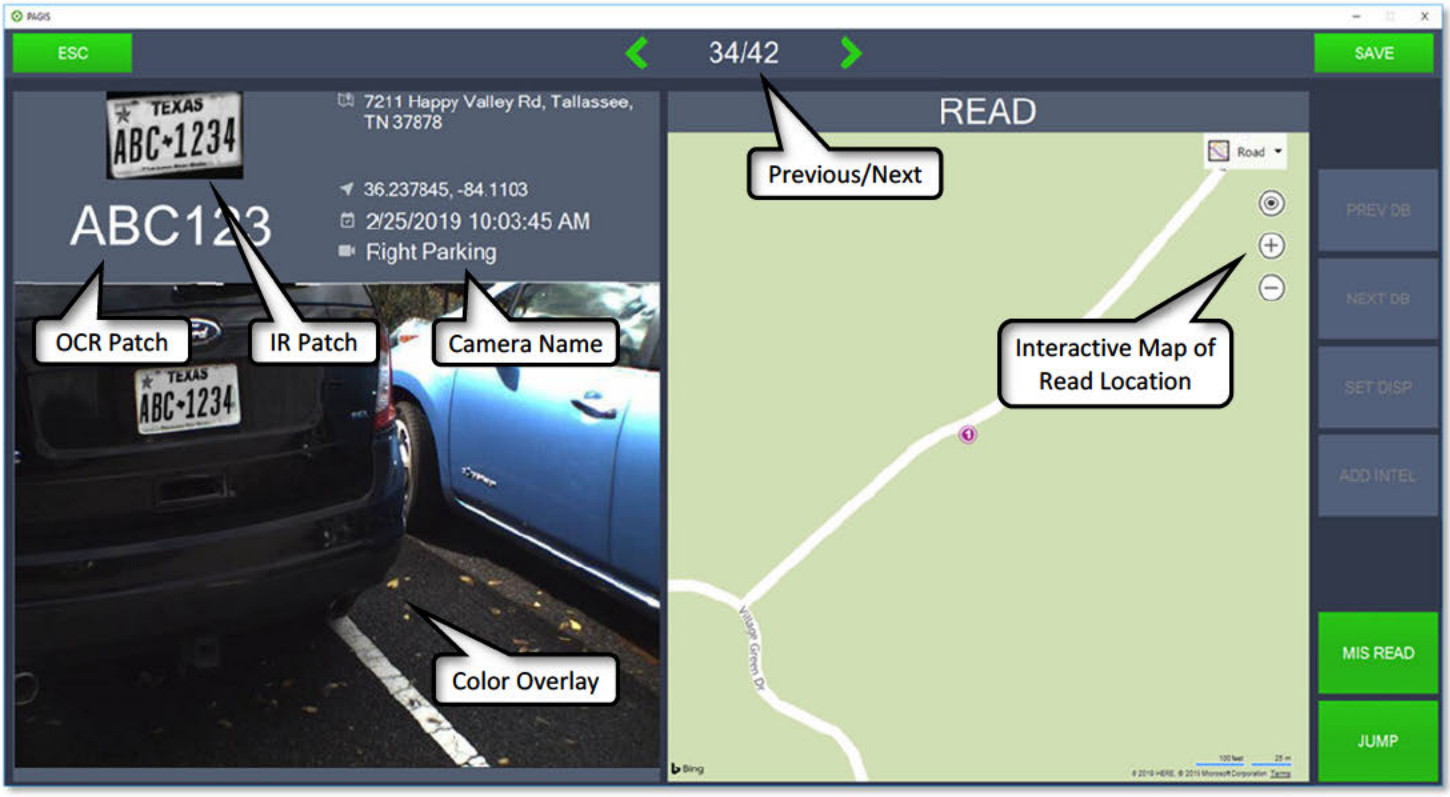
2.9.2 Review Navigation Buttons

The navigation buttons allow the user to review specific sets of information gathered during the shift.

Reads: Review all plate detections that have occurred since the last End Shift synchronization.
Hits: Review the hit alerts for Vehicle License Plate (VLP) reads that matched a Hotlist.
Misreads: Review reads and/or hits that have been manually flagged during the shift as misreads, where the plate number in the image does not match the OCR interpretation of the plate (e.g., a letter O misread as a Q or zero).
Audits: Review failed and successful logons, any manual data entered during the shift, pictures taken and all manual license plate searches.
Targets: Review targets that have been synchronized/downloaded from Boss.
Databases: Review all the Hotlists currently distributed to this PAGIS laptop/MDC.
Esc: Returns the user to the previous screen.

2.9.3 Reads

From the Main Screen, the user can review his or her accumulated Reads (those gathered since the last End Shift was completed) by clicking on the Review icon and then selecting the Reads Navigation button. The Read Review Screen is divided into two main sections. The left side displays the information gathered at the time of the read and the right side displays an interactive map of the GPS location.



NOTE: Buttons that are greyed out indicate options that are not available in the current view. For example, the Reads and Hits review screens share the same layout but different on-screen options.

2.9.3.1 Reads Result Screen Navigation Buttons



Read Count: The left number is the current record. The right number is the total available for review.

Next/Previous button: The arrows on either side of the read count allow the user to navigate back and forth to review reads/results.



MisRead button: When the button is green it indicates the record has NOT been edited as a Misread by a user. Once a Misread is saved, this button will turn grey and the record title will update.



Jump button: Allows the user to "jump" to a specific record without the need to navigate one record at a time using the Next/Previous buttons.



Save button: Apply any changes/edits and return to the Main Screen.



Escape button: Returns the user to the Main Screen.

2.9.3.2 Interactive Buttons – Reads Screen

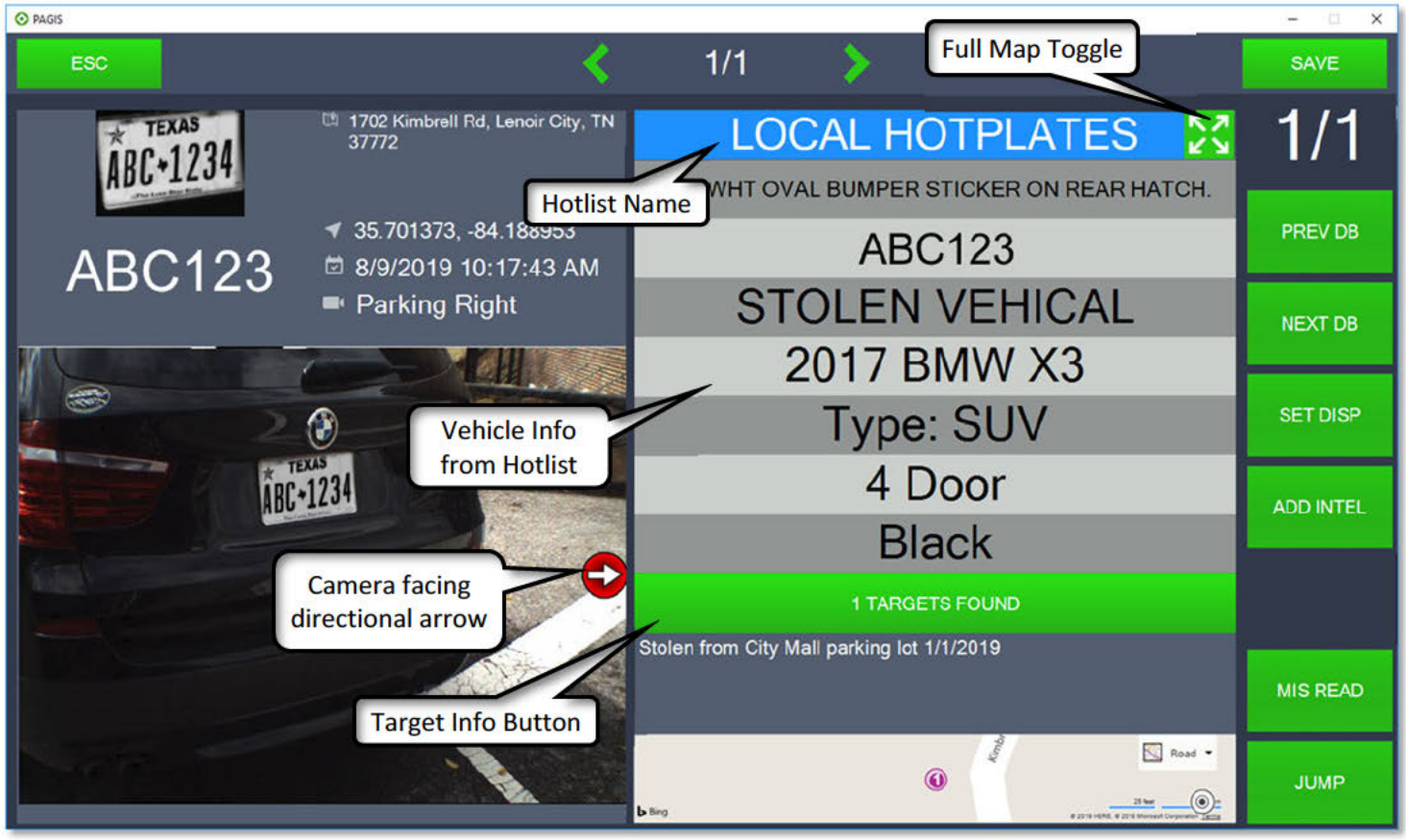
From the Reads Review, the user can interact with the following:

- IR Patch: The user can click on the IR "Patch" plate image to open a full-screen view.
- OCR Patch: The user can click on the OCR "Patch" image to edit the license plate number if necessary/Misread.
- Color OV Image: The user can click on the color image to open a full-screen view.
- Map: The user can manipulate the interactive map of the read location (Map Type, Scroll, and Zoom).

2.9.4 Hits

Users can manually access the Hits Section by first selecting the Review icon from the Live View Screen and then clicking the Hits Button. The Hits Screen is also divided into two main sections. The left side displays the information gathered from the ALPR equipment during the read. And the right side displays the information provided by the associated alert list.

NOTE: Each time a VLP matches a Database value (a license plate read by the system matches a Hotlist entry), PAGIS plays an audible tone and automatically displays the Hit Screen to alert the user.



2.9.4.1 Hit Screen Attributes

Hit Count and Navigation Buttons: Displays the total Hit count as well as the Next/Previous navigation buttons.

IR Patch Image: A thumbnail image of the license plate from the IR camera.

OCR Text: The character string the OCR engine generated from the current plate.

GPS Location: The GPS coordinates at the time of the hit. (If a GPS device is not attached, the Lat/Long is displayed as 0,0).

Date and Timestamp: The date and time when the read/hit was captured.

Overview Image: The overview image of the vehicle from the Color Camera. (**NOTE**: Color images require visible light)

Camera Name: The name of the camera that captured the read ("Right Parking" in the screenshot).

Hotlist Name: This is the name of the Hotlist or "Database" where the plate was matched.

Target Button: When available, this indicates a person of interest is associated with the Hit and opens the Targets Screen.

Vehicle Information: The area of grey bars will display the related vehicle information from the Hotlist. Any information added manually by the user will appear in the Text Box near the bottom of the screen.

Interactive Map: Shows the location the Hit took place. Users can access full-screen view by clicking the map or the toggle .

2.9.4.2 Hit Screen Function Buttons



The Hit Count Indicator: shows how many Hotlists the current Hit has registered against.



Previous DB button: This button moves the user to the previous Database/Hotlist that produced a Hit.



Next DB button: Pressing this button moves the user to the next Database/Hotlist that produced a Hit.



The Set Disposition button: prompts the user to report the disposition of the hit by selecting one of the approved codes assigned in BOSS by the Administrator.



The Add Intel button: allows the user to add additional information regarding the current Hit.



The Misread button: allows the user to flag the Hit as a misread.



The Jump button: Allows the user to "jump" to a specific Hit instead of navigating one at a time.

2.9.4.3 Interactive Buttons – Hits Screen

- IR Patch: The user can click on the IR "Patch" image to open a full-screen view.
- OCR Patch: The user can click on the OCR "Patch" image to edit the license plate number if necessary/Misread.
- Target Button: Shows associated person(s) of interest and opens the Targets Screen.
- Color OV Image: The user can click on the color image to open a full-screen view.
- Map: The user can manipulate the interactive map of the read location (Map Type, Scroll, and Zoom).

2.9.4.4 Set Disposition – Additional Detail

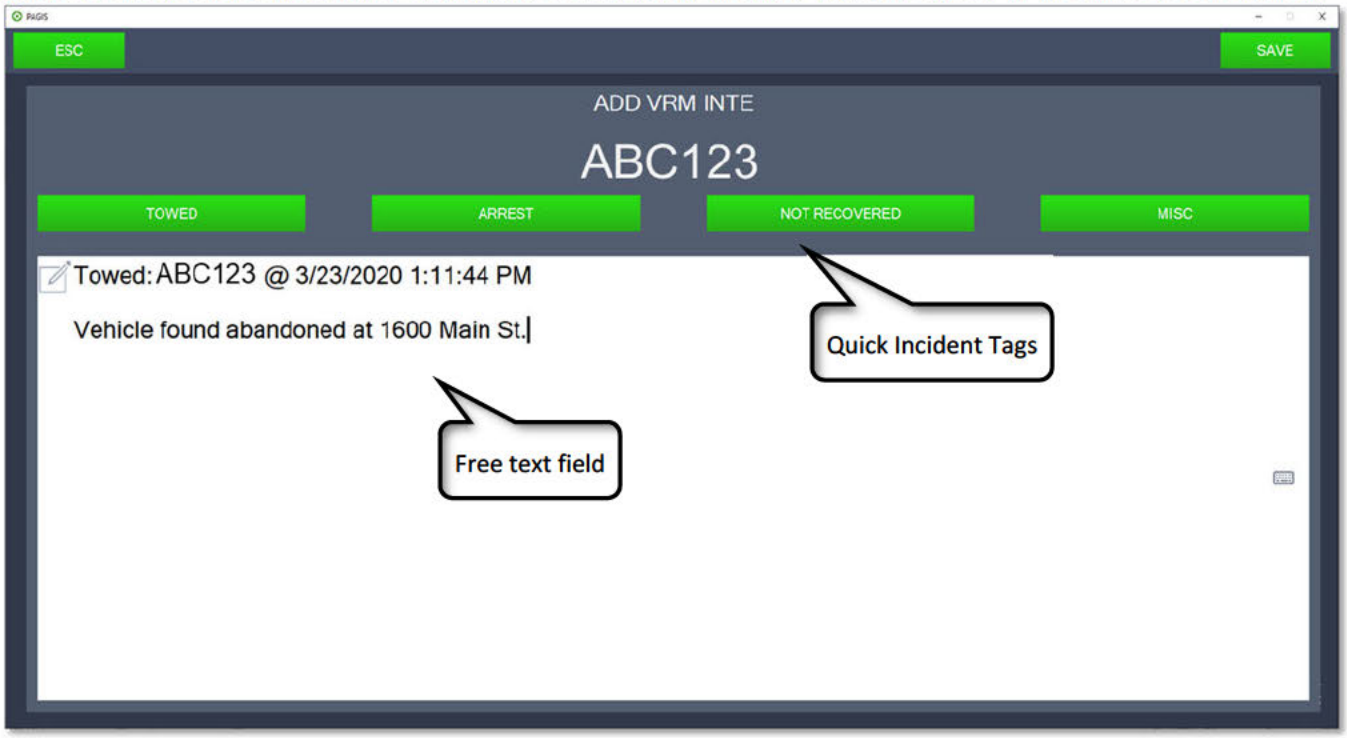


PAGIS allows for additional information to be added to a record in the form of a Disposition. Once Hits are flagged with a disposition code, the Agency is capable of running a "Reads Statistics by Disposition Report" in BOSS. Thus, providing valuable metrics and understanding to leadership in regard to their ALPR Enterprise.

When the "Set Disp" button is selected, the user is prompted to choose from a list of predefined values set by the Agency/BOSS Administrator. Once a disposition is selected and Saved, the disposition is reported to BOSS and will also show up in the Hits Review Screen text box in PAGIS on the next alert notification.

2.9.4.5 Add Intel – Additional Detail

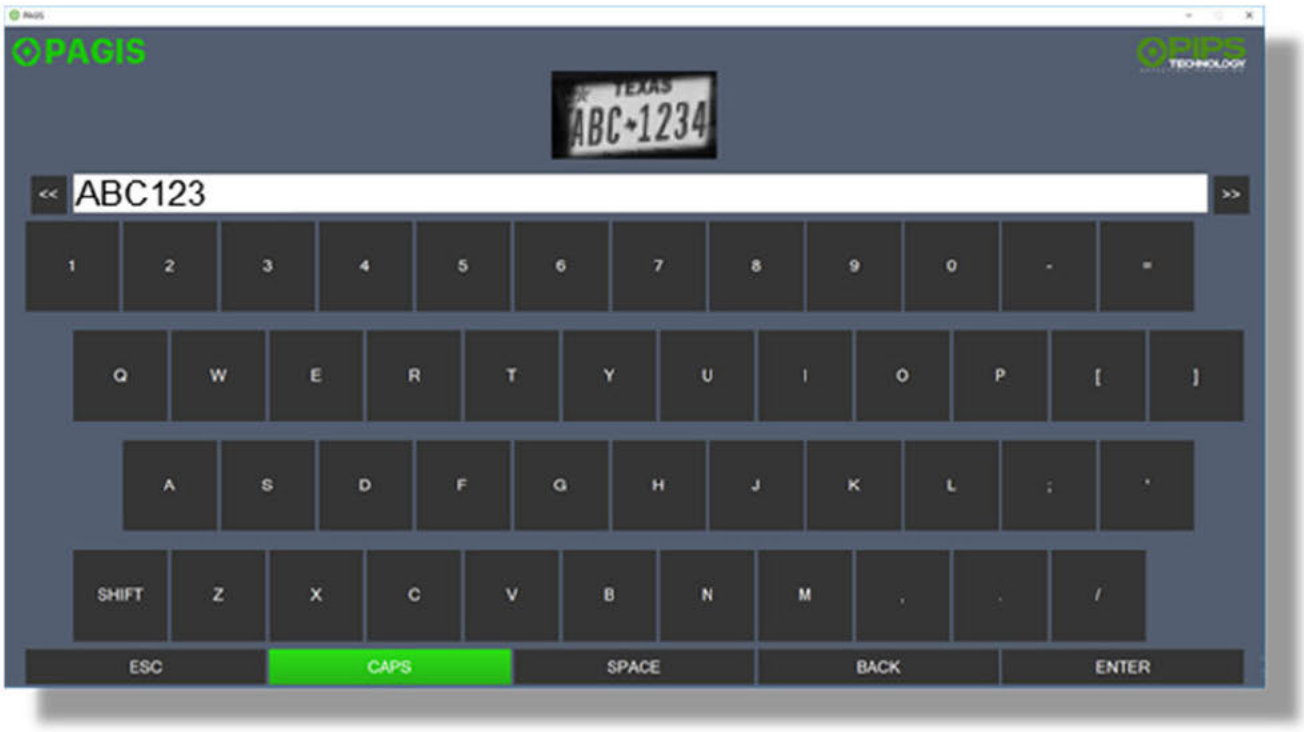
The Add Intel button launches the Intel screen. The user is prompted to assign one of four values: Towed, Arrest, Not Recovered, and Misc. by clicking the associated button at the top of the screen. The user may also enter additional detail regarding the license plate/vehicle. After clicking the Save button, the intel will now appear in the Hits Screen text box.



2.9.5 Misreads

PAGIS allows the user to mark Reads and Hits with incorrect OCR translations as a Misread. This is most commonly done by Agencies for Hits only as users typically don't have time to review every single Read from their shift. Once an errant Hit is corrected, the system updates the record to show it as a Misread and thus improves Agency Hit Reporting.

Correcting a plate read can be accomplished by clicking on the "OCR Patch" in either the Hits or Reads review screen. When the user clicks on the OCR Patch, the OCR Edit Screen opens and allows the user to update the Vehicle License Plate (VLP) data.



2.9.5.1 Marking a Record as a Misread:

The user can mark a record as a Misread from both Reads or Hits Review Screen. Each user can either simply flag the record as a Misread or update the OCR Patch information. **NOTE**: This ability is only available until the user has performed an End Shift function.

Manually Flagging a Read or Hit as a Misread:

1. Navigate to either the Reads or Hits Review Screen
2. Click on the Misread button on the Right
3. Click Save
4. Take note that the record title has now changed from “Read” to “Misread”

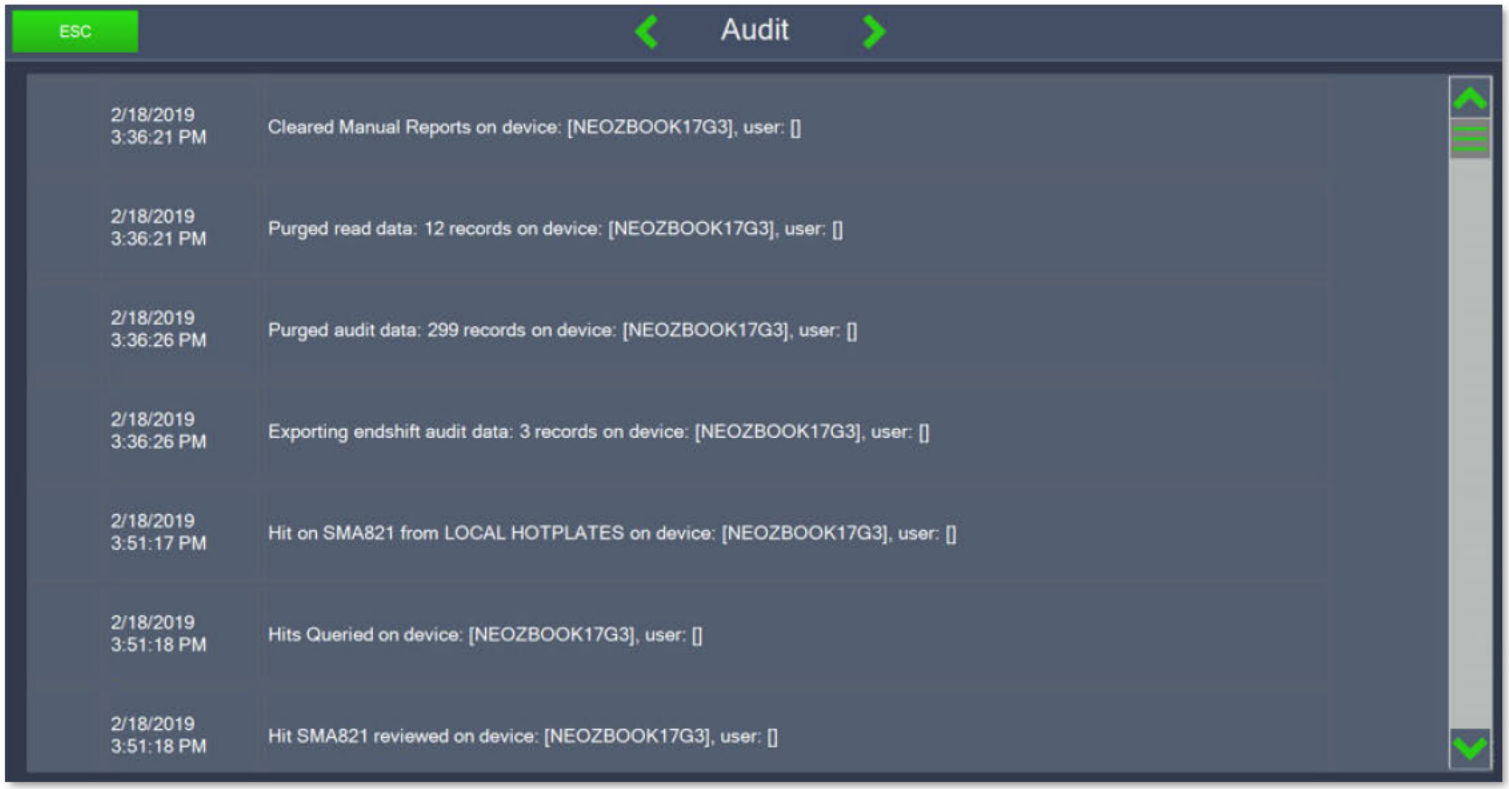
Updating the Read/Hit OCR Patch:

1. Navigate to either the Reads or Hits Review Screen
2. Click on the OCR Patch (Text just under the IR Plate Image)
3. Use the keyboard or on-screen keypad to update the Vehicle License Plate Number
4. Click the Enter Button to Save the changes (and exit back to the Review Screen)
5. When the user saves the changes to the OCR Patch, the record (Read/Hit) is automatically flagged as a Misread

2.9.6 Audits

PAGIS logs both user and key system activity during each use of the software. The audit log captures various information like Read searches, synchronizations, hits, and user login attempts. The Audit Report is viewed in PAGIS by navigating to the Review section and selecting “AUDITS”.

NOTE: Performing an End Shift or syncing the database clears the current log.



2.9.7 Targets

PAGIS has the ability to display information regarding Persons of Interest in response to a Hit alert. Targets are created by BOSS/Hotlist Administrators, and typically provide detailed information about owners of a registered vehicles. When configured, Target data is always linked to unique VLP data (a specific License Plate). If PAGIS registers a Hit on a Plate with a target ID, the Target Information Button is displayed in the Hit Alert window and allows the user to access the Target Screen.



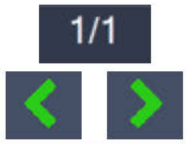
2.9.7.1 The Targets Screen

When a PAGIS user clicks the Target Information Button from a Hit Alert, the Targets Screen opens. This screen displays the information from the BOSS server about the Person(s) of Interest matched to the Hit (license plate).



2.9.7.2 Targets Screen Navigation Buttons

If a Hit alert has more than one Target associated with it, the PAGIS user can navigate all Target information with the buttons described below:



Target Count: The left number is the current record. The right number is the total available for review.

Next/Previous button: Arrows on either side of the target count allow the user to navigate back and forth to review the various targets.



Jump button: Allows the user to "jump" to a specific record without the need to navigate one record at a time using the Next/Previous buttons.

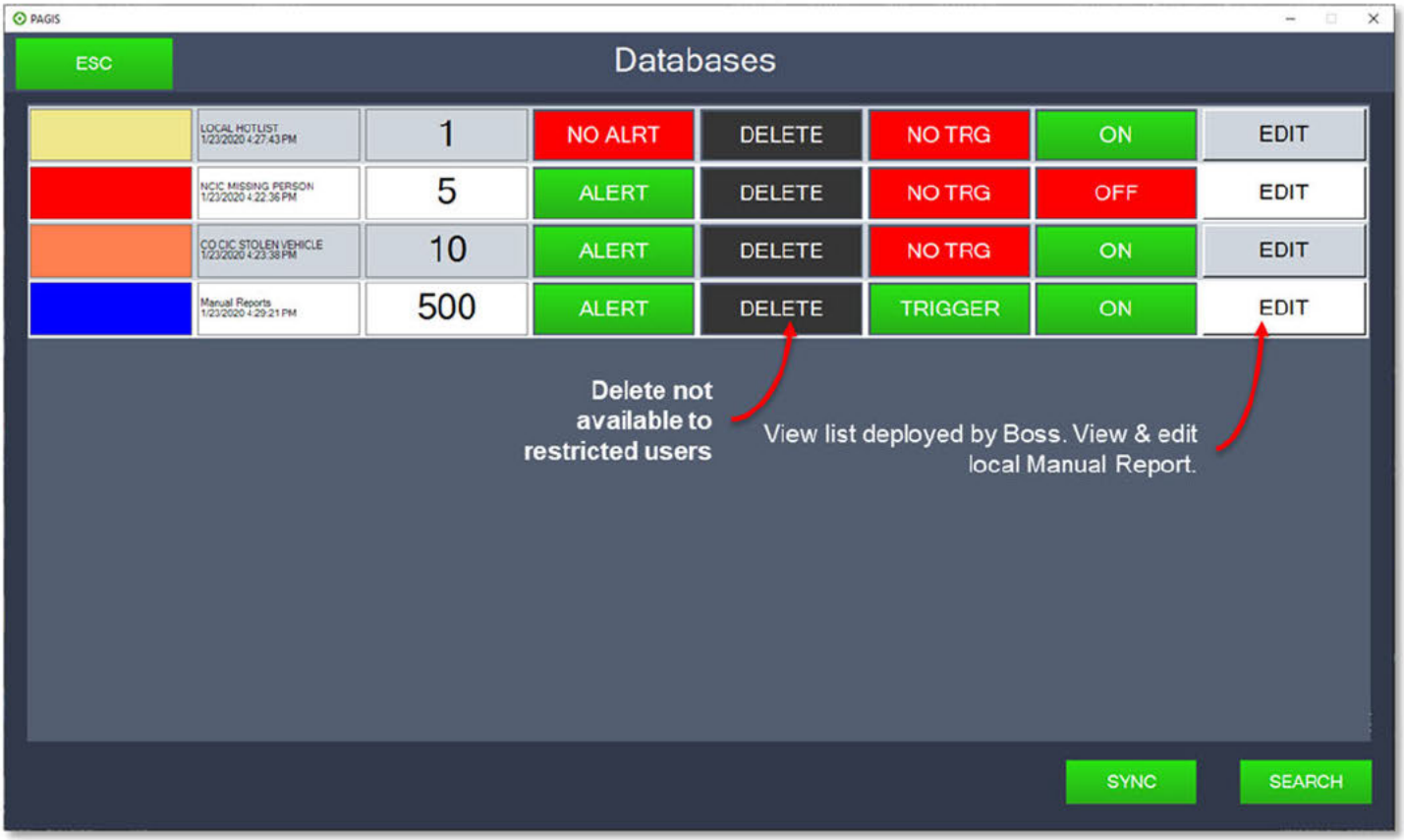


Close button: Returns the user to the previous screen.

2.9.8 Databases

Users can review Hotlists in PAGIS by navigating to the Review section and selecting "DATABASES" on the right. From the Databases Screen, users can toggle Hotlists functions On and Off based on their rights.

NOTE: User rights and Hotlist attributes are configured in BOSS.



2.9.8.1 Databases Screen Functions

Hotlist Color Code: The color attributed to each Hotlist by the BOSS Administrator.

Hotlist Name: The name of the Hotlist given by the BOSS Administrator. Also shows the time/date of the last synchronization.

Hotlist Priority: The priority of the Hotlist assigned by the BOSS Administrator. The lower the number between 1 and 999, the higher the priority. If a plate resides on multiple Hotlists, the list with the higher priority will be displayed first.

Alert Button: Toggles audible alerts On and Off for each Hotlist until the next synchronization.

Delete Button: Based on user rights, allows the user to temporarily delete a Hotlist from PAGIS until the next synchronization. To delete a hotlist, the user must click the button twice (it turns green and then deletes the list).

Trigger Button: Toggles external triggers On and Off. An example of an external trigger is a light bar.

On/Off Button: Disables and enables each Hotlist (each Hotlist is set to On by default).

Edit: View and edit localy created hotplates with a given hotlist, Hotlist/Hotplates deployed via BOSS can only be viewed.

NOTE: Hotlist settings altered in PAGIS will be reset to their default configuration during the next Sync or End Shift. The default configurations are assigned by the BOSS Server/Administrator.

2.9.8.2 Databases Screen Navigation Buttons

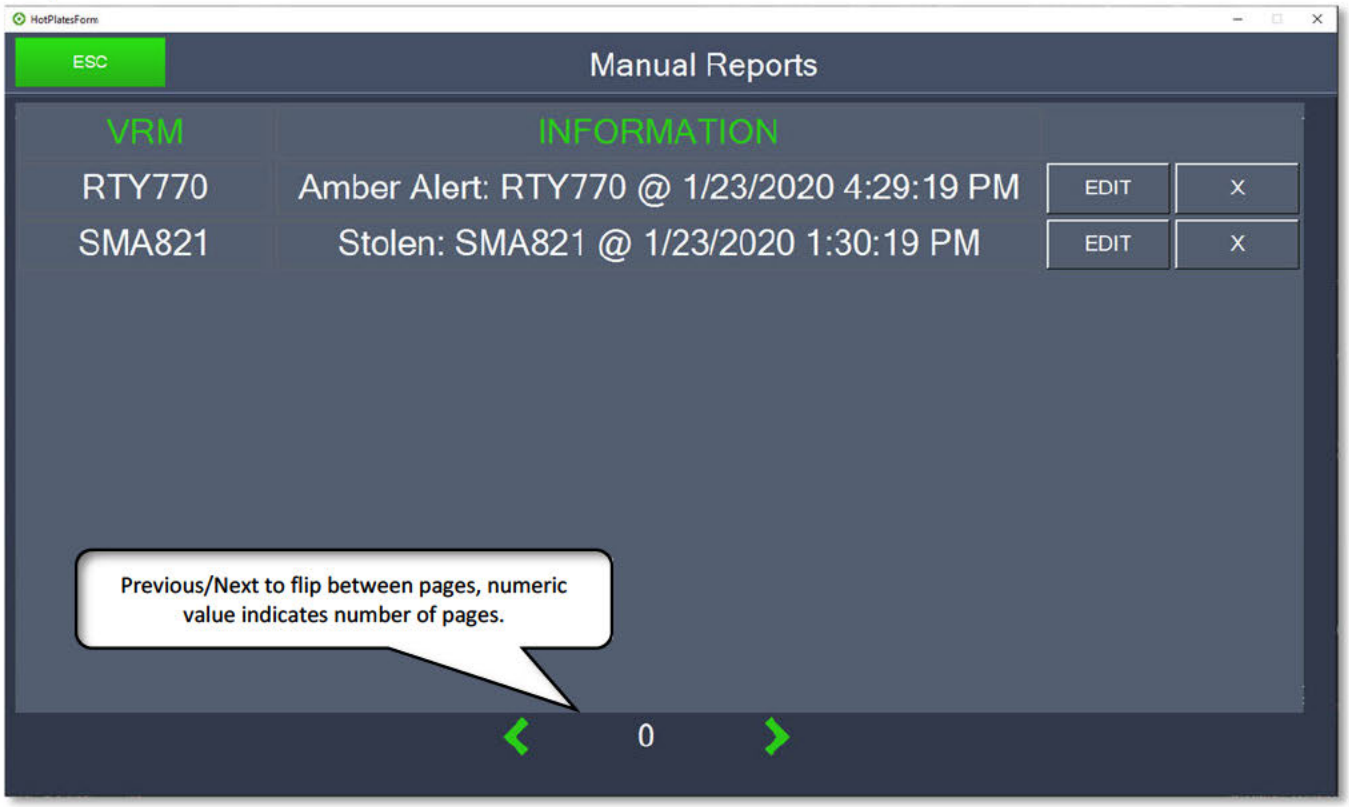
SYNC — **Sync button**: Synchronizes PAGIS with the BOSS server in order to update the Hotlists.

SEARCH — **Search button**: Open the Search Entry Screen (See section 2.8 for more information).

2.9.8.3 Databases Edit- “Manual Reports”

Editing Hotlist has two function based on origin of hotlist.

- Hotlist deployed to PAGIS via BOSS cannot be edited, only the hotplates list can be viewed. Editing/updates are indented to be managed via BOSS.
- Hotlist created in PAGIS, i.e. “Manual Reports” can be managed by PAGIS users, allowing for changes or deletion of the hotplates contained within the hotlist.



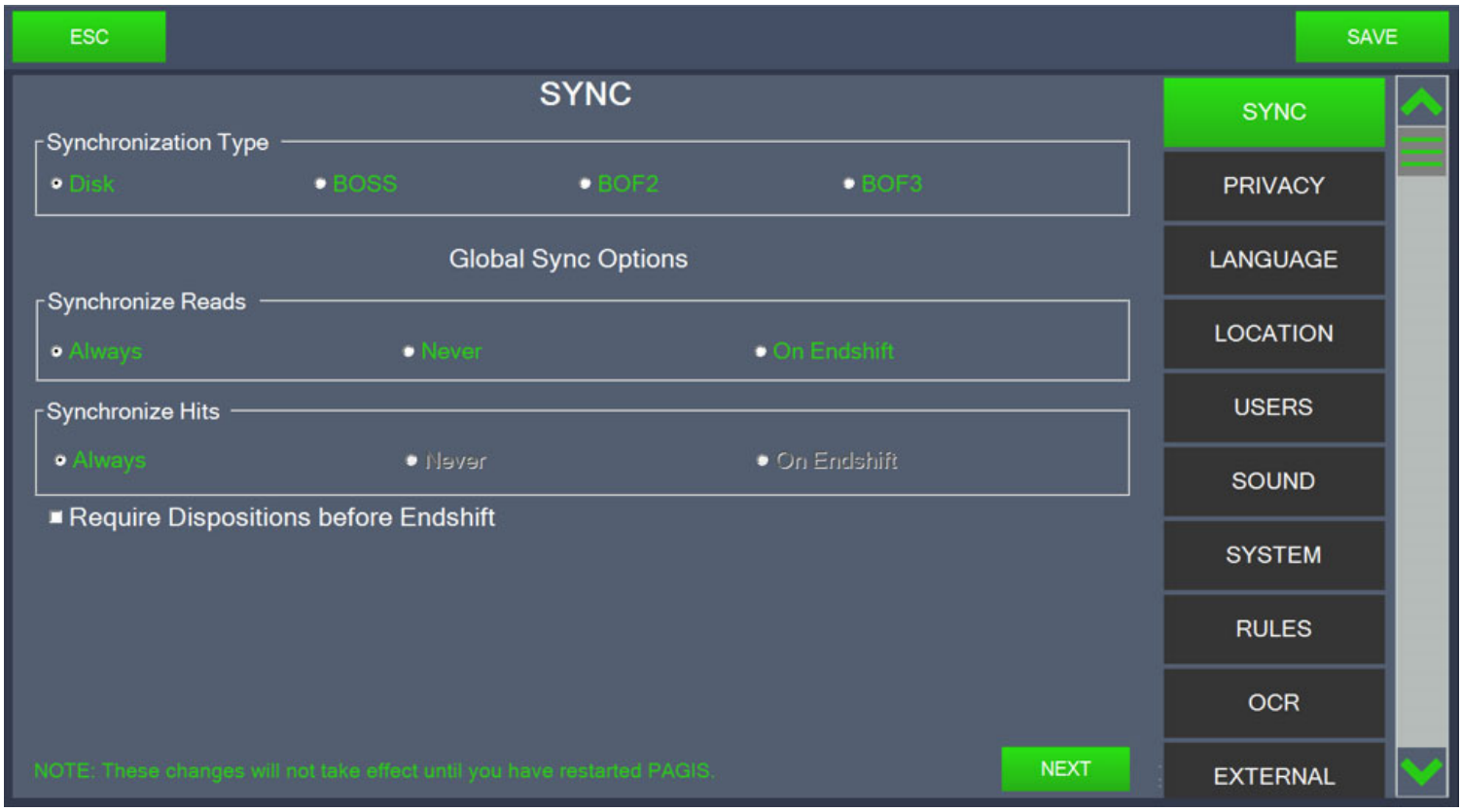
EDIT Button: Make changes to the indicustly hotplate information including licanse plate nuamber.
X Button: Remove indivualy hotlist from hotlist.
Previous/Next Button: Scroll thought lising of hotplates contaned within the hotlist. The numeric value indicates the number of pages.

ADMIN SETTINGS

The Settings Menu is the central location for configuring PAGIS Software functions endpoint by endpoint. Users with Admin level rights in PAGIS can see and click on the Settings Button from the Live View Screen. Launching Settings opens the menu to the Sync Options Screen by default. **NOTE**: Users without Admin level access will not see this icon on the Live View Screen.

3.1 Sync Options Screen

As mentioned previously in sections 2.4 and 2.5, PAGIS uses various sync options to store, update, and synchronize ALPR data to and from the BOSS server. On the Sync Screen, Administrators configure the synchronization method and options.
NOTE: Configuration changes will not take effect until they are saved and the PAGIS Software has been restarted.



3.1.1 Synchronization Types

- **Disk**: Uses local storage of Sync files in conjuction with a USB flashdrive to manually Sync to and from BOSS.
- **BOSS**: Uses a wireless data network to Sync files to and from the BOSS server.
- **BOF2**: Used predominantly in Europe (see regional guide for support).
- **BOF3**: Used predominantly in Europe (see regional guide for support).

3.1.1.1 Synchronization to Disk (Local Storage)

4252

Sync to Disk is a manual two-part process most commonly used with a USB Thumb drive. To use Begin Shift, the user accesses a centralized terminal (Ex. Patrol Room PC) to download the files from BOSS and then inserts the Thumb drive in the laptop to perform Begin Shift. At the end of the day, the user then Performs End Shift from the laptop/MDC connected to the Thumb drive and uploads those files to BOSS via the central terminal (See the "Client Tools" section of the BOSS Manual).
NOTE: From the Sync Menu, select "Disk" and click the Next button at the bottom to configure the drive location.

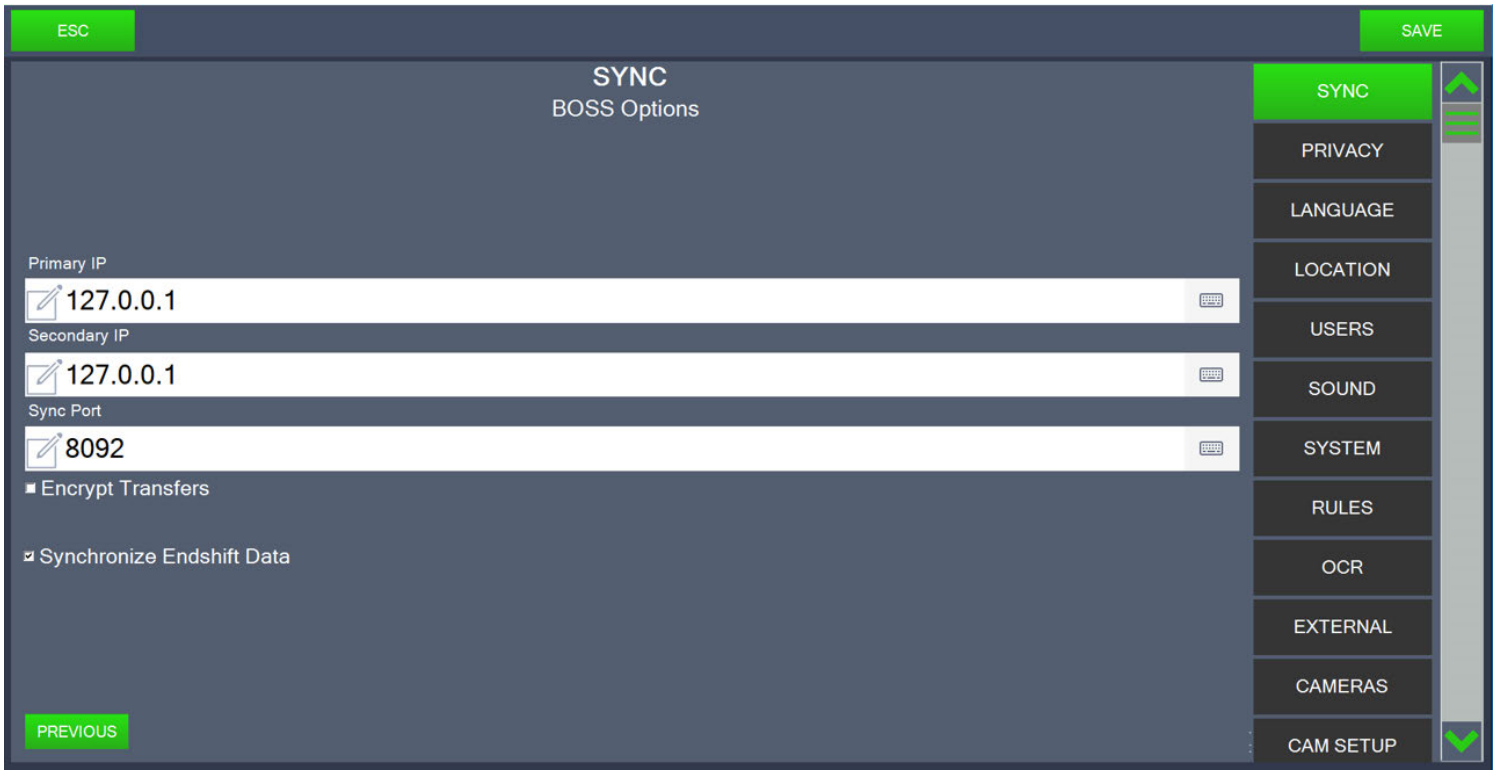


- **Delete Beginshift Data on Sync**: The sync folder on the Flash Drive is deleted once all Begin Shift data has been imported to PAGIS. This is on by default to help prevent false alerts.
- **Encrypt Endshift Data**: All uploaded End Shift data created in PAGIS is encrypted. This is off by default.
- **Copy Endshift Data on Sync**: If unchecked, no End Shift data will be transferred from PAGIS to the Drive location.
- **Keep Only Updated Databases**: Removes any Hotlists from PAGIS that were not updated during Begin Shift as "outdated". This is off by default.

Sync to Disk Setup:
In the text box, enter the drive path or letter to be used with Disk Sync. Folder name is not required as PAGIS creates the required folder(s). Once entered, select the desired options and then click the Previous button. Click Save to retain the settings.

3.1.1.2 Synchronization with BOSS

Sync to BOSS is a streamlined method for updating ALPR data to the field units and the server. Additionally, selecting this option enables the PAGIS auto-sync features that synchronize data throughout the shift without user involvement. However, this does require a stable data connection as well as some network configuration before it can be utilized.



Sync to BOSS Screen:

4253

- **Primary IP**: The IP address of the BOSS server. This can also be the DNS name (**NOTE**: using DNS adds an additional failure point via the Domain Controllers and is not recommended as the best option).
- **Secondary IP**: Used for a secondary IP in cases where users switch from a cellular network to a Domain APN thus routing to BOSS from either an internal or external IP. This field can be left blank or with the primary IP as well.
- **Encrypt Transfers**: When enabled, data transfers to BOSS will be encrypted.
- **Synchronize Endshift Data**: On by default, this enables PAGIS to sync to BOSS when End Shift is performed by the user.

Sync to BOSS Prerequisites:

To establish the wireless sync to BOSS, the Agency Network Administrator will need to open TCP 8092 to the BOSS server as well as define the internal and/or external IP address(es).

Sync to BOSS Setup:

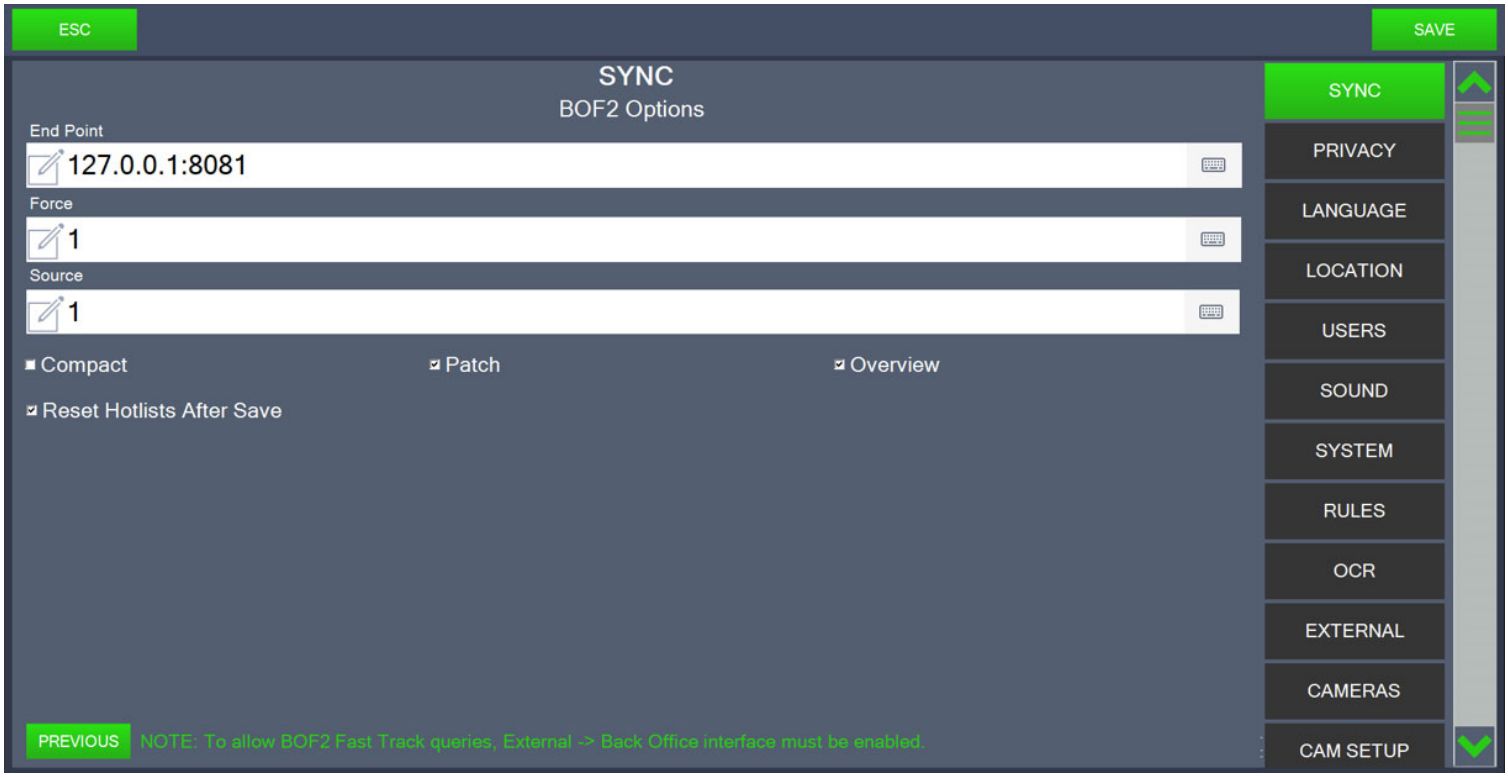
From the Sync Settings Menu, the Admin must select the BOSS option and click the Next button. Then s/he will update the Primary and Secondary IP fields as necessary and de/select any options. Once configured, click the Previous button and then click Save to retain the changes. (For more information on PAGIS Auto-Sync settings, refer to section 2.4.3)

NOTE: After synchronizing to BOSS, data is flagged in the database to prevent duplicate values on future synchronizations.

3.1.1.3 Sync to "Instation" (Formerly BOF2 and BOF3)

The Instation software was formerly known as BOF2 & BOF3 and was developed by Anite PLC. It is a web-based Back Office software suite used in European markets to provide similar features as the PIPS BOSS server and UI Client.

NOTE: These options are NOT used in the Domestic United States.

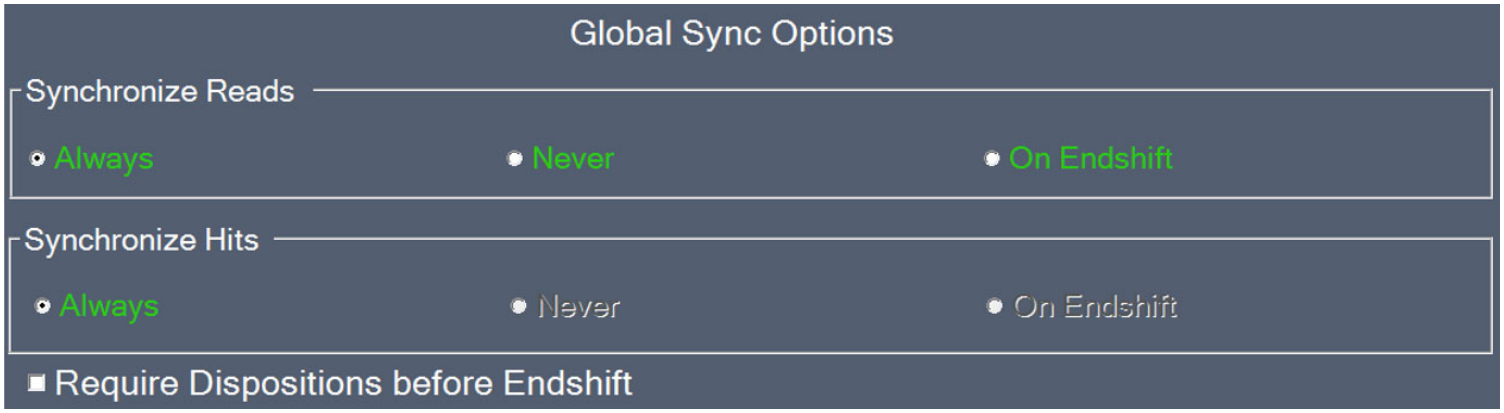


- **End Point**: The IP Address of the Instaion website. Format must be [IP Address:Port]
- **Force/Source**: Unique codes assigned to each police force.
- **Compact**: This option minimizes data transfer to Instation. Images will be deselected by default when in use.
- **Patch**: Refers to the image of the plate pulled from the read. This is on by default.
- **Overview**: Refers to the color overlay image from the read. This is on by default.
- **Reset Hotlists After Save**: When the software syncs to Instation, this will reset the hotlist tracking.

3.1.2 Global Sync Options

4254

Global Sync settings control how PAGIS synchronizes ALPR data during Begin and End Shift cycles and applies to both manually launched synchronizations as well as Auto-Sync functions. The two sections are Synchronize Reads and Synchronize Hits.



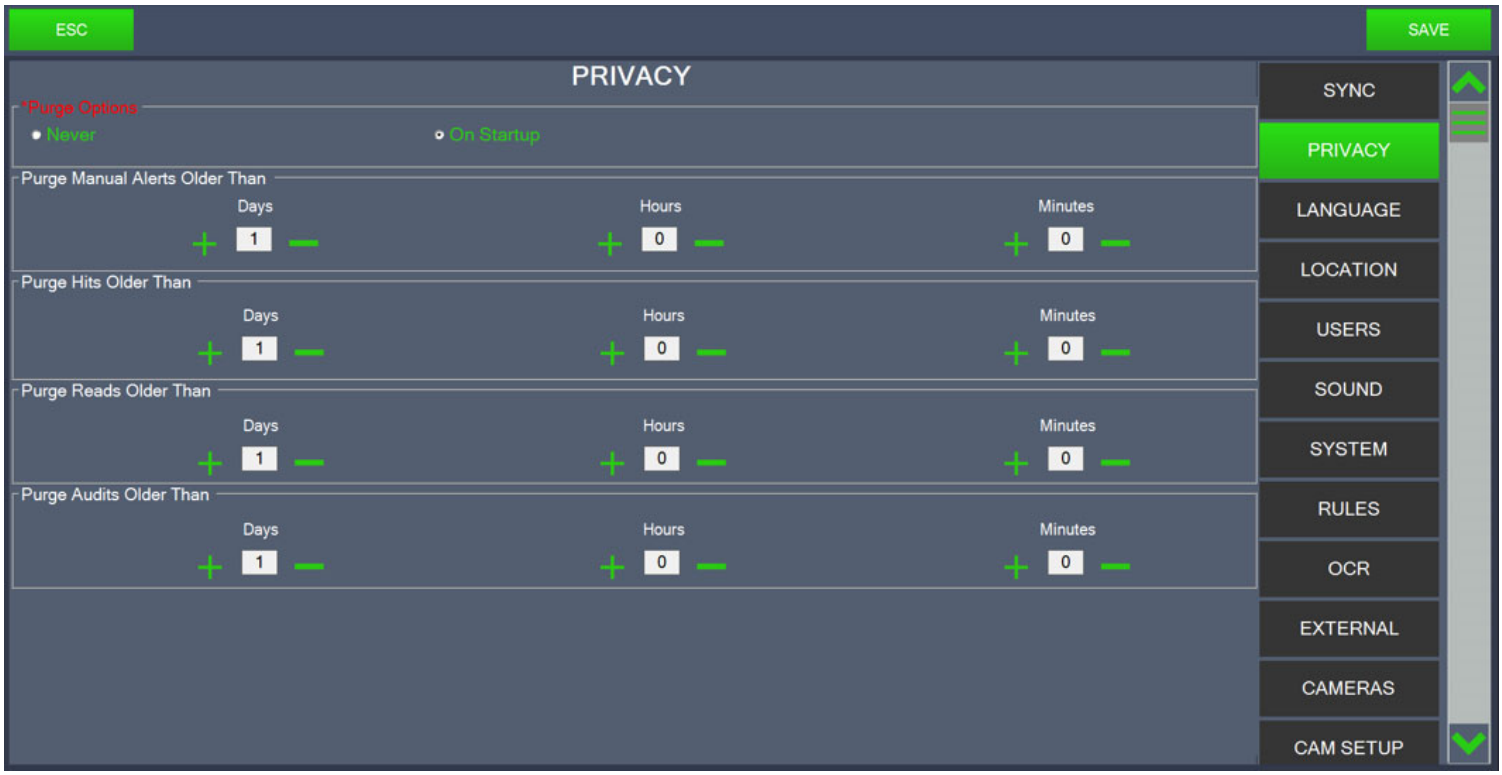
NOTE: All Hits are Reads, but not all Reads are Hits. A "hit" is a read that coincides with an Alert List. Due to this, the Options selected in the "Synchronize Reads" section dictate what options are available in the "Synchronize Hits" section. Unavailable options are greyed out.

- **Always**: Reads and Hits are synchronized to BOSS as close to real-time as the data network and PC processing allow.
- **Never:** The information gathered during the shift will be "sanitized" with each launch of End Shift. The corresponding data and images will NOT be sent to the BOSS server.
- **On End Shift**: Synchronization to BOSS will only occur when the user manually launches End Shift.
- **Require Dispositions before Endshift**: Requires the user to select a disposition code for each Hit registered in the PAGIS software since the last End Shift was completed before the Synchronization is processed.

3.2 PAGIS Privacy Settings (Local Data Retention)

4255

Although most commonly configured in BOSS, the PAGIS Software allows the Admin to configure the data retention settings for the local endpoint by minutes, hours, or days. This feature ensures the data captured/stored on the MDC is sanitized by the software itself (this is important for customers without BOSS). **NOTE**: To enable the Privacy settings, the Admin must select the "On Startup" purge option and then set at least one value in each row. Rows left with all Zero will not be sanitized or purged.



- **Never**: Selected by default, this option disables the PAGIS privacy settings and uses only those set in BOSS.
- **On Startup**: This option must be selected in order to enable the PAGIS privacy settings. Once enabled, PAGIS looks to purge/sanitize the system each time it's launched or restarted.
- **Purge Manual Alerts Older Than**: Controls how frequently all of the Databases/Hotlists in PAGIS are purged. The purge rate is calculated from the timestamp of the Hotlist. Once the retention value is surpassed, the Hotlist is deleted. Hotlists distributed from BOSS will be re-downloaded on the next Sync.
- **Purge Hits Older Than**: Controls how frequently all Hits in PAGIS are purged. The purge rate is calculated from the timestamp of read. Once the retention value is surpassed, the Hit is removed the next time PAGIS is restarted.
- **Purge Reads Older Than**: Controls how frequently all Reads in PAGIS are purged. The purge rate is calculated from the timestamp of read. Once the retention value is surpassed, the Read is removed the next time PAGIS is restarted.
- **Purge Audits Older Than**: Controls how frequently all Audits in PAGIS are purged. The purge rate is calculated from the timestamp of audit. Once the retention value is surpassed, the audit is removed the next time PAGIS is restarted.

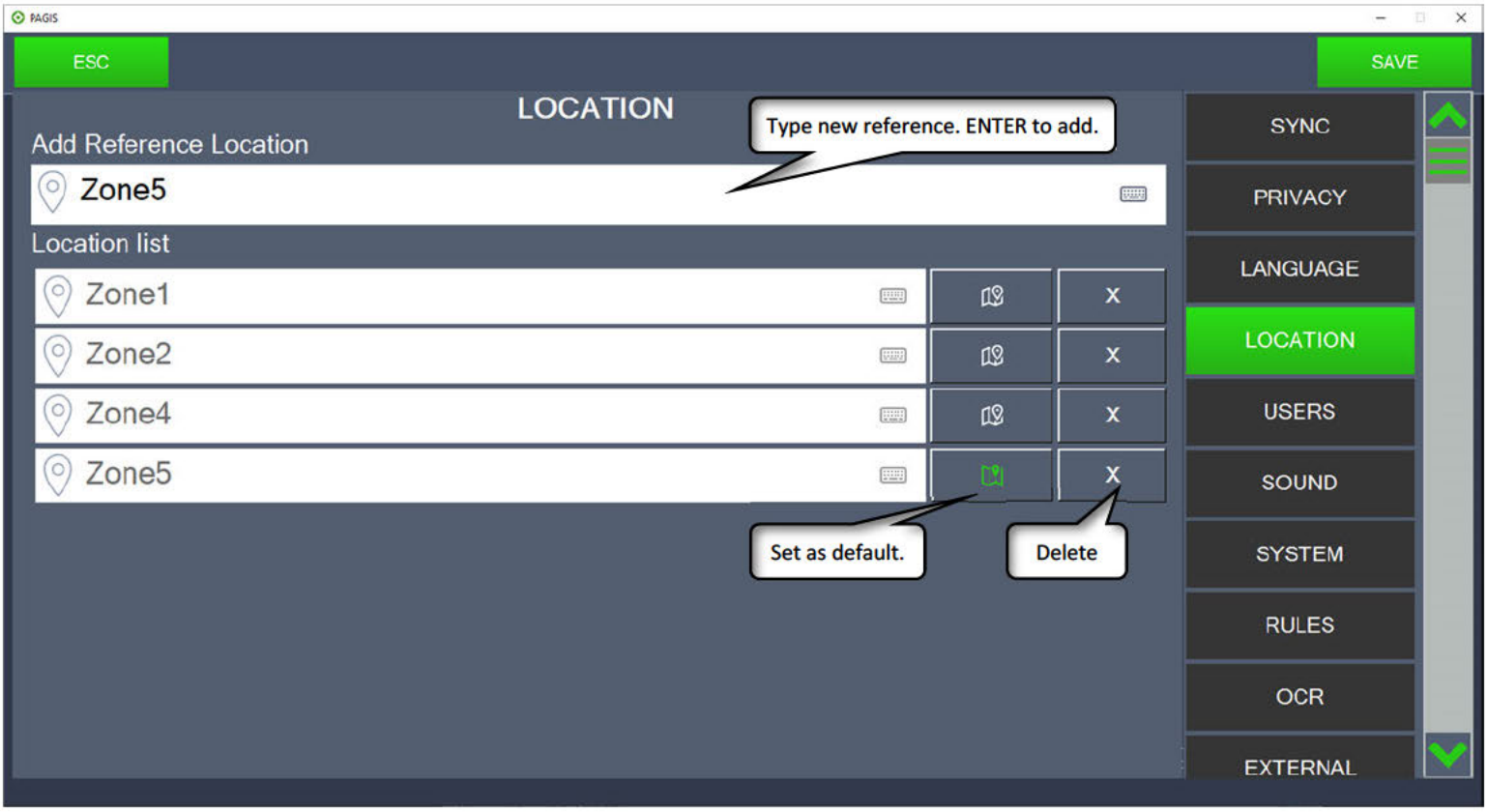
NOTE: Once the hits, reads, databases, or audits have been purged, they can no loner be viewed in the PAGIS software.

3.3 Language

The Language screen allows the Admin to change the language assignment used in the PAGIS Software. Available languages are listed in the drop-down list and are added during the installation process.

3.4 Location

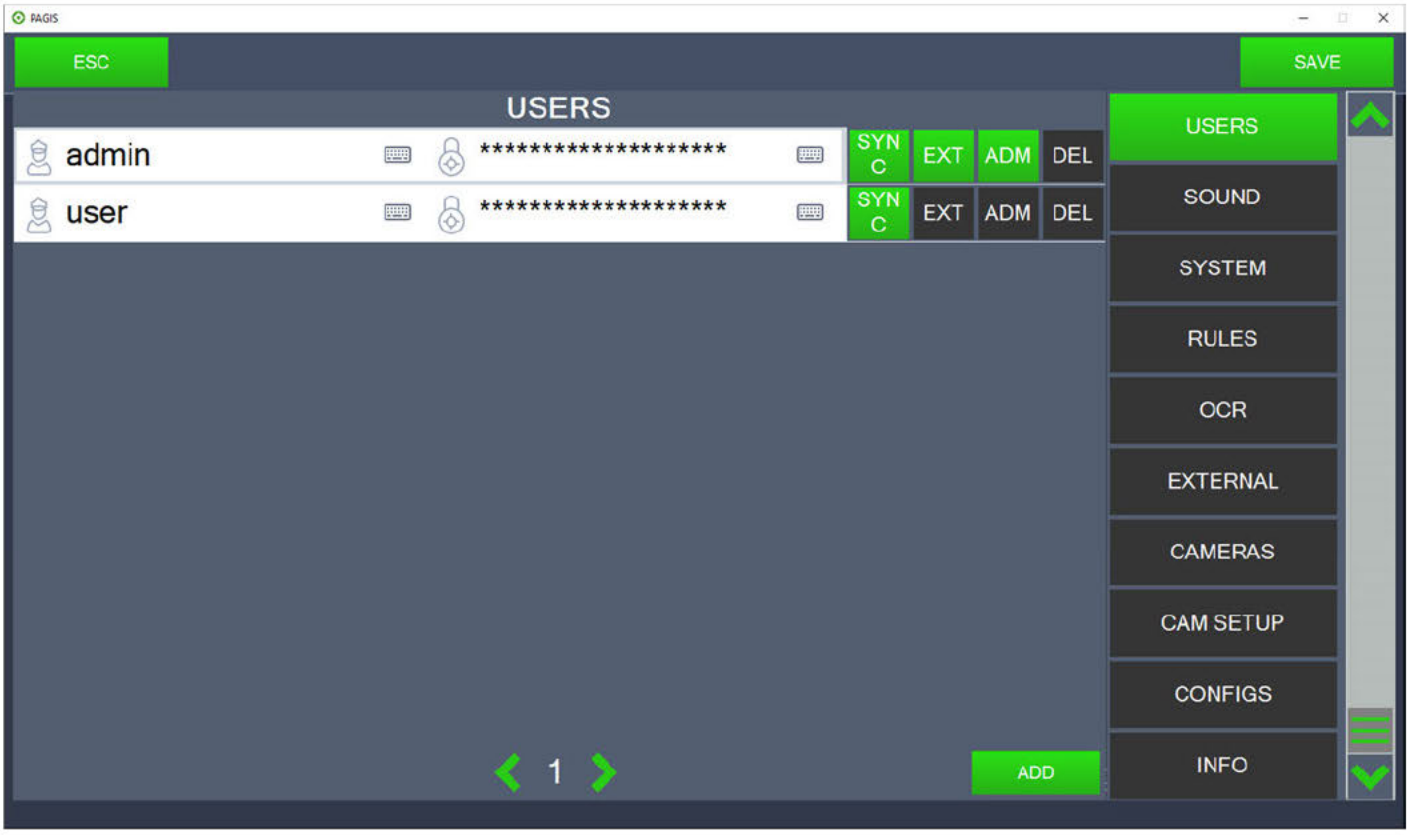
Updates to the location field will auto-fill the “Reference” section of the PAGIS Login Screen. These are often used to specify a patrol region (Examples: “North Patrol” or “A2”). Once designated all reads/hits will show this designation. Muiltiple “Referance” location can be added, the available list can then be selected from the login screen.



3.5 Users

4257

User accounts, credentials, and rights are generally administered from BOSS and then distributed to the MDC. However, PAGIS does allow for Administrators to add and delete users as well as set their privileges directly from PAGIS.



NOTE: Adding user directly in PAGIS should be limited to customers not utilizing a BOSS server. User accounts created directly in PAGIS by customers with BOSS will be overwritten/removed during the next sync.

Adding a User in PAGIS:

1. From the Admin Screen, select the Users Button on the Right
2. Click the Add Button ADD
3. Enter the case sensitive username in the Username Field (max of 15 alphanumeric characters)
4. Enter the case sensitive password in the Password Field (max of 15 alphanumeric characters)
5. Select the User's privileges
6. Click the Save Button SAVE

3.5.1 User Privileges

These are the "rights" the new user will have in the PAGIS software (When selected, each button turns green).

SYNC — **Sync:** Allows users to synchronize data.

EXT — **External**: Allows the user to access external databases.

ADM — **Admin**: Provides the user Admin rights and allows him/her to configure the PAGIS Software.

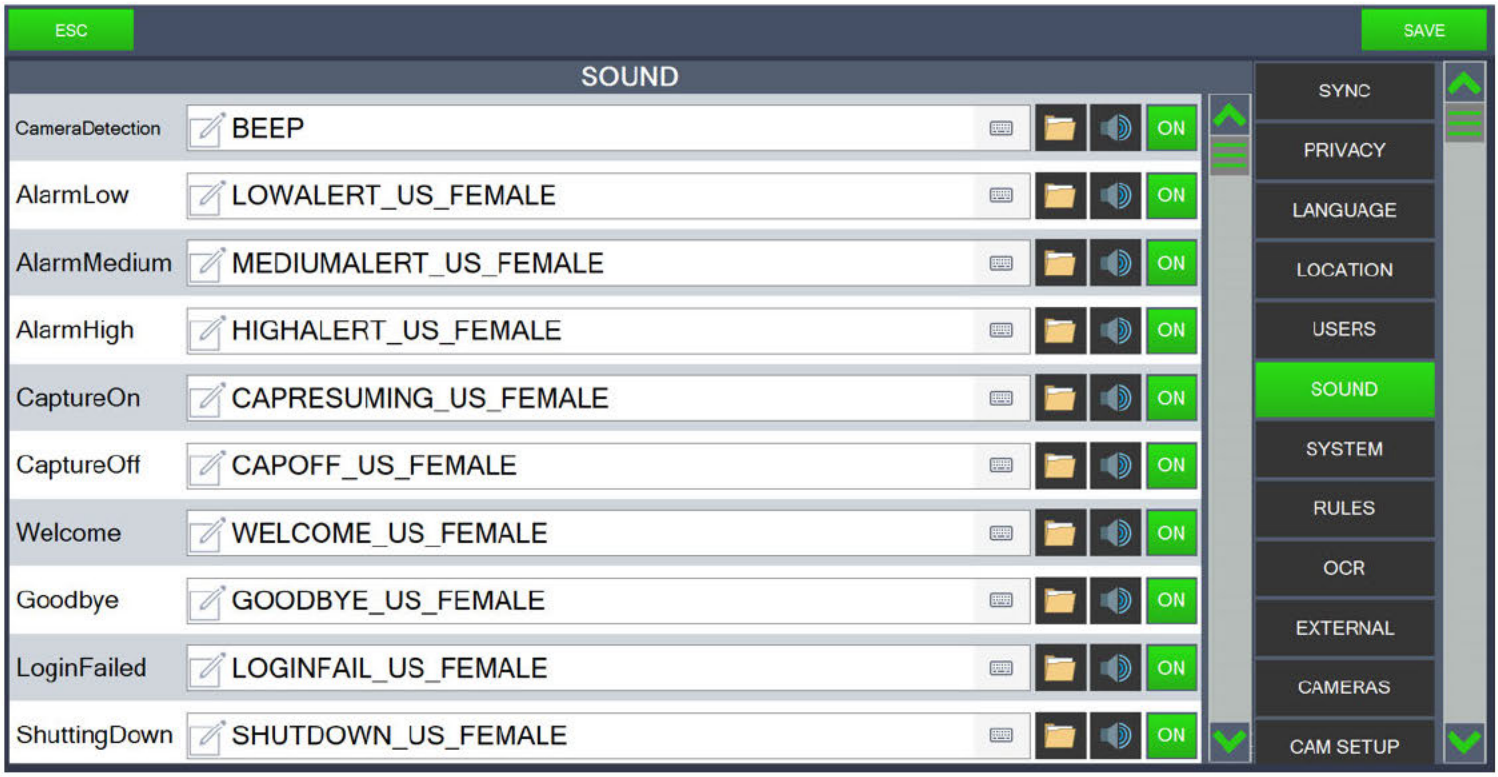
DEL — **Delete**: Allows the Admin to delete a User from the list. Click once to select and the save button to delete.

NOTE: Creating a new user in PAGIS automatically deactivates the default user account settings (Section 2.1.1).

3.6 Sound

4258

Sounds in PAGIS mirror the user or software activity (Ex. Login, Audible alert from a "Hit", and Logout) and are On by default. PAGIS Administrators can adjust the sounds from the available presets and/or load unique .wav files onto each MDC for custom use. **NOTE**: The default storage path is C:\Program Files (x86)\PIPS Technology, Inc\PAGIS2\sounds



3.6.1 Configuration Buttons

The sounds listed on the configuration screen can be altered or updated by PAGIS administrators using the buttons below. **NOTE**: Changes to any sounds must be saved before they can be played in PAGIS.



Click to browse to the sounds folder. This is used to select a new sound file.



Click to Test/Play the selected sound.



Shows the status of that sound. Click to turn each sound Off.

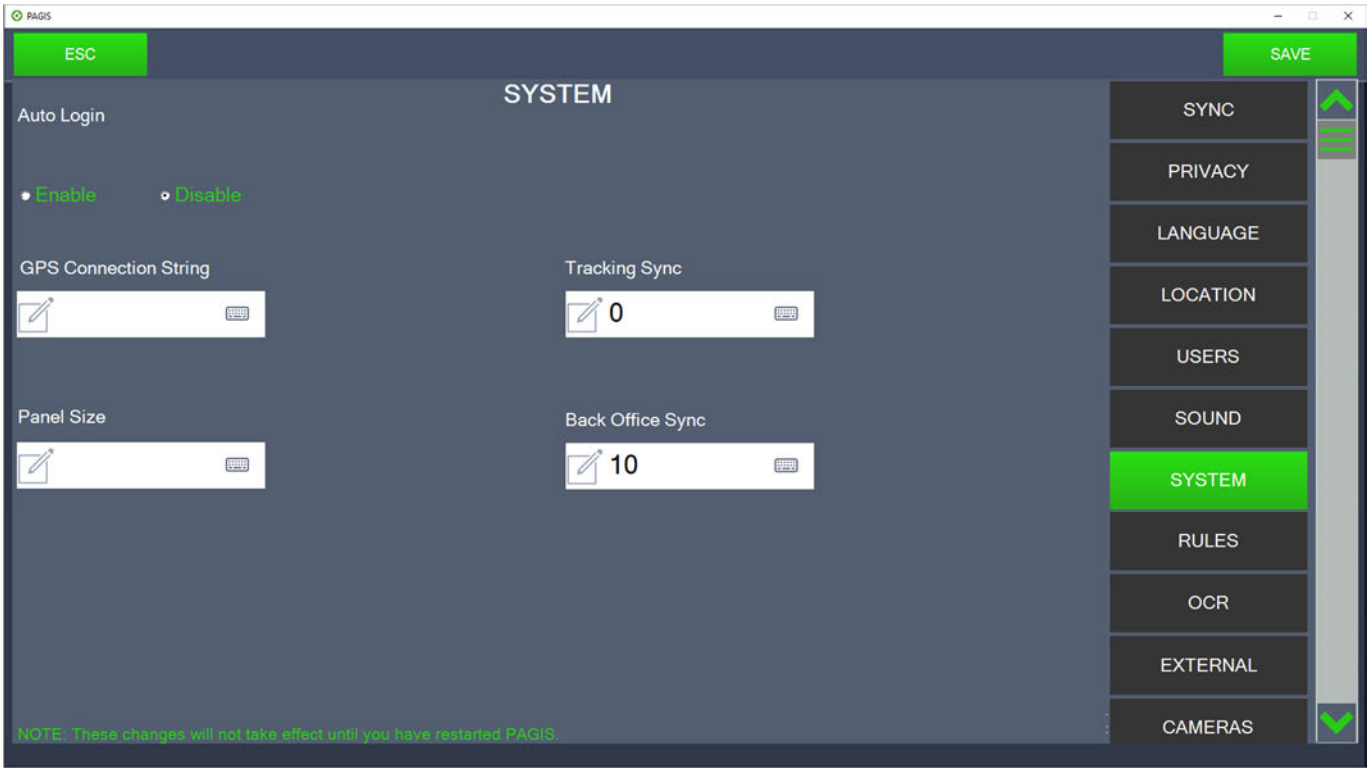


Shows the status of that sound. Click to turn each sound On.

3.7 System

4259

The System screen determines external system connections. The primary external connection is the GPS antenna. The GPS connection string will accept TCP/IP ports or COM port designations. This section also contains control of the PAGIS "Auto Login" feature (which is set to Off by default).

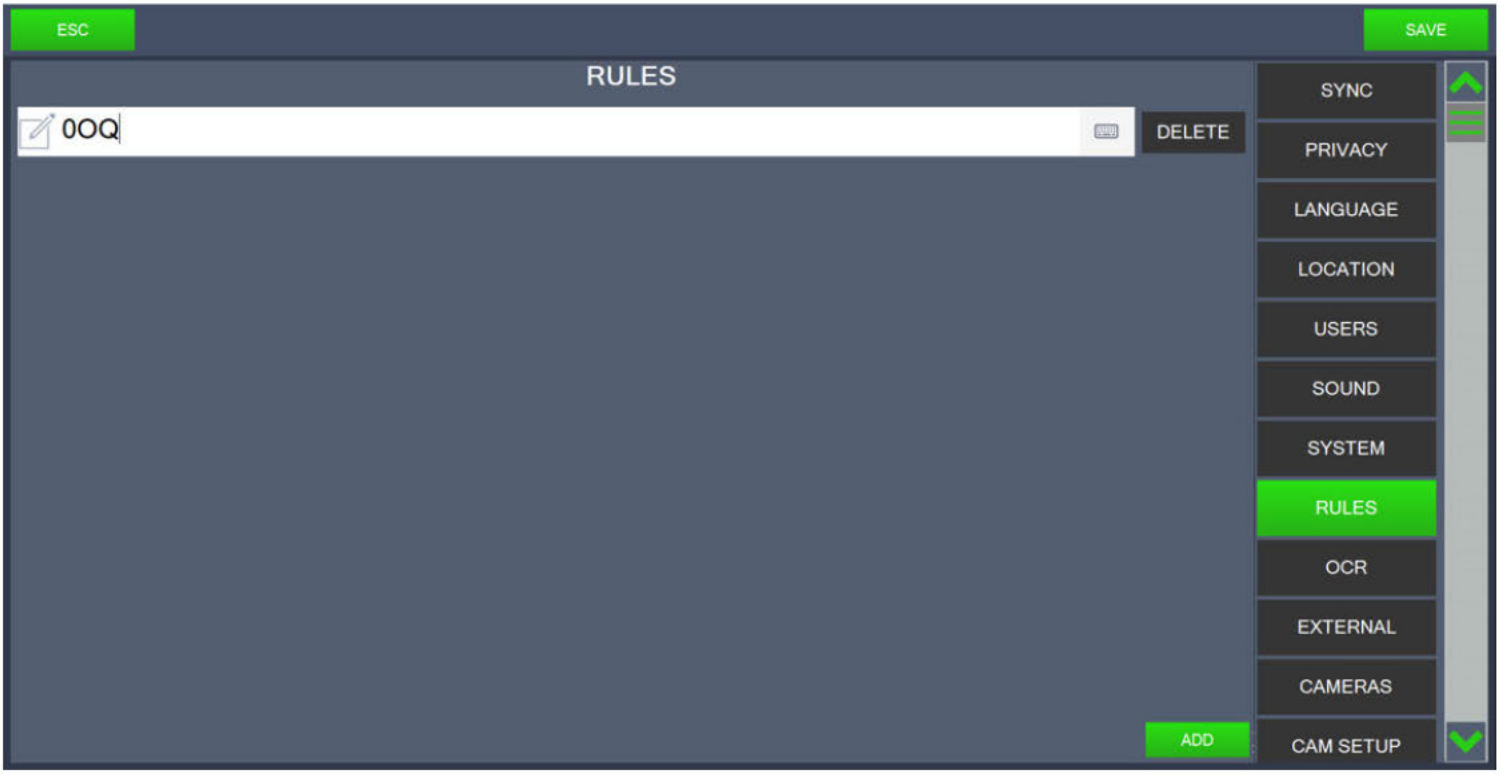


- **Auto Login**: Enabling this feature will ignore existing user account information and login to PAGIS as the Admin. This feature is recommended only for unattended use (Speed-Trailer applications and Covert Drop and Go deployments).
- **GPS Connection String**: This value is utilized by PAGIS to acquire the GPS feed from its source. The default is traditionally either blank (no entry) or 6.
- **Tracking Sync**: Controls the sync intervals in (Sec.) that PAGIS communicates with BOSS4 to update tracking status. Default off=Zero, values can range from 1-9999. BOSS4 Back Office Software requiered for this feature.
- **Panel Size**: Controls the resolution of the color image displayed on the Live View Screen. By default this is blank as PAGIS controls the aspect ratio. However a PAGIS Admin can assign custom resolutions in WxL format (720x1024) to assist with non-standard dispalys.
- **Back Office Sync**: This setting controls the sync timing that PAGIS sends data back to BOSS3/BOSS4, Timing is in (Sec.), default is 10sec, values can range from 0-9999.

NOTE: All changes must be saved and will not take effect until PAGIS is restarted.

3.8 Rules

Rules in PAGIS allow Administrators to force the software to process plate reads in specific ways. For example, in states that allow for both O and 0 (zero) on their license plates, a rule can be set to read any zero as an O and any O as a zero. This provides PAGIS greater flexibility to the standard OCR functions.



Adding a Rule to PAGIS:

1. Click the Add Button ADD
2. Enter the desired alphanumeric characters (Ex. 0 and O) into the text field
3. Click the Save Button SAVE at the top right of the screen

Deleting a Rule:

1. Locate the rule to be removed from PAGIS
2. Click the Delete Button DELETE to the right of the rule (It will turn green when selected)
3. Click the Save Button to complete the removal

3.8.1 Rules – Additional Clarifications

1. Rules are processed based on the first character entered. So in order to read any O as a zero, the Admin will need to add rule "O0". And in order to read any zero as an O, a second rule must be entered as "0O".
2. Rules are NOT designed to overhaul OCR function. Any consistently misread values should first be brought the attention of PIPS Support for review. And only those cases where further adjustments to the OCR software are impossible would rules be recommended.
3. Adding rules to PAGIS will make it less likely to miss a Hit Alert. However, it will increase the number of Hit Notifications that require the Officer to visually confirm the OCR read ("IR Patch") and the Hotlist Alert match.

3.9 OCR

The OCR Section in PAGIS provides Administrators some additional options on how they would like PAGIS to process plate reads.



- **JPEG Images**: On by default, this forces PAGIS to use compressed .JPG images instead of the full resolution Bitmap images each time a read is taken. This settings minimizes data storage requirements and preserves MDC drive space.
- **Inverse Plates**: Off by default, this setting is only used in States where plates with light color lettering over a dark background are prevalent. Enabling this option increases processing load and should remian disabled unless required.
- **Square Plates**: Off by default, this setting adjusts the read area plates that are square instead of retangular.
- **Disable Duplicate Read**: On by default, this setting helps PAGIS prevent duplicate plate reads. If a VLP is read by more than one camera within a short period, the duplicate read is ignored. This minimizes data storage requirements and improves overall system metrics related to numbers of Hits and Reads.

NOTE: Once changes are made, the Admin must click the Save Button SAVE button in the upper right corner to retain them.

3.10 External

The External Screen allows the Admin to connect PAGIS to an external database or device via XML Datastream. This feature is Off by default and any changes must be saved before they will be available.



Enabling the Datastream:

1. Click the Off Button OFF to toggle to On ON
2. Click the Save button in the upper right corner
3. Close and reopen PAGIS

NOTE: Enabling this feature will reduce the overall performance of the PAGIS Software.

3.10.1 XML Datastream Ports

Administrators will need to configure their external device or database to utilize two specific TCP ports:

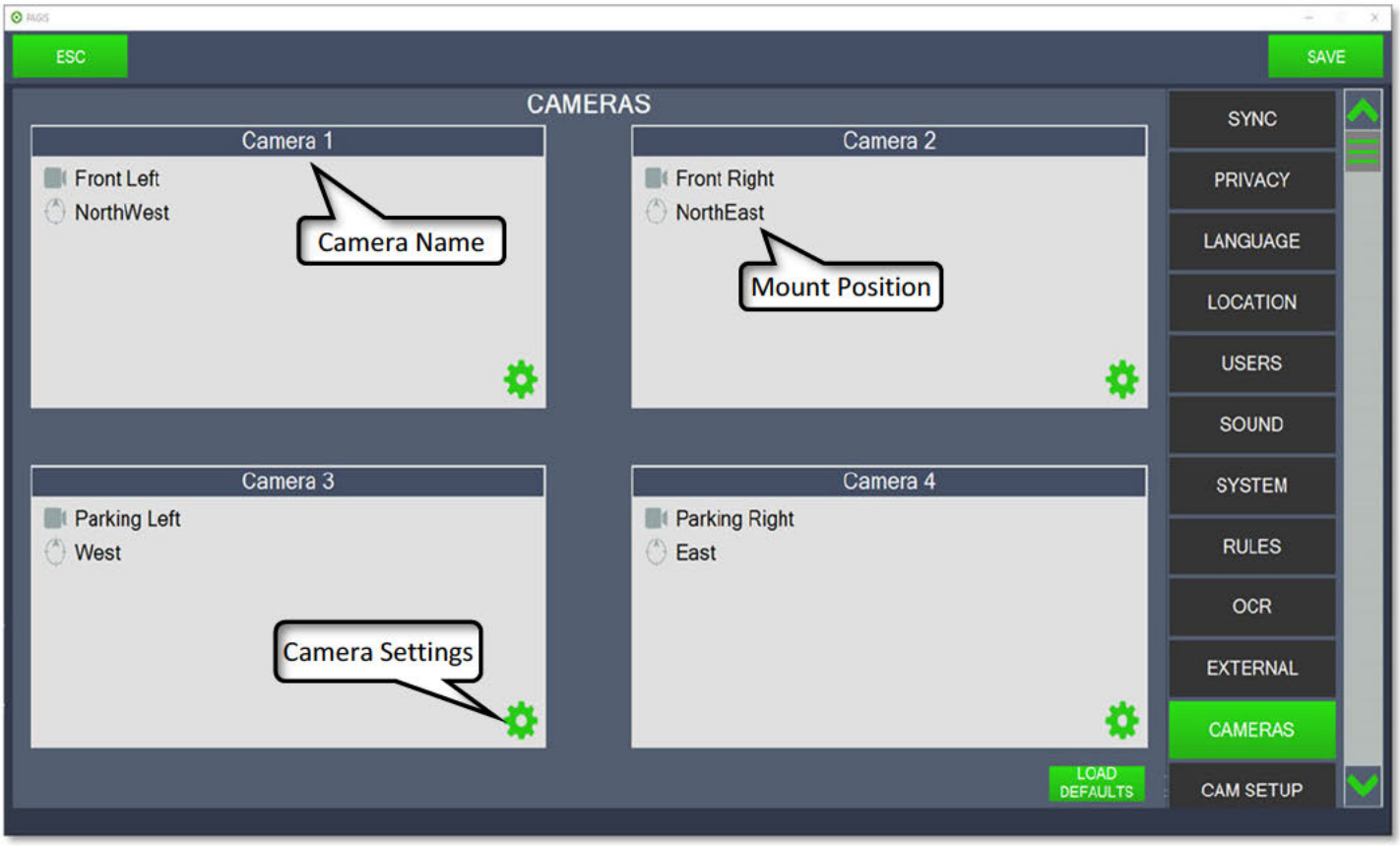
1. Query Port: TCP 7000
2. XML Datastream/Heartbeat: TCP 10100

NOTE: Greater detail on the XML Datastream can be found in Appendix D

3.11 Cameras

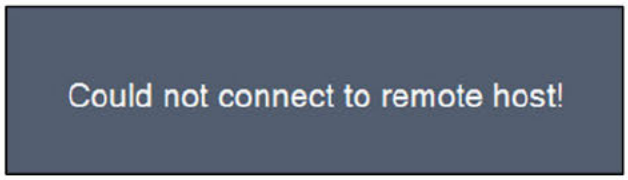
The Cameras Section provides the Administrator the means to add/delete, identify, and configure the ALPR cameras. Although the PAGIS Software comes preloaded with a default layout, best practices advise the Admin to fully review, and completely configure at least one MDC by hand in order to tailor the setup for the Agency's unique attributes.

IMPORTANT: The configuration steps completed here will dictate the available camera mode options in the Configs Section.



3.11.1 Checking the Connection

In order to configure the cameras, the PAGIS Software and the SX Processor (Black Box) must be able to communicate. If they cannot, the Administrator will receive the error message below as soon as he or she clicks on the Cameras Button CAMERAS indicating that PAGIS cannot "see" the cameras.



3.11.2 Troubleshooting Camera Connections

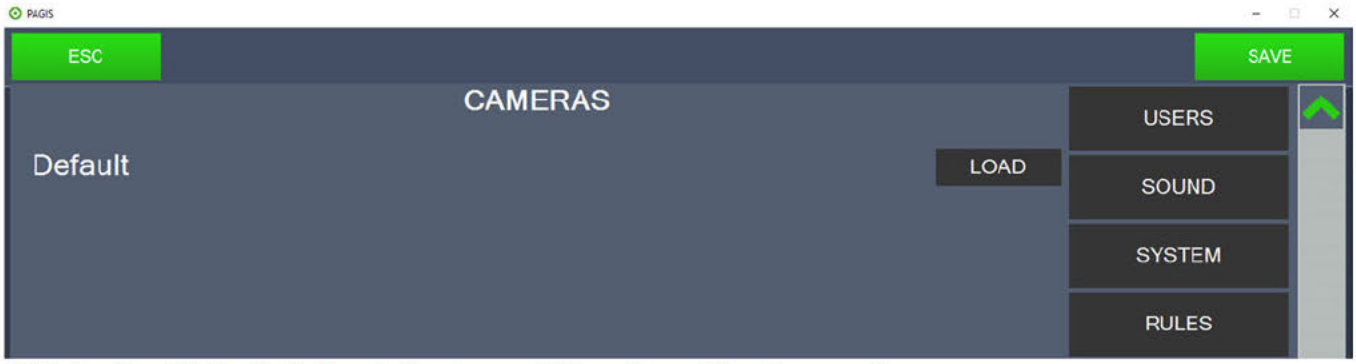
The most common troubleshooting steps have been included below for convenience. If these don't resovle the issue, please contact PIPS Support for additional assistance. **NOTE**: For more information see Appendix C – The Mobile FAQ

1. Start the vehicle and confirm power to the Processor. Confirm the SX switch, and any added in-line switch, is set to On.
2. Confirm the network adapter settings on the laptop match the proper Static IP scheme for the SX Processor in use.
3. Disable the local Windows Firewall, VPN software, and any real-time monitoring software one at a time.
4. Use a different network cable ensuring it's properly seating in NIC port on the SX as well as the MDC or Docking Station.
5. Docking Stations can also impede communication. Test by removing the laptop from thhe dock, directly connect the network cord to the laptop, and then reconfigure the network adapter settings as needed.

3.11.3 Configuring the Cameras in PAGIS

This section will assist with the general configuration of the cameras. Administrators can begin by selecting the Settings Icon to edit each of the existing cameras or by selecting the Load Defaults Button LOAD DEFAULTS. This manual will start with Load Defaults.

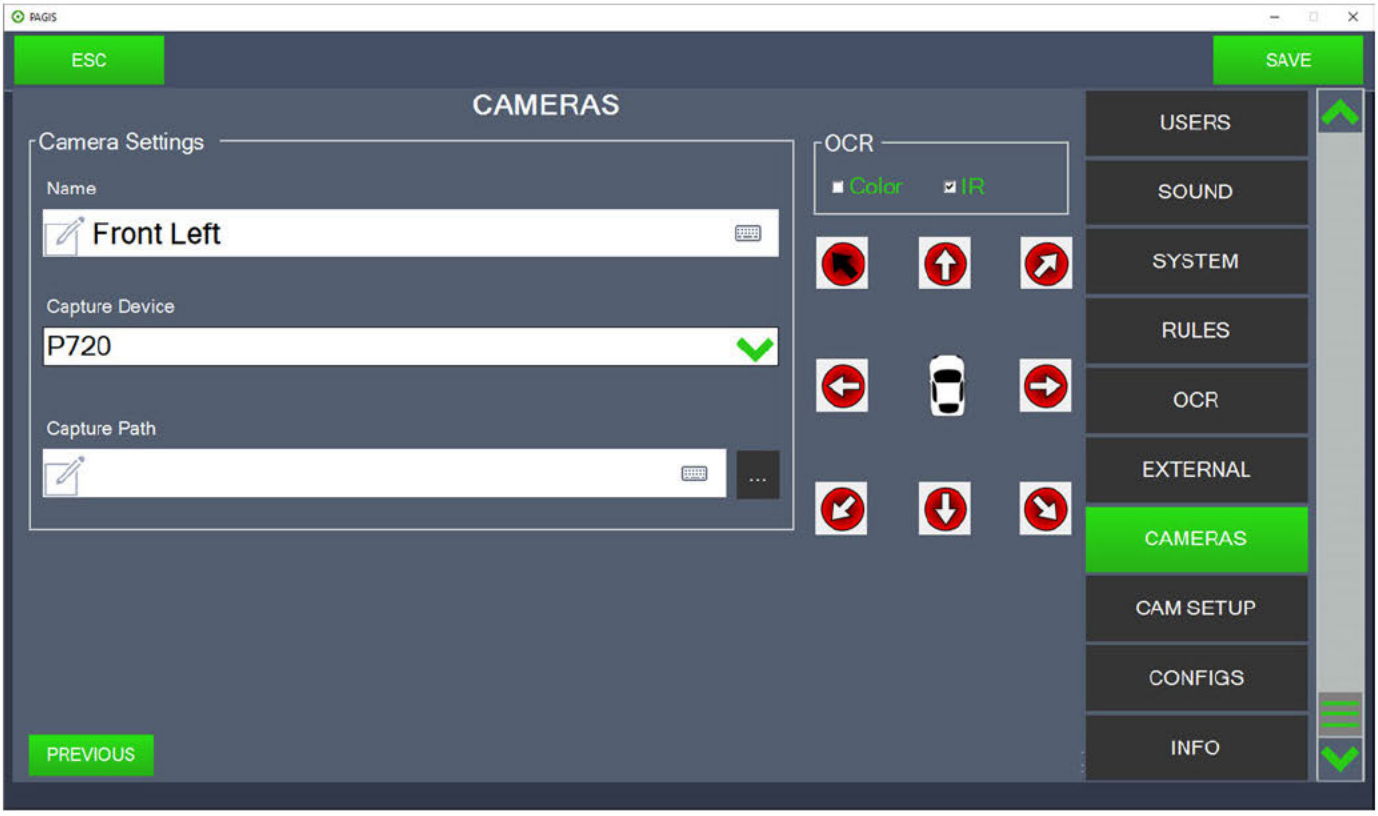
Gettings Started – Load Defaults:



1. Click the Load Defaults Button in the lower right portion of the Cameras Screen
2. Locate "Default" and click the Load Button LOAD
3. Once it's selected (and turned Green), click the Save Button (This returns the Admin to the Cameras Screen)
4. Click the Settings Icon to inspect and configure each camera one at a time

The Camera Settings (Edit) Screen:

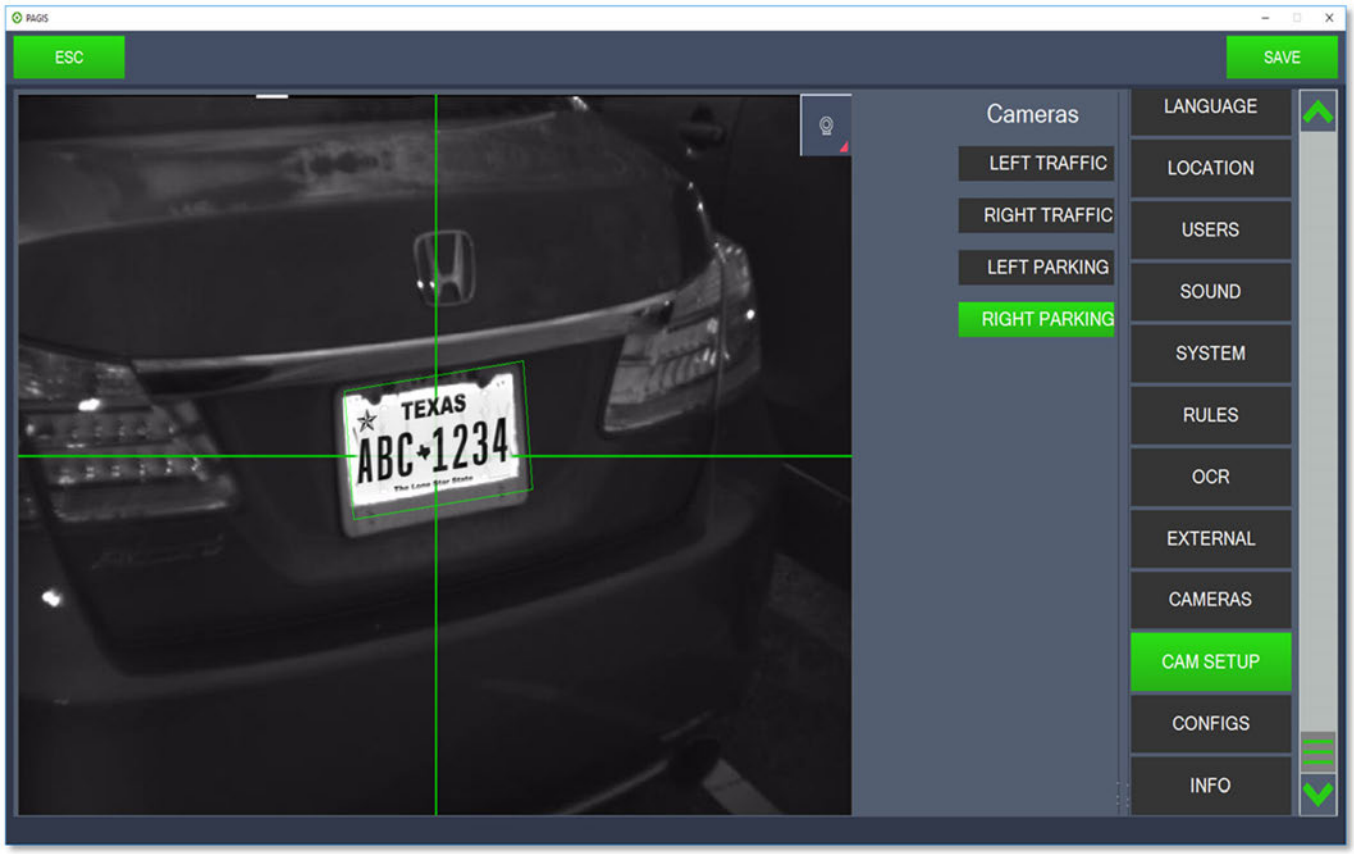
This provides the Admin a single screen to edit the name, confirm the capture device, assign camera position, and confirm OCR.



1. Confirm/Update the Camera Name **NOTE**: Use Camera Names with 11 characters or less to avoid various UI anomalies
2. Confirm the "Capture Device" field was auto-detected. If not, use the drop down to select the only Pxxx value on the list
3. Leave "Capture Path" blank (This is an optional field)
4. Select the camera mount position indicating the direction the camera is facing. The arrows turn black when selected
5. Ensure the OCR is set to IR. The color camera is used for OCR in only rare situations and will increase system load as well as the likelihood of false alerts. Use this setting with caution
6. Click the Save Button to retain the changes

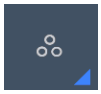
3.12 Cam Setup

The Cam Setup Screen presents Administrators with a live preview of the configured cameras. This section also allows the Admin to switch view modes from Color to IR to ensure the system is functioning properly. **NOTE**: This screen can also be utilized as a means to align newly mounted cameras when RDP access to the SX Processor is limited or unknown.



3.12.1 Cam Setup Navigation Buttons

The Admin may view the output of each camera by clicking on the camera name. When a camera is selected, the button will turn green to indicate it has been selected. In order to switch view modes, the Admin must use the following buttons:



Color View: The Color View Mode is the default view when the Admin first enters Cam Setup. This displays a live preview of the color camera.

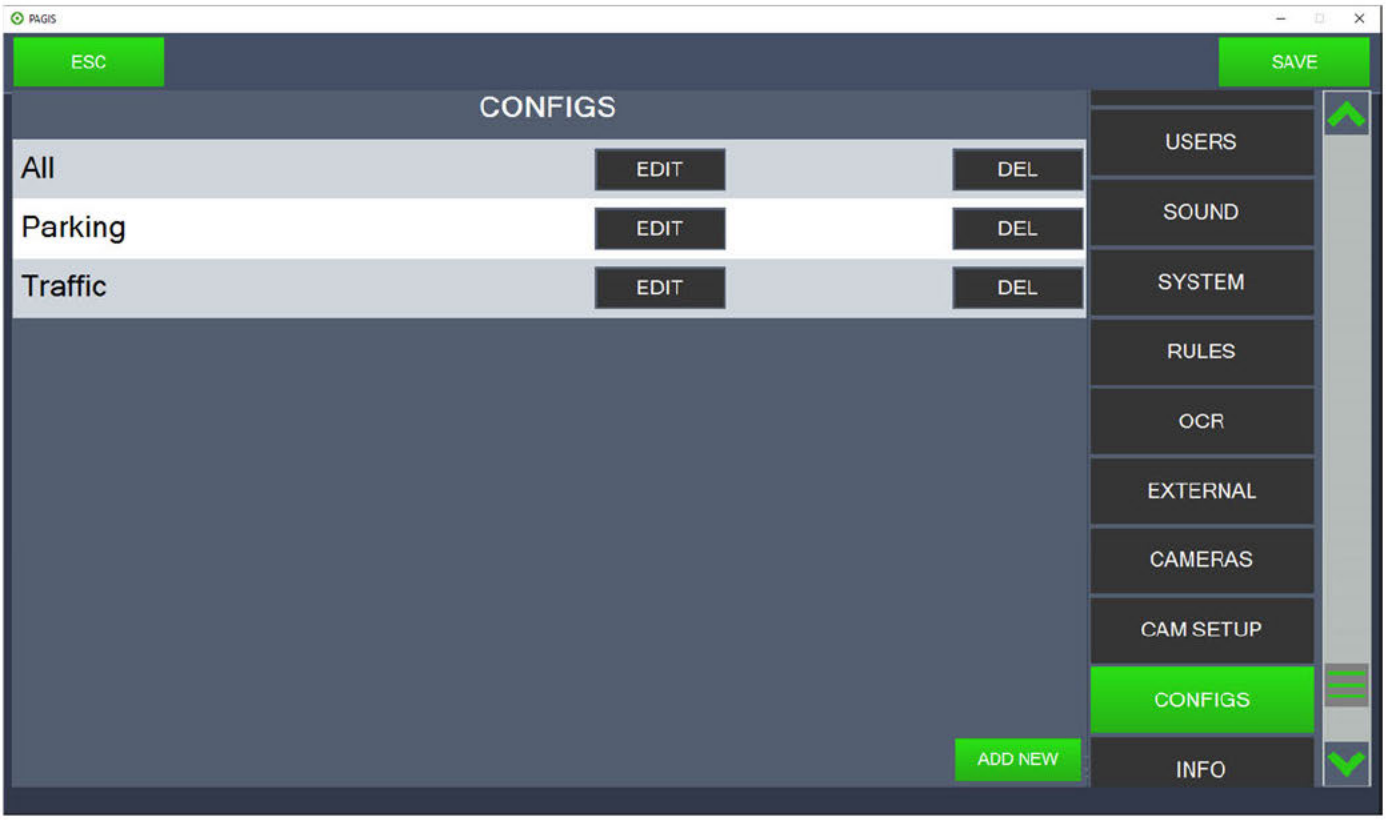


IR View: By clicking on the Camera View Selector button, the Admin will switch to the Infrared (IR) View Mode. This displays a live preview of the IR camera.

NOTE: Unlike the main Live View Screen, the camera feed shown on the Cam Setup page will not time out when in use. This feature makes it easier for the Administrator to review and align the mobile cameras.

3.13 Configs (Camera View Modes)

The Configs Screen allows the Admin to construct how the cameras will be displayed on the Live View Screen for the user. This section also allows agencies to create multiple viewing configurations to meet specific environmental needs or to add greater functionality to the software. By default, the Configs layout provides the agency with three camera modes, “ALL”, “Traffic” and “Parking”. All mode dipalys the front two cameras and rear two are activated, Traffic mode only displays the front two cameras and rear cameras are off, Parking mode only displays rear two cameras and front cameras are off.



3.13.1 Configs Navigation Buttons

To properly configure the camera modes used in PAGIS, the Admin will navigate this section with the following:



To delete a config/camera mode, click the DEL button to select it (turns Green) and then click Save



To review, edit, or modify a camera mode, click the EDIT button



To preserve changes or finalize a deletion, click the SAVE button

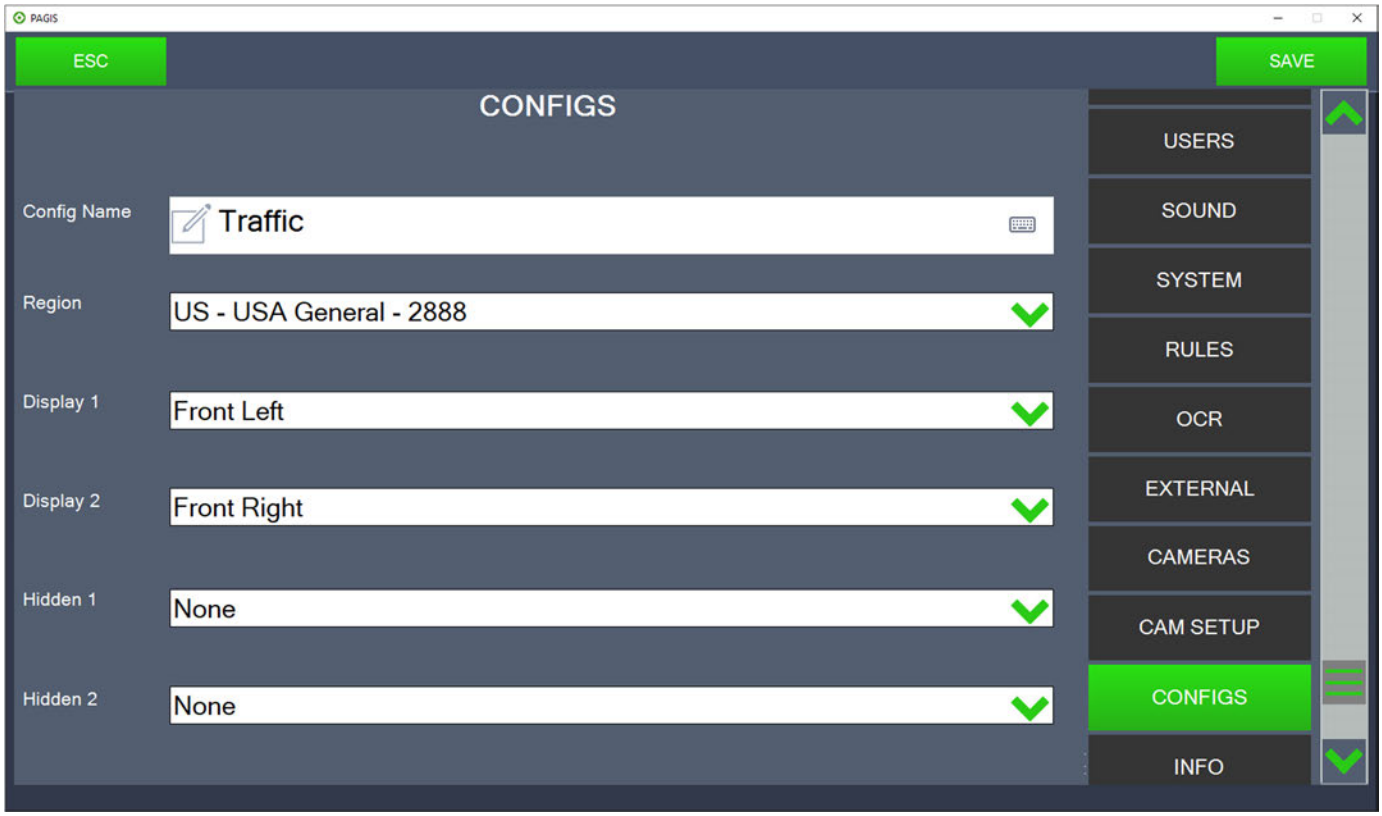


To add a new camera mode, click the ADD NEW button

NOTE: The number of Configs equals the number of Camera Modes available to the user from the Live View Screen. Each camera mode untilizes the Config name established in this section. Users cycle through the modes on the Live View Screen by clicking the Mode Selection Button in the upper left corner.

3.13.2 Reviewing and Modifying Existing Modes

When getting started, most Administrators will begin by simply modifying the existing camera modes or “configs”. The following example will demonstrate the standard configuration of a four-camera mobile unit.

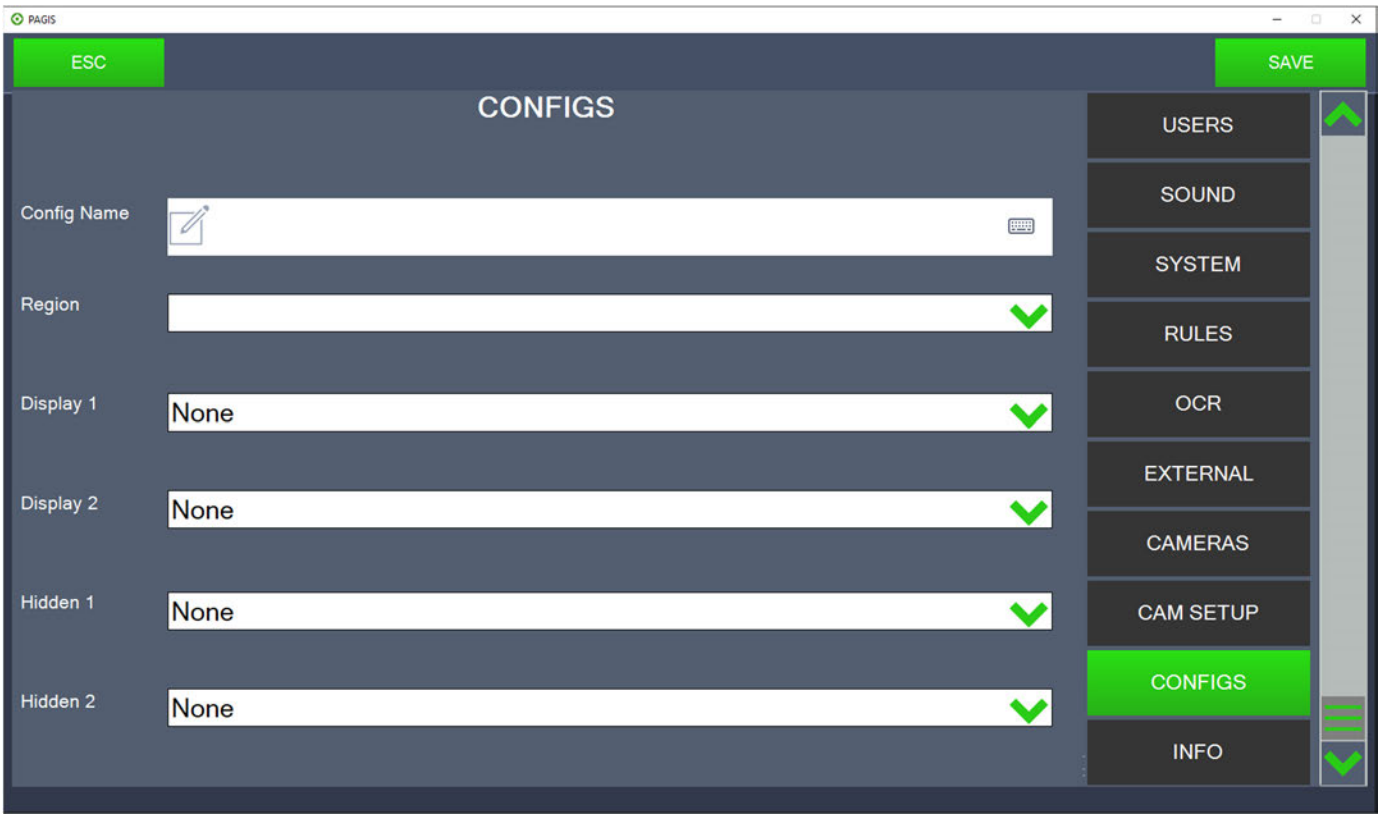


1. Click the EDIT Button EDIT from the main Configs Screen to modify a mode
2. Review/Update the name of the Mode **NOTE**: The name should be intuitive for all users as this becomes the label of the mode selection button on the Live View Screen
3. Click the drop down arrow on the Region field to select the best local option (Adds additional accuracy to OCR)
4. Confirm the camera listed in the Display 1 field. This camera will be displayed on the left side of the Live View Screen
5. Confirm the camera listed in the Display 2 field. This camera will be displayed on the right side of the Live View Screen
6. Confirm the Hidden 1 field shows one of the other cameras not listed in the Display fields
7. Confirm the Hidden 2 field shows the last available camera not yet listed (Leave field as “NONE” for 3-cam systems)
8. Click the Save button to retain the changes
9. Click the Configs Button from the menu to access the other Mode(s)
10. Perform steps 1-8 for all Configs/Camera Modes available

NOTE: Cameras listed in the Hidden fields will function, perform OCR, and capture plate reads, but they will not be displayed to the user while in the named camera mode (unless a Hit is detected opening the Alert Screen). For ALPR units with more than two cameras, best practices dictate the Admin utilize these fields.

3.13.3 Adding a New Camera Mode

When the two default modes provided in the PAGIS software do not offer the agency all the functionality desired, the Administrator can use the Configs Screen to add additional camera modes. For example, if officers request a mode to view only the cameras on the left side of the vehicle while stopped on the side of the road, the PAGIS Adminstrator can build that functionality from this screen.



1. Enter a name for the new Mode (Ex. “Left Side”)
2. Click the drop down arrow on the Region field to select the best local option (Adds additional accuracy to OCR)
3. Confirm the camera listed in the Display 1 field. This camera will be displayed on the left side of the Live View Screen
4. Confirm the camera listed in the Display 2 field. This camera will be displayed on the right side of the Live View Screen
5. Confirm the Hidden 1 field shows one of the other cameras not listed in the Display fields
6. Confirm the Hidden 2 field shows the last available camera not yet listed (Leave field as “NONE” for 3-cam systems)
7. Click the Save button to retain the changes

3.14 Info

4269

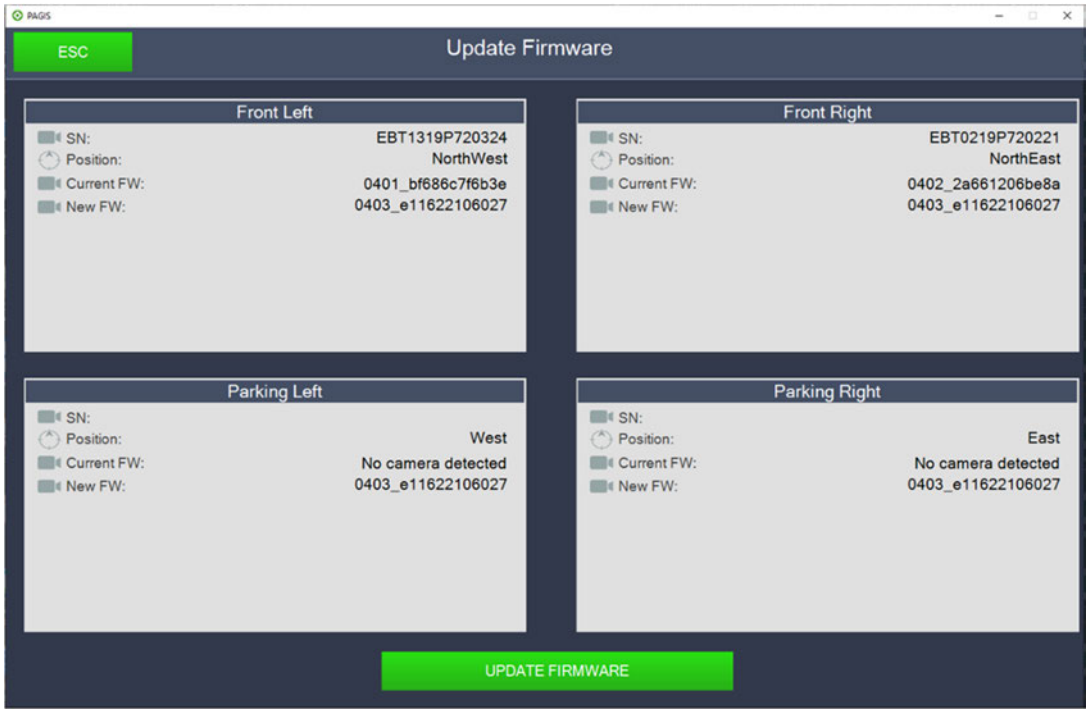
The Info screen displays additional information including the version number of the current installation. This information is helpful when contacting Technical Support.



3.15 Camera Firmware Update, (Admin)

Camera firmware update provides a means for PIPS to update the camera software to enhance and or correct camera performance. The frimware icon  will only apper when a update is avialable.

- The firmware update process only updates camera that are attached and function on the mobile processor.
- Administrator must log into PAGIS and apply the FW update. The update process takes around 4min and should not be interrupted or risk permanently damaging the cameras, PAGIS will return to normal opertaion after update.
- Once the "UPDATE FIRMWARE" button is clicked PAGIS will switch to full gray screen with message indicating "Camera Firmware is Updating", during this process you'll will notice small command windows opening on top of PAGIS, these windows represent the firmware being applied to each active camera so you may notice one or server depending. Once completed a message will appear "Firmware Updated Successfully" then PAGIS will return to normal operation.
- After FW completion and return to "Live View", its requiered to cycle thought the "Cam Mods" to refresh cameras.



Firmware Updater Window List.

- Title "Camera Name".
- Camera serial number.
- Position.
- Current FW version.
- New FW version available.

4.1 PAGIS System Requirements

The PAGIS Software requires the following minimum system requirements for the mobile data computer:

- Intel I3 CPU at 2.0 GHz or higher.
- Windows Operating System (Win7-Win10).
- Microsoft .NET Framework 3.5.
- 8 GB of RAM.
- At least 1 GB of free disk space.
- SVGA display with a minimum resolution of 800 x 600 pixels.
- Available 10/100 Ethernet port.
- Keyboard and mouse, or a touch screen monitor.
- Internet access needed for mapping and Firmware update.

4.2 PAGIS Prerequisites

Prerequisites:

1. Ability to install software.
2. Ability to configure the network adapter.
3. PAGIS 2.12 and above are only compatible with SX4 and SX4e Processors.

Network Adapter Settings:

The PIPS mobile processor operates based on a static IP and is preassigned the IP address of 192.168.200.201. When connecting laptop/MDC to the PIPS mobile processor your computer must be on the same IP network as the mobile processor, in fact the connecting compute must adopt one octet lower than the assigned IP of the PIPS processor in order for MDC installed PAGIS to connect to the mobile processor and receive data from the ALPR cameras. Below are the steps to configure your computer.

1. Navigate to Adapter Options in Windows and right click on the adapter and select properties.
2. Click to select IPv4 and click Properties
3. Click the radio button “Use the following IP Address” to set the Static IP address.
4. Enter 192.168.200.200 in “IP address” section.
5. Enter 255.255.255.0 in “Subnet mask” section.
6. Either leave the “Default gateway” blank or enter 192.168.200.201.
7. Click OK to save changes.

NOTE: The Mobile processor is pre-configured to relay its camera data connection to the .200 IP address, using alternative IP’s on Laptops will result in the software’s failure to communicate with the cameras.

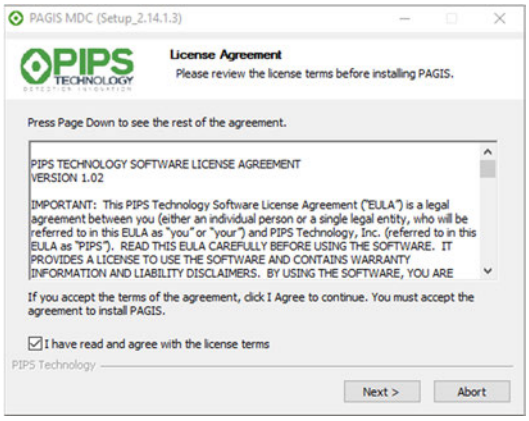
4.2.2 PAGIS Software Installation (MDC)

4271

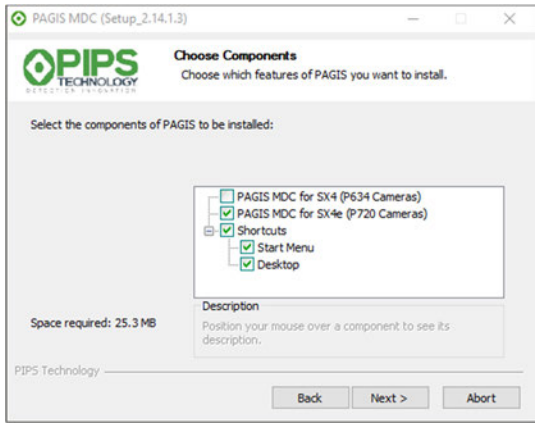
1. If PAGIS exist on your computer, it must be version 2.9 or 2.12 for installer to update. If your version of PAGIS is older it is recommended you “EndShift” any existing data, then uninstall PAGIS.
2. It is recommended you “EndShift” any existing data if upgrading a previous version of PAGIS.
3. Prior to software installation, take the time to figure out what version of PIPS mobile processor you have as the software installation requires you to select so it can properly configure the camera settings based on processor type. PAGIS version 2.14 supports processor versions SX4 & SX4e only, you can either look at the product tag located on the processor or look at the camera IO ports on the back of the processor, if the 4 camera IO ports are vertically arranged RJ45’s then it’s a SX4e, if they are vertically arranged circular shaped “LEMO” connectors then it’s a SX4. Horizonal arranged circular shaped “LEMO” connectors is a SX3 and is not compatible with PAGIS 2.14.
4. When upgrading to PAGIS V2.14.x.x also requires that the PIPS mobile processor be updated to same version in order to take advantage of Firmware update.



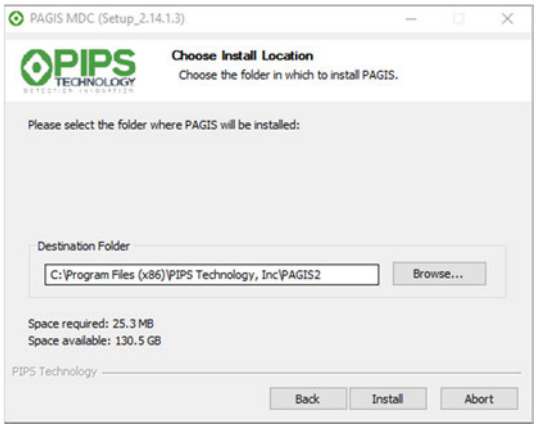
5. Place the PAGIS installer on your computer’s desktop, “PAGIS_Setup_MDC_2.14.x.x.exe”.
6. Right click the PAGIS installer executable and select “Run as administrator”.



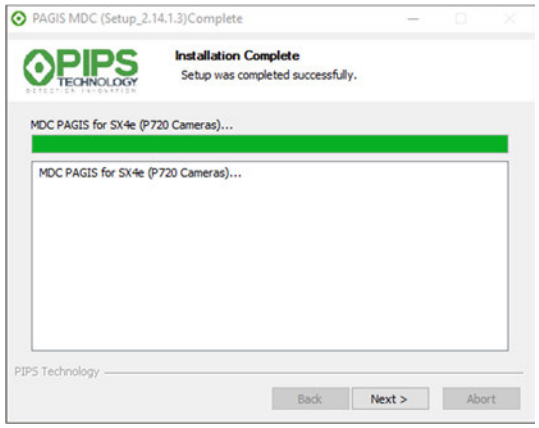
7. Check the license agreement box, then click Next.



8. Select the mobile processor type and alter “Shortcuts” if needed. Next to continue.



9. Confirm path if upgrading, click Install to proceed.



10. Installation Compete, Next to proceed.
11. Click Finish.
12. Click Yes to reboot if you would like to test PAGIS auto start at login if selected during installation, otherwise click No as its not required for PAGIS to run.

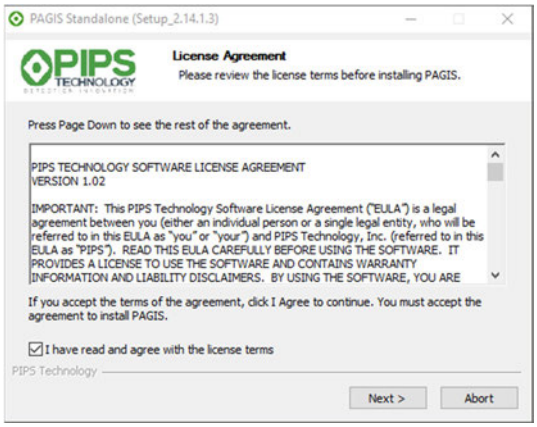
Note: See Appendix A for terminology definitions.

4.2.3 PAGIS Software Installation (Mobile Processor)

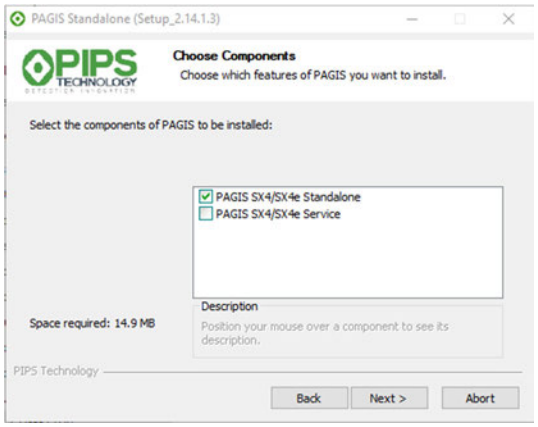
1. PAGIS v2.14.x.x updater is only compatible with PIPS mobile processors SX4 & SX4e.
2. The PAGIS updater only updates existing versions of PAGIS on mobile processor, version 2.9 and newer.
3. Update required for both “Standalone” & “Service/VPRelay” to support some of the newer features.
4. The processor must be in its respective mode to update that option as the folder path are hidden when not active, see “Change Mode” in SX4 or SX4e manual.



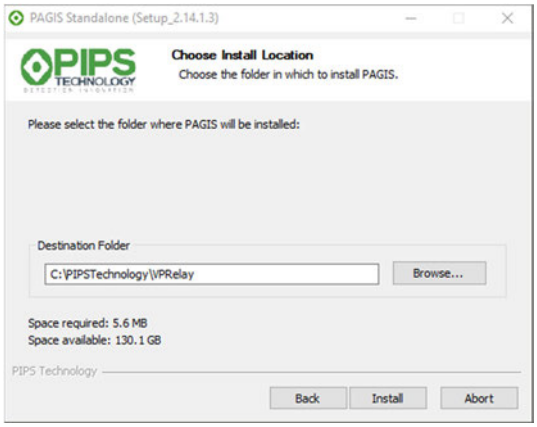
5. Remote desktop into processor or utilize attached monitor/keyboard.
6. Place the updater in C:\PIPSTechnology folder on the PIPS mobile processor.
7. Execute PAGIS Updater.



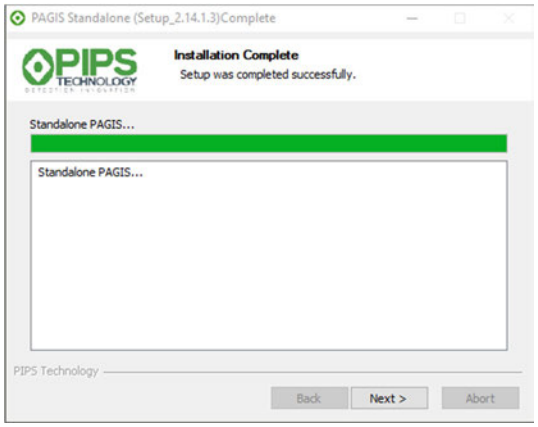
8. Check the license agreement box, then click Next.



9. Select option to update, next to continue.
   - Standalone= PAGIS login from Processor.
   - Service= PAGIS login from connected Laptop.



10. Change the default path presented by updater, see below.
    - For “Service” C:\PIPSTechnology\VPRelay.
    - For “Standalone” C:\PIPSTechnology\Standalone.



11. Installation Compete, Next to proceed.
12. Click Finish.
13. Click Yes to reboot.

Note: See Appendix A for terminology definitions.

TROUBLESHOOTING TIPS

This section provides some basic troubleshooting tips and information

5.1 Troubleshooting & Tips

- The first login to PAGIS after the new install of an unconfigured version does not require a username or password. Simply click Login to be granted Admin access to the software.
- A good means to test the communication from the MDC to BOSS is ping or telnet (over TCP 8092) through the command prompt.
- A good means to test the communication from the MDC to the SX Processor is ping or telnet (over TCP 9000) via command prompt.
- For many other troubleshooting tips, see Appendix C – Frequently Asked Questions

5.1.1 PAGIS with NetMotion VPN

Agencies utilizing NetMotion VPN software on the MDC will need to apply the following passthrough steps:

1. Login to the NetMotion server as administrator
2. Click Settings > Then select Client > Select Global Client Settings > Then select Passthrough List
3. Click the “Add…” button on the right > Select “Network Address”
4. Enter the following settings (as shown):
    A. IP address:192.168.200.0 (the zero is correct, it's an IP address “range”) Subnet Mask: 255.255.255.0.
    B. Keep all other settings default (as shown) and click OK.
5. The MDC must then disconnect from NetMotion and reconnect again for the settings to be applied locally.

5.1.2 Cisco VPN Client:

Make sure Stateful Firewall is unchecked and "Allow Local LAN".

5.1.3 Microsoft .NET 3.5 Installation

The PAGIS Software requires Microsoft .NET Framework 3.5 specifically. If the MDC doesn’t have .NET, it can be downloaded from the Microsoft website.

5.1.4 Firewall Settings for Client-Server Installations

For client-server installations, the Windows Firewall needs to allow the SX Processor and the MDC to communicate. If the MDC is maintained by a Network Administrator, he or she should be contacted before making changes to the firewall. The command prompt commands for the exceptions are below

Option 1: Allow Microsoft Windows Version 8 or newer to auto-detect the launch of the PAGIS.exe application and use the wizard to add the PAGIS.EXE to the exception list (making note of Public or Private Network settings as necessary).

Option 2: Add PAGIS to the exception list manually by browsing to the install path of PAGIS. The default is below for reference: C:\Program Files (x86)\PIPS Technology, Inc\PAGIS2\PAGIS.exe

Option 3: Add the communication ports manually:
TCP in/out 8092 = Pagis sync port to BOSS back office software.
TCP in/out 9000 = Mobile processor camera feed port.
TCP in/out 9001 = Mobile processor camera snapshot port.
TCP in/out 32023 = Mobile processor camera setup port.
TCP in/out 10000 = Mobile processor data capture port.
NOTE: XML Datastream uses TCP 10100 and TCP 7000

PAGIS/BOSS3 CONFIGURATION 4274

In order for the PAGIS software to function properly, the device must be built, enabled, and configured in BOSS3 before being deployed for service in the field.

6.1 Creating a New Device in BOSS3

Once network communication to BOSS3 has been established from the vehicle, the new device must be "built" or added to the Device List in BOSS3 before it can be used. The approved way to do this, is to simply perform a Begin Shift from the PAGIS software. **NOTE**: The computer name is what will be displayed in BOSS as device name.

1. At the PAGIS Live View Screen, click the Begin Shift button once to select it, and then click again to launch the sync.
2. If the laptop has previously been setup to communicate with BOSS and is already enabled, the sync transfer window should appear in the middle of the Live View Screen.
3. If this is a new/disabled device, a message indicating "HttpStatusCode" will be displayed.
4. This indicates the BOSS3 server has received the sync request but has rejected it due to device status.
5. Once the BOSS Admin has enabled the device, the Status Code error will not appear again, and syncs should complete as configured in BOSS3.

6.2 Enabling a New Mobile System in BOSS3

Installing PAGIS and configuring the network settings is only the first step in making the ALPR unit operational. Once PAGIS is configured to work with or on the SX Processor and the mobile cameras, it must then be enabled in BOSS3 before synchronizations can take place. **NOTE**: By default, every new device recognized by the BOSS3 server is disabled until the Admin enables it. This is done for security.

1. Log into the BOSS3 UI Client Software with Admin privileges.
2. Click the Admin button on the left to expand the options.
3. Click the Devices button. The new device should now be listed to the right.
4. Click the name of the Device to select it. (This will open the device details screen)
5. Click the Edit button at the bottom of the window.
6. Click the Enable button from the Edit window.
7. This will enable the device and return the Admin to the Device List.

NOTE: If desired, the Admin can re-enter the Edit window to assign an alternate name in BOSS3 for the new device. The Admin will need to update the "Description" field and then click the Save button. Agencies commonly use this field to signify the Unit number, Car name, or Patrol Shift. The "Name" field is the device/host name and cannot be edited in BOSS3.

NOTE: Once the Device is enabled the Admin needs to assign ownership and hotlist distribution.

6.3 Assigning Ownership to a Device in BOSS3

Every new device added to BOSS3 allows for Admin level access into PAGIS without the use of a username or password. In order to password protect the PAGIS software, the BOSS Administrator must assign "Owners" to the device in BOSS3.
NOTE: For more detail on Users, User Groups, Sites, and Roles, refer to the BOSS3 manual.

1. Login to the BOSS3 UI with Admin credentials.
2. Click the Admin button on the Left to expand the options.
3. Click Devices to review the list.
4. Click on the Device Name to open the device details screen.
5. Click on the Edit button.
6. Locate the "Owners" field. Click the Select button to the right.
7. Check the box(es) for the appropriate Site(s)/User Group(s). **NOTE**: This tells BOSS3 which sets of users will have rights to login to PAGIS from this specific device.
8. Notice the Select button has changed to a Save button. Click Save to retain changes.
9. Confirm the changes show in the Owners Field.
10. Click the Save button at the top left of the Edit window.

6.4 Assigning Hotlists to a Device in BOSS3

In order for the PAGIS users to receive alerts, one or more of the stored hotlists in BOSS3 must be distributed to the new device. **NOTE**: For more information on building and configuring Hotlists, refer to the BOSS3 manual.

1. Login to the BOSS3 UI with Admin credentials.
2. Click the Admin button on the Left to expand the options.
3. Click the "Hotlists" button to review the list of configured alert lists.
4. Click the Hotlist Name to select the first alert list. This will open the Details screen.
5. Click the Edit button at the bottom of the window.
6. Locate the "Deployment" field. Then click the Select button to the right.
7. Check the box next to the name of the new device.
8. Notice the Select button has changed to a Save button. Click Save to retain the changes.
9. Confirm the changes show in the Deployment Field.
10. Click the Save button at the top left of the Edit window.
11. Perform these steps again for all remaining Hotlists necessary for this device.

PAGIS/BOSS4 CONFIGURATION

In order for the PAGIS software to function properly, the device must be built, enabled, and configured in BOSS4 before being deployed for service in the field.

7.1 Creating a New Device in BOSS4

Once network communication to BOSS4 has been established from the vehicle, the new device must be "built" or added to the Device List in BOSS4 before it can be used. The approved way to do this, is to simply perform a Begin Shift from the PAGIS software. **NOTE**: The computer name is what will be displayed in BOSS as device name.

1. At the PAGIS Live View Screen, click the Begin Shift button once to select it, and then click again to launch the sync.
2. If the computer has previously been setup to communicate with BOSS and is already enabled, the sync transfer window should appear in the middle of the Live View Screen.
3. If this is a new/disabled device, a message indicating "HttpStatusCode" will be displayed.
4. This indicates the BOSS4 server has received the sync request but has rejected it due to device status.
5. Once the BOSS Admin has enabled the device, the Status Code error will not appear again, and syncs should complete as configured in BOSS4.

7.2 Enabling a New Mobile System in BOSS4

Installing PAGIS and configuring the network settings is only the first step in making the ALPR unit operational. Once PAGIS is configured to work with or on the SX Processor and the mobile cameras, it must then be enabled in BOSS4 before synchronizations can take place. **NOTE**: By default, every new device recognized by the BOSS4 server is disabled until the Admin enables it. This is done for security.

1. Log into the BOSS4 URL with Admin privileges.
2. Navigate to the Resources pulldown menu.
3. Select Devices from the menu options. The new device should now be listed.
4. Click the name of the Device to select it. (This will open the device details windows on the left)
5. Click the Enable slide toggle to enable device, located in upper right of device edit window then click save.
6. This will enable the device, synchronization between BOSS4 and PAGIS is allowed.

NOTE: Once the Device is enabled the Admin needs to assign ownership and hotlist distribution.

7.3 Assigning Ownership to a Device in BOSS4

Every new device added to BOSS4 allows for Admin level access into PAGIS without the use of a username or password. In order to password protect the PAGIS software, the BOSS Administrator must assign “Owners” to the device in BOSS4.

NOTE: For more detail on Users, User Groups, Sites, and Roles, refer to the BOSS4 manual.

1. Login to the BOSS4 URL with Admin credentials.
2. Navigate to the Resources pulldown menu.
3. Select Devices from the menu options. The new device should now be listed.
4. Click the name of the Device to select it. (This will open the device details windows on the left)
5. Locate the “Owner” field. Click in the Owner filed, and a list of all available Groups will appear.
6. Select group by clicking on it, it will then automatically be added to owners, see list below “Owner”.
7. To add mode groups, repeat step 15.
8. Confirm the changes show in the Owner Field.
9. Click the Save button at the bottom right of the Edit window.

7.4 Assigning Hotlists to a Device in BOSS4

In order for the PAGIS users to receive alerts, one or more of the stored hotlists in BOSS4 must be distributed to the new device.

NOTE: For more information on building and configuring Hotlists, refer to the BOSS4 manual.

1. Login to the BOSS4 URL with Admin credentials.
2. Navigate to the System pulldown menu.
3. Select Hotlists from the menu options
4. Click the Hotlist Name to select the first alert list. This will open the Details screen.
5. Locate the “Deployment” field.
6. Check the box next to the name of the new device listed.
7. Click the Save button at the bottom right of the Edit window.
8. Perform these steps again for all remaining Hotlists necessary for this device.

APPENDIX A: THE GLOSSARY

4277

ALPR/ANPR	"Automatic License Plate Recognition/Automatic Number Plate Recognition".
BOSS	"Back Office System Software". This is the ALPR server.
GPS	"Global Positioning System".
GUI	"Graphical User Interface".
Hotlist	A database or list that contains vehicle license plates of interest ("alert list").
IR	Infrared light.
License Plate	Also called a tag or number plate.
MDC	"Mobile Data Computer". This is the tablet or laptop in the vehicle.
OCR	"Optical Character Recognition" (also referred to as a "cardet").
OS	"Operating System".
PAGIS	This is the License Plate Capture Software most commonly used in an ALPR vehicle.
Service	Operation mode of the PAGIS software. Service or "VPRelay" is used to refer to PAGIS instance that is running directly on the PIPS mobile processor without a GUI interface, this mode is intended to run in conjunction with MDC version of PAGIS installed on laptop connected via Ethernet.
Standalone	Operation mode of the PAGIS software. Standalone is used to refer to PAGIS instance that is running directly on the PIPS mobile processor with a GUI interface. Same a "Service"
SX	SX is a short notation referencing PIPS's mobile processor, commonly the SX is followed by the generation number of the processor, i.e. SX3, SX4 & SX4e.
UI	A "User Interface" is the means in which the user can access and navigate the software.
USB Flash Drive	Also called a thumb drive or memory stick.
VLP	"Vehicle License Plate".
VPN	"Virtually Protected Network".
VPRelay	Operation mode of the PAGIS software. VPRelay or "Service" is used to refer to PAGIS instance that is running directly on the PIPS mobile processor without a GUI interface, this mode is intended to run in conjunction with MDC versions of PAGIS installed on laptop connected via Ethernet.
Whitelist	Opposite of a standard BOSS Hotlist. This is a list of license plates that should not trigger an alert.

APPENDIX B: PAGIS SOFTWARE DATABASE FILE

This section is used to configure the PAGIS Software when it's not being used with the Back Office System Software (BOSS). Comma-separated value (CSV) format is the only format the PAGIS Software supports for importing data into the vehicles for the purpose of matching against the captured license plate data. PAGIS will support CSV files with any number of columns, called "fields", as long as the first field is the VLP (Vehicle License Plate). **NOTE**: The CSV format is standard ASCII.

Example CSV Files:

1. *ABC123, Red, Ford, Explorer, 1996, WANTED XYZ456, Blue, Audi, A4, 2001, MURDER*
2. *45ABC234, Vehicle wanted in associated with a kidnapping on 12/5/2005 995BD233, Vehicle reported stolen from Liz's Lounge at 6am on 12/1/2005*
3. *UIO223 ABC123*

General Function:

PAGIS calls/utilizes files in pairs. Each database in PAGIS is created using two files; a CSV file, and an INI configuration file. Without both of these files, the database will not load and PAGIS will not "see" it. Each CSV file/hotlist must have the exact same name as the INI configuration file. Example: Stolen.ini and Stolen.csv will work. Stolen.ini and Plates.csv will not.

Reading an INI Configuration File

Lines that appear in brackets [] are called "Headings". The labels that appear inside the headings, are called "values". Values will always contain an equal sign (=). If a line starts with a semicolon, it is considered to be a comment and is not read by the software. There is no limit to the number of comments in the INI file.

The [SETTINGS] Heading

The values in the Settings heading are: NumFiles, DbName, DbColor, Priority, Covert, Alarm, and NumFields.

- NumFiles: Determines how many database files the system should split the specified hotlist into. Generally, this value is set to 1. But for larger hotlists (200,000+ lines), a number of 2-5 may be more desirable.
- DbName: Tells the PAGIS Software what the displayed name of the hotlist should be.
- DbColor: Sets the display color of the hotlist. This is merely an esthetic setting and not a functional setting. The right-hand side of the equal sign is the HEX value representing the ARGB values for the color. If this value is unknown, the Admin should simply leave this line out of the file.
- Priority: Designates the priority of this hotlist in relation to other hotlists in the system. The highest priority database is 1 and the lowest is 999. **NOTE**: if a plate resides on multiple lists the higher priority will be alerted first.
- Covert: Determines whether standard PAGIS Software users are alerted when a hit is made from the database. Covert database can be used for hotlists that are included for information-gathering purposes rather than eliciting user intervention. The system can also be configured to notify via email or SMS message when a hit is made from a covert hotlist.
- Alarm: Sets the audible alert to be played in PAGIS when a hit is made from the hotlist. Values for Alarm are LOW, MED, HIGH
- NumFields: Indicates how many fields (columns) are in the CSV file. If this value is less than the actual number of fields in a file, then the additional fields are placed in the general information area. This value also determines the number of headings of the [Field x] present in the file. For example, if NumFields=2 then there will be two additional headings, [Field 0] and [Field 1]. **NOTE**: Adding "Creation =" will place the timestamp the hotlist was added to the Begin Shift file.

The [FIELD X] Heading

Under the Field heading, there are two configurable values, “Name” and “PAGIS”.

- Name: Tells the system what the name of this field is. If no name is specified, then no name given to the field. The format is Name = <field>
- PAGIS: Specifies how to display the field in the GUI/PAGIS Software.
    - If no value is defined, the field is placed as general information.
    - Values 1-5 represent special fields for the PAGIS Software that translate to the information being displayed in a box of its own when a hit is processed.
    - A value of 6 represents an ID number to cross reference the vehicle from the hotlist with a person from the wanted list.
    - A value of 7 is identical to leaving the value undefined.

Sample INI Configuration File

[Settings] NumFiles=1
DbName=Stolen Vehicles DbColor=ffffff00 Priority=5 Covert=False Alarm=MED NumFields=8
;PAGIS Values
;0 is VRM / VLP (Not User Definable, always Field 0)
;1 is Special Field 1
;2 is Special Field 2
;3 is Special Field 3
;4 is Special Field 4
;5 is Special Field 5
;6 is ID Number (PNC ID, Drivers License, Social Security Number, etc.)
;7 is General Info (Default for all undefined fields) [Field 0]
PAGIS=VRM

Sample INI Configuration File

[Field 0] Name=VRM
[Field 1] Name=Color
PAGIS=3 [Field 2]
Name=Make PAGIS=1
[Field 3] Name=Model
PAGIS=2 [Field 4]
Name=Action PAGIS=4
[Field 5] Name=Warning
PAGIS=5 [Field 6]
Name=PNCID PAGIS=6
[Field 7] Name=Intelligence PAGIS=7

APPENDIX C: FAQ

Q: **HOW DO I ENTER A SUPPORT CASE?**
A: We have a webform you can use here, you can email our Support Team at Support@PIPSTechnology.com, or you can call us on the phone Monday-Friday 8am to 4pm Central Time (9am-5pm Eastern) at (833) 747-7577 Option 2.

Q: **HOW DO WE CREATE USERS IN PAGIS?**
A: The agency BOSS Administrator creates all users, both for BOSS and for PAGIS. Once the user is created in BOSS, the Admin would click the user's name to select/edit the user. Then click the Advanced button and update the PAGIS specific password. Please note that the username and password fields are both case sensitive and the PAGIS users need to be added to a group with the Role that allows them to use PAGIS/LPCS.

If you have any further questions, please feel free to enter a request for support here.

Q: **WHERE DO USERS CHANGE THEIR LOGIN PASSWORD IN PAGIS?**
A: User passwords are created and updated in BOSS via the UI client software. For the majority of our customers using both the PAGIS Software and BOSS, any user accounts or passwords created in the PAGIS Software itself will be overwritten by the user information defined in BOSS during the next sync.

If you have any further questions, please feel free to enter a request for support here.

Q: **HOW DO WE REQUEST AN RMA REPAIR?**
A: To assist with this, please navigate here to review our RMA procedure as well as to download the request form. Please keep in mind that once submitted, all repairs are reviewed for age of equipment and warranty status before final processing takes place. Additionally, incomplete forms and those without much detail often result in processing delays.

If you have any further questions, please feel free to enter a request for support here.

Q: **WE GOT NEW MDC LAPTOPS IN THE PATROL CARS, HOW DO WE ADD THOSE DEVICES TO BOSS?**
Q: **HOW DO WE EDIT THE DEVICE NAMES IN BOSS?**
A: The initial device template/skeleton is automatically created in BOSS the first time the device attempts to Sync from the field. Devices should NEVER be created manually. For PAGIS laptops, this is done after PAGIS is installed and configured and Begin Shift is launched. However, if the agency would like to organize the device list by updating the "Device Name" field, those steps are below:
1. Login to the BOSS UI with Admin rights
2. Navigate to Admin > Devices
3. Click on a device name to select it > Click Edit
4. Update the name of the device in the "Description" field (Name field cannot be altered)
5. Click Save > This will take you back to the Device Summary List. The "Device Name" field should show the new name

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **WE HAVE A NEW MOBILE COMPUTER/MDC THAT'S NOT SYNCING WITH BOSS.**
Q: **WE KEEP SEEING AN HTTP_STATUS_CODE ERROR WHEN RUNNING BEGIN SHIFT.**
A: This error most commonly means that a new device in the field (laptop/tablet) can "see" the BOSS server, but that it hasn't been enabled yet to "talk" with it. Follow the general steps below to address this issue:
1. The agency BOSS Administrator will need to login to the BOSS UI client and Select Admin
2. Then select Devices and from there, left click on the device/computer name of that MDC to edit it
3. Once in the Edit screen, Enable the device. This will take you back to the Device List.
4. Click the name to edit the device again. Now assign users/Owners and save.
NOTE: The Select button becomes a Save button when selecting which Groups/Users should have access to login to this device
5. Once that is done, navigate to Admin > Hotlists
6. From here, click on each hotlist one at a time to distribute them to the new device being sure to Save the changes next to the Distribution field. Note again that the Select button becomes a Save button. And there's another Save button at the top left of

the edit window.
7. After this is complete, perform Begin Shift from the field unit/MDC and confirm there are no further errors. 4281

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **NEW PAGIS USER CAN'T LOGIN BUT OTHERS CAN.**
Q: **USERS CAN LOGIN TO PAGIS WITH NO CREDENTIALS AT ALL.**
A: Entry or login to the PAGIS software in the field is partially controlled by the Device settings in BOSS. The users themselves must also be properly setup with an LPCS/PAGIS password. To check the current device settings/ access, perform the following steps:
1. Login to BOSS UI (with Administrator rights)
2. Select the Admin Section
3. Select Devices and then Select the Device in question by PC name
4. Once selected click on the Edit button near the bottom
5. Locate and inspect the "Owners" Field (this is a list of users/groups that have access to login to the device)
NOTE: If this field is blank, the device is in an open configuration mode allowing admin level access simply by clicking login (any credentials would also be accepted).
6. To update the device owners, click the "Select" button next to the Owners field (notice it changes to a Save button)
7. Check which Users/Groups of Users should be able to login to PAGIS from this device
8. Click the Save button next to the field
9. And then click Save in the upper left portion of the Edit window
10. Have a previous user or Admin login to PAGIS and perform Begin Shift to sync the new data
11. A PAGIS Admin can confirm by navigating to Admin, Admin, and then Users to review the list
12. Another test would be to have the new user attempt to login

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **WHEN USERS LOGIN TO PAGIS, THEY ONLY SEE A GREY SCREEN.**
Q: **CAMERAS AREN'T SHOWING UP IN PAGIS ANYMORE.**
SEE ALSO: "THE LINK LIGHTS ON OUR ALPR COMPUTER/MDC WON'T TURN ON OR FLASH"
A: Below are some basic troubleshooting steps you'll want to follow before creating a support ticket.
1. Doublecheck the physical power switch on the black box/Processor is On. In many vehicles, there is also an in-line switch in the front of the vehicle that needs to be switched On. When the units are properly powered and on, you should see lights and hear fans running.
2. Confirm that the network adapter settings on the laptop match the proper Static IP scheme for the SX Processor in use. The older scheme is 192.200… and the newer scheme is 192.168…. NOTE: the adapter status in Windows should say "unidentified network". If it says "cable unplugged" the laptop can't "see" the SX.
3. If the power and Static IP settings are good and things still aren't working, test further by disabling the three main software related culprits. Turn off/bypass the local Windows firewall, antivirus, and VPN software one at a time.
4. If you're still not able to see the camera feed after that, you may want to use a different network cable as those can get damaged over time and then confirm that the cord is properly plugged into the ports.
5. If the network cord from the SX Processor is routed through a docking station, then it's possible the dock is preventing the traffic. You should contact the dock's manufacturer for the most recent firmware. To test for this, remove the laptop from the dock, directly connect the network cord to the laptop, and then reconfigure the network adapter settings (remove the static settings from the dock's adapter/ and assign the static IP to the laptop's NIC adapter).

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.
Q: **THE LEFT FRONT CAMERA ON OUR ALPR VEHICLE IS NO LONGER SHOWING IN PAGIS**?
Q: **HOW DO WE TROUBLESHOOT MOBILE CAMERAS**?
A: Below are the main troubleshooting steps to test the camera(s) and cable(s) on a system where only one or two cameras are no longer displaying images.
Step 1: Confirm MDC/SX communication - steps shown in section "Cameras aren't showing up in PAGIS anymore."
Step 2: Access the SX Processor – RDP or directly connect a monitor, keyboard, and mouse to the SX. Contact PIPS Support for

help with RDP if the credentials are unknown to the agency.
Step 3: Confirm camera activity – Launch Tools. Then open P6Utility or Mobile Toolkit. Check the camera feeds/function by switching the Input menu to the camera(s) in question
Step 4: Unplug and Reattach the Camera Cables – Note, the cables DO NOT TWIST. The metal locking nut on the cable slides back about a millimeter and the cable comes straight out. Do this at the SX Processor and the Camera. You may need to remove the camera from the mount in order to unplug the cable successfully (most brackets use a #3.5 Hex/Allen Wrench)
Step 5: Swap Port on SX Processor – At the SX Processor, swap the camera cables from the non-working camera to a port with a working port (Take care to note the swap so the cables get back to their original ports). If the camera outage stays at the port site, the issue is most likely the capture card on the SX Processor and will require RMA (Example: working Left cam is swapped to port of non-working Right cam and no longer functions. AND the previous non-working Right cam starts working once it's plugged into the Left cam's port). If the fault/error stays with the camera regardless of SX port, continue to Step 6.
Step 6: Physically Swap Camera Locations – Once all other items are checked, move the camera itself to a working position in order to test the cable. (Example: physically move Left cam to the Right cam position on the top of the vehicle) Connect the cable at the new position and test feed in Tools > P6Utility/Mobile Toolkit. If the camera works at the new location, the issue is most likely a bad cable. If the camera still does not work, the issue is most likely a faulty camera in need of repair/RMA.

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **WE'RE NO LONGER GETTING GPS IN PAGIS.**
Q: **WE'RE NOT SEEING GPS DATA FROM SOME OF OUR FIELD UNITS IN BOSS.**
A: Below are the basic troubleshooting steps for checking the GPS of field units:
1. Login to PAGIS (as Admin)
2. Navigate to Admin section, then click the Admin button
3. Select "System" on the left pane
4. Confirm/Set the button at top to "Default"
5. Remove any value(s) stored in the GPS Connection String field. Leave '5' in the Computer String.
6. Click the Save button to retain changes made.
7. Close PAGIS fully and relaunch and log back in to test (Note: GPS will only show with test reads/hits)
8. For versions of PAGIS 2.9 and up, test with a GPS Connection String of 6 if the blank field doesn't work. Save the changes. Log out. Close the software and then relaunch to test.

Please be advised, that some GPS issues can be caused by local or domain firewall settings, antivirus software, or any other software package monitoring/transmitting network data. To test these, disable or bypass those software options on the MDC and retest.

If these initial troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **HOW DO I INSTALL THE PAGIS SOFTWARE?**
Q: **I JUST LOADED PAGIS ON A MACHINE AND IT CRASHES WITH A .DLL ERROR WHEN I TRY TO LAUNCH IT.**
A: The most common installation of PAGIS is Client/Server or "VPRelay Mode". The .dll error is caused by the installer not being run from the HDD and/or the wrong install option being selected (Example: SupeRex instead of MDC). The best practices for the installation are below. (Note, this does not cover MDC or PAGIS configuration, only the act of installation)
1. Always copy the installer over to the HDD/Desktop of the MDC. Never run it from a thumb-drive or network share
2. Regardless of how you're logged in to Windows, right click the installer and select "run as Admin" or "run with elevated privileges"
3. Continue through the message/error about OS compatibility
4. Click next on the wizard and then be sure to select the MDC option (to use with VPRelay)
5. After that, it's next, next, next, finish the reboot is not necessary

If these steps did not resolve the issue, please feel free to enter a request for support here.

Q: **USERS ARE GETTING HITS/ALERTS ON PREVIOUSLY RECOVERED STOLEN PLATES.**
Q: **USERS AREN'T GETTING HITS FROM KNOWN ACTIVE PLATES.**

Q: **THE HOTLISTS IN PAGIS DON'T SHOW TODAY'S DATE.**
Q: **THE HOTLISTS AREN'T SYNCING WITH BEGIN/END SHIFT.** 4283
A: Whether it's from data latency or just use over time, the local file structure can get some minor corruption and will need to be refreshed. The steps below show the best practices:
1. Login to Windows with Admin rights (ability to uninstall/delete software)
2. Login to PAGIS and perform an End Shift
3. When complete without error, Logout of PAGIS and then Exit/Close the program
NOTE: If the End Shift fails or displays an error, contact Support for additional assistance.
4. If there were no errors, locate the PAGIS icon on the desktop.
5. Right click on the icon and select "Open File Location" (This should open a window where the program was installed)
6. Scroll up and locate the folder labeled "data". Double-click it to open it
7. Select and delete everything in here EXCEPT for "Attributes.db"
8. Once that's complete, Login to the PAGIS software again
9. Perform a Begin Shift. This will pull down fresh data from the server
NOTE: Once complete, the files in the data subfolder as well as the Databases section of PAGIS should be restored.

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **IS PAGIS COMPATIBLE WITH OUR NEW WINDOWS 10 LAPTOPS?**
A: Although there's a warning about compatibility during the install of PAGIS on any Windows OS after XP, it is compatible with all them. However, we have seen errors occur when agencies copy and paste folder structures from previous installations. This of course is not recommended.

Q: **THE LINK LIGHTS ON OUR ALPR COMPUTER/MDC WON'T TURN ON OR FLASH.**
Q: **OUR WINDOWS 10 MDC WAS WORKING BUT HAS STOPPED COMMUNICATING TO THE SX PROCESSOR.**
A: There are many variables with troubleshooting any network connection. And the connection from the ALPR computer to the SX Processor is no different. The following troubleshooting list highlights the most common:
1. The physical network cord is bad/damaged.
A: Test with a different cable and confirm that it is plugged in fully

2. The network adapters are not configured or have incorrect static IPs
A: Confirm the Static IP scheme in use and properly configure the network adapters

3. Local and/or Domain Firewall rules have prevented the flow of communication
A: Disable or bypass these and test again

4. VPN, Anti-Spyware, Antivirus, or other monitoring software has blocked communication
A: Disable or bypass these one at a time and test after each to find the culprit(s)

5. Docking Station Firmware can be incompatible with some newer computers or become corrupt
A: Test by running the network cord straight to the MDC and then configuring the network adapters (NOTE: It would also be a good idea to contact station manufacturer to see what the latest firmware version is and upgrade as necessary)

6. The NIC Drivers have become corrupt
A: Update the specific Networking drivers in use on the MDC through the Device Manager in Windows

7. Turn off all power saving settings of the Ethernet Adapter in the device manager
A: Uncheck "Allow the computer to turn off this device to save power"

8. Check for Windows 10 update 1709 and 1803 as this update will not allow the NIC and Cellular Aircard to run simultaneously
A: Settings > Update and Security > Windows Update > "Update History" link – if there, see the steps in the FAQ

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **AS SOON AS WE DOCK OUR MDC, WE LOSE CONNECTION TO THE WIRELESS.**
Q: **OUR WINDOWS 10 LAPTOP LOSES CONNECTION TO THE INTERNET WHEN THE NETWORK CABLE IS PLUGGED IN.**
Q: **OUR MDC HAS MICROSOFT VERSION 1709 OR 1803 AND CAN'T CONNECT TO WIFI WHEN DOCKED.**
A: Microsoft Updates (1709 and 1803) prevent the Wireless connection as soon as a Network cable is plugged into the device. This also occurs for MDCs/laptops that are docked (where the Network cable from the SX Processor is run through the docking station). As of January 2019, the steps to correct this are below.
WIN10 version 1803
1. Open Regedit
2. Expand HKEY_LOCAL_MACHINE
3. Navigate to Software > Policies > Microsoft > WcmSvc > Local
4. Right click on Local > Hover over New > Select "DWORD (32-bit)"
5. Name the new value "fMinimizeConnections"
6. Right click the on the new name > select Modify > Set value data to 1 (leave base Hex) > Click OK
7. Reboot Windows and test

WIN10 version 1709 - Microsoft fixed this with Update KB 4284822. But if you still have issues, the registry steps are below:
1. Open Regedit
2. Navigate to HKEY_LOCAL_MACHINE > Software > Policies > Microsoft > WcmSvc > Local
3. Right click on Local > Hover over New > Select "DWORD (32-bit)"
4. Name the new value "fMinimizeConnections"
5. Right click the on the new name > select Modify > Set value data to 0 (leave base Hex) > Click OK
6. Then Navigate to HKEY_LOCAL_MACHINE\Software\Microsoft\Wcmsvc
7. Right click on Wcmsvc > Hover over New > Select DWORD (32-bit)
8. Name the value "IgnoreNonRoutableEthernet"
9. Right click on the new value > Modify > Set value data to 1 (leave base in Hex) > OK
10. Reboot Win10 and test

If the steps above did not resolve the issue, you may need to address this with Microsoft. Their support site is here.

APPENDIX D: XML DATASTREAM

Overview

The XML Datastream can be used to push the current data from a running PAGIS system to another application. The data available via the Datastream includes reads, hits and current images. The connection to the Datastream is a TCP/IP socket (default port: 10100). When initially connecting, an XML packet is passed to the PAGIS Software to subscribe to the Datastream. The data connection is configured as "push only" and doesn't allow receipt of additional external data. The current image stream is pushed periodically whereas reads and hits are passed as close to real-time as possible.

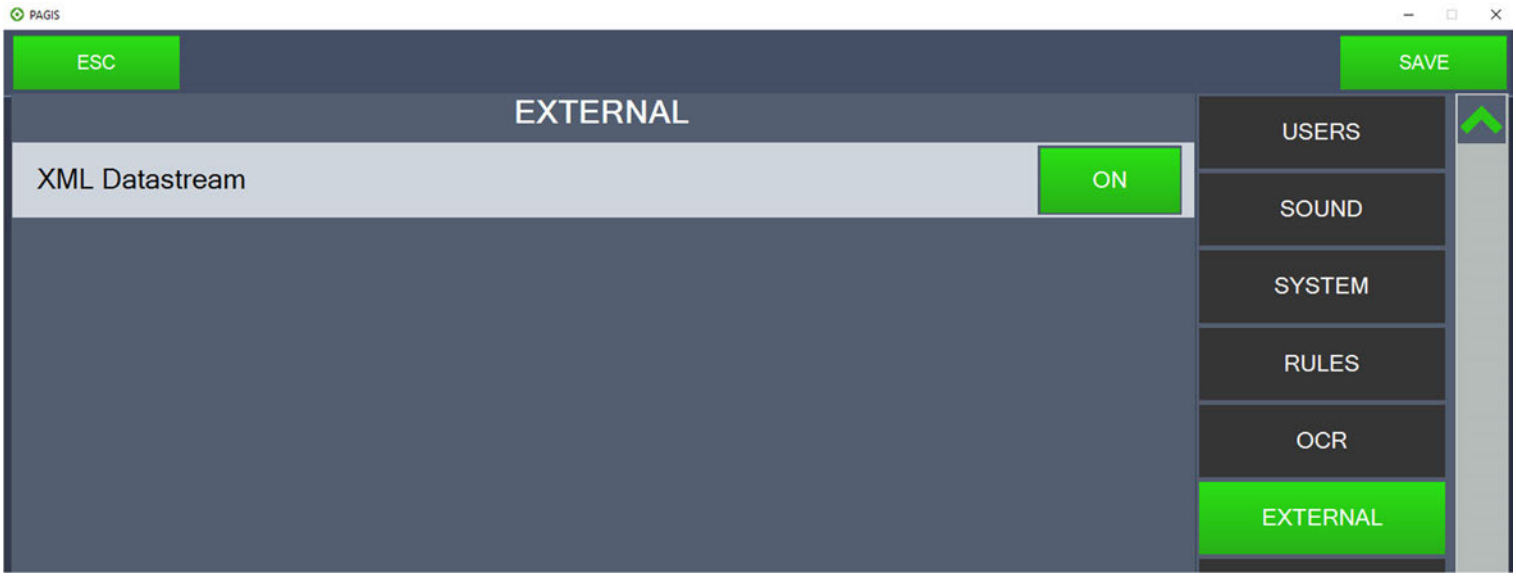
PAGIS Port

By default, the PAGIS.exe.config file has a key for defining the port number for the XML Datastream. The default value is 10100. This setting does not need to be changed unless the default port is unavailable.
The key has the following format:

```
<!--XML Datastream Settings/-->
<add key="XML.Datastream.Port" value="10100"/>
```

PAGIS Admin Setting

To utilize this feature, the XML Datastream needs to be enabled in PAGIS. To do this, navigate to Settings > Admin > External. The "XML Datastream" option should be turned on as shown in the image below and then saved.



XML Subscription

When initially connecting to PAGIS, the Datastream subscriber will receive only a Heartbeat XML packet (see example below) until PAGIS receives a subscription packet from the subscriber. The properly formed subscription packet defines the specific data that the subscriber wishes to receive.

Heartbeat XML Packet

The Heartbeat Packet is sent once every 10 seconds. The purpose of the heartbeat packet is to let the subscriber know that the communications channel is working between PAGIS and the subscriber. The timestamp is sent in the format of "`YYYY-MM-DDThh:mm:ss`".

Sample of the Subscription XML Packet

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-heartbeat>
  <timestamp>2011-10-13T09:41:56Z</timestamp>
</pips-datastream-heartbeat>
```

Subscription XML Packet

A properly formed subscription packet will have all of the data being requested from PAGIS. To receive a specific datatype, a tag must be added to the subscription to define the desired datatype. The valid entries for datatype are: Reads, Hits, and CurrentImage. 4286

- Subscribing to Reads will send all plates that are detected by PAGIS regardless of whether or not it has an associated hit.
- Subscribing to Hits will send all plates detected by PAGIS that are on a hotlist and the associated Read data for that Hit.
- Subscribing to the CurrentImage Datastream offers two additional attributes that may be passed as well. The "camera" attribute can be set to determine which camera the image is coming from. If no value is passed for "camera" the value defaults to zero. The "milliseconds" attribute determines how long the system waits between sending the current image. The default value for milliseconds is 1000. If a value of zero is sent, the system will send a single snapshot.

Sample of the Subscription XML Packet

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-subscription>
  <datatype>Reads</datatype>
  <datatype>Hits</datatype>
  <datatype>HitTrigger</datatype>
  <datatype camera="0" milliseconds="1000">CurrentImage</datatype>
</pips-datastream-subscription>
```

HitTrigger

The HitTrigger packet is used to alert other systems that a hit has occurred on the PAGIS system. The packet is greatly simplified from the Reads/Hits XML packet and only contains the license plate text, timestamp and a description of the hit. The description will contain the name of the hotlist that originated the hit and may be used to send additional information.

Sample of the HitTrigger XML Packet

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-hittrigger>
  <timestamp>2011-10-13T09:41:56Z</timestamp>
  <vrm>SBX989</vrm>
  <hotList name='Alpha'>
    <field1><![CDATA[This is Alpha Field 1]]></field1>
    <field2><![CDATA[This is Alpha Field 2]]></field2>
    <field3><![CDATA[This is Alpha Field 3]]></field3>
    <field4><![CDATA[This is Alpha Field 4]]></field4>
    <field5><![CDATA[This is Alpha Field 5]]></field5>
  </hotList>
</pips-datastream-hittrigger>
```

Reads/Hits XML Packet

The Reads/Hits packet contains information about the plate that was detected. This information includes:

- Source – The device that detected the plate
- Camera – The camera on the device that detected the plate
- Read – The Information about the plate that was captured
- VRM – The plate translated to text
- Timestamp – When the read occurred
- GPS – The location coordinates where the read took place
- ImagesPatch – The image of plate in infrared (IR)
- Overview – The image of scene/car in Color
- Hits – The associated hotlist(s) data

Sample of the Current Image XML Packet

NOTE: The Current/Live Image XML Packet contains the current image from the camera. It is sent every 5 seconds.

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-currentimage>
  <timestamp>2011-10-13T09:41:56</timestamp>
  <data>(Image data here)</data>
</pips-datastream-currentimage>
```

Sample Read with Hits XML

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-reads>
  <reads>
    <source>
      <name>PAGIS_90210</name>
      <software name="PAGIS" version="2.6.8" />
      <camera name="Front Left">
        <read>
          <state>TN</state>
          <vrm>SBX989</vrm>
          <confidence>97.5</confidence>
          <timestamp>2011-09-30T09:30:10Z</timestamp>
          <username><![CDATA[shronski]]></username>
          <gps>
            <latitude>-87.4567</latitude>
            <longitude>98.7654</longitude>
          </gps>
          <images>
            <image name='Patch'>
              <type>IR</type>
              <data>

<![CDATA[/9j/4AAQSkZJRgABAQAAAQABA.....................................................................
.....................................................................................................
..... /9k=]]>
              </data>
            </image>
            <image name='Overview'>
              <type>Color</type>
              <data>

<![CDATA[/9j/4AAQSkZJRgABAQAAAQABAAD..................................................................
.....................................................................................................
.... //2Q==]]>
              </data>
            </image>
          </images>
          <misread>0</misread>
          <manual>0</manual>
          <hits>
            <hotList name='Alpha'>
              <field1><![CDATA[This is Alpha Field 1]]></field1>
              <field2><![CDATA[This is Alpha Field 2]]></field2>
              <field3><![CDATA[This is Alpha Field 3]]></field3>
              <field4><![CDATA[This is Alpha Field 4]]></field4>
              <field5><![CDATA[This is Alpha Field 5]]></field5>
            </hotList>
            <hotList name='Beta'>
              <field1><![CDATA[This is Beta Field 1]]></field1>
              <field2><![CDATA[This is Beta Field 2]]></field2>
              <field3><![CDATA[This is Beta Field 3]]></field3>
              <field4><![CDATA[This is Beta Field 4]]></field4>
              <field5><![CDATA[This is Beta Field 5]]></field5>
            </hotList>
          </hits>
        </read>
      </camera>
    </source>
  </reads>
</pips-datastream-reads>
```



PIPS TECHNOLOGY™

DETECTION INNOVATION



PAGIS User's Manual

Version 2.14

Updated 3/30/2020

NEOLOGY MOBILITY TECHNOLOGIES

Table of Contents

Table of Contents 2

NOTICES 3

Technical Support 3

Design Changes 3

Trademarks 3

Copyright 3

Version 3

INTRODUCTION 4

1.1 Dual Lens Color and Infrared Camera 4

1.1.1 Available Products 4

1.2 Using This Manual 5

SCREEN REFERENCE 6

2.1 The PAGIS Software Login Screen 6

2.1.1 Logging on with the Default Administrative Account 6

2.2 Main Screen - Live View 7

2.2.1 Getting Started in PAGIS 7

2.3 The PAGIS Navigation Buttons 8

2.3.1 Camera Control Buttons 8

2.3.2 GPS Indicators 9

2.3.3 Camera Firmware Update (Restricted Users) 9

2.3.4 Day/Night Mode 9

2.4 Begin Shift 10

2.4.1 Sync via USB Thumb drive (or Local Source) 10

2.4.2 Sync via Wireless Network 10

2.4.3 PAGIS Auto-Sync Settings 10

2.4.4 Begin Shift – Additional Information 10

2.5 End Shift 10

2.5.1 Sync to BOSS 10

2.6 Cam Mode Button 11

2.6.1 Camera Modes 11

2.7 Taking a Picture 11

2.8 Search Entry Screen 12

2.8.1 Searching Synchronized Hotlists for License Plates 12

2.8.2 Searching Locally Stored Reads and Hits 12

2.8.2.1 Searching for a Match 13

2.8.3 Wild Card Symbols 13

2.8.4 Manually Adding a Plate to PAGIS 14

2.8.4.1 ADD VLP Query 14

2.8.4.2 ADD VRM Report Screen 14

2.9 The Review Screen 15

2.9.1 Summary Review Section 15

2.9.2 Review Navigation Buttons 15

2.9.3 Reads 16

2.9.3.1 Reads Result Screen Navigation Buttons 16

2.9.3.2 Interactive Buttons – Reads Screen 16

2.9.4 Hits 17

2.9.4.1 Hit Screen Attributes 17

2.9.4.2 Hit Screen Function Buttons 18

2.9.4.3 Interactive Buttons – Hits Screen 18

2.9.4.4 Set Disposition – Additional Detail 18

2.9.4.5 Add Intel – Additional Detail 19

2.9.5 Misreads 19

2.9.5.1 Marking a Record as a Misread: 20

2.9.6 Audits 21

2.9.7 Targets 21

2.9.7.1 The Targets Screen 22

2.9.7.2 Targets Screen Navigation Buttons 22

2.9.8 Databases 23

2.9.8.1 Databases Screen Functions 23

2.9.8.2 Databases Screen Navigation Buttons 23

2.9.8.3 Databases Edit- “Manual Reports” 24

TROUBLESHOOTING TIPS 25

3.1 Troubleshooting & Tips 25

3.1.1 PAGIS with NetMotion VPN 25

3.1.2 Cisco VPN Client: 25

3.1.3 Microsoft .NET 3.5 Installation 25

3.1.4 Firewall Settings for Client-Server Installations 25

APPENDIX A: THE GLOSSARY 26

APPENDIX B: PAGIS SOFTWARE DATABASE FILE 27

APPENDIX C: FAQ 29

NOTICES

The information within this manual is authorized for distribution to customers, authorized service center personnel, and distributors of Neology. Every effort has been made to supply correct information. However, Neology assumes neither responsibility for its use, nor for any infringements of patents or other rights of third parties, which may result from its use. No license is granted by the manufacturer under any patent or patent rights. Neology reserves the right to modify and update the equipment at any time without prior notice. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means to a third party without the prior consent of the copyright holder. The manufacturer's warranty will be invalidated if untrained personnel operate the equipment or if any attempt is made to service the equipment by unauthorized personnel.

This manual contains confidential and proprietary information and should not be redistributed except as needed for proper use and maintenance of the agency's Mobile ALPR system.

Technical Support

Service of this equipment by replacement of parts, on-site repair, routine maintenance inspection, and scheduled remote support session is available. Please contact PIPS Technology's ALPR Technical Support.
Phone: 833-PIPS-LPR (833-747-7577), Option 2
Support Team Email: Support@PIPSTechnology.com
For Customers in Europe, Middle East and Africa: Support@PIPSTechnology.co.uk
Web: www.pipstechnology.com
Fax: 858-391-0264
Corporate Office: 13520 Evening Creek Drive Suite 460. San Diego, CA 92128

Design Changes

Neology reserves the right to change the design of any product from time to time without notice and with no obligation to make corresponding changes in products previously manufactured.

Trademarks

PIPS Technology™ is a trademark of Neology Inc., and either registered or pending registrations in several jurisdictions. Windows, Windows 7, Windows 8, Window 10, and .NET are all trademarks of the Microsoft Corporation. Other trademarks and registered trademarks are the property of their respective owners.

Copyright

The Neology / PIPS Technology PAGIS Software is copyright of Neology. All rights reserved. This product contains confidential and trade secret information of Neology and is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portions of it, may result in civil and criminal penalties.

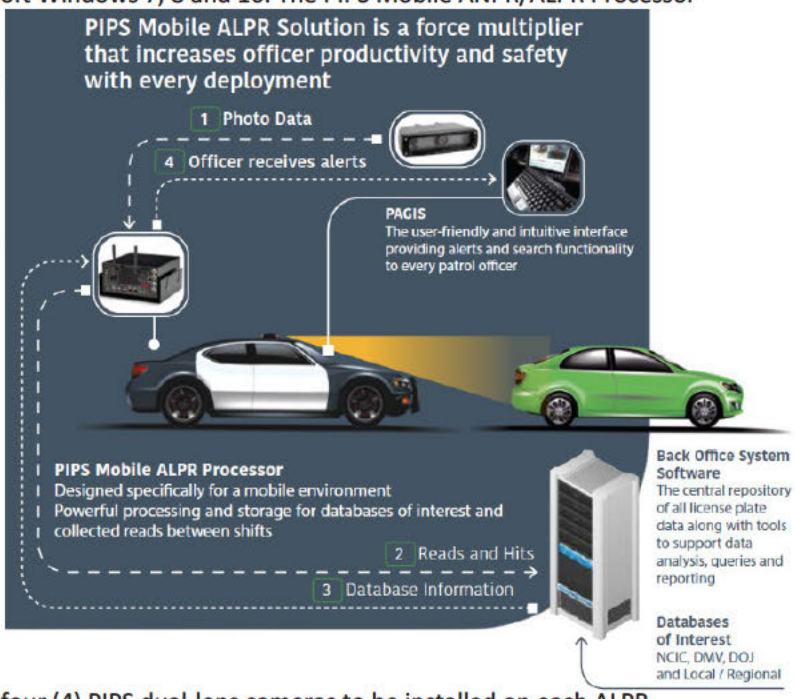
Version

This manual demonstrates the attributes of the Neology / PIPS Technology PAGIS Software Version 2.14 and was last updated in March 2020.

INTRODUCTION

PIPS Technology's Automated License Plate Recognition (ALPR) software solution called PAGIS utilizes dual-channel, dual-lens, cameras to "read" plates. Our software is optimized to run on the Mobile Processor itself or in conjunction with a mobile data computer (MDC). Our mobile software is compatible with Microsoft Windows 7, 8 and 10. The PIPS Mobile ANPR/ALPR Processor comes equipped with Microsoft Windows 7 Embedded.

The PAGIS Software processes the infrared plate image provided by any of the cameras and then interprets the plate number through Optical Character Recognition (OCR) via the mobile processor. The PAGIS application then searches for any matches of the plate with those listed in the databases, or "hotlists," distributed from the PIPS Back Office System Software (BOSS) or other external sources.



WARNING: To reduce the risks associated with impact, which if not avoided, could result in serious injury or death: Do Not interact with the ALPR system while driving in hazardous situations. The PIPS mobile camera series and License Plate Capture Software are not intended for use in hazardous environments, so that the User and/or others are not put at risk for personal injury and/or property damage.

1.1 Dual Lens Color and Infrared Camera

The PIPS Technology Mobile ALPR System allows for a maximum of four (4) PIPS dual-lens cameras to be installed on each ALPR vehicle provided that the vehicle supports the additional mounting equipment.

Each dual-lens mobile camera uses visible light to take color overview pictures of the vehicle and uses infrared (IR) illumination to capture the license plate's alphanumeric characters. IR illumination offers the best capture performance of reflective license plate characters for the following reasons:

- State issued license plates are designed to be highly reflective to IR light.
- Cameras using IR capture technology do not depend on the presence of visible light to function.
- Cameras using IR capture technology are not negatively impacted by the effects of headlights, solar glare, or total darkness.
- IR light penetrates rain and fog better than visible light.
- Due to these attributes, the system can be used 24 hours a day, seven days a week.

1.1.1 Available Products

Additional information about this and other PIPS Technology applications, cameras, and solutions are available on the PIPS web site: http://www.pipstechnology.com

1.2 Using This Manual

4292

The section overview of this software manual are as follows:

Section 1: The Introduction and Basics

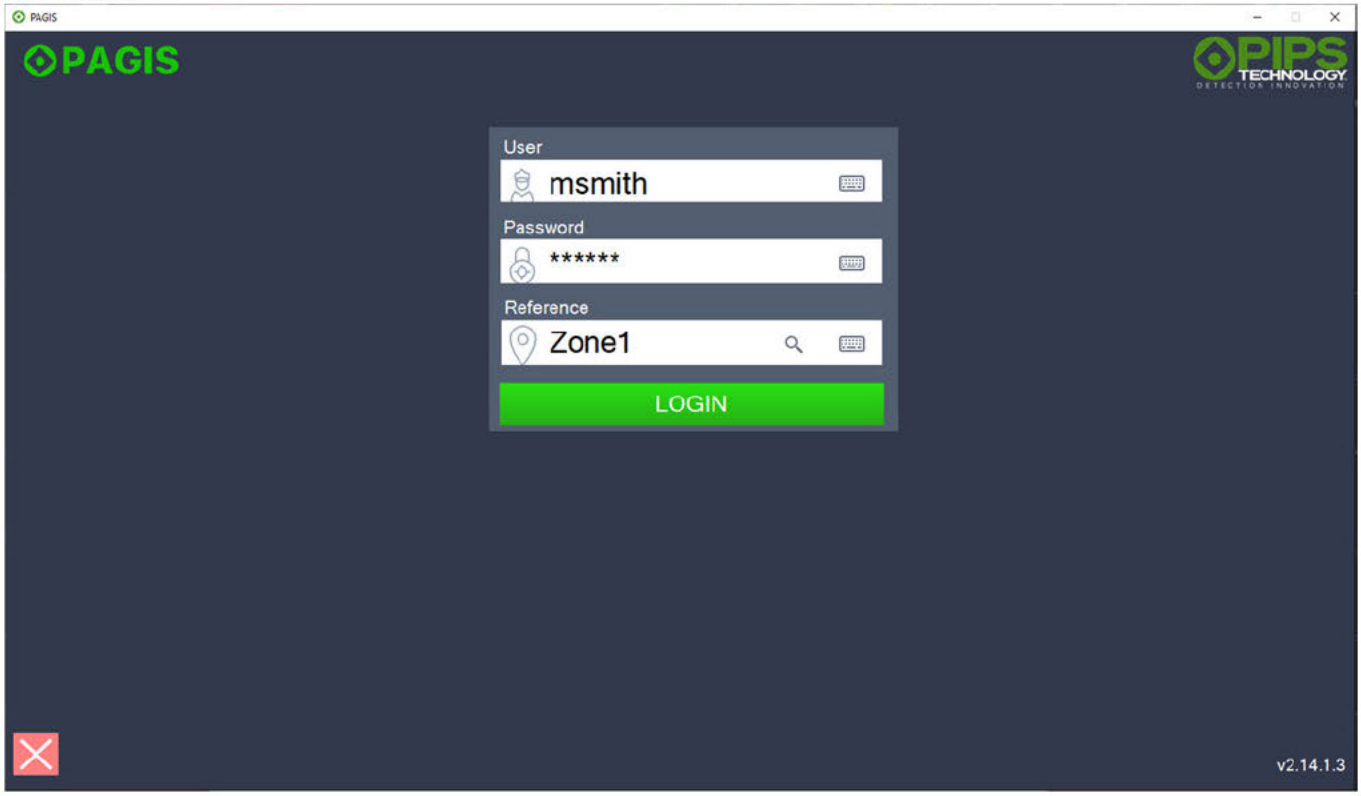
Section 2: PAGIS User's Section: Explains screen function and User Operations in the PAGIS Software

Section 3: Troubleshooting Tips

Appendices: Additional features and details

SCREEN REFERENCE

This section guides the user through the PAGIS Software screens and the available options. Screens are grouped according to function. When a button is grayed out or missing, the option is not available, or no information has been accrued to activate it.



2.1 The PAGIS Software Login Screen

The PAGIS Software allows users with various access privileges to use the same MDC. For users with touch screen monitors, the Keypad button immediately to the right of any text box gives the user access to an on-screen keyboard for data entry.

User Field: The alphanumeric string assigned to identify the user. Usernames are not case sensitive.
Password Field: Password of the assigned user logging in. Passwords are case sensitive.
Reference Field: This is an optional field utilized to fit a number of use cases. A user can manually enter a reference at logon, leave the field blank, or select list of unique tags that will be associated with all data captured while logged in. If the Administrator has configured a default reference tags, that information will be displayed automatically. Otherwise, it will be blank.
Login Button: Submits the username and password to attempt a login.
Exit Button: By clicking the X icon in the lower left-hand corner, the user can exit/close the PAGIS Software.

2.1.1 Logging on with the Default Administrative Account

The PAGIS Software includes a default administrative account that can be used for the initial configuration. To do so, simply click the **Login** button with the User and Password fields blank.

NOTE: System Administrators are strongly encouraged to configure users for PAGIS just before, or soon after the installation and setup. PAGIS users accounts are created and maintained in BOSS. Once Users are established by the BOSS System Administrator, the default user account is automatically disabled. Best practices are to be certain at least one User account has administrative privileges.

2.2 Main Screen - Live View

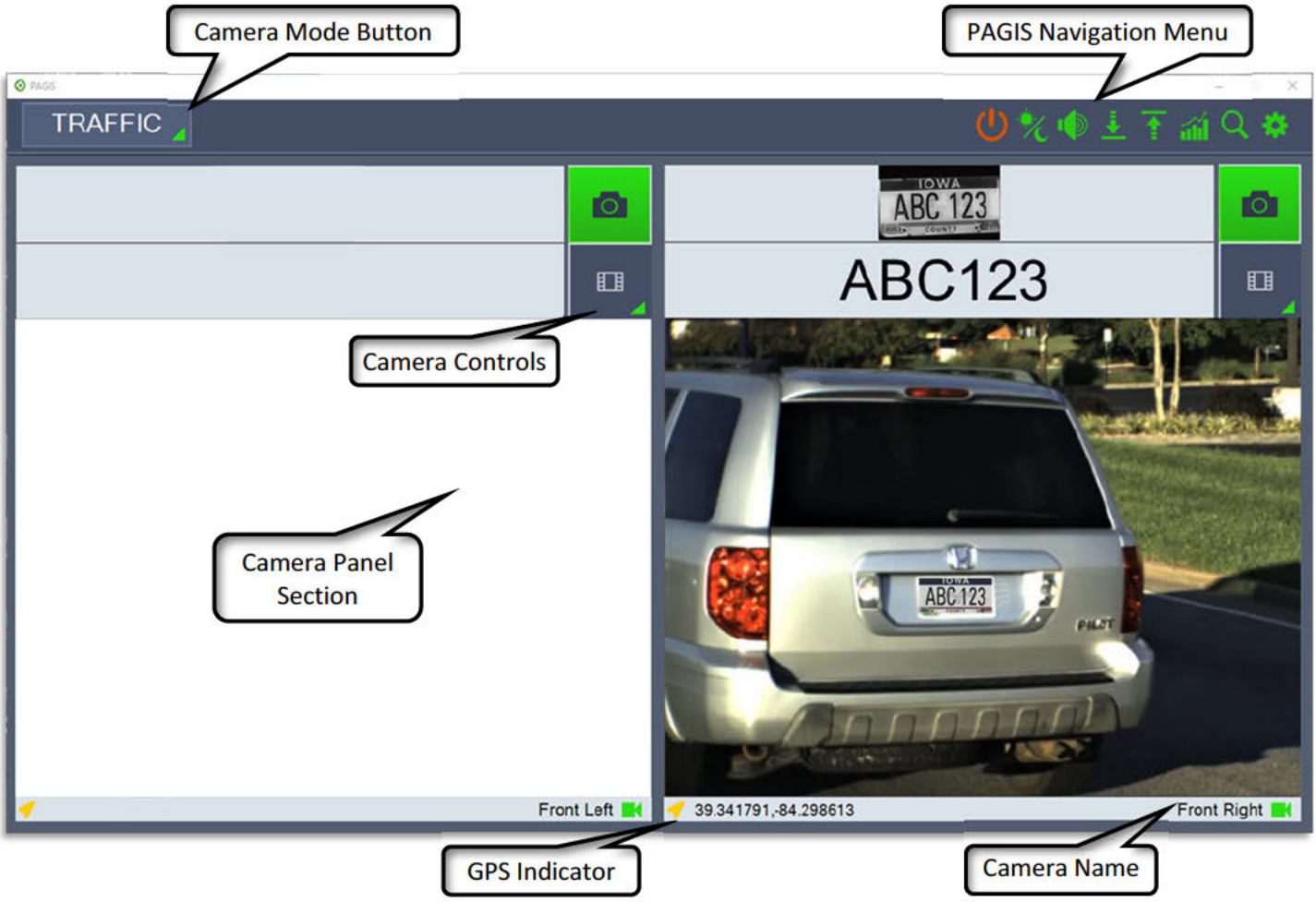
Upon a successful login, the user will see the Main screen (Live View). This is the default view and starting place of all PAGIS Software features. (NOTE: Access to features is based on user group rights established in BOSS.)

The Main Screen is also the place users will monitor read images and ALPR "hits". At the initial startup of the system it is normal to see only a blank/grey screen for a few seconds. Once a connection has been established with the mobile cameras, white boxes will be displayed showing the live-feed camera panels. At this point, the system is ready to capture reads/plates.

2.2.1 Getting Started in PAGIS

By default, PAGIS loads into a static view. This means live video will not automatically appear in the camera panels (white boxes) until a plate has be captured or the user selects one of the live feed options.

Once a plate is "seen" by a camera assigned to the current viewing mode (Traffic vs Parking), it will display the captured information in the corresponding camera panel. Each plate capture is also accompanied by a short "Beep" to audibly alert the user a read has taken place. (NOTE: If the user is in the Traffic Mode at the time a parking camera reads a plate, there will be a sound effect, but no plate image will be displayed on screen unless that plate is on a synchronized Hotlist or until the user switches to Parking Mode.)



2.3 The PAGIS Navigation Buttons

4295

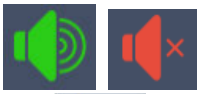
This section provides a quick reference guide to the available navigation buttons of the Live View screen.



The Camera Mode button is located in the upper left corner and is used to switch between the configured camera modes. Once configured, the name will change to a selected mode. The default values are “ALL”, “Traffic” and “Parking”.



The Logoff button is located in the upper right of the window. When selected, the user will be logged out of PAGIS and return to the login screen.



The Sound button is located to the right of the Logoff button. When selected, this button with toggle the PAGIS system sounds On and Off.



Day/Nite mode switches PAGIS between day & night mode screen skins.



The Begin Shift Synchronization button is located to the right of the Sound button. When selected, this will reach out to the BOSS server to download users, hotlists, and other system settings.



The End Shift Synchronization button is located to the right of the Begin Shift Button. When selected, this will upload any previously unsent reads, images, and audits to the BOSS server.



The Statistics/Review button is located to the right of the End Shift Button. When selected the user is able to review Databases/Hotlists, Reads, Targets, and other PAGIS information.



The Search button is located to the right of the Review Button. When selected the user can search his/her reads as well as manually add a license plate to a temporary hotlist.



The Admin/Settings button is located in the upper right corner of the screen. This button is only viewable to Admin level users and allows for system configuration changes and setup.



Firmware update icon will atomically appear when PAGIS detects a new firmware is available for the P720 mobile cameras. All user types are notified, but only Admins can apply the update.

2.3.1 Camera Control Buttons

The dual-lens cameras can capture both color and an infrared image. Formerly, there were a total of three buttons that allowed the user to view the IR and color feed as well as capture a picture directly from PAGIS. Now there is a toggle button to switch between color and IR views and a separate button to take a picture. These buttons are displayed on the main Live Screen as shown below:



The Camera View Selector button: This is the default state at login showing the Static View. (**NOTE**: PAGIS does not automatically display a life feed.)



Color View: by clicking on the Camera View Selector button once, the user will switch to the Color View Mode. This displays the current view of the color camera and will time out after 60 seconds.



IR View: by clicking on the Camera View Selector button twice, the user will switch to the Infrared (IR) View Mode. This displays the current view of the IR camera and will time out after 60 seconds.



The Take Pic button: Just above the Camera View Selector button is the “Take Pic” button. This button allows the user to quickly take a picture from the camera currently viewed.

2.3.2 GPS Indicators

4296

GPS is stamped on each read and hit as capture events take place by the system. The signal strength and location indicators are located underneath the camera panels at the bottom of the Live Screen.

39.341788,-84.298518 Shows an example of the Location Indicator displaying the Lat/Long on the most recent read

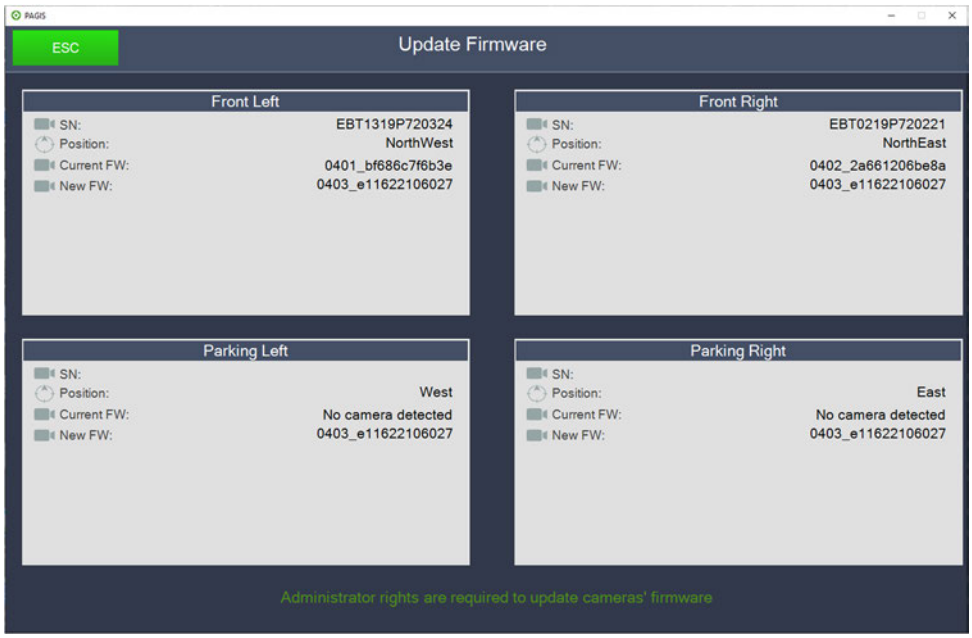
A green or yellow indicator shows a strong or medium strength GPS lock.

A red indicator shows there is no available GPS information.

2.3.3 Camera Firmware Update (Restricted Users)

Camera firmware update provides a means for PIPS to update the camera software to enhance and or correct camera performance. The frimware icon will only apper when update is avialable.

- The firmware update process only updates camera that are attached and function on the mobile processor.
- Restricted PAGIS users are only notified and displayed update information, only a PAGIS administrator can apply the FW update.

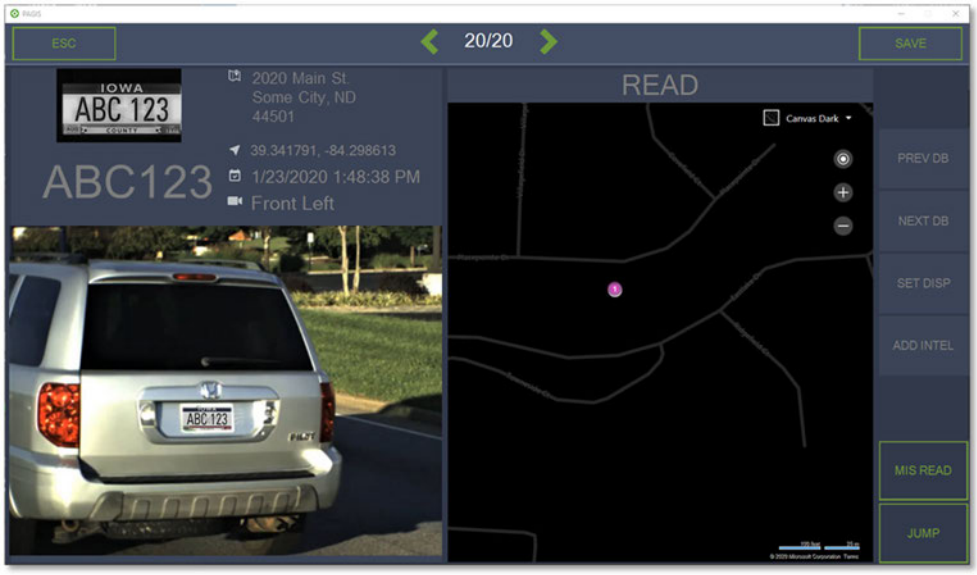


Firmware Updater Window List.

- Title “Camera Name”.
- Camera serial number.
- Position.
- Current FW version.
- New FW version available.

2.3.4 Day/Night Mode

Day/Night mode changes PAGIS user interface skins to a darker appearance to reduce illuminating the vehicle interior.



2.4 Begin Shift

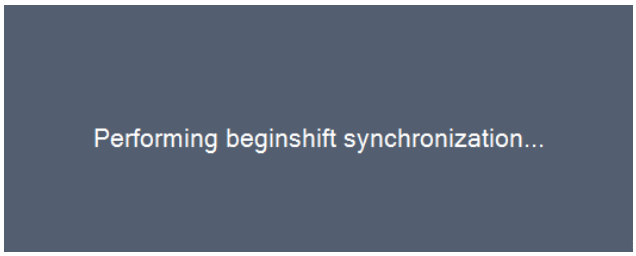
Begin Shift is thought of as the first step for all PAGIS users. From the Live View Screen, the PAGIS user must click the Begin Shift button twice. Once to select the function and once more to launch the Sync. With most agencies, this action utilizes a wireless network to import all the necessary data used during a shift (Hotlists, Dispositions, and Targets) directly from the BOSS Server. However, agencies can also configure their systems to perform this function via Thumb drive or a local source file.

2.4.1 Sync via USB Thumb drive (or Local Source)

Depending on the agency network, some alter the default PAGIS/BOSS configuration mode to use a USB Thumb drive or locally stored file on the MDC/Laptop instead of the wireless Sync. In order to synchronize effectively, the user must first confirm he/she has access to the source location before initiating Begin Shift. **NOTE**: All synchronizations using this method must be performed manually. To learn more about this process, refer to the "Client Tools" section of the BOSS Manual.

2.4.2 Sync via Wireless Network

Synchronizations over a wireless network provide the agency with additional automated features. Best practices recommend the user manually launch Begin Shift from the Live View Screen at the beginning of every patrol shift. However, it is possible for users to allow PAGIS to synchronize via its auto-sync settings. When a manual Begin Shift is launched, the Main View Screen removes the camera feeds and displays a status window of the Sync process. Once the Begin Shift operation is complete, PAGIS will return to the normal Main View Screen.





2.4.3 PAGIS Auto-Sync Settings

PAGIS auto-sync settings are best thought of as how PAGIS receives additional updates and maintains the downloaded ALPR data throughout the entire patrol shift. This prevents the need for the officer to manually perform Begin Shift functions multiple times a day. The auto-sync occurs every 30 seconds and receives data in small batches. The batches are not to exceed 1MB in size for every minute of download. In addition to receiving data, the auto-sync function also uploads a copy of data collected by PAGIS and sends it to BOSS for reporting/processing.

2.4.4 Begin Shift – Additional Information

By default, the synchronizations in PAGIS receive only what has been changed to the ALPR data since the last Sync. Meaning, if some plates have been removed from a Hotlist and others have been added, the system will only transfer that data instead of downloading the entire Hotlist each time the Begin Shift is launched. This helps to reduce the amount of data transferred over the agency's network. **NOTE**: Begin and End Shift synchronization, as well as all auto-sync features, are dependent upon stable communication to the BOSS server via an active data connection.

2.5 End Shift

End Shift in PAGIS is the process in which all the collected ALPR data (Reads, Hits, and Images) from the recent shift is uploaded to the BOSS server and cleared from the local cache. As with Begin Shift, the agency has two options. They can choose to Sync via USB Thumb drive or via wireless connection. Best practices recommend users perform an End Shift Sync at the end of every patrol.

2.5.1 Sync to BOSS

At the end of every shift, the accrued ALPR data should be exported to BOSS. Just like with Begin Shift, the user must click the button twice to launch it (once to select it and once more to execute the Sync). During the Sync, PAGIS uploads any Reads, Hits, and Images not already synchronized to BOSS and purges these items from the local cache on the MDC's hard drive. Completing an End Shift also removes any VLP entries manually added to PAGIS during the shift.

2.6 Cam Mode Button

Clicking the Cam Mode button in the upper left corner of the Live View Screen allows the user to cycle through the different camera modes configured by the PAGIS Administrator. Changing the camera mode changes which cameras are displayed on the Main Screen.

2.6.1 Camera Modes

By default, PAGIS provides "Parking" and "Traffic" as the two configuration modes. Users often switch these modes to suit their current use-case. For example, an officer in a parking lot will often switch the mode to "Parking" so s/he can see the parking cameras on the Live View Screen. They can then switch back to "Traffic" when monitoring city streets.

2.7 Taking a Picture

The PAGIS software has ability to quickly take a picture from one of the currently displayed ALPR cameras on the Live Screen. The user only needs to click on the Take Pic button.



To Take a Picture:

1. From the Live View Screen, press the Take Pic button from the desired camera
2. The image taken will be displayed
3. Enter a description of the picture in the text field at the bottom of the screen
4. Press Save to save the picture or Escape to cancel. Either action will return you to Live View.

NOTE: The picture will Not be saved if a description/note is not entered in the text box.

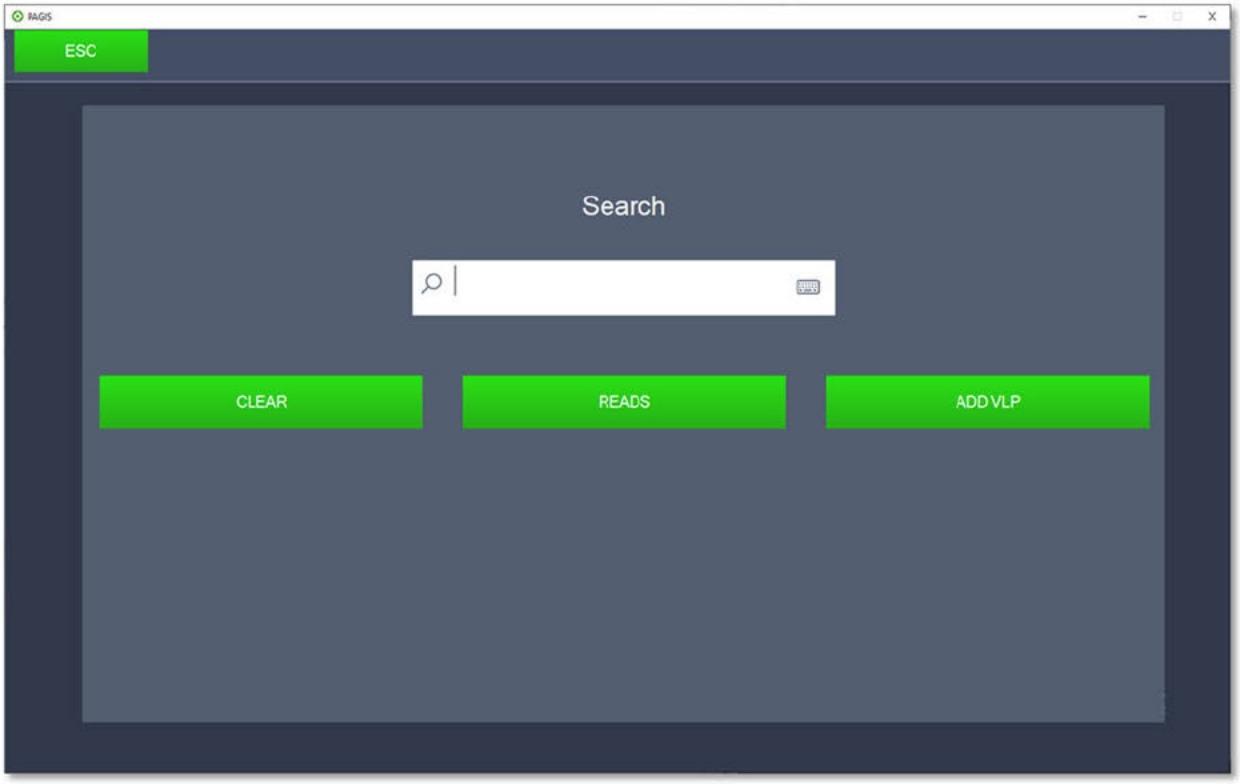
To View the Saved Images:

1. Navigate to the Review menu in PAGIS
2. Select Audits
3. The user will be able to see a thumbnail of the image and the saved text/note
4. In order to review the saved images at a later time, the user will need to run the Audit Report from BOSS.

2.8 Search Entry Screen

4299

Pressing the Search button icon from the Live View screen or SEARCH from the Databases window allows the user to search all manually entered plates as well as all BOSS synchronized databases (Hotlists) for license plate and target information. Users can also search all locally stored reads/images accrued since the last End Shift by clicking the Reads button instead of pressing the Enter key.



2.8.1 Searching Synchronized Hotlists for License Plates

By entering a vehicle license plate number (VLP) and pressing the Enter key or the ADD VLP button, the user can quickly search all the stored plate information locally collected as well as the information from all synchronized hotlists distributed from the BOSS server. **NOTE**: Hotlists can only be searched by entering complete VLPs. Wildcards and partial plate numbers will not return results.

Search Box: The text field used to enter the desired plate search via alphanumeric characters and/or wild card symbols.

Clear Button: Clears the contents of the search box.

Driver's License Info: The search field can also check the Hotlists for any DL information stored (Not available all countries).

Reads Button: This button searches for a match from all the reads/hits locally stored on the MDC/Laptop.

ADD VLP: Searches all locally stored hotlists for the plate and if there's no match, allows the user to add the plate to the "Manual Reports" alert list for use in the field. **NOTE**: All manual entries are cleared with each End Shift

ESC: The Escape button allows the user to exit to the Main/ Live View screen.

2.8.2 Searching Locally Stored Reads and Hits

As mentioned previously, this search function allows users to find reads and hits directly from their recent patrols using the search field and the Reads button. These searches pull only the reads and hits locally gathered/stored since the last time the user completed an End Shift. **NOTE**: The search results are specific to each Windows User Profile and do NOT pull images from the BOSS server.

2.8.2.1 Searching for a Match

4300

- From the Search field, users may enter a plate (or partial plate with wildcards) and then click the **READS** button.
- Results are displayed with the data gathered at the time the read was taken (See example below).
- Each result should display the infrared (IR) image of the plate as well as the color overlay of the vehicle for review.
- Each result shows the GPS data, Closest address point, Time and Date, and the Camera that read the plate.
- If there are multiple results, the user can cycle through them by clicking the left and right navigation arrows.



2.8.3 Wild Card Symbols

The use of wild card symbols in the Search box allows greater flexibility for the user, but may return a larger set of results.

- Wild card searches performed using the asterisk (*) designates an unknown number of characters.
- Wild card searches performed using the underscore (_) indicates a single missing or unknown character.
- Searches can be performed using one, both or no wild card symbols.

Example: The officer received an alert from Dispatch looking for a vehicle plate containing the letter J and the number 8 separated by one character. Because the officer doesn't know how many characters there are before or after the J and 8, he enters *J_8* in the search box to review all possible matches of J and 8 separated by only one digit.

2.8.4 Manually Adding a Plate to PAGIS

PAGIS allows users to manually add a plate of interest directly into the software as needed. Once saved, these entries are stored as part of the Manual Reports alert list and work just like any other Hotlist synchronized from the BOSS server.
NOTE: These additions are designed to be temporary and are cleared from the software with each End Shift.

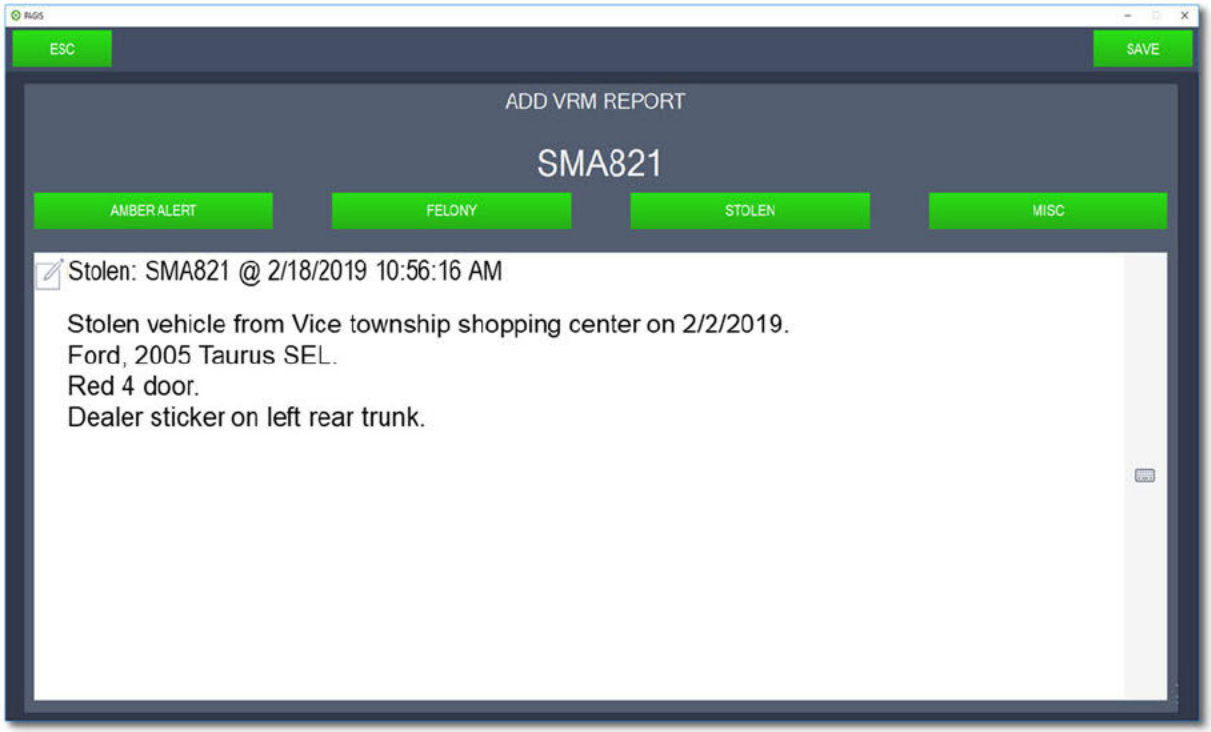
2.8.4.1 ADD VLP Query

Before an entry is added to the Manual Reports Hotlist in PAGIS, the software searches all stored databases for a match. If a match occurs, a message will display under the search box showing which Hotlist(s) it has been found in. If the VLP query does not return a match, the "ADD VRM REPORT" screen appears.



2.8.4.2 ADD VRM Report Screen

If the desired plate does not already reside in another Hotlist, the ADD VRM Report Screen becomes accessible to the user.



1. From the Search Entry Screen, enter the desired plate to add.
2. Click the ADD VLP button. If no match is found on any other hotlist, the "Add VRM Report" screen will appear.
3. Click to select the applicable alert type (AMBER ALERT , FELONY , STOLEN , or MISC)
4. Either leave the default information or add additional detail.
5. Click Save at the top right to add the plate to the Manual Entries Hotlist

2.9 The Review Screen

4302

PAGIS allows users to review all locally stored data from one easy location. Clicking the Review icon from the Main Screen launches Review. This screen is divided into the Summary View Chart and sub-section navigation buttons to the right.



2.9.1 Summary Review Section

The Summary View Chart is divided into five categories and allows a user to review the information collected during their shift at a glance.

Total Reads: Shows the total number of Reads/Hits synced to BOSS and the total number of reads captured during the shift.
Reads: Shows the total number of reads synced to BOSS and the total number of reads captured during the shift.
Hits: Shows the total number of hits synced to BOSS and the total number captured during the shift.
Misreads: Shows the total number of reads marked as a "misread" synced to BOSS and the total marked during the shift.
Audits: Shows the total number of audits synced to BOSS and the total number of audits during the shift.
Targets: Shows only the number of targets downloaded from BOSS.
(NOTE: The Sync value will always be zero for customers using Disk Sync mode/Client Tools.)

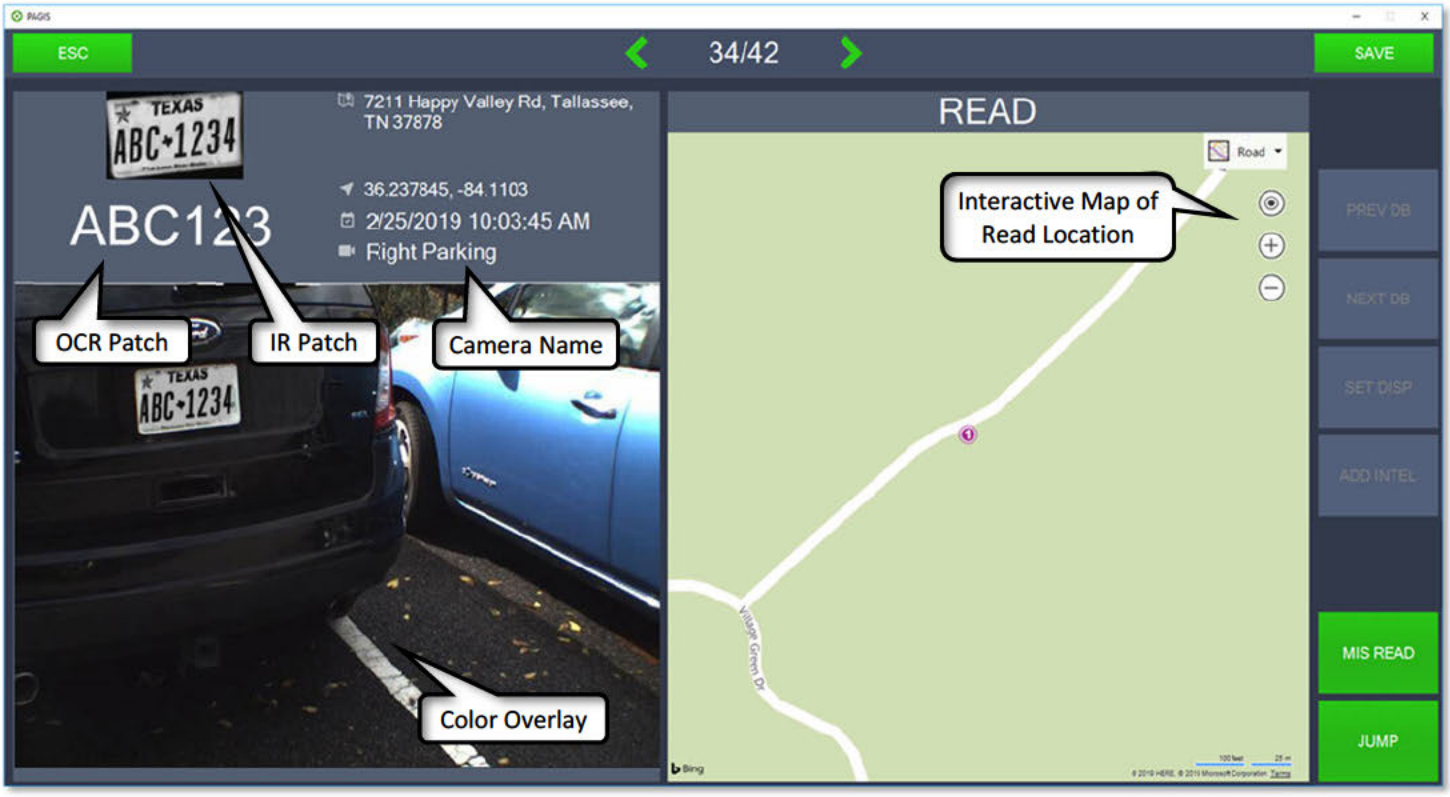
2.9.2 Review Navigation Buttons

The navigation buttons allow the user to review specific sets of information gathered during the shift.

Reads: Review all plate detections that have occurred since the last End Shift synchronization.
Hits: Review the hit alerts for Vehicle License Plate (VLP) reads that matched a Hotlist.
Misreads: Review reads and/or hits that have been manually flagged during the shift as misreads, where the plate number in the image does not match the OCR interpretation of the plate (e.g., a letter O misread as a Q or zero).
Audits: Review failed and successful logons, any manual data entered during the shift, pictures taken and all manual license plate searches.
Targets: Review targets that have been synchronized/downloaded from Boss.
Databases: Review all the Hotlists currently distributed to this PAGIS laptop/MDC.
Esc: Returns the user to the previous screen.

2.9.3 Reads

From the Main Screen, the user can review his or her accumulated Reads (those gathered since the last End Shift was completed) by clicking on the Review icon and then selecting the Reads Navigation button. The Read Review Screen is divided into two main sections. The left side displays the information gathered at the time of the read and the right side displays an interactive map of the GPS location.



NOTE: Buttons that are greyed out indicate options that are not available in the current view. For example, the Reads and Hits review screens share the same layout but different on-screen options.

2.9.3.1 Reads Result Screen Navigation Buttons



Read Count: The left number is the current record. The right number is the total available for review.

Next/Previous button: The arrows on either side of the read count allow the user to navigate back and forth to review reads/results.



MisRead button: When the button is green it indicates the record has NOT been edited as a Misread by a user. Once a Misread is saved, this button will turn grey and the record title will update.



Jump button: Allows the user to "jump" to a specific record without the need to navigate one record at a time using the Next/Previous buttons.



Save button: Apply any changes/edits and return to the Main Screen.



Escape button: Returns the user to the Main Screen.

2.9.3.2 Interactive Buttons – Reads Screen

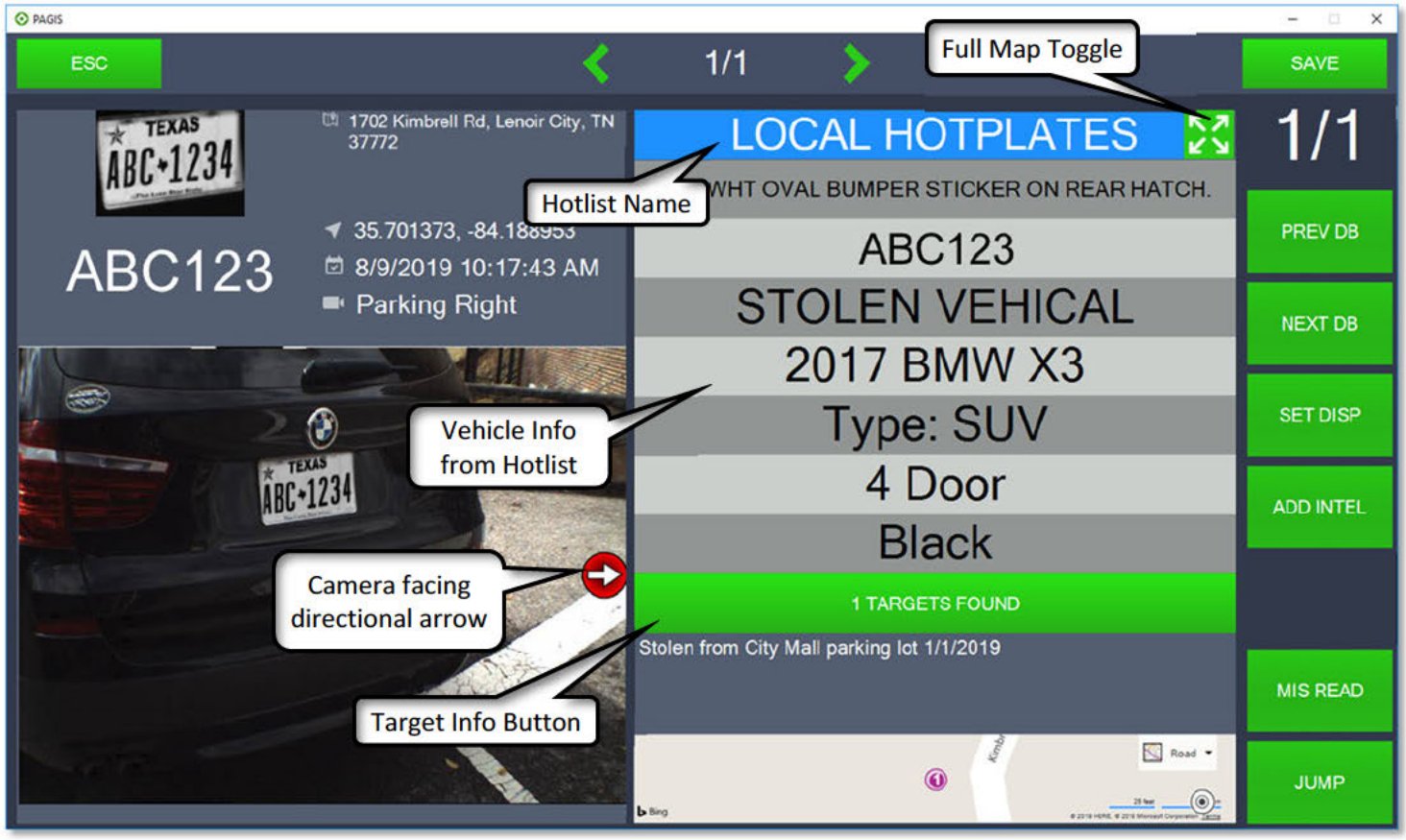
From the Reads Review, the user can interact with the following:

- IR Patch: The user can click on the IR "Patch" plate image to open a full-screen view.
- OCR Patch: The user can click on the OCR "Patch" image to edit the license plate number if necessary/Misread.
- Color OV Image: The user can click on the color image to open a full-screen view.
- Map: The user can manipulate the interactive map of the read location (Map Type, Scroll, and Zoom).

2.9.4 Hits

Users can manually access the Hits Section by first selecting the Review icon from the Live View Screen and then clicking the Hits Button. The Hits Screen is also divided into two main sections. The left side displays the information gathered from the ALPR equipment during the read. And the right side displays the information provided by the associated alert list.

NOTE: Each time a VLP matches a Database value (a license plate read by the system matches a Hotlist entry), PAGIS plays an audible tone and automatically displays the Hit Screen to alert the user.



2.9.4.1 Hit Screen Attributes

Hit Count and Navigation Buttons: Displays the total Hit count as well as the Next/Previous navigation buttons.

IR Patch Image: A thumbnail image of the license plate from the IR camera.

OCR Text: The character string the OCR engine generated from the current plate.

GPS Location: The GPS coordinates at the time of the hit. (If a GPS device is not attached, the Lat/Long is displayed as 0,0).

Date and Timestamp: The date and time when the read/hit was captured.

Overview Image: The overview image of the vehicle from the Color Camera. (**NOTE**: Color images require visible light)

Camera Name: The name of the camera that captured the read ("Right Parking" in the screenshot).

Hotlist Name: This is the name of the Hotlist or "Database" where the plate was matched.

Target Button: When available, this indicates a person of interest is associated with the Hit and opens the Targets Screen.

Vehicle Information: The area of grey bars will display the related vehicle information from the Hotlist. Any information added manually by the user will appear in the Text Box near the bottom of the screen.

Interactive Map: Shows the location the Hit took place. Users can access full-screen view by clicking the map or the toggle .

2.9.4.2 Hit Screen Function Buttons



The Hit Count Indicator: shows how many Hotlists the current Hit has registered against.



Previous DB button: This button moves the user to the previous Database/Hotlist that produced a Hit.



Next DB button: Pressing this button moves the user to the next Database/Hotlist that produced a Hit.



The Set Disposition button: prompts the user to report the disposition of the hit by selecting one of the approved codes assigned in BOSS by the Administrator.



The Add Intel button: allows the user to add additional information regarding the current Hit.



The Misread button: allows the user to flag the Hit as a misread.



The Jump button: Allows the user to "jump" to a specific Hit instead of navigating one at a time.

2.9.4.3 Interactive Buttons – Hits Screen

- IR Patch: The user can click on the IR "Patch" image to open a full-screen view.
- OCR Patch: The user can click on the OCR "Patch" image to edit the license plate number if necessary/Misread.
- Target Button: Shows associated person(s) of interest and opens the Targets Screen.
- Color OV Image: The user can click on the color image to open a full-screen view.
- Map: The user can manipulate the interactive map of the read location (Map Type, Scroll, and Zoom).

2.9.4.4 Set Disposition – Additional Detail

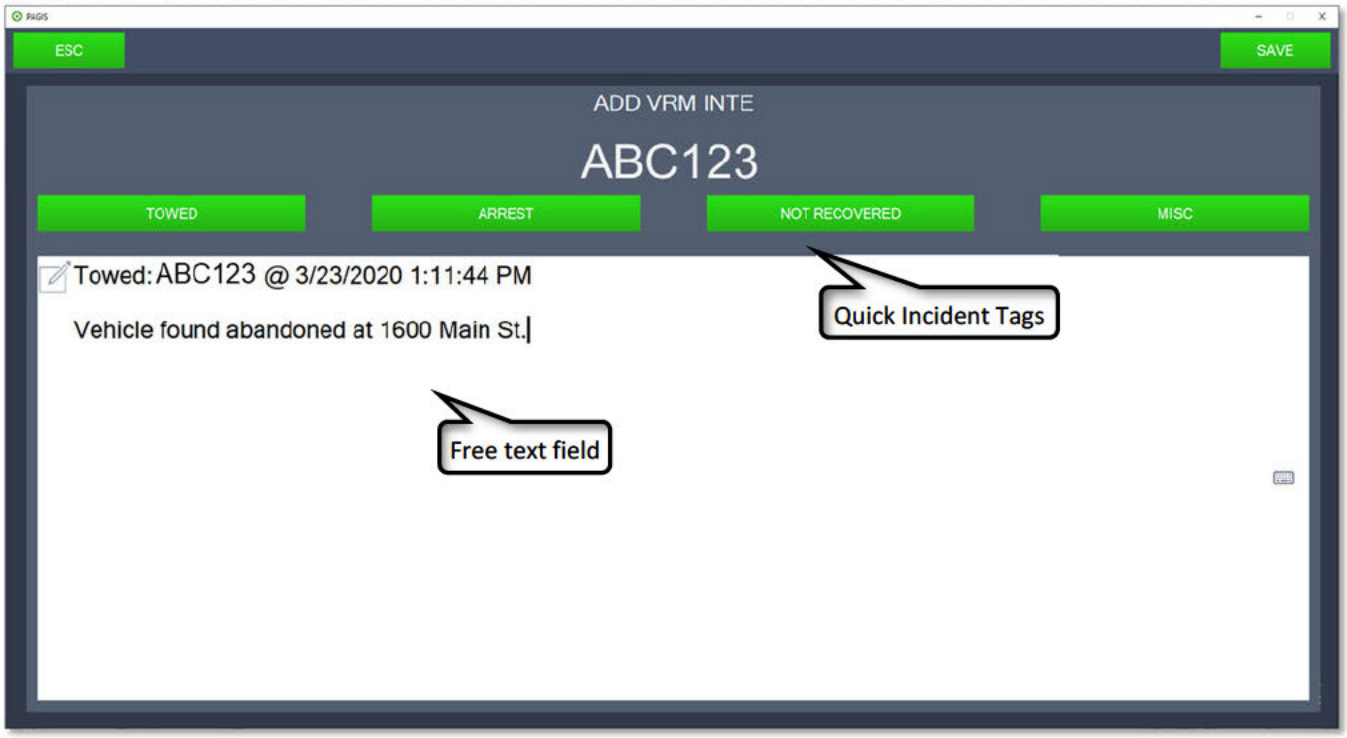


PAGIS allows for additional information to be added to a record in the form of a Disposition. Once Hits are flagged with a disposition code, the Agency is capable of running a "Reads Statistics by Disposition Report" in BOSS. Thus, providing valuable metrics and understanding to leadership in regard to their ALPR Enterprise.

When the "Set Disp" button is selected, the user is prompted to choose from a list of predefined values set by the Agency/BOSS Administrator. Once a disposition is selected and Saved, the disposition is reported to BOSS and will also show up in the Hits Review Screen text box in PAGIS on the next alert notification.

2.9.4.5 Add Intel – Additional Detail

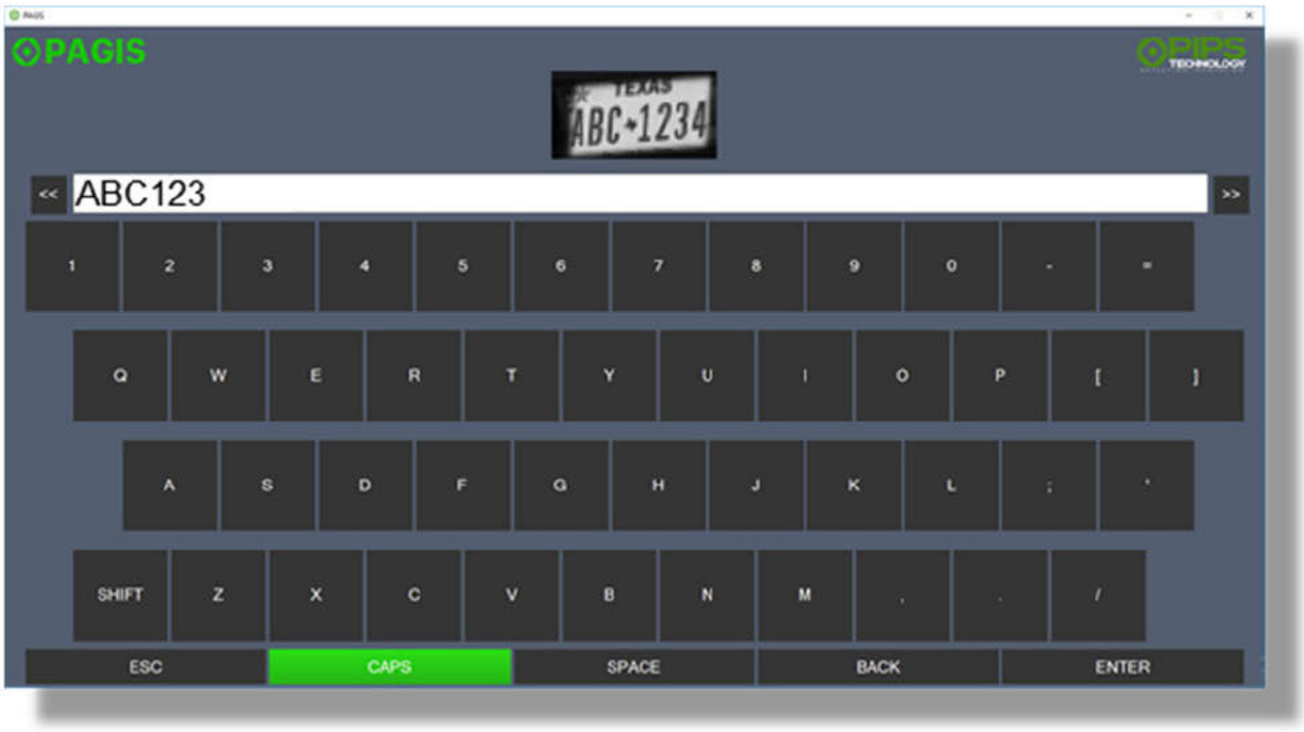
The Add Intel button launches the Intel screen. The user is prompted to assign one of four values: Towed, Arrest, Not Recovered, and Misc. by clicking the associated button at the top of the screen. The user may also enter additional detail regarding the license plate/vehicle. After clicking the Save button, the intel will now appear in the Hits Screen text box.



2.9.5 Misreads

PAGIS allows the user to mark Reads and Hits with incorrect OCR translations as a Misread. This is most commonly done by Agencies for Hits only as users typically don't have time to review every single Read from their shift. Once an errant Hit is corrected, the system updates the record to show it as a Misread and thus improves Agency Hit Reporting.

Correcting a plate read can be accomplished by clicking on the "OCR Patch" in either the Hits or Reads review screen. When the user clicks on the OCR Patch, the OCR Edit Screen opens and allows the user to update the Vehicle License Plate (VLP) data.



2.9.5.1 Marking a Record as a Misread:

The user can mark a record as a Misread from both Reads or Hits Review Screen. Each user can either simply flag the record as a Misread or update the OCR Patch information. **NOTE**: This ability is only available until the user has performed an End Shift function.

Manually Flagging a Read or Hit as a Misread:

1. Navigate to either the Reads or Hits Review Screen
2. Click on the Misread button on the Right
3. Click Save
4. Take note that the record title has now changed from “Read” to “Misread”

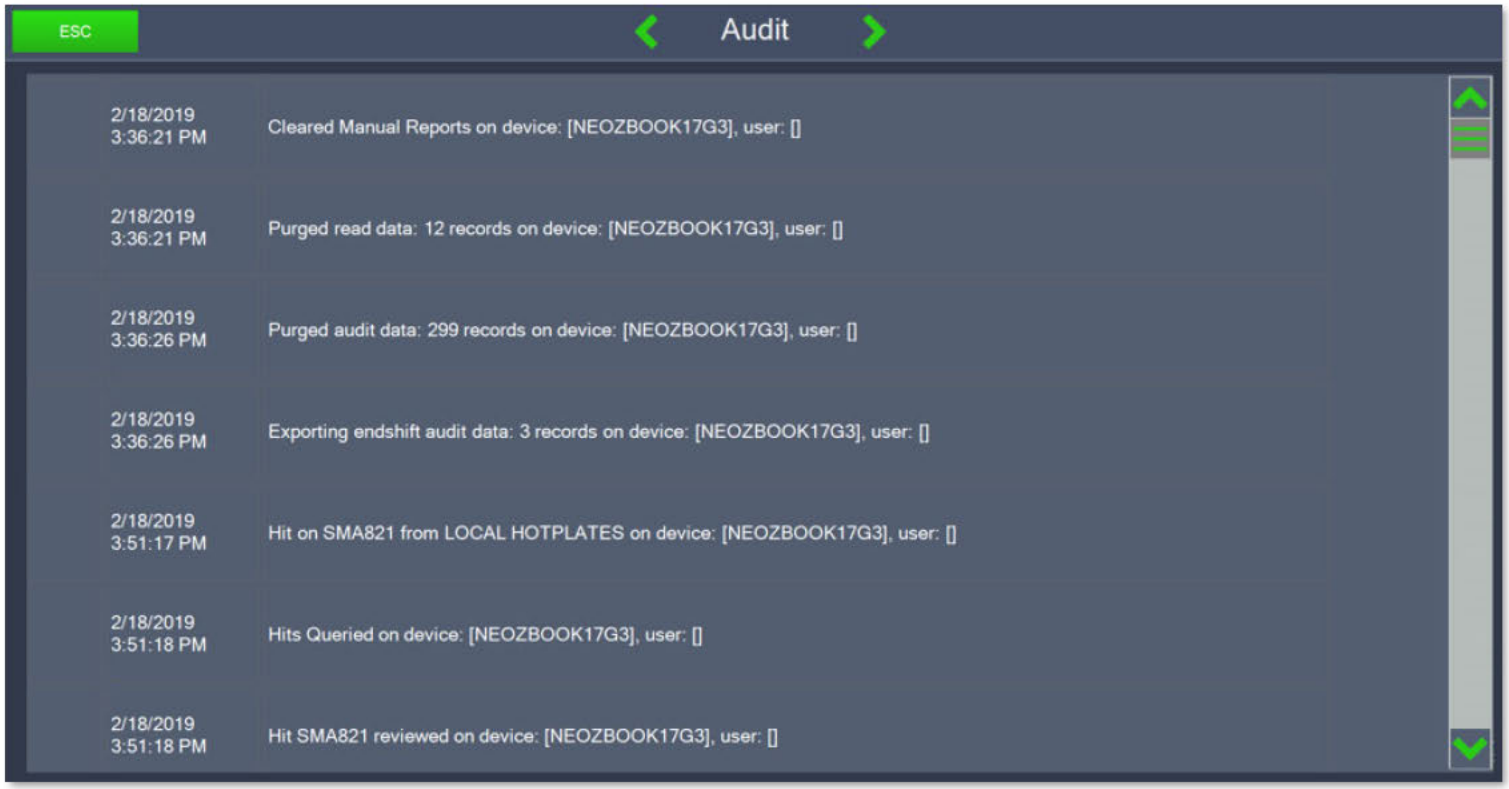
Updating the Read/Hit OCR Patch:

1. Navigate to either the Reads or Hits Review Screen
2. Click on the OCR Patch (Text just under the IR Plate Image)
3. Use the keyboard or on-screen keypad to update the Vehicle License Plate Number
4. Click the Enter Button to Save the changes (and exit back to the Review Screen)
5. When the user saves the changes to the OCR Patch, the record (Read/Hit) is automatically flagged as a Misread

2.9.6 Audits

PAGIS logs both user and key system activity during each use of the software. The audit log captures various information like Read searches, synchronizations, hits, and user login attempts. The Audit Report is viewed in PAGIS by navigating to the Review section and selecting “AUDITS”.

NOTE: Performing an End Shift or syncing the database clears the current log.



2.9.7 Targets

PAGIS has the ability to display information regarding Persons of Interest in response to a Hit alert. Targets are created by BOSS/Hotlist Administrators, and typically provide detailed information about owners of a registered vehicles. When configured, Target data is always linked to unique VLP data (a specific License Plate). If PAGIS registers a Hit on a Plate with a target ID, the Target Information Button is displayed in the Hit Alert window and allows the user to access the Target Screen.



2.9.7.1 The Targets Screen

When a PAGIS user clicks the Target Information Button from a Hit Alert, the Targets Screen opens. This screen displays the information from the BOSS server about the Person(s) of Interest matched to the Hit (license plate).



2.9.7.2 Targets Screen Navigation Buttons

If a Hit alert has more than one Target associated with it, the PAGIS user can navigate all Target information with the buttons described below:



Target Count: The left number is the current record. The right number is the total available for review.



Next/Previous button: Arrows on either side of the target count allow the user to navigate back and forth to review the various targets.



Jump button: Allows the user to "jump" to a specific record without the need to navigate one record at a time using the Next/Previous buttons.

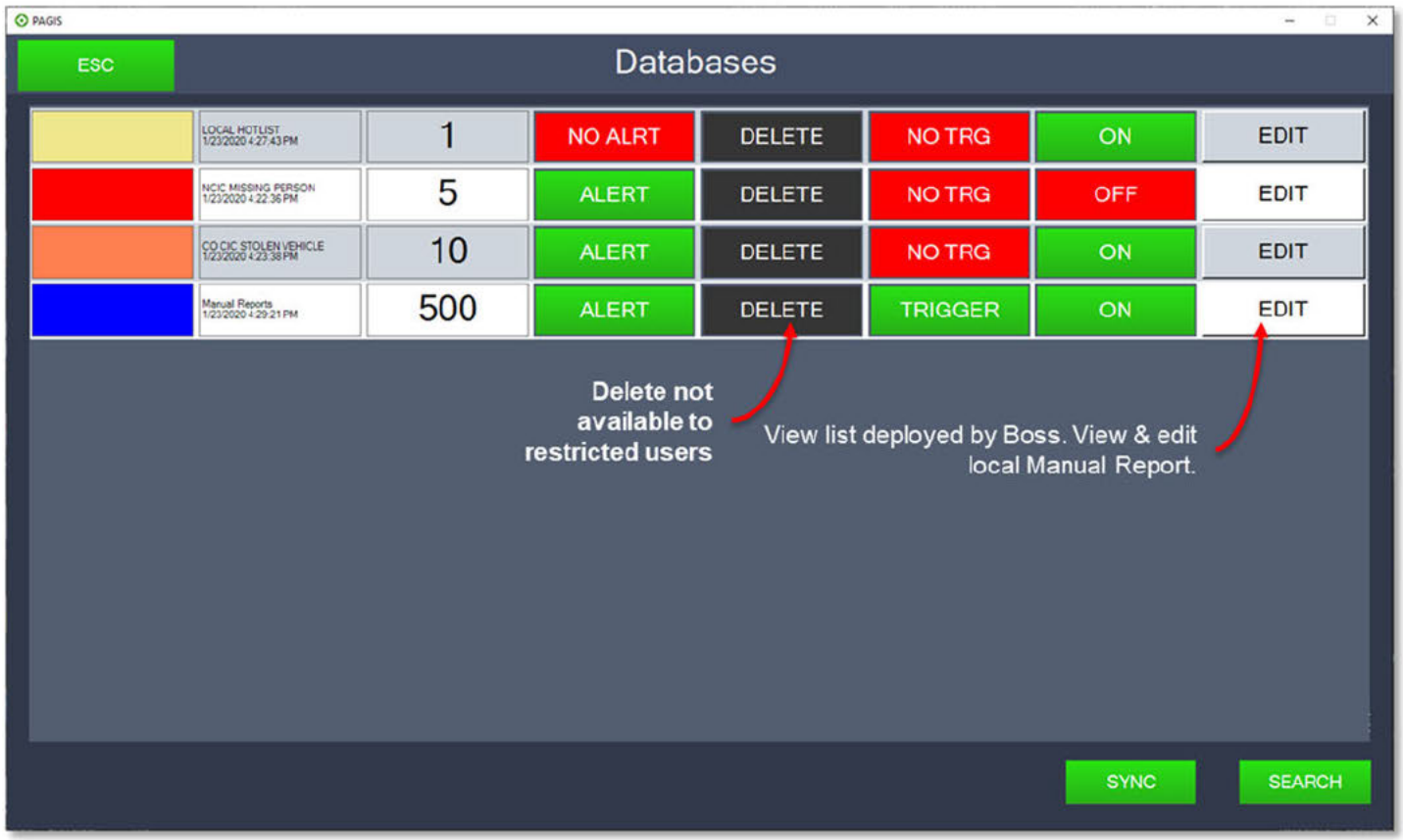


Close button: Returns the user to the previous screen.

2.9.8 Databases

Users can review Hotlists in PAGIS by navigating to the Review section and selecting "DATABASES" on the right. From the Databases Screen, users can toggle Hotlists functions On and Off based on their rights.

NOTE: User rights and Hotlist attributes are configured in BOSS.



2.9.8.1 Databases Screen Functions

Hotlist Color Code: The color attributed to each Hotlist by the BOSS Administrator.

Hotlist Name: The name of the Hotlist given by the BOSS Administrator. Also shows the time/date of the last synchronization.

Hotlist Priority: The priority of the Hotlist assigned by the BOSS Administrator. The lower the number between 1 and 999, the higher the priority. If a plate resides on multiple Hotlists, the list with the higher priority will be displayed first.

Alert Button: Toggles audible alerts On and Off for each Hotlist until the next synchronization.

Delete Button: Based on user rights, allows the user to temporarily delete a Hotlist from PAGIS until the next synchronization. To delete a hotlist, the user must click the button twice (it turns green and then deletes the list).

Trigger Button: Toggles external triggers On and Off. An example of an external trigger is a light bar.

On/Off Button: Disables and enables each Hotlist (each Hotlist is set to On by default).

Edit: View and edit localy created hotplates with a given hotlist, Hotlist/Hotplates deployed via BOSS can only be viewed.

NOTE: Hotlist settings altered in PAGIS will be reset to their default configuration during the next Sync or End Shift. The default configurations are assigned by the BOSS Server/Administrator.

2.9.8.2 Databases Screen Navigation Buttons

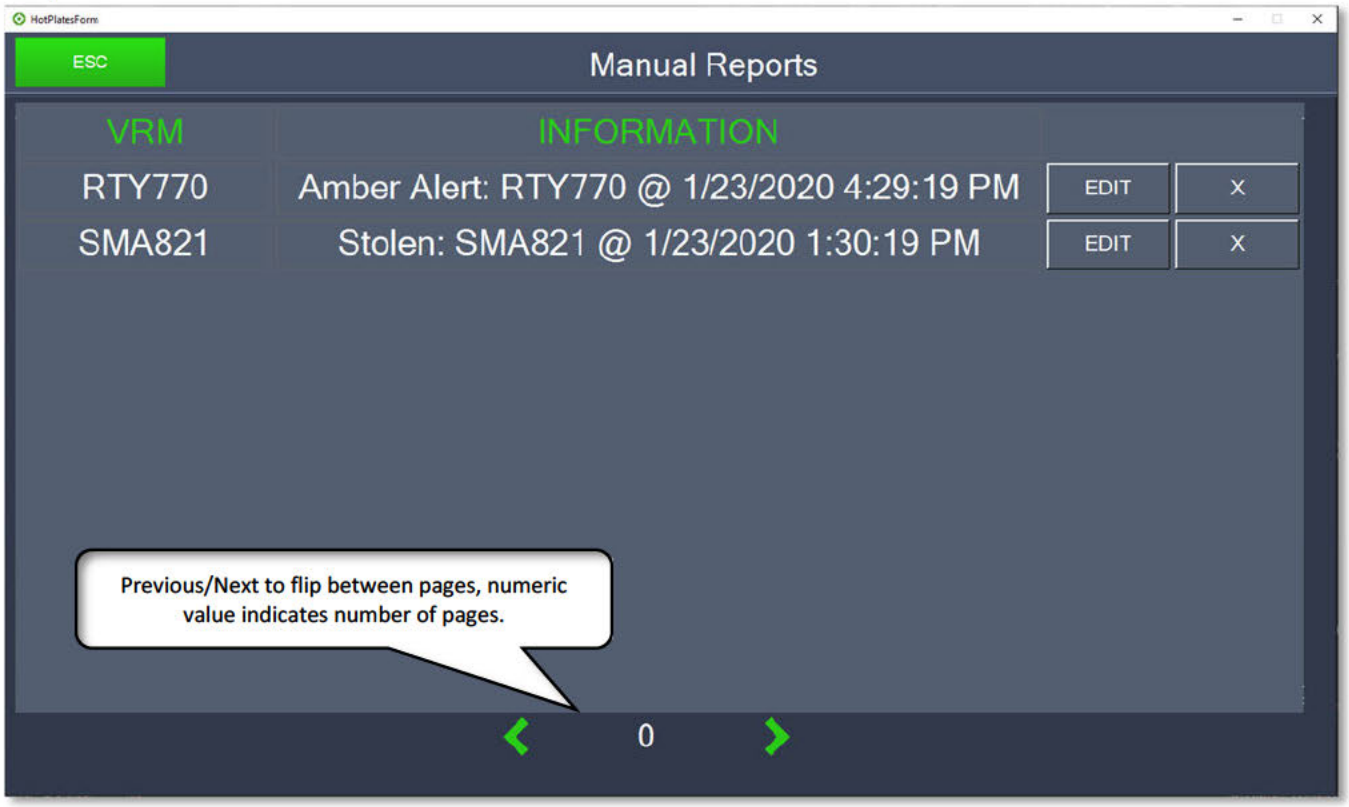
SYNC — **Sync button**: Synchronizes PAGIS with the BOSS server in order to update the Hotlists.

SEARCH — **Search button**: Open the Search Entry Screen (See section 2.8 for more information).

2.9.8.3 Databases Edit- “Manual Reports”

Editing Hotlist has two function based on origin of hotlist.

- Hotlist deployed to PAGIS via BOSS cannot be edited, only the hotplates list can be viewed. Editing/updates are indented to be managed via BOSS.
- Hotlist created in PAGIS, i.e. “Manual Reports” can be managed by PAGIS users, allowing for changes or deletion of the hotplates contained within the hotlist.



EDIT Button: Make changes to the indicustly hotplate information including licanse plate nuamber.
X Button: Remove indivualy hotlist from hotlist.
Previous/Next Button: Scroll thought lising of hotplates contaned within the hotlist. The numeric value indicates the number of pages.

TROUBLESHOOTING TIPS

This section provides some basic troubleshooting tips and information

3.1 Troubleshooting & Tips

- The first login to PAGIS after the new install of an unconfigured version does not require a username or password. Simply click Login to be granted Admin access to the software.
- A good means to test the communication from the MDC to BOSS is ping or telnet (over TCP 8092) through the command prompt.
- A good means to test the communication from the MDC to the SX Processor is ping or telnet (over TCP 9000) via command prompt.
- For many other troubleshooting tips, see Appendix C – Frequently Asked Questions

3.1.1 PAGIS with NetMotion VPN

Agencies utilizing NetMotion VPN software on the MDC will need to apply the following passthrough steps:

1. Login to the NetMotion server as administrator
2. Click Settings > Then select Client > Select Global Client Settings > Then select Passthrough List
3. Click the “Add…” button on the right > Select “Network Address”
4. Enter the following settings (as shown):
    A. IP address:192.168.200.0 (the zero is correct, it's an IP address “range”) Subnet Mask: 255.255.255.0.
    B. Keep all other settings default (as shown) and click OK.
5. The MDC must then disconnect from NetMotion and reconnect again for the settings to be applied locally.

3.1.2 Cisco VPN Client:

Make sure Stateful Firewall is unchecked and "Allow Local LAN".

3.1.3 Microsoft .NET 3.5 Installation

The PAGIS Software requires Microsoft .NET Framework 3.5 specifically. If the MDC doesn’t have .NET, it can be downloaded from the Microsoft website.

3.1.4 Firewall Settings for Client-Server Installations

For client-server installations, the Windows Firewall needs to allow the SX Processor and the MDC to communicate. If the MDC is maintained by a Network Administrator, he or she should be contacted before making changes to the firewall.

Option 1: Allow Microsoft Windows Version 8 or newer to auto-detect the launch of the PAGIS.exe application and use the wizard to add the EXE to the exception list (making note of Public or Private Network settings as necessary).

Option 2: Add PAGIS to the exception list manually by browsing to the install path of PAGIS. The default is below for reference: “C:\Program Files (x86)\PIPS Technology, Inc\PAGIS2\PAGIS.exe”

Option 3: Add the communication ports manually:
TCP 8092
TCP 9000
TCP 9001
TCP 32023
TCP 32029
TCP 10000
TCP 10010
NOTE: XML Datastream uses TCP 10100 and TCP 7000

APPENDIX A: THE GLOSSARY

ALPR/ANPR	"Automatic License Plate Recognition/Automatic Number Plate Recognition".
BOSS	"Back Office System Software". This is the ALPR server.
GPS	"Global Positioning System".
GUI	"Graphical User Interface".
Hotlist	A database or list that contains vehicle license plates of interest ("alert list").
IR	Infrared light.
License Plate	Also called a tag or number plate.
MDC	"Mobile Data Computer". This is the tablet or laptop in the vehicle.
OCR	"Optical Character Recognition" (also referred to as a "cardet").
OS	"Operating System".
PAGIS	This is the License Plate Capture Software most commonly used in an ALPR vehicle.
Service	Operation mode of the PAGIS software. Service or "VPRelay" is used to refer to PAGIS instance that is running directly on the PIPS mobile processor without a GUI interface, this mode is intended to run in conjunction with MDC version of PAGIS installed on laptop connected via Ethernet.
Standalone	Operation mode of the PAGIS software. Standalone is used to refer to PAGIS instance that is running directly on the PIPS mobile processor with a GUI interface.
SX	SX is a short notation referencing PIPS's mobile processor, commonly the SX is followed by the generation number of the processor, i.e. SX3, SX4 & SX4e.
UI	A "User Interface" is the means in which the user can access and navigate the software.
USB Flash Drive	Also called a thumb drive or memory stick.
VLP	"Vehicle License Plate".
VPN	"Virtually Protected Network".
VPRelay	Operation mode of the PAGIS software. VPRelay or "Service" is used to refer to PAGIS instance that is running directly on the PIPS mobile processor without a GUI interface, this mode is intended to run in conjunction with MDC versions of PAGIS installed on laptop connected via Ethernet.
Whitelist	Opposite of a standard BOSS Hotlist. This is a list of license plates that should not trigger an alert.

APPENDIX B: PAGIS SOFTWARE DATABASE FILE

This section is used to configure the PAGIS Software when it's not being used with the Back Office System Software (BOSS). Comma-separated value (CSV) format is the only format the PAGIS Software supports for importing data into the vehicles for the purpose of matching against the captured license plate data. PAGIS will support CSV files with any number of columns, called "fields", as long as the first field is the VLP (Vehicle License Plate). **NOTE**: The CSV format is standard ASCII.

Example CSV Files:

1. *ABC123, Red, Ford, Explorer, 1996, WANTED XYZ456, Blue, Audi, A4, 2001, MURDER*
2. *45ABC234, Vehicle wanted in associated with a kidnapping on 12/5/2005 995BD233, Vehicle reported stolen from Liz's Lounge at 6am on 12/1/2005*
3. *UIO223 ABC123*

General Function:

PAGIS calls/utilizes files in pairs. Each database in PAGIS is created using two files; a CSV file, and an INI configuration file. Without both of these files, the database will not load and PAGIS will not "see" it. Each CSV file/hotlist must have the exact same name as the INI configuration file. Example: Stolen.ini and Stolen.csv will work. Stolen.ini and Plates.csv will not.

Reading an INI Configuration File

Lines that appear in brackets [] are called "Headings". The labels that appear inside the headings, are called "values". Values will always contain an equal sign (=). If a line starts with a semicolon, it is considered to be a comment and is not read by the software. There is no limit to the number of comments in the INI file.

The [SETTINGS] Heading

The values in the Settings heading are: NumFiles, DbName, DbColor, Priority, Covert, Alarm, and NumFields.

- NumFiles: Determines how many database files the system should split the specified hotlist into. Generally, this value is set to 1. But for larger hotlists (200,000+ lines), a number of 2-5 may be more desirable.
- DbName: Tells the PAGIS Software what the displayed name of the hotlist should be.
- DbColor: Sets the display color of the hotlist. This is merely an esthetic setting and not a functional setting. The right-hand side of the equal sign is the HEX value representing the ARGB values for the color. If this value is unknown, the Admin should simply leave this line out of the file.
- Priority: Designates the priority of this hotlist in relation to other hotlists in the system. The highest priority database is 1 and the lowest is 999. **NOTE**: if a plate resides on multiple lists the higher priority will be alerted first.
- Covert: Determines whether standard PAGIS Software users are alerted when a hit is made from the database. Covert database can be used for hotlists that are included for information-gathering purposes rather than eliciting user intervention. The system can also be configured to notify via email or SMS message when a hit is made from a covert hotlist.
- Alarm: Sets the audible alert to be played in PAGIS when a hit is made from the hotlist. Values for Alarm are LOW, MED, HIGH
- NumFields: Indicates how many fields (columns) are in the CSV file. If this value is less than the actual number of fields in a file, then the additional fields are placed in the general information area. This value also determines the number of headings of the [Field x] present in the file. For example, if NumFields=2 then there will be two additional headings, [Field 0] and [Field 1]. **NOTE**: Adding "Creation =" will place the timestamp the hotlist was added to the Begin Shift file.

The [FIELD X] Heading

Under the Field heading, there are two configurable values, “Name” and “PAGIS”.

- Name: Tells the system what the name of this field is. If no name is specified, then no name given to the field. The format is Name = <field>
- PAGIS: Specifies how to display the field in the GUI/PAGIS Software.
    - If no value is defined, the field is placed as general information.
    - Values 1-5 represent special fields for the PAGIS Software that translate to the information being displayed in a box of its own when a hit is processed.
    - A value of 6 represents an ID number to cross reference the vehicle from the hotlist with a person from the wanted list.
    - A value of 7 is identical to leaving the value undefined.

Sample INI Configuration File

[Settings] NumFiles=1
DbName=Stolen Vehicles DbColor=ffffff00 Priority=5 Covert=False Alarm=MED NumFields=8
;PAGIS Values
;0 is VRM / VLP (Not User Definable, always Field 0)
;1 is Special Field 1
;2 is Special Field 2
;3 is Special Field 3
;4 is Special Field 4
;5 is Special Field 5
;6 is ID Number (PNC ID, Drivers License, Social Security Number, etc.)
;7 is General Info (Default for all undefined fields) [Field 0]
PAGIS=VRM

Sample INI Configuration File

[Field 0] Name=VRM
[Field 1] Name=Color
PAGIS=3 [Field 2]
Name=Make PAGIS=1
[Field 3] Name=Model
PAGIS=2 [Field 4]
Name=Action PAGIS=4
[Field 5] Name=Warning
PAGIS=5 [Field 6]
Name=PNCID PAGIS=6
[Field 7] Name=Intelligence PAGIS=7

APPENDIX C: FAQ

Q: **HOW DO I ENTER A SUPPORT CASE?**
A: We have a webform you can use here, you can email our Support Team at Support@PIPSTechnology.com, or you can call us on the phone Monday-Friday 8am to 4pm Central Time (9am-5pm Eastern) at (833) 747-7577 Option 2.

Q: **HOW DO WE CREATE USERS IN PAGIS?**
A: The agency BOSS Administrator creates all users, both for BOSS and for PAGIS. Once the user is created in BOSS, the Admin would click the user's name to select/edit the user. Then click the Advanced button and update the PAGIS specific password. Please note that the username and password fields are both case sensitive and the PAGIS users need to be added to a group with the Role that allows them to use PAGIS/LPCS.

If you have any further questions, please feel free to enter a request for support here.

Q: **WHERE DO USERS CHANGE THEIR LOGIN PASSWORD IN PAGIS?**
A: User passwords are created and updated in BOSS via the UI client software. For the majority of our customers using both the PAGIS Software and BOSS, any user accounts or passwords created in the PAGIS Software itself will be overwritten by the user information defined in BOSS during the next sync.

If you have any further questions, please feel free to enter a request for support here.

Q: **HOW DO WE REQUEST AN RMA REPAIR?**
A: To assist with this, please navigate here to review our RMA procedure as well as to download the request form. Please keep in mind that once submitted, all repairs are reviewed for age of equipment and warranty status before final processing takes place. Additionally, incomplete forms and those without much detail often result in processing delays.

If you have any further questions, please feel free to enter a request for support here.

Q: **WE HAVE NEW MDC LAPTOPS IN THE PATROL CARS, HOW DO WE ADD THOSE DEVICES TO BOSS?**
Q: **HOW DO WE EDIT THE DEVICE NAMES IN BOSS?**
A: The initial device template/skeleton is automatically created in BOSS the first time the device attempts to Sync from the field. Devices should NEVER be created manually. For PAGIS laptops, this is done after PAGIS is installed and configured and Begin Shift is launched. However, if the agency would like to organize the device list by updating the "Device Name" field, those steps are below:
1. Login to the BOSS UI with Admin rights
2. Navigate to Admin > Devices
3. Click on a device name to select it > Click Edit
4. Update the name of the device in the "Description" field (Name field cannot be altered)
5. Click Save > This will take you back to the Device Summary List. The "Device Name" field should show the new name

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **WE HAVE A NEW MOBILE COMPUTER/MDC THAT'S NOT SYNCING WITH BOSS.**
Q: **WE KEEP SEEING AN HTTP_STATUS_CODE ERROR WHEN RUNNING BEGIN SHIFT.**
A: This error most commonly means that a new device in the field (laptop/tablet) can "see" the BOSS server, but that it hasn't been enabled yet to "talk" with it. Follow the general steps below to address this issue:
1. The agency BOSS Administrator will need to login to the BOSS UI client and Select Admin
2. Then select Devices and from there, left click on the device/computer name of that MDC to edit it
3. Once in the Edit screen, Enable the device. This will take you back to the Device List.
4. Click the name to edit the device again. Now assign users/Owners and save.
NOTE: The Select button becomes a Save button when selecting which Groups/Users should have access to login to this device
5. Once that is done, navigate to Admin > Hotlists
6. From here, click on each hotlist one at a time to distribute them to the new device being sure to Save the changes next to the

Distribution field. Note again that the Select button becomes a Save button. And there's another Save button at the top left of the edit window.
7. After this is complete, perform Begin Shift from the field unit/MDC and confirm there are no further errors.

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **NEW PAGIS USER CAN'T LOGIN BUT OTHERS CAN.**
Q: **USERS CAN LOGIN TO PAGIS WITH NO CREDENTIALS AT ALL.**
A: Entry or login to the PAGIS software in the field is partially controlled by the Device settings in BOSS. The users themselves must also be properly setup with an LPCS/PAGIS password. To check the current device settings/ access, perform the following steps:
1. Login to BOSS UI (with Administrator rights)
2. Select the Admin Section
3. Select Devices and then Select the Device in question by PC name
4. Once selected click on the Edit button near the bottom
5. Locate and inspect the "Owners" Field (this is a list of users/groups that have access to login to the device)
NOTE: If this field is blank, the device is in an open configuration mode allowing admin level access simply by clicking login (any credentials would also be accepted).
6. To update the device owners, click the "Select" button next to the Owners field (notice it changes to a Save button)
7. Check which Users/Groups of Users should be able to login to PAGIS from this device
8. Click the Save button next to the field
9. And then click Save in the upper left portion of the Edit window
10. Have a previous user or Admin login to PAGIS and perform Begin Shift to sync the new data
11. A PAGIS Admin can confirm by navigating to Admin, Admin, and then Users to review the list
12. Another test would be to have the new user attempt to login

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **WHEN USERS LOGIN TO PAGIS, THEY ONLY SEE A GREY SCREEN.**
Q: **CAMERAS AREN'T SHOWING UP IN PAGIS ANYMORE.**
SEE ALSO: "THE LINK LIGHTS ON OUR ALPR COMPUTER/MDC WON'T TURN ON OR FLASH"
A: Below are some basic troubleshooting steps you'll want to follow before creating a support ticket.
1. Doublecheck the physical power switch on the black box/Processor is On. In many vehicles, there is also an in-line switch in the front of the vehicle that needs to be switched On. When the units are properly powered and on, you should see lights and hear fans running.
2. Confirm that the network adapter settings on the laptop match the proper Static IP scheme for the SX Processor in use. The older scheme is 192.200… and the newer scheme is 192.168…. NOTE: the adapter status in Windows should say "unidentified network". If it says "cable unplugged" the laptop can't "see" the SX.
3. If the power and Static IP settings are good and things still aren't working, test further by disabling the three main software related culprits. Turn off/bypass the local Windows firewall, antivirus, and VPN software one at a time.
4. If you're still not able to see the camera feed after that, you may want to use a different network cable as those can get damaged over time and then confirm that the cord is properly plugged into the ports.
5. If the network cord from the SX Processor is routed through a docking station, then it's possible the dock is preventing the traffic. You should contact the dock's manufacturer for the most recent firmware. To test for this, remove the laptop from the dock, directly connect the network cord to the laptop, and then reconfigure the network adapter settings (remove the static settings from the dock's adapter/ and assign the static IP to the laptop's NIC adapter).

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.
Q: **THE LEFT FRONT CAMERA ON OUR ALPR VEHICLE IS NO LONGER SHOWING IN PAGIS**?
Q: **HOW DO WE TROUBLESHOOT MOBILE CAMERAS**?
A: Below are the main troubleshooting steps to test the camera(s) and cable(s) on a system where only one or two cameras are no longer displaying images.
Step 1: Confirm MDC/SX communication - steps shown in section "Cameras aren't showing up in PAGIS anymore."

Step 2: Access the SX Processor – RDP or directly connect a monitor, keyboard, and mouse to the SX. Contact PIPS Support for help with RDP if the credentials are unknown to the agency.
Step 3: Confirm camera activity – Launch Tools. Then open P6Utility or Mobile Toolkit. Check the camera feeds/function by switching the Input menu to the camera(s) in question
Step 4: Unplug and Reattach the Camera Cables – Note, the cables DO NOT TWIST. The metal locking nut on the cable slides back about a millimeter and the cable comes straight out. Do this at the SX Processor and the Camera. You may need to remove the camera from the mount in order to unplug the cable successfully (most brackets use a #3.5 Hex/Allen Wrench)
Step 5: Swap Port on SX Processor – At the SX Processor, swap the camera cables from the non-working camera to a port with a working port (Take care to note the swap so the cables get back to their original ports). If the camera outage stays at the port site, the issue is most likely the capture card on the SX Processor and will require RMA (Example: working Left cam is swapped to port of non-working Right cam and no longer functions. AND the previous non-working Right cam starts working once it's plugged into the Left cam's port). If the fault/error stays with the camera regardless of SX port, continue to Step 6.
Step 6: Physically Swap Camera Locations – Once all other items are checked, move the camera itself to a working position in order to test the cable. (Example: physically move Left camera to the Right camera position on the top of the vehicle) Connect the cable at the new position and test feed in Tools > P6Utility/Mobile Toolkit. If the camera works at the new location, the issue is most likely a bad cable. If the camera still does not work, the issue is most likely a faulty camera in need of repair/RMA.

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **WE'RE NO LONGER GETTING GPS IN PAGIS.**
Q: **WE'RE NOT SEEING GPS DATA FROM SOME OF OUR FIELD UNITS IN BOSS.**
A: Below are the basic troubleshooting steps for checking the GPS of field units:
1. Login to PAGIS (as Admin)
2. Navigate to Admin section, then click the Admin button
3. Select "System" on the left pane
4. Confirm/Set the button at top to "Default"
5. Remove any value(s) stored in the GPS Connection String field. Leave '5' in the Computer String.
6. Click the Save button to retain changes made.
7. Close PAGIS fully and relaunch and log back in to test (Note: GPS will only show with test reads/hits)
8. For versions of PAGIS 2.9 and up, test with a GPS Connection String of 6 if the blank field doesn't work. Save the changes. Log out. Close the software and then relaunch to test.

Please be advised, that some GPS issues can be caused by local or domain firewall settings, antivirus software, or any other software package monitoring/transmitting network data. To test these, disable or bypass those software options on the MDC and retest.

If these initial troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **HOW DO I INSTALL THE PAGIS SOFTWARE?**
Q: **I JUST LOADED PAGIS ON A MACHINE AND IT CRASHES WITH A .DLL ERROR WHEN I TRY TO LAUNCH IT.**
A: The most common installation of PAGIS is Client/Server or "VPRelay Mode". The .dll error is caused by the installer not being run from the HDD and/or the wrong install option being selected (Example: SupeRex instead of MDC). The best practices for the installation are below. (Note, this does not cover MDC or PAGIS configuration, only the act of installation)
1. Always copy the installer over to the HDD/Desktop of the MDC. Never run it from a thumb-drive or network share
2. Regardless of how you're logged in to Windows, right click the installer and select "run as Admin" or "run with elevated privileges"
3. Continue through the message/error about OS compatibility
4. Click next on the wizard and then be sure to select the MDC option (to use with VPRelay)
5. After that, it's next, next, next, finish the reboot is not necessary

If these steps did not resolve the issue, please feel free to enter a request for support here.

Q: **USERS ARE GETTING HITS/ALERTS ON PREVIOUSLY RECOVERED STOLEN PLATES.**
Q: **USERS AREN'T GETTING HITS FROM KNOWN ACTIVE PLATES.**
Q: **THE HOTLISTS IN PAGIS DON'T SHOW TODAY'S DATE.**
Q: **THE HOTLISTS AREN'T SYNCING WITH BEGIN/END SHIFT.**
A: Whether it's from data latency or just use over time, the local file structure can get some minor corruption and will need to be refreshed. The steps below show the best practices:
1. Login to Windows with Admin rights (ability to uninstall/delete software)
2. Login to PAGIS and perform an End Shift
3. When complete without error, Logout of PAGIS and then Exit/Close the program
NOTE: If the End Shift fails or displays an error, contact Support for additional assistance.
4. If there were no errors, locate the PAGIS icon on the desktop.
5. Right click on the icon and select "Open File Location" (This should open a window where the program was installed)
6. Scroll up and locate the folder labeled "data". Double-click it to open it
7. Select and delete everything in here EXCEPT for "Attributes.db"
8. Once that's complete, Login to the PAGIS software again
9. Perform a Begin Shift. This will pull down fresh data from the server
NOTE: Once complete, the files in the data subfolder as well as the Databases section of PAGIS should be restored.

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **IS PAGIS COMPATIBLE WITH OUR NEW WINDOWS 10 LAPTOPS?**
A: Although there's a warning about compatibility during the install of PAGIS on any Windows OS after XP, it is compatible with all them. However, we have seen errors occur when agencies copy and paste folder structures from previous installations. This of course is not recommended.

Q: **THE LINK LIGHTS ON OUR ALPR COMPUTER/MDC WON'T TURN ON OR FLASH.**
Q: **OUR WINDOWS 10 MDC WAS WORKING BUT HAS STOPPED COMMUNICATING TO THE SX PROCESSOR.**
A: There are many variables with troubleshooting any network connection. And the connection from the ALPR computer to the SX Processor is no different. The following troubleshooting list highlights the most common:
1. The physical network cord is bad/damaged.
A: Test with a different cable and confirm that it is plugged in fully

2. The network adapters are not configured or have incorrect static IPs
A: Confirm the Static IP scheme in use and properly configure the network adapters

3. Local and/or Domain Firewall rules have prevented the flow of communication
A: Disable or bypass these and test again

4. VPN, Anti-Spyware, Antivirus, or other monitoring software has blocked communication
A: Disable or bypass these one at a time and test after each to find the culprit(s)

5. Docking Station Firmware can be incompatible with some newer computers or become corrupt
A: Test by running the network cord straight to the MDC and then configuring the network adapters (NOTE: It would also be a good idea to contact station manufacturer to see what the latest firmware version is and upgrade as necessary)

6. The NIC Drivers have become corrupt
A: Update the specific Networking drivers in use on the MDC through the Device Manager in Windows

7. Turn off all power saving settings of the Ethernet Adapter in the device manager
A: Uncheck "Allow the computer to turn off this device to save power"

8. Check for Windows 10 update 1709 and 1803 as this update will not allow the NIC and Cellular Aircard to run simultaneously
A: Settings > Update and Security > Windows Update > "Update History" link – if there, see the steps in the FAQ

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **AS SOON AS WE DOCK OUR MDC, WE LOSE CONNECTION TO THE WIRELESS.**
Q: **OUR WINDOWS 10 LAPTOP LOSES CONNECTION TO THE INTERNET WHEN THE NETWORK CABLE IS PLUGGED IN.**
Q: **OUR MDC HAS MICROSOFT VERSION 1709 OR 1803 AND CAN'T CONNECT TO WIFI WHEN DOCKED.**
A: Microsoft Updates (1709 and 1803) prevent the Wireless connection as soon as a Network cable is plugged into the device. This also occurs for MDCs/laptops that are docked (where the Network cable from the SX Processor is run through the docking station). As of January 2019, the steps to correct this are below.
WIN10 version 1803
1. Open Regedit
2. Expand HKEY_LOCAL_MACHINE
3. Navigate to Software > Policies > Microsoft > WcmSvc > Local
4. Right click on Local > Hover over New > Select "DWORD (32-bit)"
5. Name the new value "fMinimizeConnections"
6. Right click the on the new name > select Modify > Set value data to 1 (leave base Hex) > Click OK
7. Reboot Windows and test

WIN10 version 1709 - Microsoft fixed this with Update KB 4284822. But if you still have issues, the registry steps are below:
1. Open Regedit
2. Navigate to HKEY_LOCAL_MACHINE > Software > Policies > Microsoft > WcmSvc > Local
3. Right click on Local > Hover over New > Select "DWORD (32-bit)"
4. Name the new value "fMinimizeConnections"
5. Right click the on the new name > select Modify > Set value data to 0 (leave base Hex) > Click OK
6. Then Navigate to HKEY_LOCAL_MACHINE\Software\Microsoft\Wcmsvc
7. Right click on Wcmsvc > Hover over New > Select DWORD (32-bit)
8. Name the value "IgnoreNonRoutableEthernet"
9. Right click on the new value > Modify > Set value data to 1 (leave base in Hex) > OK
10. Reboot Win10 and test

If the steps above did not resolve the issue, you may need to address this with Microsoft. Their support site is here.

6 January 2020

PIPS Product Bulletin

With the start of the new year, we have a few announcements and reminders regarding PIPS Technology™ solutions. We are starting 2020 with revamped software and product solutions that have greater capabilities to help you in your daily mission! We dedicate a third of our staff to product and solution improvements and innovations to make your job easier, safer, and more efficient.

BOSS 4 Continued Roll Out

In 2019, we released an early version of our new BOSS 4 software. This new software is a leap forward in design and usability compared to our BOSS 3 product and provides additional features not currently in existing software. The new web-based design also offers the ability to rapidly add features and deploy the software to any number of users in your network. As before, the BOSS software gives you complete control over your data and allows you to dictate who you share data with and how much access to give them.



BOSS 4 provides the ability for you to host inside your own servers/data center as with previous generations of BOSS. However, in response to feedback from the customers, we are also now offering a Hosted Managed Service. Providing industry leading infrastructure and service management, including 99.999% infrastructure availability with the latest in security, this option provides the ability for your teams to focus on front-line duties rather than worrying about Databases, Servers and Infrastructure.

Give us a call at 833-PIPS-LPR (833-747-7577) and speak with our sales team to get a free online demonstration and test run.

New Mobile System Hardware and Software Continued Roll Out

Also, in 2019, we released a new version of our popular mobile system with the SX4e processor and P720 camera. The P720 uses the same form factor as the robust P634 camera, but provides better lenses, better sensors which provides higher quality images, and more lane coverage. The optical performance improvements this technology provides improves detection and recognition rates compared to previous generations of PIPS' products and those of our competitors.

The SX4e is the power-over-ethernet (PoE) version of the processor allowing more versatility in configuration and deployment of the mobile system. System configuration still allows between one to four cameras per processor, but the PoE cable can have 100 feet between processor and camera.

Questions / Concerns? Contact Technical Services (833) PIPS-LPR or (833) 747-7577

Along with the new hardware, we are making continuous improvements to our PAGIS in-car mobile software. This includes security enhancements, more firmware updating, and additional mapping tools. Our development team continues to roll out new changes and features which are available free of charge, during their warranty phase, to those customers who have already upgraded.



If you are interested in any of our new mobile products, please reach out to our sales team for a demonstration. You can also contact our support team to see if your existing system is on the latest software or firmware version. Contact us at 833-PIPS-LPR or at support@pipstechnology.com.

BOSS 3 End of Life Notice – December 31, 2020

At the end of 2020, we will no longer support our BOSS 3 software. This includes software updates and service/support inquires related to this product.

The migration from BOSS 3 to BOSS 4 is designed to be made as simple as possible for the customer, with specific migration tools developed by PIPS to aid the process. Please get in touch so we can discuss how you could migrate to BOSS 4 from BOSS 3. For any customers committing to upgrade before the end of March 2020 we will be crediting any pro-rata BOSS3 support fees against the BOSS 4 license as well as waiving the migration cost.

We will naturally continue to support those customers who have recently purchased software support for the BOSS 3 product until the end of the current obligation.

Questions / Concerns? Contact Technical Services (833) PIPS-LPR or (833) 747-7577

IRIS P500 Latest Software Build with feature enhancements and bug fixes
The IRIS P500 series camera was newly released in 2019 and received superb feedback from those customers who used it, including beating competitor products in numerous “head to head” performance evaluations by customers.

As with all new products we were providing software releases throughout the year in direct feedback from customers for enhancements as well as reported bug fixing highlighted to our Service / Support teams.



We formally released 4 updates during the year and one hot-fix in response to feedback, including the latest hot fix in December 2019. These releases resolved the reported issues, including one that can appear in some of the earlier IRIS cameras under certain circumstances which were not running on the latest released software standard. This manifest itself when the camera first booted, it may erroneously use GMT time instead of the configured time zone. This will cause the camera to record images with the time stamp of GMT instead of local, but not give an indication that the image is using an incorrect time zone. Once the camera is finished booting and synchronizing with its time source (typically within 1 minute), it will use the local time zone, but the images captured during the booting process will have an incorrect timestamp.

We have issued a firmware update to correct this issue. This ensures that the correct time zone is applied to all reads, even during boot up. Please call our support line, 833-PIPS-LPR, to receive the latest firmware and have it setup on your camera system.

NOTE – this only applies to the IRIS P500 series cameras and does not manifest itself in previous generations of our products.

Questions / Concerns? Contact Technical Services (833) PIPS-LPR or (833) 747-7577

New Termination Box (T-Box) Design
In 2020, we begin rolling out a new T-Box design. This design reduces the weight and size of the previous T-Box, while continuing to provide the same functionality. The new design also helps control costs, which in turn helps prevent price increases on the product.

Please call our support line at 833-PIPS-LPR or email us at support@pipstechnology.com to let us know how we can continue to improve this and our other products.

Update to Latest Versions of Software and Camera Firmware
Throughout the year, we have released updates to the firmware of our camera products (both mobile and fixed) along with software updates to PAGIS. We recommend that either your IT staff check to see if your cameras are on the latest patch or contact us to determine your camera status.

Our service staff would be happy to evaluate any of your PIPS products to determine if they are on the latest version. Give our support team a call at 833-PIPS-LPR.

Update Product Passwords
As a means of providing sound security, we recommend changing that the passwords on each camera system and software. In following CJIS policy (code 5.6.2.1.1), we recommend passwords should contain the following:

1. Be a minimum length of eight (8) characters on all systems.
2. Not be a dictionary word or proper name.
3. Not be the same as the User ID.
4. Changed regularly (ideally every 90 days)
5. Not be identical to the previous ten (10) passwords.
6. Not be transmitted in the clear outside the secure location.

Remember, every law enforcement agency that uses CJIS is audited at least once every three years. We are aware of customer being asked about their password policy in relation to their ALPR infrastructure and would urge the ALPR cameras to be considered as part your organizations' password policy.

Regards,



Peter Crary
Global R&D Director, ALPR/ANPR

Questions / Concerns? Contact Technical Services (833) PIPS-LPR or (833) 747-7577

Requirements and Specifications
Back Office Server Software (BOSS4)

On-Premise Applications Server

Below, there are the minimal recommended configurations for different capacity configurations for BOSS4 On-Premise infrastructure.

Application Servers Specifications				
Configuration	**Demo**	**Medium**	**Large**	**High Capacity**
ALPR Devices	1 to 3	3 to 50	50 to 150	Beyond 150
Average Daily Intake	Around 30,000 events	Around 500,000 events	Around 1,500,000 events	Beyond 1,500,000 events
Average of users querying data	3 users	15 users	25 users	Beyond 25 users
Alert list averaging	Around 1M records	Around 2M records	Around 2M records	Around 2M records
Operating System	Amazon Linux / Amazon Linux 2 x64 Linux x64 (RHEL/CentOS, Ubuntu, Debian, SUSE) macOS x64 Windows 10 Professional x64 Windows Server 2016 x64			
Memory	16GB	32GB	64GB	192GB
Processor	x64 2.0 GHz 8 cores o better	Server Processor x64 (Intel Xeon Gold) 2 GHz 4 cores, 8 threads, 4MB cache	Server Processor x64 (Intel Xeon Platinum) 2.4 GHz 16 cores, 32 threads, 8MB cache	Server Processor x64 (Intel Xeon Platinum) 2.4 GHz 24 cores, 48 threads, 24MB cache
Hard Drive	7200 RPM SATA3	SSD SATA3	SSD SATA3 or NVMe PCI Express	SSD SATA3 or NVMe PCI Express
Application Space	128 GB of available space	256GB of available space	320GB of available space	512GB of available space

On-Premise Database Server

BOSS4 uses the MongoDB Database Engine.

Specifications of the Database Server				
Configuration	**Demo**	**Medium**	**Large**	**High Capacity**
ALPR Devices	1 to 3	3 to 50	50 to 150	Beyond 150
Average Daily Intake	Around 30,000 events	Around 500,000 events	Around 1,500,000 events	Beyond 1,500,000 events
Average of users querying data	3 users	15 users	25 users	Beyond 25 users
Alert list averaging	Around 1M records	Around 2M records	Around 2M records	Around 2M records
Database Engine	Mongo DB Community	MongoDB Enterprise		
Operating System	Amazon Linux / Amazon Linux 2 x64 Linux x64 (RHEL/CentOS, Ubuntu, Debian, SUSE) macOS x64 Windows 10 Professional x64 Windows Server 2016 x64			
Processor	x64 2.0 GHz 8 cores o better	Server Processor x64 (Intel Xeon Gold) 2.5 GHz 4 cores, 8 threads, 4MB cache	Server Processor x64 (Intel Xeon Platinum) 2.4 GHz 16 cores, 32 threads, 16MB cache	Server Processor x64 (Intel Xeon Platinum) 2.4 GHz 24 cores, 48 threads, 24MB cache
Memory	N/A	32 GB	128GB	256GB
Hard Drive	7200 RPM SATA3 Not suitable for camera implantation with any kind of data retention expected	SSD SATA3 RAID level redundancy and scheduled DB backups recommended *See sizing chart for storage.*	SSD SATA3 or NVMe PCI Express RAID level redundancy and scheduled DB backups recommended *See sizing chart for storage.*	SSD SATA3 or NVMe PCI Express RAID level redundancy and scheduled DB backups recommended *See sizing chart for storage.*

This document and its contents are intended for the recipient only. Copying, redistributing, or discussing with any other party outside of the intended recipient and PIPS-Neology is prohibited.

Data Storage Requirements

The calculation of storage applies to Cloud and On-Premise configurations.

Approximant Sizing based on Hybrid data, Mobile & Fixed Camera data			
# of records	Database size Metadata and indexes	Repository Size Imagery	Total
1 Million	32GB	153GB	**185GB**
5 Million	64GB	763GB	**827GB**
10 Million	320GB	1.5TB	**1.82TB**
50 Million	1.6TB	7.5TB	**6.1TB**
100 Million	3.2TB	15TB	**18.2TB**

The calculations for storage are approximated based on an average sampling of around 192KB per event.

System Communication Ports

Ports	TCP / UDP	Description
80	TCP	HTTP Web access port for mapping.
443**	TCP	HTTPS Web access for client access, SW Updates, AWS Services.
8090	TCP	Legacy Pagis 268 data port, not required unless using older Pagis SW.
8092	TCP	REST API data port for PAGIS, supports TLS v1.0.
8093	TCP	REST API data port for PAGIS, supports TLS v1.3.
10000	TCP	VES Image port for fixed cameras.
10005	TCP	VES Heartbeat for fixed cameras.
10010	UDP	VES Ping port for fixed cameras.
27017	TCP	MongoDB data connection port.
**	Specific BOSS4 Micro Services require Internet access to AWS Services managed by Neology.	

Additional System Requirements

Application Server:

- Linux x64 (RHEL/CentOS, Ubuntu, Debian, SUSE).
- MacOS x64.
- Windows 10 Professional x64 or newer.
- Windows Server 2016 x64 or newer.

Database Server:

- MongoDB.

Client-Side:

- Chrome v72 and newer, we are currently working to validate more browsers.
- Standalone Alert application- Windows version 7 and up, x32/x64.

Remote Access:

- Scheduled or 24x7 remote access is required during installation and testing.

This document and its contents are intended for the recipient only. Copying, redistributing, or discussing with any other party outside of the intended recipient and PIPS-Neology is prohibited.

Frequently Asked Questions, FAQ's.

Q. Support for other Operating Systems?
A. Currently supported are Windows based x64 OS's, MacOS x64, Linux x64 (RHEL/CentOS, Ubuntu, Debian, SUSE). The preferred OS is Linux for BOSS application server.

Q. Can Boss work in virtual OS's?
A. Yes, supported are Windows based x64 OS's, MacOS x64, Linux x64 (RHEL/CentOS, Ubuntu, Debian, SUSE). The preferred OS is Linux for BOSS application server.

Q. How long does a typical BOSS4 installation take?
A. Boss4 installation and setup can vary depending on requirements, typical installations can take anywhere for 1-3 days to complete and possible longer depending on data migration.

Q. What Database programs are supported?
A. Currently MongoDB is supported, other databases will be supported in future releases.

Q. Can you migrate data from non-PIPS ALPR servers into BOSS4?
A. No. We can only migrate data from existing BOSS3 systems.

Q. Can existing BOSS3 database files be utilized when upgrading to BOSS4?
A. No. BOSS4 is a completely new database structure, however data can be migrated.

Q. How long can data migration take.
A. Data migration can vary depending on volume, anywhere from hours to days.

Q. What data is miraged from BOSS3?
A. Customizable among the following. Reads, Hits, Users, Groups, Roles, Devices, Sites, and Hotlist.

Q. Can BOSS4 reside on same OS as database application?
A. Yes. Only small demo or trial configurations can support same OS for both.
A. No. Production deployments it is not recommended.

Q. Can BOSS4 ports be customized?
A. No. Current BOSS4 version does not support customer port configurations.

Q. Can BOSS4 versions share data with older BOSS3 versions?
A. Yes. Data sharing is built into our latest versions to connect with other older versions of BOSS3.

Q. How are the database tables created?
A. BOSS4 application installation and start configures the required database structure needed.

This document and its contents are intended for the recipient only. Copying, redistributing, or discussing with any other party outside of the intended recipient and PIPS-Neology is prohibited.

PIPS Fixed ANPR Camera User Manual

PIPS Fixed ANPR Camera User Manual

Version 4.9.11308 created on 2020-12-04 13:14:46 ; with commands from versions: P492:version 4.9.11308 .
Copyright © 2007-2017 Neology

Table of Contents

1. Introduction 1
P382 1
P392+/P492 2
Assumptions 2
Conventions 2
2. Getting started 4
Connectivity 4
Discovery 4
Serial RS-232 5
Ethernet 5
Networking setup 5
Basic Configuration 6
Connecting 6
SSH 6
Restarting and Shutting Down 7
Restarting after changing settings 7
Switching off for planned maintenance 7
Power-cycling 7
3. PIPS ANPR Toolkit 8
Viewfinder 8
Vehicle Events 9
Review 9
Camera Software 9
Software Management 10
Software Installation 10
4. Camera technical overview 11
Interfaces: Output mechanisms 11
5. Configuration using Webmin 13
Camera control 13
Network 13
Mounting network disks 13
NFS 14
Windows shares 14
6. PIPS ANPR Shell 15
PIPS Shell Commands 15
ACS - Access Control System (acs) 15
ANPR Vehicle Analyser (anpr) 24
Asynchronous Payload Matching (asyncp) 27
BOF2 protocol (bof2) 28
IR Camera (cam1) 30
Overview Camera (cam2) 34
Client vehicle event reporter (client) 36
Contexts (contexts) 37
Plate Database Matcher (dbmatcher) 40
Diagnostics and Exceptions Manager (diagnostics) 42
File Logger (filelog) 43
Vehicle Fusion (fusion) 43
GPS Time Manager (gps) 46
Heartbeat (heartbeat) 46
Image File Outputter (ifo) 47
JPEG Service (jpegService) 48
JTMS - Journey Time Measurement System (jtms) 49
External Led Control (ledControl) 50
Metadata store (metadata) 50
OEM Modules (modules) 53

Network user interface manager (netuis) 54
NTP Monitor (ntpMonitor) 54
Licence options (options) 55
Patch Overlay Control (patchoverlay) 55
PCI Camera Source (pciSource) 56
PIXI Contexts (pixicontexts) 56
Power Manager (power) 56
Relay Out (relayOut) 56
SAP - Serial Application Port (sap) 57
Vehicle Image Selector (selector) 57
Hardware Monitoring sensors (sensors) 58
Console Logger (stdout) 58
System Details (system) 58
Trigger Control (trig) 60
Trigger Script (trigScript) 64
UTMC Delivery Module (utmc) 65
UTMC V1.2 Delivery Module (utmcv12) 67
VES - Violation Enforcement System (ves) 68
Vehicle Event Database (vfeDB) 78
Logging bits 79
Notifications 82
7. Format strings 84
Control Characters 84
Replacement specifier 85
Format 85
Format Detail 85
List of replacement values 86
Examples 96
8. PIXI Protocol 98
Protocol 98
Example documents 101
Root objects 102
Subobjects 103
Properties 104
Logging 105
Notifications 107
Issue Command 108
Event data 109
Event data with pull 110
PIXI Documents 111
commands.xsd 111
output.xsd 113
common.xsd 117
List of PIXI values 119
PIXI values image_* 119
PIXI values cam_* 119
PIXI values hazcam_* 120
PIXI values event_* 120
PIXI values file_* 120
PIXI values hazard_* 121
PIXI values heartbeat_* 121
PIXI values imglocaltime_* 122
PIXI values imgutctime_* 122
PIXI values jpeg_* 123
PIXI values location_* 123
PIXI values globalmeta_* 124
PIXI values timeoffset_* 125
PIXI values plate_* 126

PIXI values triglocaltime_* 127
PIXI values trigutctime_* 128
PIXI values site_* 128
PIXI values supplementary_* 129
PIXI values localtime_* 129
PIXI values utctime_* 130
A. Technical Details 131
Communication 131
Console Serial RS-232 131
Ethernet 131
Network details 132
Filesystem layout 133
Backup 135
B. Software installation and upgrades 136
C. Factory Defaults 137
D. File transfers 138
SFTP 138
SCP 138
FTP 138
NFS 140
CIFS/Samba (Windows shares) 140
Transfer troubleshooting 140
Network problems 140
Permissions 141
E. Software tools 142
PIPS ANPR Toolkit 142
Windows 7 142
PuTTY 142
Filezilla 142
WinSCP 142
NFS Server on Windows 142
F. Nano - text editor 143
Opening and creating files 143
Saving and exiting 143
Cutting and pasting 143
Searching for text 143
G. rc-update 144
Introduction 144
rc-update commands 144
runlevels 144
Examples 144
Other information 144
H. Viewfinder Protocol 145
Viewfinder commands 145
Viewfinder messages 146
Version 1 146
Version 2 146
Version 3 147
Version 4 148
I. Vehicle Event Viewer Protocol 149
Vehicle Event Viewer commands 149
Vehicle Event Viewer data 149
Header Format 149
J. Legal Notices 152
English 152
Copyright Notice 152
Warranty 152
Service 152

Technical Support 152
Design Changes 153
Trademarks 153
FCC Declaration 153
Français 153
Notification de Copyright 153
Garantie 153
Service 153
Support Technique 153
Changements de Conception 154
Marques Déposées 154
K. Contact information 155

List of Figures

4.1. Objects in the system and how they fit together. 11
8.1. Link with no heartbeat, camera will close when no command has been received for 5 minutes. 100
8.2. Link with heartbeat, client chooses when to end by closing the link. 101
8.3. Get Root Objects - a list of all configureable objects is collected, some may have subobjects 102
8.4. Get subobjects of an object - a list of all subobjects is collected, some may have subobjects. The list may be empty, as in the example 103
8.5. Get properties of an object - a list of all the properties of an object. The list may be empty. 104
8.6. Start some logging. Asynchronous messages will be sent back by the Camera containing the log messages 105
8.7. Start notification messages. Asynchronous messages will be sent back by the Camera containing the notification messages of the requested events 107
8.8. Issue a command and receive the responses. 108
8.9. Connect to the camera and get events as it reads vehicles. 109
8.10. Here we are collecting (pulling) certain vehicle details when a particular vehicle is found. 110

List of Tables

7.1. Format characters 85
8.1. PIXI Packet Format 99
A.1. TCP/IP and UDP/IP Port numbers 133
C.1. Default IP configuration 137
K.1. Contact Information 155

Chapter 1. Introduction

This manual is for the Neology ANPR cameras listed inside the front cover. These cameras are very similar so most of this manual covers them all. Where differences occur the manual will note them.

The P382, P392+ and P492 share many common features, the highlights of which are

- ANPR Camera, illuminator and processor in one package
- Provides savings in system cost, complexity and timescales
- Neology proven camera and processor technology

This manual is only as up to date as the software it ships with. The corresponding version number is listed in the Revision note. Trying to use this manual with the wrong version of the software will be frustrating where differences occur.

P382

P382 is a fully integrated number plate reading camera incorporating both the camera and the recogniser within a single sealed enclosure. It is designed for use in the highest performance applications where it is necessary to provide the ANPR function across a full 4metre carriageway (3.5m with 0.5m overlap). The unit comprises a high resolution monochrome CCD camera with high sensitivity in the infra-red, surrounded by two banks of IR LEDs. Patented filter / flash technique gives suppression of headlights and bright sunlight. Field-by-field control of camera parameters allows the use of the ‘triple flash’ technique to reduce problems of plate-to-plate variability.

An optional independent, integrated, synchronous, colour camera may be configured to the same focal length as the monochrome camera, or to a wider field of view, as required. Therefore an ANPR read will have a colour overview image associated with it.

The integrated number-plate recogniser incorporates the Neology ‘Autoplate’ ANPR engine, which has been proven in many countries worldwide. Patented real-time video triggering upon plate presence provides excellent plate detection. A vehicle presence trigger input is also provided for the most demanding applications, e.g. taking an overview picture of a vehicle with a missing plate.

P382 can be integrated into a wide variety of systems via relay output, RS232, TCP/IP Ethernet with socket and FTP protocols (100baseT). Wireless IP connectivity over GPRS, EDGE or 3G is provided by fitting an optional modem. Additionally IEE802.11b/g ‘WiFi’ may be fitted to give local wireless operation. IP connectivity, (wired or wireless), provides time-lock of distributed cameras to a central server via NTP. A GPS unit may be fitted giving very high accuracy time and position information.

Real-time JPEG hardware compression is provided for both IR and colour images and can be used to provide a real-time IP video stream of the traffic. This can be used to record the image stream for ground-truthing.

P382 is fully web-enabled and can be configured and monitored from a standard web-browser on a PC.

External devices such as DSRC, Radar, Weigh-in-Motion or ticketing systems can be integrated into the system via RS232 or TCP/IP. A flexible interface allows this data to trigger the camera or be added asynchronously to the data set which the camera provides for each vehicle.

The Vehicle Enforcement System (VES) application software offers socket based transfer of Summary and Evidential Records via either push or pull protocols with full key handling, authentication, encryption and local storage of up to 60,000 events. Pre and post event contextual images showing the direction of travel may also optionally be captured. The direction of travel may also be captured.

- 4 metre road width coverage, using 1392 x 512 pixel sensor
- Powerful processor
- Reading multiple number plates in a single field of view

- Embedded Linux operating system, offering standard Linux connectivity including encrypted links
- Multiple concurrent access to viewfinder and event viewer
- Hardware MJPEG streaming of the video streams (50fps, 1392 x 512) eliminating the need for a high performance frame-grabber on a PC for data acquisition

P392+/P492

P392+/P492 is a fully-integrated number plate recognition unit incorporating camera (s), illuminator and data and image processing within a single sealed enclosure. The unit comprises a monochrome camera surrounded by two sets of IR LEDs. Neology patented filter/flash technique provides suppression of headlights and bright sunlight. Field-by-field control of camera parameters allows the use of ‘triple flash’ technique to reduce any problems of plate to plate variability.

P392+/P492 can also include an optional independent, integrated, synchronous, colour camera. The colour camera can be configured to the same focal length as the monochrome camera, or to a wider field of view as required enabling ANPR (Automatic Number Plate Recognition) reads to have associated colour overview images.

The integrated number-plate recogniser incorporates the Neology ‘AutoPlate’ ANPR engine, proven in many countries worldwide. Patented real-time video triggering upon plate presence provides excellent plate detection. A vehicle presence trigger is also provided for the most demanding applications, for example taking an overview picture of a vehicle with a missing plate.

P392+/P492 can be integrated into a wide variety of systems. Wireless IP connectivity over GPRS, EDGE or 3G can be provided by fitting an optional internal modem.

IP connectivity (wired or wireless), provides a time-lock of distributed cameras to a central server via NTP.

Real-time JPEG hardware compression is provided for both IR and colour images and can be used to provide a real-time IP video stream of the traffic. This can be used to record the image stream for ANPR data verification.

P392+/P492 is fully web-enabled and can be configured and monitored from a standard web-browser. External devices such as DSRC, radar, weigh-in-motion or ticketing systems can be integrated into the system. A flexible interface allows this data to trigger the camera or be added, without synchronisation, to the data set which the camera generates for each vehicle.

- Reading multiple number plates in a single field of view.
- Embedded Linux operating system, offering standard Linux connectivity including encrypted links.
- Multiple concurrent access to viewfinder and Neology client monitor application.
- Hardware MJPEG streaming of the video streams (50fps, 752x480 - P392/P392+ or 2048x720 P492) eliminating the need for a high performance frame-grabber on a PC for data acquisition.

Assumptions

The P382, P392+ and P492 are networked cameras, and a course in networking is beyond the scope of this manual. You are expected to have a working understanding of TCP/IP networking, or be able to consult with someone who can help you with this.

Conventions

We use several typographic conventions in this manual to describe things including interaction with a computer terminal.

Commands to be typed in are described as follows:

- `command`

The name of the command.

- {required_argument}
  A required argument to the command.
- [optional_arument]
  An optional argument to the command.
- [*replace_me*]
  Text which should be replaced by you to indicate, for example, the file to be worked on

these can be combined, for example

`ls` [-l] [*directory*]
describes part of how to use the ls command in Linux.

Some text needs to be typed in exactly as given

```
type this in exactly
```

and sometimes we give some representative response from the system

```
and it will print this out,
or at least something similar
```

We will also provide links to other sections of the book, for example this section is the section called “Conventions”[2] or sometimes external references, like this one to our web homepage: http://solutions.Pips.co.uk/wps/portal/Neology/en_GB/TrafficSafety/Systems/-/AutomaticNumberPlateRecognition/. If the medium you are reading this on supports it, you may be able to click to go to the appropriate place. Obviously, this doesn't work on printed copies!

Chapter 2. Getting started

It is highly recommended that you get familiar with your P382, P392+ or P492 camera indoors prior to taking the camera to the roadside.

Connectivity

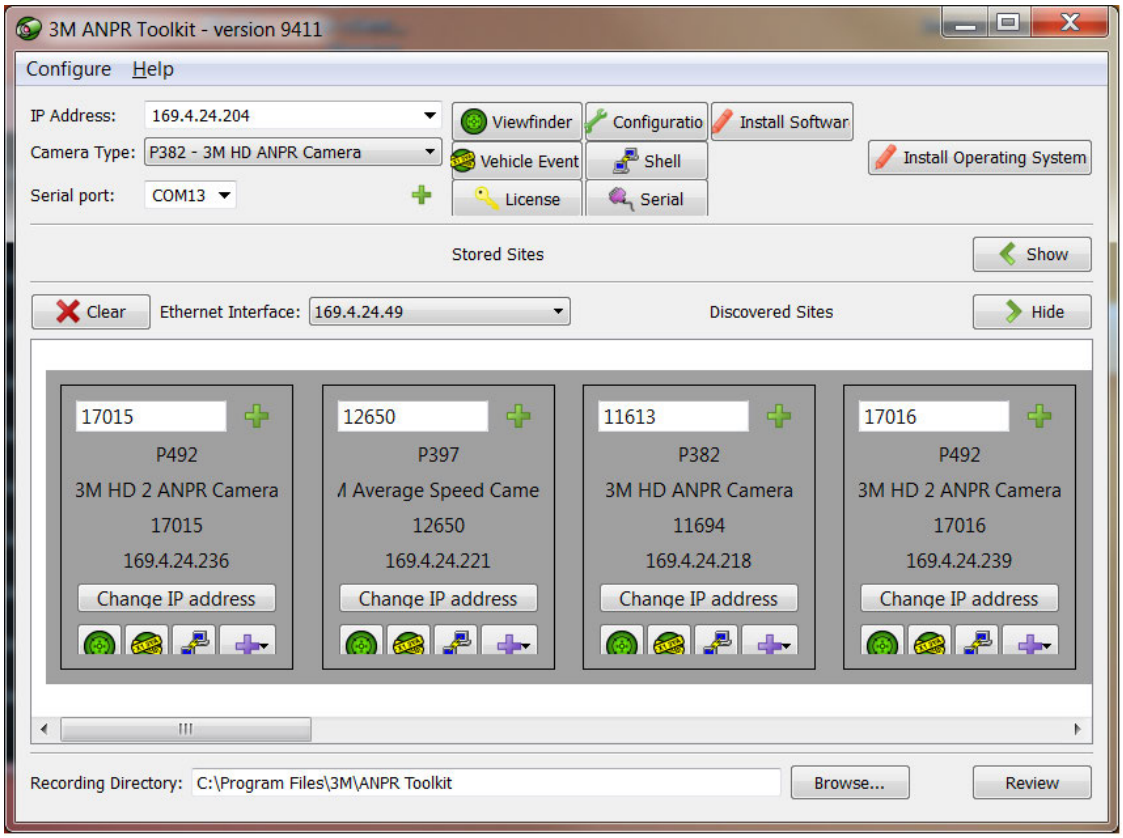
The PIPS ANPR Toolkit application should be installed on your PC, the camera connected to is often the easiest way to connect to the camera. If for some reason you cannot use this you will either need to connect via serial or via SSH and configure the network by hand the section called “Networking setup” [5].

Discovery

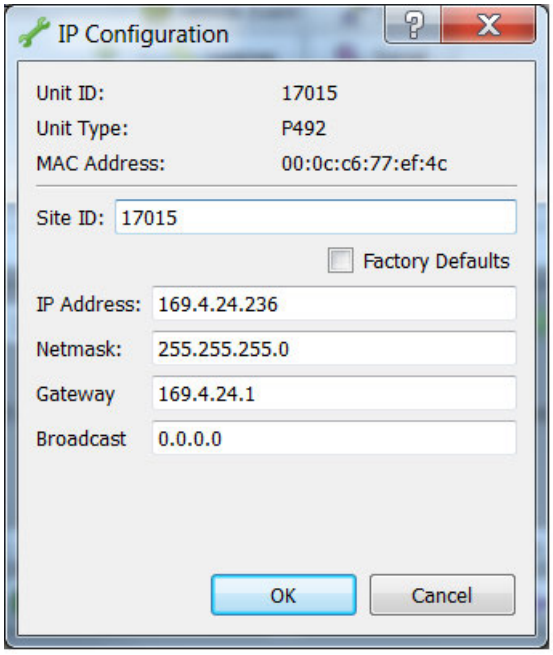
To use Discovery you will need to install the PIPS ANPR Toolkit (refer to Chapter 3, *PIPS ANPR Toolkit*[8]). If you connect the camera to the same ethernet as the PC on which you are running the toolkit and run the Toolkit you should be able to see the P382, P392+ or P492 in the list of discovered cameras.

Note

You can connect the camera to the same switch or hub, through multiple switches and hubs, or just use a cross over ethernet lead. However, the discovery protocol cannot traverse routers or gateways in your network.



If you start the application and select the network interface on your PC which matches the one to which the P382, P392+ or P492 is connected you should be able to see the camera. To identify the correct camera if you have multiple cameras on the network you should cross reference the serial number with that printed on the back of the camera. To configure the IP address of the camera click on `Change IP Address` edit the values displayed. Once you press OK, the camera will store the options and the address will change.



After around one minute you should be able to ping the camera and go on to configure the rest of the camera (see the section called “Connecting” [6]).

Serial RS-232

Full details on the console serial port are available in the hardware manual.

You will need a serial terminal, such as Kea! Term for Windows, PuTTY for Windows (see the section called “PuTTY” [142]), Minicom for Linux, or Hyperterminal for Windows (not recommended due to quirky behaviour). This should be connected at a line speed of 38,400 bits per second with 8 bits of data, no parity and 1 stop bit. This is often abbreviated to 38,400 8N1. No flow control is necessary. This should be connected to an appropriate serial port on the PC.

The system will boot into linux, eventually presenting you with the login prompt:

```
 * Starting portmap ...                                    [ ok ]
 * Mounting network filesystems ...                        [ ok ]
 * Starting sshd ...                                       [ ok ]
 * Starting vixie-cron ...                                 [ ok ]
 * Starting Webmin ...                                     [ ok ]
 * Starting local ...                                      [ ok ]


This is localhost.(none) (Linux i586 2.6.19.2) 01:42:51

localhost login:
```

If this is successful you can log in as root using by typing in **root** and then entering the root password (given in Appendix C, *Factory Defaults* [137].

Ethernet

As an alternative you can connect via ethernet. Knowledge of TCP/IP networking is assumed when reading this manual. The camera will be shipped from the factory with the settings specified in Appendix C, *Factory Defaults* [137]. If you can set up an SSH session to the camera then you do not need to use the serial port to configure the camera.

Networking setup

To use this section you are already logged into the camera via serial or SSH. You do not need to do this if you can use the IP discovery program (see the section called “Discovery”[4]). If you are not logged in, return to an earlier section to get a login prompt working. To set up networking we edit `/opt/config/current/netmon.xml`.

```
nano /opt/config/current/netmon.xml
```

Note

A guide to how to use nano is available in Appendix F, *Nano - text editor* [143]

Basic Configuration

In its basic form you can just edit the existing contents to change the IP address, netmask and gateway. The file should look like:

```
<?xml version="1.0"?>
<netmon>
  <main>
    <services>ethernet</services>
    <hostname>Camera</hostname>
  </main>
  <ethernet>
    <ip>aa.aa.aa.aa</ip>
    <netmask>bb.bb.bb.bb</netmask>
  </ethernet>
  <routes>
    <default>ethernet cc.cc.cc.cc</default>
  </routes>
</netmon>
```

Where `aa.aa.aa.aa` is the IP address you'd like to assign to the camera, `bb.bb.bb.bb` is the netmask, and `cc.cc.cc.cc` is the default gateway (remove this section if you don't want one). Under many circumstances this is acceptable.

Connecting

Although configuration is possible over the console serial port, the natural way to connect to the P382, P392+ or P492 is via the network, so we will get that working next. You may wish to skip this and move straight onto Chapter 5, *Configuration using Webmin* [13] to use the built in webserver to configure the camera.

SSH

Secure Shell or SSH is a secure networking protocol which can be used for many things, but here we will use it to provide a shell on the camera. It is running on the standard port, 22.

Many operating systems have an ssh client built in which can be invoked by typing ssh from the command line. Briefly:

`ssh` [*`user`*`@`] {*`hostname`*}
However Windows does not have one, we recommend PuTTY (see the section called “PuTTY” [142]). Any ssh client capable of SSH2 should work, feedback is welcomed on other implimentations. There is an SSH client available in Webmin under Others → SSH/Telnet Login which requires Java, but if you can see webmin I'd recommend you use that instead where possible as documented in Chapter 5, *Configuration using Webmin* [13]

Launch your ssh client to log into the camera, referring to Appendix C, *Factory Defaults* [137] for the root password. Once you have logged in you have the network working correctly and you can configure and use the camera.

You are logged into a Linux shell, and can use many normal Linux commands to navigate. A brief set of useful commands and arguments are given here.

- `ls` [-l] [*`directory`*]
  get a directory listing, similar to **dir** under DOS
- `pwd`
  display the current working directory
- `cd` {*`directory`*}

change directory to given directory. Use `..` to go up one directory

- `nano` {*`filename`*}
  edit a file. See Appendix F, *Nano - text editor* [143] for more details.
- `cat` {*`filename`*}
  quickly show a file.
- `less` {*`filename`*}
  display a file, so you can scroll up and down.
- `ftp` [*`ip_address`*]
  launch the FTP client to transfer files to or from a remote machine. TODO - xref

This is only a very brief list. A good list can be found online at http://www.ss64.com/bash/, and a comprehensive introduction which is worth reading at http://en.flossmanuals.net/command-line/. These links are not under our control and may expire with time.

Note

Manual pages are *not* installed on the camera so you cannot refer to them there. Sorry.

Restarting and Shutting Down

Due to the possibility of corrupting the filesystem, the following should as far as possible be adhered to for P382, P392+ and P492 cameras.

Restarting after changing settings

Some settings require that the camera is restarted before the change is applied. To do this, users must issue the reboot command via ssh or use the reboot button in webmin. Users must not switch off the power supply to the camera.

Switching off for planned maintenance

When wanting to switch off the camera, it is recommended that users do not simply remove the power from the camera or unplug the connector. Instead, best practice is to connect to the camera using ssh (eg. Putty) and issue the shutdown now command. After this, you should wait approximately 30 seconds for the camera to shut down, and then remove the power within a further 30 seconds.

Power-cycling

If you wish to power cycle the camera to attempt to recover from some error you should use the shutdown now command via ssh to cleanly shutdown the camera and remove power from the camera 30 seconds after issuing this command. Keep power off the camera for over 30 seconds before re-applying it.

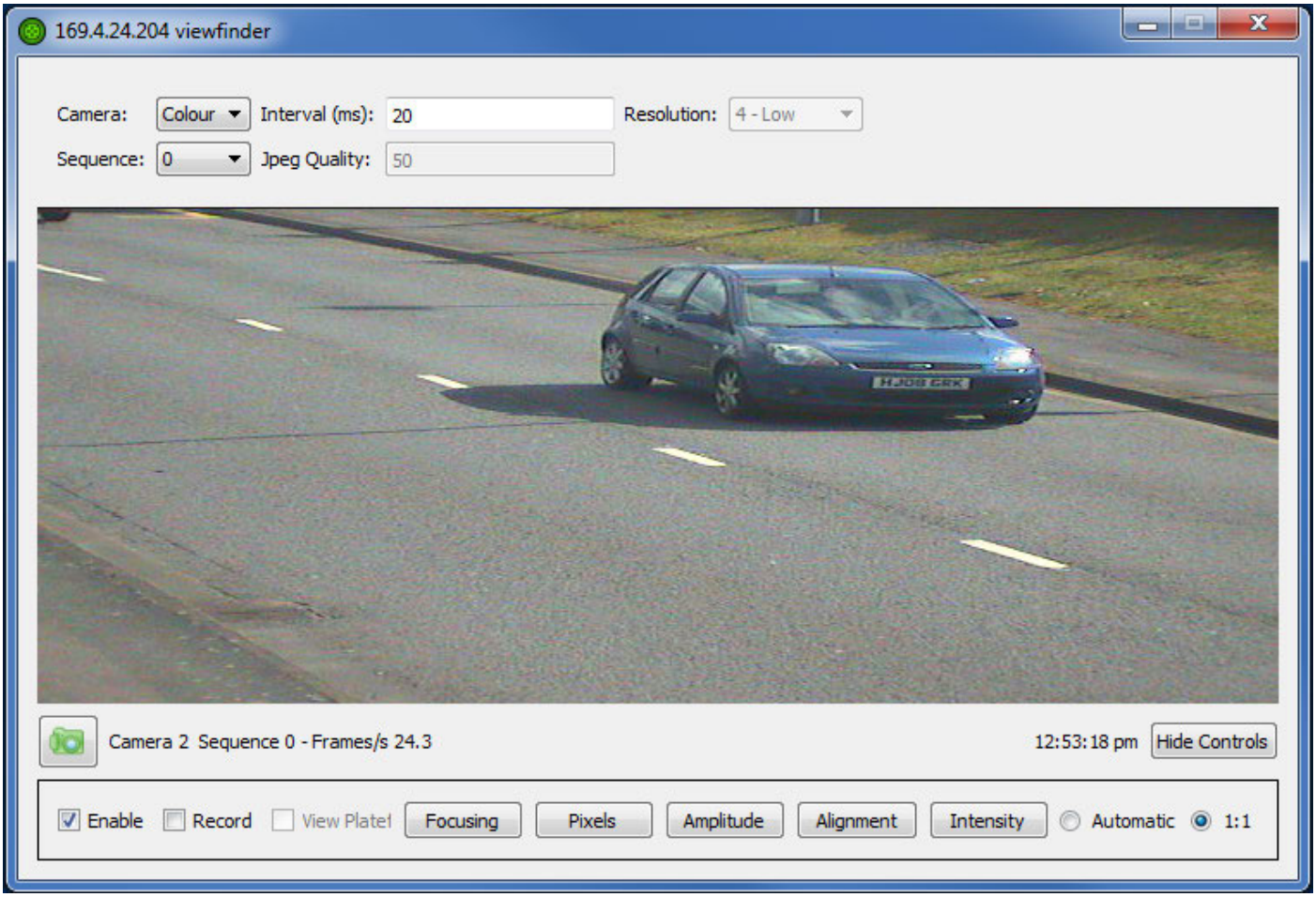
If you are unable to issue the shutdown command due to the problem you are trying to resolve, you must still observe the long delay between removing power and re-applying it – re-applying power to the camera too quickly can cause problems.

Chapter 3. PIPS ANPR Toolkit

PIPS ANPR Toolkit (see the section called “PIPS ANPR Toolkit”[142]) is a valuable tool in diagnosing, setting up and maintaining your camera. To use it, launch the viewer from the Start → PIPS → Toolkit on Windows. You can then enter the IP address of the camera you wish to view, or select it from the drop down list if you have viewed it before.

Viewfinder

By pressing the **`Viewfinder`** button, you can launch a "through the camera" viewer.



From this you can select to view either camera, and whichever sequence number of the camera you wish (which are valid is dependent on the `numentries` parameter of the camera you are viewing, by changing the drop down list. Camera 1 is the infra-red camera, 2 is the colour one.

You can speed up or slow down the image rate dependent on your PC loading and network bandwidth - if you select a low interval it will cause more loading. Quality and Resolution have no effect on a P382, P392+ or P492.

The Enable checkbox connects or disconnects the viewfinder from the camera. If the Record box is checked then the Toolkit will record the received images. The radio buttons can be used to select the size of the images as displayed by the viewfinder.

The buttons along the bottom of the window provide access to other tools. The Enable checkbox connects or disconnects the viewfinder from the camera.

Vehicle Events

By pressing the **`Vehicle Events`** button, you can launch an event viewer, which shows each vehicle that the camera detects separately.



The Enable checkbox connects or disconnects the event viewer from the camera. If the Record box is checked then the Toolkit will record the received data and images.

The radio buttons are used to select the protocol used to connect to the camera. If the PIXI protocol is selected then the Configure PIXI button can be used to select the event data and image to display. The Expand All Show More option can be used to show additional data received via PIXI.

The trigger button can be used to send a TCP trigger to the camera. The trigger message can be configured using the Trigger Config tab.

The Clear button clears the display.

Review

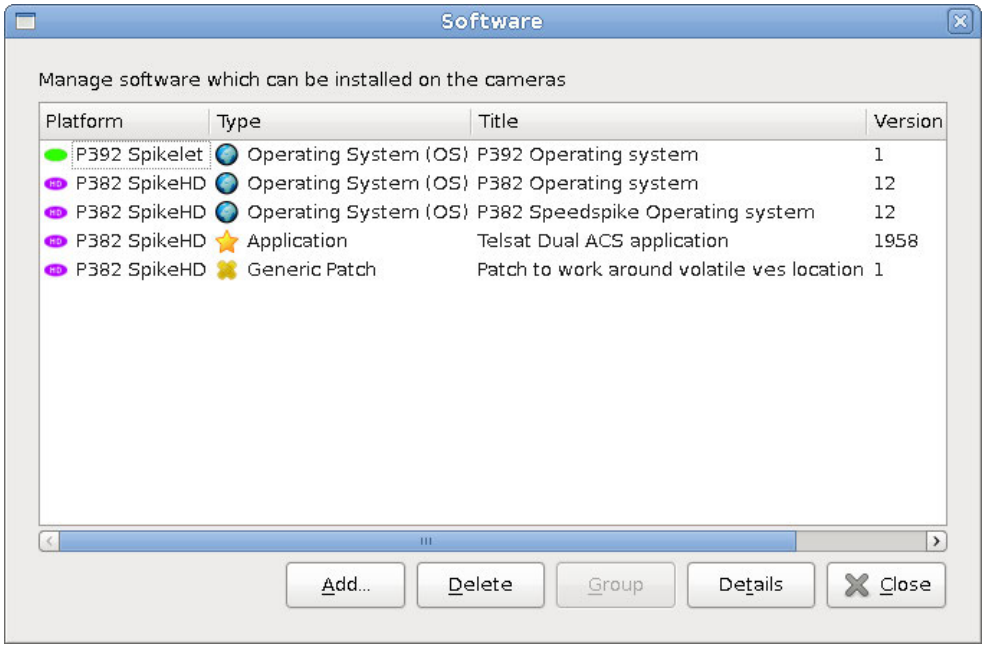
In the viewfinder and vehicle events view you can select to disable or enable updates, and also record the data using the tick boxes in the lower left hand corner. If you have recorded events you can view them by pressing the **`Review`** button. This is currently functional but not complete.

Camera Software

The toolkit allows you to maintain the software on your cameras. There are two parts to this.

Software Management

By selecting Configure → Software from the menus of the toolkit you can *locally* manage software which you can install on the camera.



- Add: You can add software distributed from PIPS to your pool of available software to install. Mostly these will be .tar.lzma files, but also the libcardet files which are number plate reading engines can be placed here. The files will be copied and stored by the application in it's own private repository..
- Delete: Delete items from your local pool of files. Any groups which depend on these files also get deleted.
- Group: Group a set of items together for ease of installation. Once grouped together a set of files will behave like a single unit and can all be installed together to ease installation. Example uses are grouping an ANPR library with an application to install the two together, or adding a patch to an os to install as one.
- Close: Close the dialogue box.

Software Installation

Software can be installed on the camera by clicking on the small orange pencil. Some basic options as to what type of installation to do, and it will ask you to enter details for the camera so that it can connect. To perform an operating system installation you must be connected via a serial port and via ethernet.

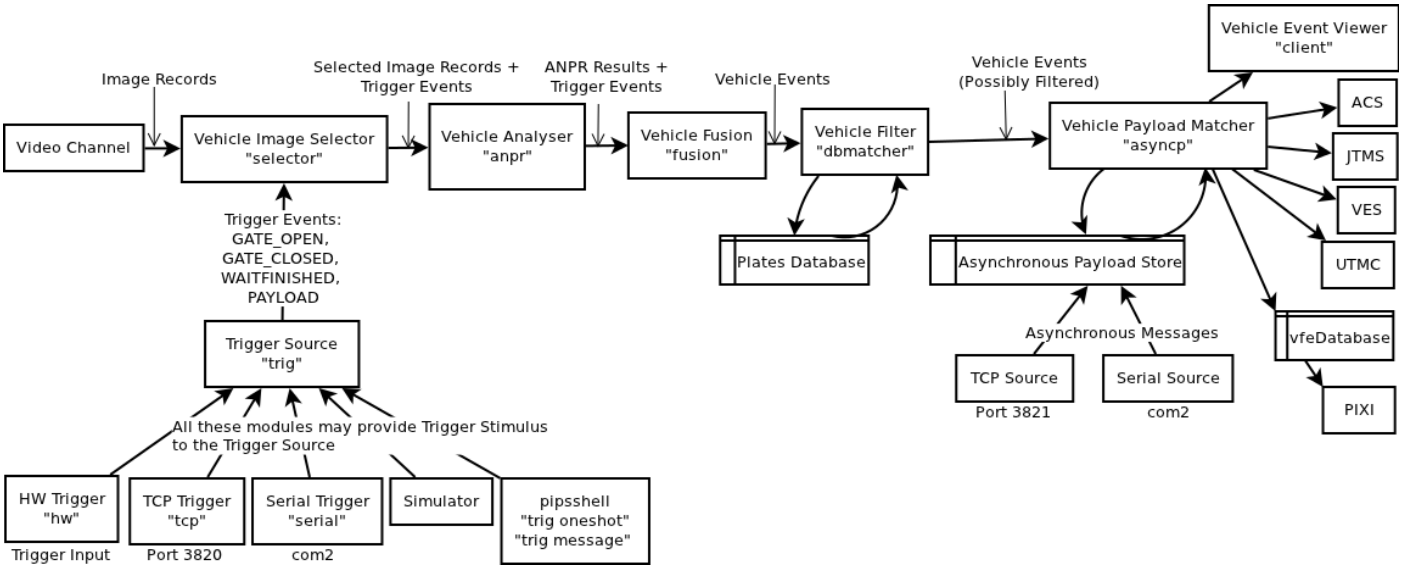
A critical concept is that some software contains a 'complete operating system' (OS) and some does not. To install a complete operating system there is quite a lot more work required, so these software packages are separated from the non-OS components

Chapter 4. Camera technical overview

The P382, P392+ and P492 are very configurable, and complex to understand. This chapter will hopefully help you to understand the internals and what they do so that you can make wise choices in setting up.

This diagram shows the objects in the system and how they fit together. Each of the individual objects is documented more completely in the section called “PIPS Shell Commands”[15], but this overview will help you put those pieces together.

Figure 4.1. Objects in the system and how they fit together.



Interfaces: Output mechanisms

The P382, P392+ and P492 have various mechanisms for outputting the resulting data from their operation and delivering it to another system for processing. This chapter describes them each in brief to allow you to understand and choose what to use. Most of these systems can be used at the same time as one another.

- *ACS* stands for Access Control System. It is a simple network delivery of image and text files via FTP or SFTP. It is designed for production use, and is recommended as a simple way to get started. This simplicity does not mean it is unsuitable for large scale deployments, but it does require a reasonable amount of bandwidth. It is very flexible in which images are available and what metadata is contained in the text file and the filenames. More detail on configuring the system is available in the section called “ACS - Access Control System (acs)”[15] and the available metadata list is Chapter 7, *Format strings* [84]. I would recommend developing with ACS unless you have a reason why you cannot use it. You can use this delivery mechanism alongside others, such as PIXI. There is a separate ACS interface document available which is for legacy systems, and not particularly relevant to the P382, P392+ and P492.

- *PIXI* is an XML based interface for collecting information and controlling all aspects of the camera. It can flexibly push and pull data from the camera, and requires no configuration on the camera. All configuration can be done via this protocol. For more complex requirements that cannot be met with ACS we would encourage the use of this protocol, which is fully documented in Chapter 8, *PIXI Protocol* [98].

- *JTMS* stands for Journey Time Measurement System. This is a relatively simple TCP/IP mechanism for delivering data suitable for measuring journey times. It uses very little bandwidth, and is not flexible for other uses. It does not provide any images. More detail on configuring this system is available in the section called “JTMS - Journey Time Measurement System (jtms)” [49]

- *VES* stands for Violation Enforcement System. This is a complex TCP/IP mechanism for delivering data suitable for many uses. It can provide images, encryption and push and pull of data. There is a separate interface document

available under an NDA (Non-Disclosure Agreement) from Neology describing this interface in detail. For new developments, unless you need encryption we'd encourage the use of PIXI instead of VES.

- *UTMC* stands for Urban Traffic Management and Control. This is a web-base mechanism for delivering data. A camera can be configured to deliver data to one or more UTMC servers. Protocol versions 1.0 and 1.2 are supported.
- *SAP* is the serial application port. This provides delivery of the plate or other metadata via the second serial port on the camera (COM2). It is flexible, but obviously cannot deliver images. More detail on configuring the system is available in the section called “SAP - Serial Application Port (sap)”[57] and the available metadata list is Chapter 7, *Format strings* [84]. You may (as with all the other output systems) use this in conjunction with other output mechanisms listed here. The serial port may only be used for one function at once.
- *Image File Output* is a debugging system, and should not be used for any production system. It places fixed filename images on the local /storage device. It may have a performance impact on the system if it is used.
- *Viewfinder* is a legacy TCP/IP protocol for viewing live images from the camera. It does not guarantee the delivery of any images. The protocol is defined in Appendix H, *Viewfinder Protocol* [145]. This is used by the Toolkit.
- *Vehicle Event Viewer* is a legacy TCP/IP protocol for viewing read images from the camera. It does not guarantee the delivery of any images and is therefore not suitable for production use. The protocol is defined in Appendix I, *Vehicle Event Viewer Protocol* [149]. This is used by the Toolkit.

Chapter 5. Configuration using Webmin

The camera provides a web administration utility called webmin. You can access this from your web browser on

`https://camera.ip.address/`

You will need to log in, referring to Appendix C, *Factory Defaults* [137] for the root password.

From here you can configure many aspects of the camera. This manual will take you through some of the more important ones. You can break the camera using some of these options, don't play unless you understand what you are doing.

Note

The web interface is only available over the https protocol, not the http protocol. Ensure you put the s in the URL

On the P392+ and P492 cameras (and only these models) should have the /backup.pl script run from the command line after any change - once that change is determined to be satisfactory. Changes include:

- New OS and application installations
- Application upgrades, Cardet upgrades
- Configuration changes

Running backup ensures that should a file system corruption be recoverable via this mechanism, the recovery will be to the last backed up state.

Camera control

Initially you will be presented with the camera application interface to configure the camera aspects of the system. This is accessible under Others → Camera Application if you need to get back to it. This manual is available from this page (indeed, you may be reading it there right now!). As well as this all the configuration options and commands are available with online help. This help is also printed for reference in Chapter 6, *PIPS ANPR Shell* [15] should you need it.

Webmin allows all of the shell parameters and commands to be accessed, as listed in Chapter 6, *PIPS ANPR Shell* [15].

You can also manage the anpr libraries from here and upload new ones by selecting Spike II (382) Application → ANPR Vehicle Analyser → Library Manager → Manage number plate libraries

Network

The network configuration is available under Networking → Networking Configuration and allows control of the IP address parameters and the hostname of the camera. It is important to set up the hostname of the camera to something useful and unique as several subsystems use it to identify the camera. The factory default is the serial number of the camera.

You can also set up an on camera firewall Networking → Linux Firewall.

Caution

Incorrectly configuring the firewall can make the camera *completely unresponsive* to network control, including webmin and SSH, requiring you to access it via the RS232 port or return it to Pips.

Mounting network disks

The P382, P392+ and P492 have the ability to save files to disk, which can be remotely mounted over NFS. Most operating systems come with an NFS server, so you can just use those. Windows users may wish to see the section

called “NFS Server on Windows”[142]. You can also mount CIFS and SMB "Windows shares" from windows servers or workstations.

NFS

Once you have a directory exported so that the camera can see it you can mount it via the System → Disk and Network Filesystems menu option. Use the drop down list to select **`Network Filesystem (nfs)`** and make sure you fill in the Mounted As, NFS Hostname and NFS Directory to be **`/storage/`*`pre-created-directory`***, the IP address of the server and the directory you have entered in `/etc/exports` respectively.

Windows shares

There are so many versions of Windows, and depending upon what you have installed it is hard to tell if you will need to use CIFS. In theory it is downwards compatible, but you definitly need it for Windows 2003 server shares. If it fails try **`Windows Networking Filesystem`** instead of **`Common Internet Filesystem`** in the instructions below.

You can mount a windows share via the System → Disk and Network Filesystems menu option. Use the drop down list to select **`Common Internet Filesystem (cifs)`** and make sure you fill in the Mounted As, Server Name and ShareName to be **`/storage/`*`pre-created-directory`***, the IP address of the server and the share name you have shared respectively. I would not attempt to use server names rather than IP addresses, although it may work for you, it may be unreliable. You will almost definitly have to fill in Login Name and Login Password details.

Chapter 6. PIPS ANPR Shell

The shell is an alternative way to access and control the camera's parameters. You can start it whilst at the linux command prompt (either via SSH or on the console serial port) by typing

```
/opt/PIPS/PIPSshell

 Welcome to the PIPS ANPR Camera shell - 127.0.0.1
 Shell Version Version 4.7.9540 built at 13:06:54 on Mar 17 2015
 (Using library version Version 9540 built at 15:02:53 on Mar 20 2015)

 Log: Mon Mar 23 11:39:24 2015 - NetUI.cpp:1179:Copyright (C) Neology UK Ltd., 2006-2013. All Rights Reserved. on 17015
 Log: Mon Mar 23 11:39:24 2015 - NetUI.cpp:1180:Serial number: 17015
 Log: Mon Mar 23 11:39:24 2015 - NetUI.cpp:1181:Version 4.7.9540 built at 15:03:29 on Mar 20 2015
 Log: Mon Mar 23 11:39:24 2015 - NetUI.cpp:1182:libPIPSLinux:Version 9540 built at 15:02:53 on Mar 20 2015
 Log: Mon Mar 23 11:39:24 2015 - NetUI.cpp:1183:Hardware: Version 647 (Cap 406), Internal JPEG Compressor, Square Platefinder, Dual JPEG, Mono flash table,
 Log: Mon Mar 23 11:39:24 2015 - NetUI.cpp:1211:Sensor 0CMV2000 (CMOS): Width: 2048, Height: 720 @ 50FPS as a Monochrome Processing sensor
 Log: Mon Mar 23 11:39:24 2015 - NetUI.cpp:1211:Sensor 1CMV2000 (CMOS): Width: 2048, Height: 720 @ 50FPS as a Colour Overview sensor
 Log: Mon Mar 23 11:39:24 2015 - NetUI.cpp:1226:uname: Linux 17015 2.6.36.2 #4 Mon Jan 27 09:49:07 Local time zone must be set--see zic manu armv5tel
 >>
```

The double chevrons are the prompt and you can type in commands here.

The model of commands is one of objects, which have properties and commands. Objects can be nested, and the sub-object's name is separated by a space from the parent. This may sound confusing, re-read it after you have read the list of commands.

- `help` [*`object`*]
  You can see a list of objects by typing **help** with no arguments, and see properties and commands of each object by giving the object name as an argument.
- `history`
  Display a list of old commands you have typed in. The command line supports full “GNU readline” command line editing and history. Basically the arrow keys work like you might hope.
- `quit`
  Leave the shell.

The complete list of objects with their properties and commands follows, but this may be out of date as with any printed material, and I suggest referring to the command line help.

The objects, properties and commands are not guaranteed to stay the same between software releases - although all functionality formally available will remain. Please consult with Neology of details on how to upgrade.

On the P392+ and P492 cameras (and only these models) should have the /backup.pl script run from the command line after any change - once that change is determined to be satisfactory.

PIPS Shell Commands

ACS - Access Control System (acs)

Available on platforms: All

The Access Control System is an output module which sends vehicle details to an external computer for processing. It will output a (configurable) number of jpeg images of the vehicle along with a text record describing the license plate event (LPR). This data may be sent as separate files, named according to the lpr_filename (with .lpr extension) and img_filename (with .jpg extension) properties. Alternatively, the data may be sent within a single packed file consisting of an XML header followed by the binary image data. In this case the filename will be the lpr_filename with a .axi extension and the LPR text record is contained withing the XML header. The XML header also contains data allowing the extraction of the image data.

Platforms	Name	Command	Default Value	Description
All	Append lpr text data	`acs set append_lpr {`*`value`*`}`	false	When using FTP/SFTP the LPR file can be appended onto an existing file if this option

Platforms	Name	Command	Default Value	Description
				is set to true. This can be used for example to create a single .csv file for all events delivered.
All	Buffer the transfer	`acs set buffer_transfers {value}`	true	Stores images in internal non-volatile storage to allow them to be transferred later should the file server be inaccssable for any reason.
All	Output Character Encoding for filenames	`acs set char_set {value}`	0	If in doubt, set this to 0. The character encoding used for strings for filepaths. 0 - ASCII-7bit 1 - ISO8859-1 2 - UTF-8 If using ASCII-7bit any special characters will be converted to nearest ASCII equivalents. If using anything other than ASCII-7, please ensure your server and other software is capable of handling the specific encoding
All	The Delivery Order	`acs set delivery_order {value}`	FIFO	The delivery order is a choise between First In First Out (FIFO) or Last In First Out (LIFO). (If switching between modes the data stored before switching will be lost). (If order is not FIFO or LIFO it will be treated as FIFO).
All	Enabled	`acs set enabled {value}`	false	Allows the ACS system to be enabled and disabled. Disable it unless you are using it.
All	Fast Ftp	`acs set fast_ftp {value}`	false	Accelerate FTP by ignoring what RFC1738 says and just transferring files directly into directories with STOR, rather than CWD first. Most off the shelf FTP servers will accept this happily, and it reduces latency.
All	Output Character Encoding For file Contents	`acs set file_char_set {value}`	0	If in doubt, set this to 0. The character encoding used for strings for LPR file contents. 0 - ASCII-7bit 1 - ISO8859-1 2 - UTF-8 If using ASCII-7bit any special characters will be converted to nearest ASCII equivalents. If using anything other than ASCII-7, please ensure your server and other software is capable of handling the specific encoding
All	Host	`acs set host {value}`		The IP address to which the files will be transferred. LPR files will be transferred last, after the jpeg files.

Platforms	Name	Command	Default Value	Description
All	Fallback Host	`acs set host2` {*value*}		Fallback IP address to which the files will be transferred if transfer to Host fails. LPR files will be transferred last, after the jpeg files.
All	Image filename	`acs set img_filename` {*value*}	%Jts%Id02u%Vm02u%Vd02u%Vh02u%Vn02u%Vs02u%Id02u,%Pps	A format string containing how to construct the image filename. You MUST put %Jtc in this string if you are outputting multiple images per event or else they WILL all have the same filename and overwrite each other. Note this property is only meaningful if transfer_packed is false
All	LPR contents	`acs set lpr_contents` {*value*}	%PNs\n%Pas\n%Pat%Jtu%Etx%Fnw	A format string containing how to construct the data you would like in the LPR file
All	LPR filename	`acs set lpr_filename` {*value*}	%Ei08X.lpr	A format string containing how to construct an LPR or AXI filename. If the transfer_packed property is set 1 (true) an AXI file is transferred. Otherwise an LPR file will sent with any required image files sent separately.
All	Maximum Disk Queue Length	`acs set nlog` {*value*}	100	The maximum number of ACS events which will be stored on the local filesystem before they are overwritten if it is not possible to contact the instation. Warning, arbitrarily setting this to a high value may fill up the device on which you are storing the files and then the system will lose the wrong data or may perform badly.
All	Password	`acs set pass` {*value*}		The password used to log in to the server or to unlock your private key, depending upon which method you're using to transfer.
All	Noread patch	`acs set patch_noread` {*value*}	false	When there is a no read there is also no patch. If you set this to true you'll get the full IR image output as a patch instead of no output.
All	Timeout	`acs set timeout` {*value*}	60	The timeout on operations over the file transfer link. NB: May not be what you expect from legacy systems.
All	Transfer overview context images	`acs set transfer_contexts` {*value*}	true	Transfer the overview context images (if any). The number and offsets of context images are configured under Contexts. Depending on the setting of transfer_packed this may be sent as a JPG file or within an AXI file
All	Transfer hazard IR images	`acs set transfer_hazard_ir` {*value*}	true	Transfer the full infra-red monochrome images. Depending on the setting of transfer_packed this may be sent as a JPG file or within an AXI file
All	Transfer hazard overview images	`acs set transfer_hazard_overview` {*value*}	true	Transfer the overview images (e.g. the colour images). Depending on the setting of transfer_packed this may be sent as a JPG file or within an AXI file
All	Transfer hazard patch images	`acs set transfer_hazard_patch` {*value*}	true	Transfer a small image of just the number plate patch. Depending on the setting of transfer_packed this may be sent as a JPG file or within an AXI file

Platforms	Name	Command	Default Value	Description
All	Transfer IR images	`acs set transfer_ir {value}`	true	Transfer the full infra-red monochrome images. Depending on the setting of transfer_packed this may be sent as a JPG file or within an AXI file
All	Transfer lpr text data	`acs set transfer_lpr {value}`	true	Transfer a text block containing metadata, called LPR data. Depending on the setting of transfer_packed this may be sent as an LPR file or within an AXI file
All	Transfer overview images	`acs set transfer_overview {value}`	true	Transfer the overview images (e.g. the colour images). Depending on the setting of transfer_packed this may be sent as a JPG file or within an AXI file
All	Transfer all data in a single AXI file	`acs set transfer_packed {value}`	false	Normally the data is transferred as separate LPR file and up to 3 image (JPG) files. Set this to true to transfer all required data in a single file (with file name lpr_filename.axi) consisting of an XML header followed by image data if required
All	Transfer patch images	`acs set transfer_patch {value}`	true	Transfer a small image of just the number plate patch. Depending on the setting of transfer_packed this may be sent as a JPG file or within an AXI file
All	Transfer path	`acs set transfer_path {value}`	%Shs/	A format string containing the path on theserver you'd like the files transferred to. This should contain / or \ as directory separators. It should end with a directory separator.
All	Transport	`acs set transport {value}`	sftp	The transport mechanism by which the system will transfer files. The options are sftp (recommended), scp, ftp, file. If you use scp the system is unable to create directories, so you must do that for it. File will deliver to the local filesystem under /storage.
All	Username	`acs set user {value}`		The username used to log in to the server

- `acs clearStats`

  Resets all Statistics. Platforms: All.

  Resets all Statistics

- `acs diskq_flush`

  Empty the Disk Queue. Platforms: All.

  All ACS events currently stored in the persistant Disk Queue will be deleted and will not be recoverable. Use this with care.

- `acs diskq_length`

  Length of Disk Queue. Platforms: All.

The number of ACS events stored in the persistant Disk Queue will be reported. Note this value may be non zero even if buffer_transfers is false. If buffer_transfers is false, the system still uses the disk queue, it just wont store items between reboots.

- `acs stats`

  Statistics. Platforms: All.

  Statistics for debugging

Specific Filenames (acs filenames)

Available on platforms: All

If you wish to have more control over the image filenames of the ACS output this section is for you, otherwise you can ignore it. You can specify filenames for each individual image that ACS outputs. If you leave the filenames blank then the standard ACS configuration will apply for that file. If you specify anything for a file, that file will be output with that filename. It will have the transfer_path prepended like with the standard naming scheme. If you want to output to different directories for each file, you can specify the path as part of the filename. If the transfer_path is blank you could output each file to a completely different directory. You cannot specify the lpr filename here as it is already available as a solo format string in the main ACS section.

Platforms	Name	Command	Default Value	Description
All	Hazard Full IR Filename	`acs filenames set haz_ir_filename {value}`		The format string used for the filename for the hazard full IR images.
All	Hazard Overview Filename	`acs filenames set haz_oview_filename {value}`		The format string used for the filename for the hazard overview images.
All	Hazard Patch Filename	`acs filenames set haz_patch_filename {value}`		The format string used for the filename for the hazard patch images.
All	Full IR Filename	`acs filenames set ir_filename {value}`		The format string used for the filename for the full IR images.
All	Overview Filename	`acs filenames set oview_filename {value}`		The format string used for the filename for the overview images.
All	Patch Filename	`acs filenames set patch_filename {value}`		The format string used for the filename for the patch images.

Context 1 (acs filenames context1)

Available on platforms: All

If you wish to have more control over the image filenames of the ACS output this section is for you, otherwise you can ignore it. You can specify filenames for each individual image that ACS outputs. If you leave the filenames blank then the standard ACS configuration will apply for that file. If you specify anything for a file, that file will be output with that filename. It will have the transfer_path prepended like with the standard naming scheme. If you want to output to different directories for each file, you can specify the path as part of the filename. If the transfer_path is blank you could output each file to a completely different directory. You cannot specify the lpr filename here as it is already available as a solo format string in the main ACS section.

Platforms	Name	Command	Default Value	Description
All	Contexts Filename			

Platforms	Name	Command	Default Value	Description
		`acs filenames context1 set filename {`*`value`*`}`		The format string used for the filename for this context images.

Context 2 (acs filenames context2)

Available on platforms: All

If you wish to have more control over the image filenames of the ACS output this section is for you, otherwise you can ignore it. You can specify filenames for each individual image that ACS outputs. If you leave the filenames blank then the standard ACS configuration will apply for that file. If you specify anything for a file, that file will be output with that filename. It will have the transfer_path prepended like with the standard naming scheme. If you want to output to different directories for each file, you can specify the path as part of the filename. If the transfer_path is blank you could output each file to a completely different directory. You cannot specify the lpr filename here as it is already available as a solo format string in the main ACS section.

Platforms	Name	Command	Default Value	Description
All	Contexts Filename	`acs filenames context2 set filename {`*`value`*`}`		The format string used for the filename for this context images.

Context 3 (acs filenames context3)

Available on platforms: All

If you wish to have more control over the image filenames of the ACS output this section is for you, otherwise you can ignore it. You can specify filenames for each individual image that ACS outputs. If you leave the filenames blank then the standard ACS configuration will apply for that file. If you specify anything for a file, that file will be output with that filename. It will have the transfer_path prepended like with the standard naming scheme. If you want to output to different directories for each file, you can specify the path as part of the filename. If the transfer_path is blank you could output each file to a completely different directory. You cannot specify the lpr filename here as it is already available as a solo format string in the main ACS section.

Platforms	Name	Command	Default Value	Description
All	Contexts Filename	`acs filenames context3 set filename {`*`value`*`}`		The format string used for the filename for this context images.

Context 4 (acs filenames context4)

Available on platforms: All

If you wish to have more control over the image filenames of the ACS output this section is for you, otherwise you can ignore it. You can specify filenames for each individual image that ACS outputs. If you leave the filenames blank then the standard ACS configuration will apply for that file. If you specify anything for a file, that file will be output with that filename. It will have the transfer_path prepended like with the standard naming scheme. If you want to output to different directories for each file, you can specify the path as part of the filename. If the transfer_path is blank you could output each file to a completely different directory. You cannot specify the lpr filename here as it is already available as a solo format string in the main ACS section.

Platforms	Name	Command	Default Value	Description
All	Contexts Filename			

Platforms	Name	Command	Default Value	Description
		`acs filenames context4 set filename {`*`value`*`}`		The format string used for the filename for this context images.

Context 5 (acs filenames context5)

Available on platforms: All

If you wish to have more control over the image filenames of the ACS output this section is for you, otherwise you can ignore it. You can specify filenames for each individual image that ACS outputs. If you leave the filenames blank then the standard ACS configuration will apply for that file. If you specify anything for a file, that file will be output with that filename. It will have the transfer_path prepended like with the standard naming scheme. If you want to output to different directories for each file, you can specify the path as part of the filename. If the transfer_path is blank you could output each file to a completely different directory. You cannot specify the lpr filename here as it is already available as a solo format string in the main ACS section.

Platforms	Name	Command	Default Value	Description
All	Contexts Filename	`acs filenames context5 set filename {`*`value`*`}`		The format string used for the filename for this context images.

Context 6 (acs filenames context6)

Available on platforms: All

If you wish to have more control over the image filenames of the ACS output this section is for you, otherwise you can ignore it. You can specify filenames for each individual image that ACS outputs. If you leave the filenames blank then the standard ACS configuration will apply for that file. If you specify anything for a file, that file will be output with that filename. It will have the transfer_path prepended like with the standard naming scheme. If you want to output to different directories for each file, you can specify the path as part of the filename. If the transfer_path is blank you could output each file to a completely different directory. You cannot specify the lpr filename here as it is already available as a solo format string in the main ACS section.

Platforms	Name	Command	Default Value	Description
All	Contexts Filename	`acs filenames context6 set filename {`*`value`*`}`		The format string used for the filename for this context images.

Context 7 (acs filenames context7)

Available on platforms: All

If you wish to have more control over the image filenames of the ACS output this section is for you, otherwise you can ignore it. You can specify filenames for each individual image that ACS outputs. If you leave the filenames blank then the standard ACS configuration will apply for that file. If you specify anything for a file, that file will be output with that filename. It will have the transfer_path prepended like with the standard naming scheme. If you want to output to different directories for each file, you can specify the path as part of the filename. If the transfer_path is blank you could output each file to a completely different directory. You cannot specify the lpr filename here as it is already available as a solo format string in the main ACS section.

Platforms	Name	Command	Default Value	Description
All	Contexts Filename			

Platforms	Name	Command	Default Value	Description
		`acs filenames context7 set filename {`*`value`*`}`		The format string used for the filename for this context images.

Context 8 (acs filenames context8)

Available on platforms: All

If you wish to have more control over the image filenames of the ACS output this section is for you, otherwise you can ignore it. You can specify filenames for each individual image that ACS outputs. If you leave the filenames blank then the standard ACS configuration will apply for that file. If you specify anything for a file, that file will be output with that filename. It will have the transfer_path prepended like with the standard naming scheme. If you want to output to different directories for each file, you can specify the path as part of the filename. If the transfer_path is blank you could output each file to a completely different directory. You cannot specify the lpr filename here as it is already available as a solo format string in the main ACS section.

Platforms	Name	Command	Default Value	Description
All	Contexts Filename	`acs filenames context8 set filename {`*`value`*`}`		The format string used for the filename for this context images.

Event Filter (acs filter)

Available on platforms: All

Platforms	Name	Command	Default Value	Description
All	Tag Regex	`acs filter set tag_regex {`*`value`*`}`	.*	

Using ACS

ACS uses various different file transfer protocols. It is recommended that you use SFTP as it is secure, can create directories, and has less network overhead than the FTP protocol. Historically ACS used the FTP protocol and that is also still possible. A suitable FTP server is required (FileZilla server is recommended for MS Windows platforms). SCP is also supported, but most platforms which work with SCP also work with SFTP which is able to create directories, wheras SCP is not.

Based on a number plate read event, ACS can transfer the following information:

- LPR data which consists of text metadata regarding the plate read event. LPR data will be transferred if **`transfer_lpr`** is set. The exact content of LPR text may be specified with the **`lpr_contents`** format string.
- A plate patch image in jpeg format. A patch image will be transferred if **`transfer_patch`** is set.
- A complete Infrared (IR) image in jpeg format. An IR image will be transferred if **`transfer_ir`** is set.
- A colour overview image in jpeg format. An overview image will be transferred if **`transfer_overview`** is set.

This ACS event data data may be transferred as separate files (up to 3 jpeg image files and an LPR textfile). These files are named according to the **`lpr_filename`** and **`image_filename`** properties.

Alternatively, if the **`transfer_packed`** property is set, all the required data is packed into a single AXI file. An AXI file consists of an XML header section followed by binary image data for whichever of the images are required. The advantage of using a packed AXI file is that there is less transfer overhead (a particular problem with normal FTP, a single transfer vs. up to four separate transfers) and may simplify processing at the receiver (no need to correlate the multiple files that relate to a single plate read event). One disadvantage with the packed format is that the file needs to be unpacked. However, the format is very simple (see the section called “ACS Event XML Schema”[23]) and should be easy to decode.

Older ACS systems only ever transferred separate files. Thus, for compatibility reasons, it may be necessary to disable the **`transfer_packed`** property.

Authentication

If you are using SFTP or SCP you can authenticate with your server in two ways.

- Conventional username and password, in a similar way to keyboard authentication. This is generally accepted as less secure, but is trivial to setup and may be good enough. To do this just set the **`user`** and **`pass`** properties and log in with those. This is the only option with conventional FTP.
- Using an SSH public key. You will need to create a public/private key pairing and install both of these onto your camera as `/opt/config/current/key_acs` and `/opt/config/current/key_acs.pub`. You can do this on the camera using **`ssh-keygen -t rsa`**. You must also give the public key to the server to allow it to authenticate - on a conventional openssh system this would be done by appending the public key into `~/.ssh/authorized_keys2` for the user you're going to transfer as. Once this is done you set up the user in the **`user`** field and if your private key has a passphrase enter that into the **`pass`** property.

ACS Event XML Schema

The packed AXI file format consists of an XML header followed by binary data for whatever images are required. The XML header part is a NULL terminated string. Binary data starts immediately after the NULL character. This XML header data contains the LPR text (if required) and, for each required image, the offset from the start of the binary data to the start of the image and the image length. This information is sufficient to extract the individual jpeg images.

The XML schema for the header is as follows:

axi.xsd

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
  <xs:element name="acs_event_header">
    <xs:complexType>
      <xs:sequence>
        <xs:element minOccurs="0" maxOccurs="1" ref="lpr"/>
        <xs:element minOccurs="0" maxOccurs="1" ref="patch"/>
        <xs:element minOccurs="0" maxOccurs="1" ref="full"/>
        <xs:element minOccurs="0" maxOccurs="1" ref="overview"/>
        <xs:element minOccurs="0" maxOccurs="1" ref="hazardPatch"/>
        <xs:element minOccurs="0" maxOccurs="1" ref="hazardFull"/>
        <xs:element minOccurs="0" maxOccurs="1" ref="hazardOverview"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="lpr" type="xs:string"/>
  <xs:element name="patch">
    <xs:complexType>
      <xs:attribute name="length" use="required" type="xs:integer"/>
      <xs:attribute name="offset" use="required" type="xs:integer"/>
    </xs:complexType>
  </xs:element>
  <xs:element name="full">
    <xs:complexType>
      <xs:attribute name="length" use="required" type="xs:integer"/>
      <xs:attribute name="offset" use="required" type="xs:integer"/>
    </xs:complexType>
  </xs:element>
  <xs:element name="overview">
    <xs:complexType>
      <xs:attribute name="length" use="required" type="xs:integer"/>
      <xs:attribute name="offset" use="required" type="xs:integer"/>
    </xs:complexType>
  </xs:element>
  <xs:element name="hazardPatch">
    <xs:complexType>
      <xs:attribute name="length" use="required" type="xs:integer"/>
      <xs:attribute name="offset" use="required" type="xs:integer"/>
    </xs:complexType>
  </xs:element>
  <xs:element name="hazardFull">
    <xs:complexType>
      <xs:attribute name="length" use="required" type="xs:integer"/>
      <xs:attribute name="offset" use="required" type="xs:integer"/>
    </xs:complexType>
  </xs:element>
  <xs:element name="hazardOverview">
    <xs:complexType>
      <xs:attribute name="length" use="required" type="xs:integer"/>
      <xs:attribute name="offset" use="required" type="xs:integer"/>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

ANPR Vehicle Analyser (anpr)

Available on platforms: All

This module processes images to read the number plates in them.

Platforms	Name	Command	Default Value	Description
All	Cardet Debugging	`anpr set debugging {value}`	false	Make the engine output debugging files to dlldeb
All	Prioritse Hazard	`anpr set hazard_priority {value}`	false	Only relevant if hazard plate reading engine is loaded. If set true, will try harder to read hazard plates and may therefore improve hazard reading performance. However setting true may cause overall performance to deteriorate slightly.
All	Maximum mean character height	`anpr set max_char {value}`	32	Maximum mean character height above which an exception will be generated
All	Maximum mean horizontal plate angle	`anpr set max_mhpa {value}`	5	Maximum mean horizontal plate angle above which an exception will be generated
All	Maximum mean vertical plate angle	`anpr set max_mvpa {value}`	10	Maximum mean vertical plate angle above which an exception will be generated
All	Maximum Syntax Error Ratio	`anpr set max_ser {value}`	40	The maximum syntax error ratio (as percentage) above which an exception will be generated
All	Minimum mean character height	`anpr set min_char {value}`	16	Minimum mean character height below which an exception will be generated
All	Minimum Mean Plate Quality	`anpr set min_mpq {value}`	2000	The minimum mean plate quality below which an exception will be generated
All	Minimum mean tag confidence	`anpr set min_mtc {value}`	90	Minimum mean tag confidence below which an exception will be generated.
All	Square Plates	`anpr set square {value}`	false	Tell the engine that you have a high number of square plates and to try harder to read these. If you have only a small number of these plates this may degrade overall performance. The system will still read long plates.
All	Threshold of Confidence	`anpr set threshold {value}`	60	The minimum read confidence that the system will pass on to further modules. Set this to zero to pass through images from triggers (in an externally triggered system) when the trigger fires even if we didn't manage to read any number plate.
All	Trigger Passthrough	`anpr set trigger_pass {value}`	true	If selected the system will always pass through an image during a trigger, guaranteeing that you see a picture of a vehicle from which we couldn't read anything when you trigger. This overrides the threshold for triggers only.

Platforms	Name	Command	Default Value	Description
All	White On Black	`anpr set whiteonblack {value}`	false	Tell the engine that you have a high number of white on black plates and to try harder to read these. If you have only a small number of these plates this may degrade overall performance. The system will still read black on white plates.

- `anpr clearstats`

  Clears Cumulative statistics. Platforms: All.

  Resets all statistics collection variables to initial values

- `anpr stats`

  Cumulative statistics. Platforms: All.

  Provides cumulative statistics of longterm vehicle processing

Lane Identification Control (anpr laneId)

Available on platforms: All

This control is for determining what lane a number plate is travelling in. There is a maximum of four lanes which is designated by the lanes property. There are a lines which is used to differentiate between different lanes. The user will need to ensure that the lines do not cross, if they do no lane information will be provided within the region, a programatic method to prevent crossing has not been provided to enhance the users ability to setup the lane id system.

Platforms	Name	Command	Default Value	Description
All	Lane 1 name	`anpr laneId set Lane1Name {value}`	1	This is the lane which is the left of line 1
All	Lane 2 name	`anpr laneId set Lane2Name {value}`	2	This is the lane which is the left of line 2 and right of line 1
All	Lane 3 name	`anpr laneId set Lane3Name {value}`	3	This is the lane which is the left of line 3 and right of line 2
All	Lane 4 name	`anpr laneId set Lane4Name {value}`	4	This is the lane which is the right of line 3
All	Bottom X position of line 1	`anpr laneId set Line1bottomX {value}`	2048	This is the position of line 1 at the bottom of the image.
All	Top X position of line 1	`anpr laneId set Line1topX {value}`	2048	This is the position of line 1 at the top of the image
All	Bottom X position of line 2	`anpr laneId set Line2bottomX {value}`	2048	This is the position of line 2 at the bottom of the image.
All	Top X position of line 2	`anpr laneId set Line2topX {value}`	2048	This is the position of line 2 at the top of the image
All	Bottom X position of line 3	`anpr laneId set Line3bottomX {value}`	2048	This is the position of line 3 at the bottom of the image.
All	Top X position of line 3	`anpr laneId set Line3topX {value}`	2048	This is the position of line 3 at the top of the image
All	Enables the lane identification system	`anpr laneId set enabled {value}`	false	Enables the lane identification system.

Platforms	Name	Command	Default Value	Description
All	Sets the number of lanes	`anpr laneId set lanes` {*value*}	1	Set the number of lanes the system will recognise

Library Manager (anpr library)

Available on platforms: All

Management of which library you are using for plate recognition. Different libraries are tuned for different regions of the world to enhance recognition of local plates correctly. Using the correct engine for the location and type of plates you are likely to see is important to ensure good read rates. The libraries live in /opt/pips/

Platforms	Name	Command	Default Value	Description
All	Colour Plate Reading Engine	`anpr library set colour` {*value*}	none	The filename of the libcardet colour plate reading engine in use
All	Plate Reading Engine	`anpr library set engine` {*value*}	none	The filename of the libcardet plate reading engine in use
All	Hazard Plate Reading Engine	`anpr library set hazard` {*value*}	none	The filename of the libcardet Hazard plate reading engine in use

- `anpr library list`

  List. Platforms: All.

  List all available engines on this camera

Overview Crop Control (anpr overviewCrop)

Available on platforms: All

Control the overview crop

Platforms	Name	Command	Default Value	Description
All	Overlay Overlay Crop	`anpr overviewCrop set enabled` {*value*}	false	Enables the overlay crop. This creates smaller, cropped, overview images. Ensure that the FocalLength values for cam1 and cam2 are correct if this feature is enabled.
All	Image Height	`anpr overviewCrop set height` {*value*}	480	The height in pixels of the area cropped from the overview image. A value of 0 will cause the images to be cropped to the height of the plate.
All	Horizontal Offset	`anpr overviewCrop set horizontalOffset` {*value*}	-240	The offset in pixels from left edge of the plate to the left edge of the cropped overview image. A negative value indicates that the left edge of the image is to the left of the plate. A positive value indicates that the left edge of the image is to the right of the plate.
All	Horizontal Scale	`anpr overviewCrop set horizontalScale` {*value*}	0	Reduces the width of the cropped image: 0, No scaling; 1, Half Scale; 2, Quarter Scale.
All	Vertical Offset	`anpr overviewCrop set verticalOffset` {*value*}	-400	The offset in pixels from top edge of the plate to the top edge of the cropped overview

Platforms	Name	Command	Default Value	Description
				image. A negative value indicates that the top edge of the image is above the plate. A positive value indicates that the top edge of the image is below the plate.
All	Vertical Scale	`anpr overviewCrop set verticalScale {value}`	0	Reduces the height of the cropped image: 0, No scaling; 1, Half Scale; 2, Quarter Scale.
All	Image Width	`anpr overviewCrop set width {value}`	752	The width in pixels of the area cropped from the overview image. A value of 0 will cause the images to be cropped to the width of the plate.

Asynchronous Payload Matching (asyncp)

Available on platforms: All

The payload matching system allows the system to match up Vehicle Events with asynchronously provided payloads (user supplied data).

This data may then be included with the final event sent to the user.

See also the %PA format specifier.

Platforms	Name	Command	Default Value	Description
All	Acknowledge	`asyncp set ack_enabled {value}`	false	To enable/disable the generation of acks. If enabled the whole message, exactly as sent, will be echoed back to you.
All	Serial Baud Rate	`asyncp set baud {value}`	115200	The serial port baud rate. For changes to take effect, disable then re-enable. Valid values 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400
All	Binary	`asyncp set binary {value}`	false	If set true, will allow binary data. Otherwise data must be XML legal ASCII
All	Drop unmatched	`asyncp set drop_unmatched {value}`	false	Allows the vehicle events to be surpressed if no matching payload is found.
All	Enabled	`asyncp set enabled {value}`	false	Allows the Filter system to be enabled and disabled. Disable it unless you are using it.
All	Event Match Regex	`asyncp set eventmatch_regex {value}`		A regular expression (matching the Perl Regular Expression Syntax). If set to anything other than an empty string, it will be used to select an appropriate matching payload for the read event. If set it will be used instead of time proximity. (Selecting by time proximity within the time window is the default behaviour). Unlike the above regex in that this one can use format specifiers to extract information from the vehicle read event - to match to the async payloads.

Platforms	Name	Command	Default Value	Description
All	Match Window in milliseconds	`asyncp set matchwindow {value}`	1000	The maximum period that the times of the async payload and vehicle event may differ and still be considered for matching
All	Maximum age	`asyncp set max_age {value}`	20000	The maximum time in milliseconds that payloads are kept in memory.
All	Payload Regular Expression	`asyncp set payload_regex {value}`	(.*)\n	A regular expression (matching the Perl Regular Expression Syntax) that the incoming string must match in order for a payload to be recognised and stored. The actual payload will be the concatination of those parts of the incoming string that match any subexpressions in the regex, as specified by ()'s. If no ()'s are present in the payload_regex, then the entire incoming string, that matches the regex, will be used as the actual stored payload. Note: If the binary flag is set to false then a payload may only contain XML legal ASCII. If it contains any illegal characters, the entire string will be discarded.
All	TCP Port	`asyncp set port {value}`	3821	The TCP port to be used to accept incoming connections.
All	Message Source	`asyncp set source {value}`	tcp	The source of the messages. Set to either tcp or serial

- `asyncp statistics`

  Cumulative statistics. Platforms: All.

  Provides cumulative statistics of longterm vehicle filter processing

BOF2 protocol (bof2)

Available on platforms: All

The module implements the BOF 2.2 Protocol

Platforms	Name	Command	Default Value	Description
All	Authenticate using username and password	`bof2 set authenticate {value}`	false	Authenticate using username and password
All	Camera Identifier	`bof2 set cameraId {value}`	1	Specified through the use of the a format string, if the value of the format string does not evaluate between -32768 and 32767 it will be 0.
All	Delivery Order	`bof2 set delivery_order {value}`	FIFO	The order in which events can be delivered, First in First Out (FIFO) or Last In First Out (LIFO). NB: Switching between modes deletes all data queued for delivery.

Platforms	Name	Command	Default Value	Description
All	Enabled	`bof2 set enabled {value}`	false	Allows the BOF2 system to be enabled and disabled. Disable it unless you are using it.
All	Feed Identifier	`bof2 set feedId {value}`	1	Also known as Force ID. Specified through the use of the a format string, if the value of the format string does not evaluate between -32768 and 32767 it will be 0.
All	Host	`bof2 set host {value}`	192.168.1.1:8080	IP address and port of the instation which will receive the BOF2.2 data.
All	Event Queue Size	`bof2 set nlog {value}`	100	The maximum number of events which will be enqueued for delivery. This delivery module uses the VFE Database, so events will get deleted based upon the rules set within the VFE database. If an event has been deleted we will continue on to the next in the queue
All	Camera Pan	`bof2 set pan {value}`	0	For CCTV cameras.
All	Password	`bof2 set password {value}`		Password for BOF transport user
All	Path	`bof2 set path {value}`	/bof2/services/InputCaptureWebService	The path on the http url.
All	Camera Preset Position	`bof2 set position {value}`	0	Used to indicate direction of travel on multi-use CCTV cameras
All	Send overview	`bof2 set send_overview {value}`	true	Allows sending of overview image to the BOF2 system to be enabled and disabled.
All	Send Patch	`bof2 set send_patch {value}`	true	Allows sending of patch image to the BOF2 system to be enabled and disabled.
All	Public Signature Of Sender	`bof2 set signature {value}`		Format not specified in BOF 2.2 spec, left as std::string for users
All	Source Identifier	`bof2 set sourceId {value}`	1	Specified through the use of the a format string, if the value of the format string does not evaluate between -32768 and 32767 it will be 0.
All	Camera Tilt	`bof2 set tilt {value}`	0	For CCTV cameras.
All	BOF2.2 transport	`bof2 set transport {value}`	HTTPS	HTTP or HTTPS
All	username	`bof2 set username {value}`	Unattended	Username for BOF user
All	Verify Peer	`bof2 set verifyPeer {value}`	true	Allows the verification of the BOF2 server certificate to be disabled when set to false.
All	Camera Zoom	`bof2 set zoom {value}`	0	For CCTV cameras.

- `bof2 clearStats`

  Resets all Statistics. Platforms: All.

  Resets all Statistics

- `bof2 diskq_flush`

  Empty the Disk Queue. Platforms: All.

All BOF events currently stored in the persistant Disk Queue will be deleted and will not be recoverable. Use this with care.

- `bof2 diskq_length`

  Length of Disk Queue. Platforms: All.

  The number of BOF events stored in the persistant Disk Queue will be reported.

- `bof2 stats`

  Statistics. Platforms: All.

  Statistics for debugging

IR Camera (cam1)

Available on platforms: All

Controls for managing the camera and images that it takes

Platforms	Name	Command	Default Value	Description
All	Sensor ADC gain	`cam1 set ADCgain {value}`	52	This sets the adc gain for the Overview sensor Warning don't alter this value. When finished commit will need to be run.
All	Lens Focal Length	`cam1 set FocalLength {value}`	35	The focal length of the lens in front of the IR sensor. This value must be set correctly if overview cropping is in use
All	Platefinder Regions of Interest Coordinates	`cam1 set ROICoordinates {value}`	(0,0),(2048,0),(2048,720),(0,720)	Region polygon(s) co-ordinates clockwise from Top Left. Region polygons are separated by a semi-colon.
All	Platefinder Regions of Interest	`cam1 set ROIEnabled {value}`	false	Sets whether Region of Interest polygon(s) is used or not.
All	Sensor Vramp	`cam1 set Vramp {value}`	109	This sets the Vramp value for the Overview sensor Warning don't alter this value. When finished commit will need to be run.
All	Points at front of vehicles	`cam1 set front_facing {value}`	true	Sets whether the camera is reading from the front of the vehicle. If you have bi-directional traffic set this false.
All	Horizontal Scale	`cam1 set horizontalScale {value}`	0	This will control the scale the channel (but not the plate patch), 0 = no scaling, 1 = half scaling, 2 = quarter scaling
All	Number of Exposure entries cycled in a sequence	`cam1 set numentries {value}`	0	Number of exposure entries cycled through. Set to 1 to disable exposure sequencing, just using the first entry. Otherwise each exposure will be taken with a different entry from the table.
All	Platefinder bottom plate width	`cam1 set platewidth_b {value}`	180	Sets the plate width for this channel in pixels at the bottom of the image. Try to get your plates to be between 180 and 220 pixels wide (for UK style plates), or 140-180 pixels (for US style plates). Getting this right will improve plate recognition.

Platforms	Name	Command	Default Value	Description
All	Platefinder top plate width	`cam1 set platewidth_t {value}`	180	Sets the plate width for this channel in pixels at the top of the image. Try to get your plates to be between 180 and 220 pixels wide (for UK style plates), or 140-180 pixels (for US style plates). Getting this right will improve plate recognition.
All	Fields of Retard	`cam1 set retard {value}`	0	Sets the number of fields of retard for this video channel. The video will be delayed by this number of fields .This feature is only useful in triggered systems. It adds flexibility by allowing compensation for a chronically late trigger. It is suggested that this feature only be used as a last resort.
All	Sharpening mode	`cam1 set sharpening {value}`	1	ENGINEERING USE ONLY:Then enables image sharpening - mode 0 off, mode 1 old sharpening mode, mode 2 a new sharpening mode
All	Vertical Scale	`cam1 set verticalScale {value}`	0	This will control the scale the channel (but not the plate patch), 0 = no scaling, 1 = half scaling, 2 = quarter scaling

- `cam1 commit`

  Commit the new ADC gain and V Ramp settings. Platforms: All.

  Commits the ADC gain and V Ramp to nand flash

Exposure Controller (cam1 exposure)

Available on platforms: All

An automated controller for the exposures on the camera. It will run with our triple flash system and adjust the sequence entries for shutter and gain appropriatly to optimise the image for plate reading.

Platforms	Name	Command	Default Value	Description
All	Brightness cutoff	`cam1 exposure set bright_cutoff {value}`	5	This value determines the percentage of pixels in the plate which differentiate between an underexposed and a correctly exposed plate .If brightness control is making your plates too bright lower this value or vice-versa. Also see the Brightness overexposure setting and set the two in parallel.
All	Exposure control enabled	`cam1 exposure set enabled {value}`	true	Allows you to switch the exposure controller on or off. It is recommended to use this system, if you disable it you should manually set up the exposure sequence.
All	Good DB Value	`cam1 exposure set good_db_value {value}`	2000	Not normally set by user except for testing purposes (it is automatically updated). This

Platforms	Name	Command	Default Value	Description
				determines at what brightness the system starts after a reboot. This value will be used to adjust the brightness when there is not enough traffic.
All	Maximum gain	`cam1 exposure set max_gain {value}`	11	Maximum gain value that is used by the exposure controller.
All	Maximum shutter length	`cam1 exposure set max_shutter {value}`	1000	Maximum shutter length in microseconds that the exposure controller will use. For most uses leave this at 1000, but if you are trying to read very high speed (>160kph) traffic all the time you can shorten this at the expense of all other traffic reads. This is not recommended.
All	Single Sequence Outside Trigger	`cam1 exposure set single_seq_outside_trig {value}`	false	

- `cam1 exposure info`

  Information. Platforms: All.

  Get detailed information of the status of the exposure controller. For debugging purposes.

- `cam1 exposure setBrightDBValue {dbValue}`

  Set absolute brightness DB value. Platforms: All.

  Instantly, manually set the brightness to a DB value. Mostly used for testing, if the exposure controller is on it will adapt the image again after you do this.

#	Name	Parameter	Description
1	Brightness to set to	dbValue	Brightness DB value.

- `cam1 exposure setbrightness {brightness}`

  Set Brightness. Platforms: All.

  Instantly, manually set the brightness to a value. Mostly used for testing, if the exposure controller is on it will adapt the image again after you do this.

#	Name	Parameter	Description
1	Brightness to set to	brightness	Brightness value.

Overlay Control (cam1 overlay)

Available on platforms: All

One overlay control per chanel

Platforms	Name	Command	Default Value	Description
All	Image Below	`cam1 overlay set below {value}`	false	Enables overlayed text on the Image. If not set the text will be above the image.

Platforms	Name	Command	Default Value	Description
All	Overlay Text Enable	`cam1 overlay set enabled {value}`	false	Enables additional text on the Image
All	Expand	`cam1 overlay set expand {value}`	true	Makes the image larger when the text is added. If not set the text will eat into the visible image area.
All	Text	`cam1 overlay set text {value}`	%Shs %Iy04u/ %Io02d/ %Id02u %Ih02u:%Im02u:%Is02u.%Ii03u	The format string for the overlayed text. This has limitations

Platewidth Control (cam1 platewidth)

Available on platforms: All

Automatically calculate and setup plate widths

Platforms	Name	Command	Default Value	Description
All	Plate width Control Enable	`cam1 platewidth set enabled {value}`	false	Enables Automatic Platewidth Control

- `cam1 platewidth info`

  Information. Platforms: All.

  Get detailed information of the status of the platewidth controller. For debugging purposes.

Sequence 1 (cam1 seq1)

Available on platforms: All

One exposure in the sequence for camera

Platforms	Name	Command	Default Value	Description
All	Gain	`cam1 seq1 set gain {value}`	48	Gain in the camera, which increases brightness (and noise) in the image. An aribrary but linear value.
All	Shutter length	`cam1 seq1 set shutter {value}`	16	Length of time that the shutter is open for, and the flash is fired for. This is 0 for 10 microseconds and 31 for 1 millisecond, linearly running between those values.

Sequence 2 (cam1 seq2)

Available on platforms: All

One exposure in the sequence for camera

Platforms	Name	Command	Default Value	Description
All	Gain	`cam1 seq2 set gain {value}`	48	Gain in the camera, which increases brightness (and noise) in the image. An aribrary but linear value.

Platforms	Name	Command	Default Value	Description
All	Shutter length	`cam1 seq2 set shutter {value}`	16	Length of time that the shutter is open for, and the flash is fired for. This is 0 for 10 microseconds and 31 for 1 millisecond, linearly running between those values.

Sequence 3 (cam1 seq3)

Available on platforms: All

One exposure in the sequence for camera

Platforms	Name	Command	Default Value	Description
All	Gain	`cam1 seq3 set gain {value}`	48	Gain in the camera, which increases brightness (and noise) in the image. An aribrary but linear value.
All	Shutter length	`cam1 seq3 set shutter {value}`	16	Length of time that the shutter is open for, and the flash is fired for. This is 0 for 10 microseconds and 31 for 1 millisecond, linearly running between those values.

Sequence 4 (cam1 seq4)

Available on platforms: All

One exposure in the sequence for camera

Platforms	Name	Command	Default Value	Description
All	Gain	`cam1 seq4 set gain {value}`	48	Gain in the camera, which increases brightness (and noise) in the image. An aribrary but linear value.
All	Shutter length	`cam1 seq4 set shutter {value}`	16	Length of time that the shutter is open for, and the flash is fired for. This is 0 for 10 microseconds and 31 for 1 millisecond, linearly running between those values.

Overview Camera (cam2)

Available on platforms: All

Controls for managing the camera and images that it takes

Platforms	Name	Command	Default Value	Description
All	Sensor ADC gain	`cam2 set ADCgain {value}`	52	This sets the adc gain for the Overview sensor Warning don't alter this value. When finished commit will need to be run.
All	Lens Focal Length	`cam2 set FocalLength {value}`	25	The focal length of the lens in front of the overview sensor. This value must be set correctly if overview cropping is in use
All	Sensor Vramp	`cam2 set Vramp {value}`	109	This sets the Vramp value for the Overview sensor Warning don't alter this value. When finished commit will need to be run.

Platforms	Name	Command	Default Value	Description
All	Automatic White Balance	`cam2 set autoWhiteBalance {value}`	true	Enables automatic white balance.
All	Exposure mode	`cam2 set auto_mode {value}`	true	The exposure mode settings, true - auto mode, false - manual mode.
All	Bayer Pattern	`cam2 set bayerOrder {value}`	1	0, 1, 2 or 3. For PIPS engineering use only.
All	Bypass the Bayer Filter	`cam2 set bypassBayer {value}`	false	For PIPS engineering use only.
All	Chroma Order	`cam2 set chromaOrder {value}`	1	0 = YCbCr, 1 = YCrCb, For PIPS engineering use only.
All	FPN removal enabled	`cam2 set fpnRemovalEnabled {value}`	false	Enables and disables FPN removal. Requires the camera to have had the removal image calibrated using calibrateFPN
All	Gain	`cam2 set gain {value}`	0	The gain value(0-15). This only can be set when in manual mode. Mainly for debug use.
All	Gamma Value	`cam2 set gammaCurve {value}`	2	Specifies the gamma correction value. 0 = 1.00, 1 = 0.45, 2 = 0.50 (recommended), 3 = 0.55.
All	Horizontal Scale	`cam2 set horizontalScale {value}`	0	This will control the scale of the whole channel (but not the overview crop), 0 = no scaling, 1 = half scaling, 2 = quarter scaling
All	Maximum Gain	`cam2 set max_gain {value}`	15	The maximum gain value. This camera will automatically set gain and shutter. Setting this higher will result in less blurring, but may cause more noise
All	Maximum shutter length	`cam2 set max_shutter {value}`	4	The maximum shutter length. This camera will automatically set gain and shutter. Setting this lower will give less blurring in the picture, but in low light you may not be able to see anything in the picture if you set it too low as it will not get enough light. Your hardware description must mention that you have a Overview Shutter Limiter for this to work. Values 1-8 are interpreted as milli-seconds. Other values are interpreted as micro-seconds
All	Colour Saturation	`cam2 set saturation {value}`	256	Sets the image saturation level. The recommended value is 256.
All	Sharpening Mode	`cam2 set sharpening {value}`	0	Selects the image sharpening algorithm. 0 = off (for PIPS engineering use only), 1 = the algorithm used in earlier releases, 2 = the improved algorithm (recommended).
All	Shutter length	`cam2 set shutter {value}`	5000	The shutter length in microseconds(16-7500). This only can be set when in manual mode. Mainly for debug use.
All	Target Brightness	`cam2 set target {value}`	110	The target brightness is value that the brightness controller will try and adjust the average pixel value to reach

Platforms	Name	Command	Default Value	Description
All	Vertical Scale	`cam2 set verticalScale {value}`	0	This will control the scale of the whole channel (but not the overview crop), 0 = no scaling, 1 = half scaling, 2 = quarter scaling
All	White Balance Blue Coefficient	`cam2 set whiteBalanceCoeffBlue {value}`	0	The blue coefficient for the white balance operation. This is a read-only value showing the output of auto white balance.
All	White Balance Red Coefficient	`cam2 set whiteBalanceCoeffRed {value}`	0	The red coefficient for the white balance operation. This is a read-only value showing the output of auto white balance.

- `cam2 calibrateFPN`

  Calibrate the Fixed Pattern Noise reference image. Platforms: All.

  Automatically builds a reference image of the Fixed Pattern Noise on the sensor, to allow this to be removed from the images.

- `cam2 ccm`

  Dump Colour Correction Matrix. Platforms: All.

  Dump Colour Correction Matrix

- `cam2 commit`

  Commit the new ADC gain and V Ramp settings. Platforms: All.

  Commits the ADC gain and V Ramp to nand flash

Overlay Control (cam2 overlay)

Available on platforms: All

One overlay control per chanel

Platforms	Name	Command	Default Value	Description
All	Image Below	`cam2 overlay set below {value}`	false	Enables overlayed text on the Image. If not set the text will be above the image.
All	Overlay Text Enable	`cam2 overlay set enabled {value}`	false	Enables additional text on the Image
All	Expand	`cam2 overlay set expand {value}`	true	Makes the image larger when the text is added. If not set the text will eat into the visible image area.
All	Text	`cam2 overlay set text {value}`	%Shs %Iy04u/%Io02d/%Id02u %Ih02u:%Im02u:%Is02u.%Ii03u	The format string for the overlayed text. This has limitations

Client vehicle event reporter (client)

Available on platforms: All

Reports individual vehicle events over the network to a client for live monitoring and diagnostics. Using the ClientView application you can see these images.

Platforms	Name	Command	Default Value	Description
All	Platefinder position instead	`client set platefinder {value}`	false	Show the plate patches from the hardware platefinder rather than the ANPR engine. This is for debugging purposes.

Contexts (contexts)

Available on platforms: All

Control for managing context images associated with an event

Platforms	Name	Command	Default Value	Description
All	Number of Context Images	`contexts set number {value}`	0	Number of context images associated with a vehicle event

Context 1 (contexts ctx1)

Available on platforms: All

An entry defining the offset of a single context image.

Platforms	Name	Command	Default Value	Description
All	Offset	`contexts ctx1 set offset {value}`	250	The offset in milliseconds from the actual read event time. Negative offset will give images prior to the read. Positive offset will give images after the read. Note, the images returned may not have the exact timestamps as specified by the offsets. They will however be the nearest time matching images available. Image timestamp best resolution is affected by the frame rate (for example 50fps implies images are 20ms apart). Images older than a certain period may also be subject to decimation due to limited RAM storage.

Context 2 (contexts ctx2)

Available on platforms: All

An entry defining the offset of a single context image.

Platforms	Name	Command	Default Value	Description
All	Offset	`contexts ctx2 set offset {value}`	250	The offset in milliseconds from the actual read event time. Negative offset will give

Platforms	Name	Command	Default Value	Description
				images prior to the read. Positive offset will give images after the read. Note, the images returned may not have the exact timestamps as specified by the offsets. They will however be the nearest time matching images available. Image timestamp best resolution is affected by the frame rate (for example 50fps implies images are 20ms apart). Images older than a certain period may also be subject to decimation due to limited RAM storage.

Context 3 (contexts ctx3)

Available on platforms: All

An entry defining the offset of a single context image.

Platforms	Name	Command	Default Value	Description
All	Offset	`contexts ctx3 set offset {`*`value`*`}`	250	The offset in milliseconds from the actual read event time. Negative offset will give images prior to the read. Positive offset will give images after the read. Note, the images returned may not have the exact timestamps as specified by the offsets. They will however be the nearest time matching images available. Image timestamp best resolution is affected by the frame rate (for example 50fps implies images are 20ms apart). Images older than a certain period may also be subject to decimation due to limited RAM storage.

Context 4 (contexts ctx4)

Available on platforms: All

An entry defining the offset of a single context image.

Platforms	Name	Command	Default Value	Description
All	Offset	`contexts ctx4 set offset {`*`value`*`}`	250	The offset in milliseconds from the actual read event time. Negative offset will give images prior to the read. Positive offset will give images after the read. Note, the images returned may not have the exact timestamps as specified by the offsets. They will however be the nearest time matching images available. Image timestamp best resolution is affected by the frame rate

Platforms	Name	Command	Default Value	Description
				(for example 50fps implies images are 20ms apart). Images older than a certain period may also be subject to decimation due to limited RAM storage.

Context 5 (contexts ctx5)

Available on platforms: All

An entry defining the offset of a single context image.

Platforms	Name	Command	Default Value	Description
All	Offset	`contexts ctx5 set offset {`*`value`*`}`	250	The offset in milliseconds from the actual read event time. Negative offset will give images prior to the read. Positive offset will give images after the read. Note, the images returned may not have the exact timestamps as specified by the offsets. They will however be the nearest time matching images available. Image timestamp best resolution is affected by the frame rate (for example 50fps implies images are 20ms apart). Images older than a certain period may also be subject to decimation due to limited RAM storage.

Context 6 (contexts ctx6)

Available on platforms: All

An entry defining the offset of a single context image.

Platforms	Name	Command	Default Value	Description
All	Offset	`contexts ctx6 set offset {`*`value`*`}`	250	The offset in milliseconds from the actual read event time. Negative offset will give images prior to the read. Positive offset will give images after the read. Note, the images returned may not have the exact timestamps as specified by the offsets. They will however be the nearest time matching images available. Image timestamp best resolution is affected by the frame rate (for example 50fps implies images are 20ms apart). Images older than a certain period may also be subject to decimation due to limited RAM storage.

Context 7 (contexts ctx7)

Available on platforms: All

An entry defining the offset of a single context image.

Platforms	Name	Command	Default Value	Description
All	Offset	`contexts ctx7 set offset {value}`	250	The offset in milliseconds from the actual read event time. Negative offset will give images prior to the read. Positive offset will give images after the read. Note, the images returned may not have the exact timestamps as specified by the offsets. They will however be the nearest time matching images available. Image timestamp best resolution is affected by the frame rate (for example 50fps implies images are 20ms apart). Images older than a certain period may also be subject to decimation due to limited RAM storage.

Context 8 (contexts ctx8)

Available on platforms: All

An entry defining the offset of a single context image.

Platforms	Name	Command	Default Value	Description
All	Offset	`contexts ctx8 set offset {value}`	250	The offset in milliseconds from the actual read event time. Negative offset will give images prior to the read. Positive offset will give images after the read. Note, the images returned may not have the exact timestamps as specified by the offsets. They will however be the nearest time matching images available. Image timestamp best resolution is affected by the frame rate (for example 50fps implies images are 20ms apart). Images older than a certain period may also be subject to decimation due to limited RAM storage.

Plate Database Matcher (dbmatcher)

Available on platforms: All

The database matching system allows the system to look up number plates in a database.

It is possible to filter out plates based on whether they are found or not.

It is also possible to collect a tag string for plates which are found which can be output by the delivery system.

No spaces or commas are allowed in the plate or tag string.

INSTALLING NEW DATABASE FILES:

Copy a file named [YourPlatesDatabaseName].install into the camera /storage/db/ directory.

For example, for the default plates.db name, you would copy a file named plates.db.install into the /storage/db/ directory.

The system should automatically detect this and install the new file. To confirm this, do a directory listing of the /storage/db/ directory and confirm:

1)That the plates.db.install you just copied in has disappeared (GUI Tool may need refreshing)

2)That the plates.db file md5sum matches the file you installed.

If for some reason this does not work, then copy your plates.db.install into /storage/

and then, using the linux command prompt, move this file into /storage/db/

mv /storage/plates.db.install /storage/db/.

and then verify as above.

Platforms	Name	Command	Default Value	Description
All	Enabled	`dbmatcher set enabled {value}`	false	Allows the Filter system to be enabled and disabled. Disable it unless you are using it.
All	Forward Event on match	`dbmatcher set forward_on_match {value}`	false	Will forward the plate read event only if a match is found in the database. May be enabled simultaneously with forward_on_nomatch. This will have the effect of all plates being forwarded but matching plates will carry their corresponding tags.
All	Forward Event on no match	`dbmatcher set forward_on_nomatch {value}`	false	Will forward the plate read event if no match is found in the database. May be enabled simultaneously with forward_on_match. This will have the effect of all plates being forwarded but matching plates will carry their corresponding tags.
All	Plate Database File Name	`dbmatcher set plates_filename {value}`	plates.db	Specify the filename of the plates SQLite database. This file may be pre-created and placed in the /storage/db/ directory. The SQL to create a compatible database is: CREATE TABLE plateDB(plate TEXT PRIMARY KEY ASC, tag TEXT);

- `dbmatcher insert {plate} {tag}`

  Insert a plate+tag. Platforms: All.

  Adds a plate+tag combination to the plates database.

#	Name	Parameter	Description
1		plate	The plate you wish to insert

#	Name	Parameter	Description
	Plate Entry to insert		
2	Plate Tag	tag	The tag associated with the plate you wish to insert

- `dbmatcher lookup` {*`plate`*}

  Lookup a plate. Platforms: All.

  Determines if a plate exists in the current database. Will confirm if the plate is found and print its tag value

#	Name	Parameter	Description
1	Plate Entry to lookup	plate	The plate you wish to find in the database

- `dbmatcher reload`

  Load the database file. Platforms: All.

  Load the file named by plates_filename. Use this command to reload the plates database file if it has been changed or replaced, or if you have changed the name.

- `dbmatcher remove` {*`plate`*}

  Remove a plate. Platforms: All.

  If the plate exists in the current database it (and its associated tag) will be removed.

#	Name	Parameter	Description
1	Plate Entry to remove	plate	The plate you wish to remove from the database

- `dbmatcher statistics`

  Cumulative statistics. Platforms: All.

  Provides cumulative statistics of longterm vehicle filter processing

Diagnostics and Exceptions Manager (diagnostics)

Available on platforms: All

Diagnostics and Exceptions

Platforms	Name	Command	Default Value	Description
All	Acknowledgents Enabled	`diagnostics set ack_enabled` {*`value`*}	true	If true, the delivery system will await acknowledgement
All	Diagnostic/ Exception ack wait timeout	`diagnostics set ack_timeout` {*`value`*}	30	Period in seconds to wait for an acknowledgement of a diagnostic or exception message
All	Minimum Samples for Diagnostics	`diagnostics set min_samples` {*`value`*}	10	Certain types of diagnostics (e.g. mean values or ratios) are only considered valid after a certain number of samples.

Platforms	Name	Command	Default Value	Description
All	Diagnostic period	`diagnostics set diagnostic_period {value}`	20	Period in minutes between diagnostic updates
All	Diagnostic Delivery Port	`diagnostics set diagnostic_port {value}`	5001	The TCP port that diagnostic messages will be delivered on. Set to
All	Disk Queue Length	`diagnostics set disk_queue_length {value}`	5	The number of diagnostic and exception events that are maintained in a persistent disk queue while the in station receiver is offline. Diagnostics are kept in a seperate queue to exceptions. This value applies to all queues
All	Diagnostics enabled	`diagnostics set enabled {value}`	false	Allows diagnostic and exception reporting to be enabled/disabled
All	Minimum Samples for Exceptions	`diagnostics set exception_min_samples {value}`	20	Certain types of exceptions (e.g. mean values or ratios) are only considered valid after a certain number of samples.
All	Exception Period	`diagnostics set exception_period {value}`	5	Period in minutes between (non-realtime) exception updates
All	Exception Delivery Port	`diagnostics set exception_port {value}`	5002	The TCP port that exception messages will be delivered on
All	Delivery Host	`diagnostics set host {value}`	10.1.1.1	The IP address to which the diagnsotic and exception messages will be transferred.
All	JTMS Compatible	`diagnostics set jtms {value}`	false	Generate JTMS compatible diagnostics instead of VES compatible diagnostics. The differences are small but significant.

File Logger (filelog)

Available on platforms: All

The logger which reports information to specified file. NB: A log file can grow to fill the disk. Use logrotate to manage log files.

Platforms	Name	Command	Default Value	Description
All	Enable file logging	`filelog set enabled {value}`	false	Enable logging to a file. NB, the camera does not manage the file size or archiving. Please use logrotate
All	Log File Name	`filelog set filename {value}`	/var/log/start382.log	Specify the filename to receive log output. NB: To avoid this file growing too large, please use logrotate
All	Print line/file	`filelog set lineFilePrint {value}`	true	Print Linenumber and Filename for logging messages
All	Print time	`filelog set timePrint {value}`	true	Print time for logging messages

Vehicle Fusion (fusion)

Available on platforms: All

The system may read multiple images of any given vehicle, and this subsystem merges those multiple vehicle reads into a single coherant result for output.

Platforms	Name	Command	Default Value	Description
All	Combine hazard and normal plates	`fusion set combine_hazard {value}`	false	If this is set true, an attempt will be made to match the hazard plate with the normal plate of the same vehicle. If successful, a combined event will be forwarded. If a hazard plate is read, it will normally be forwarded as an independant plate read.
All	Distance from edge	`fusion set distance {value}`	256	Distance from the edge specified in the selector parameter to the centre of the plate which will be used to try to select an appropriate plate for you (measured in pixels). May not be used if no distance selector in use.
All	Duplicate Level	`fusion set duplicate_level {value}`	60	Percentage match level at which the numberplates will be considered as duplicates for matching multiple reads of a vehicle together. 100 means they must be identical, and 0 means anything will match anything else (which makes the camera pretty useless).
All	Early result	`fusion set early {value}`	false	Output the first event from a vehicle even if it may well be wrong. Useful if the time between a vehicle being seen and the camera reporting it is critical, otherwise don't choose this
All	Maximum gap	`fusion set gap {value}`	700	Length of time after seeing a vehicle when we pass on the vehicle when we haven't seen it again for this long. Given in milliseconds.
All	Maximum age of vehicle	`fusion set max_age {value}`	2000	Maximum time the vehicle can be in the field of view before we pass it on anyway. Given in milliseconds.
All	No Event Timeout	`fusion set noevent_timeout {value}`	4294967295	If no vehicle event has been delivered within this timeout period (in seconds) a Vehicle Detect Timeout exception will be generated. This is a boolean exception and will be cleared as soon as a vehicle event is forwarded. This cannot be set below 10 seconds
All	Allow out of trigger images	`fusion set outoftrigger {value}`	false	If a vehicle arrives during a trigger we will only deliver images from within the trigger period unless you tick this box. This allows us to deliver better images from earlier.
All	Persistant event id	`fusion set persistantEventId {value}`	true	Set this value to true to keep the next event id in a separate file. Setting this value to false causes the camera to calculate the next event id using the data stored on the VFE database. It takes some time to update the VFE database and

Platforms	Name	Command	Default Value	Description
				the event id sequence may not be updated correctly if the camera app is restarted. If the VFE database is disabled then the event id sequence is reset to 0 when the camera app is restarted. Set this value to true if the uniqueness of event ids is important. Set the value to false if performance is important.
All	Repeating vehicles	`fusion set repeat {value}`	true	If a vehicle stays in the field of view we will pass it on every max_age milliseconds if this is set true, otherwise just once. In the presence of triggers, all vehicles are flushed when the trigger gate closes. Repeats may then still be experienced. In order to prevent repeats in the presence of triggers, set the repeat_on_trigger to false.
All	Repeating vehicles per trigger	`fusion set repeat_on_trigger {value}`	true	If true, a vehicle staying in the field of view we will be forwarded on every trigger (default). Otherwise the vehicle will only be forwarded the first time it is detected within a trigger period.
All	Plate Selector	`fusion set selector {value}`	0	This parameter will allow the system to select an appropriate plate for you. Sometimes we may not be able to select a plate which matches your criteria very well, but we will do what we can. 0=Best plate read. 1=Distance from top edge. 2=Distance from left edge. 3=Plate exposure quality, for better visibility of the non plate text details
All	Set reads forwarded from a trigger to 1	`fusion set single_read_on_trigger {value}`	false	Only applies to triggered systems. Will limit the maximum number of read events delivered per trigger to 1. The vehicle chosen for delivery will be decided according to read confidence. Beware of setting this as vehicles (such as adjacent vehicles) may be missed. Also, if set, a parked vehicle may prevent any other vehicles being read.
All	Supplementary IR Images	`fusion set supplementary_images {value}`	false	Only works for images within a trigger gate open period.

Platforms	Name	Command	Default Value	Description
				If true, up to two additional full IR image will be available for delivery. These will be alternatively exposed IR images (if alternative exposure sequence images are available). If no other sequence images are available the best exposed of the remaining IR images (if any) will be available. In the case where only one image was analysed for the vehicle, no additional image will be available.

- `fusion clearstats`

  Clears Cumulative statistics. Platforms: All.

  Resets all statistics collection variables to initial values

- `fusion stats`

  Cumulative statistics. Platforms: All.

  Provides cumulative statistics of longterm vehicle processing

- `fusion status`

  Current status. Platforms: All.

  Gets the current status of the vehicles being processed by the module

GPS Time Manager (gps)

Available on platforms: All

Manages GPS Time Sync

Platforms	Name	Command	Default Value	Description
All	Enabled	`gps set enabled` {*`value`*}	false	Enables gps time manager

- `gps status`

  Current status of GPS/PPS. Platforms: All.

  Gets the current status of the GPS and PPS time management

Heartbeat (heartbeat)

Available on platforms: All

Platforms	Name	Command	Default Value	Description
All	Heartbeat Content	`heartbeat set content` {*`value`*}	%Shs,%hsx,%fcm,%hfm	A format string specifying the content of the heartbeat message.

Platforms	Name	Command	Default Value	Description
All	Enabled	`heartbeat set enabled {value}`	false	Allows the Heartbeat system to be enabled and disabled. Disable it unless you are using it.
All	Delivery Host	`heartbeat set host {value}`	10.1.1.1	The IP address to which the heartbeat messages will be transferred.
All	Heartbeat period	`heartbeat set period {value}`	60	Period in seconds between heartbeats
All	Heartbeat Delivery Port	`heartbeat set port {value}`	10005	The TCP port that heartbeat messages will be delivered on.

Image File Outputter (ifo)

Available on platforms: All

Stores the images from the camera onto disk. These are just periodic images from the selected camera, like a video stream, not ones of particular interest, and they may or may not contain plates. If you have network mounted a disk this would be most useful, as otherwise you'll quickly fill up the internal storage of the camera. Look at mounting a disk in /storage to use this. This module is designed purely for testing and debugging, not for production systems. There is no guarantee that images will come out at all if the rest of the system is too busy. Image metadata is stored in the filename. The filename format may change without notice.

Platforms	Name	Command	Default Value	Description
All	Anpr Patches	`ifo set anprpatch {value}`	true	When looking at plates, output an extra file for the anpr patch. This file will have the prefix A
All	Bitmap	`ifo set bitmap {value}`	false	Enable this to output bitmap files, otherwise the output is jpeg format. Only works for monochrome images, colour ones are always jpeg format.
All	Colour	`ifo set colour {value}`	false	Enable this to store video images from the colour camera, otherwise look at the monochrome camera. Has no effect on plate images which are always monochrome.
All	Output Directory	`ifo set directory {value}`	/tmp	Directory to receive the files relative to the /storage directory. It is recommended you mount an external network disk here to collect the images.
All	Enabled	`ifo set enabled {value}`	false	Enable or disable the output of raw image files (e.g. this whole module). Should be turned off on production systems.
All	Minimum interval	`ifo set interval {value}`	1000	Minimum number of milliseconds between files, with a busy camera, filesystem or network this may not be adhered to.
All	Hardware Platefinder Patches	`ifo set pfpatch {value}`	false	When looking at plates, output an extra file for the platefinder patch. This file will have the prefix H
All	Plates	`ifo set plates {value}`	true	Enable or disable the output of plate images. These are images where we have read a plate. May be used simultaneously with video if you want. These files will have the prefix P

Platforms	Name	Command	Default Value	Description
All	PreFusion	`ifo set prefusion {value}`	false	When looking at plates, enable or disable looking at the plates prior to processing by the vehicle fusion, instead of after. These plates may be rubbish. If you have no idea what this means you will want it off, it is mainly for debugging.
All	Video	`ifo set video {value}`	false	Enable or disable the output of the video stream. This does not contain every field, just a periodic selection. Enabling this produces a LOT of data. These files will have the prefix V.

- `ifo burst`

  Burst Video. Platforms: All.

  Output a burst of consecutive video fields from the selected camera in the selected format. Will burst for a short while based upon the data rate we can write at. May upset the rest of the camera during the burst, so never do this on a production system. This will work even if the rest of this subsystem is disabled.

JPEG Service (jpegService)

Available on platforms: All

Controls the generation of JPEG images

Platforms	Name	Command	Default Value	Description
All	NASP compliant jpeg patch of 120x60	`jpegService set fixedPatch {value}`	false	Forces the size of the patch to match the requirement in the UK Govenments NASP specification of 120x60 pixels
All	Enable Histogram Stretching	`jpegService set histogramEnable {value}`	true	Set true to enable histogram stretching to improve contrast (recommended).
All	Lower Ignore	`jpegService set lowIgnoreAmount {value}`	300	100 times the percentage of dark pixels excluded from histogram stretching (e.g. 300 = 3%). Only change this value if you are familiar with image processing algorithms or under instruction from PIPS engineers.
All	Maximum Stretch Percentage	`jpegService set maxStretchPercent {value}`	80	Maximum amount to stretch the histogram (1-100%). Only change this value if you are familiar with image processing algorithms or under instruction from PIPS engineers.
All	Minimum Stretch Percentage	`jpegService set minStretchPercent {value}`	40	Minimum amount to stretch the histogram (1-100%). Only change this value if you are familiar with image processing algorithms or under instruction from PIPS engineers.
All	JPEG Target Size	`jpegService set size {value}`	192	Varies the target size of the jpegs, in KB, Patches will be 1/4 of the size
All		`jpegService set targetQuality {value}`	0	
All	Upper Ignore	`jpegService set upIgnoreAmount {value}`	200	100 times the percentage of bright pixels excluded from histogram stretching (e.g. 200 = 2%). Only change this value if you are

Platforms	Name	Command	Default Value	Description
				familiar with image processing algorithms or under instruction from PIPS engineers.

- `jpegService qualities`

  Display qualities. Platforms: All.

  Display the controller selected quality for each channel (or each exposure sequence of each channel) and for patches.

JTMS - Journey Time Measurement System (jtms)

Available on platforms: All

A system for delivering numberplates using very low bandwidth specifically for journey time measurement. Only minimal information is transmitted by the system. To use JTMS you must give your camera a 4 digit numerical hostname, which will be its site ID. This module only supplies tags, you should look at the diagnostics module to enable diagnostics and exceptions in jtms compatible format.

Platforms	Name	Command	Default Value	Description
All	Tag format	`jtms set binary` {*value*}	1	The format of the tag messages. 0 - human readable text messages. 1 - binary messages (more compact). 2 - Extended binary format with state/country, classification, confidence and 24 bit hashed tags.
All	Enabled	`jtms set enabled` {*value*}	false	Allows the JTMS system to be enabled and disabled. Disable it unless you are using it.
All	Host	`jtms set host` {*value*}	192.168.1.1	The IP address of the instation which will receive the JTMS data.
All	Merge Characters	`jtms set mergechars` {*value*}	true	Enable merging of possible ambiguous characters such as 8 and B prior to transmission
All	Maximum Files	`jtms set nlog` {*value*}	6	The maximum number of files which will be stored on the local filesystem before they are overwritten if it is not possible to contact the instation. Warning, arbitrarily setting this to a high value may fill up the device on which you are storing the files and then the system will lose the wrong data or may perform badly.
All	Tag Period	`jtms set period` {*value*}	5	The number of minutes between sending tag messages
All	Time Slot	`jtms set time_slot` {*value*}	0	Time slot which is used by this system for transmission. Use this to spread the network load of your outstations. This is a percentage value and is used as an offset from the beginning of the time which could be used for transmission verses the end of that transmission slot - e.g. 0 it will transmit at the very beginning of the slot, at 100 at the very end.
All	ACK Timeout	`jtms set timeout` {*value*}	60	Number of seconds to wait for an ACK (if ACKs are enabled). Set to zero to disable

- `jtms reset`

Reset statistics. Platforms: All.

Reset the statistics for this module

- `jtms statistics`

  Statistics. Platforms: All.

  Display statistics from this module

External Led Control (ledControl)

Available on platforms: All

Setting to Control the pips illuminator

Platforms	Name	Command	Default Value	Description
All	Length of flash in microseconds	`ledControl set flashTime` {*value*}	1000	Sets the length of the flash in microseconds
All	Enable internal Led's	`ledControl set internalEnable` {*value*}	true	Set this to false to disable the internal LED's
All	Set mode of external Led's	`ledControl set mode` {*value*}	0	Mode 0 = Off, Mode 1 = Synced to Cam1(triple sequence), Mode 2 = Synced to Cam2, Mode 3 = Fixed Length

Metadata store (metadata)

Available on platforms: All

This is an object for storing site metadata as string values. The information stored in here is NOT used by the system, and is just for you to use when creating format strings. The data will be output in the format strings unchanged, and allows you to put per-site data in here, keeping the format strings the same on all sites. You might wish to store lane IDs, zones, site direction or anything else similar in here. We would recommend setting the hostname as the unique site identifer which may be accessed though %Sh. It also provides a way of mapping from long event metadata into short codes for output with the %E* variables. You enter into map_a the long name of the variable you'd like available as %Ea. This part is probably not useful to you at the moment unless you understand this without further explanation.

Platforms	Name	Command	Default Value	Description
All	Mapping a	`metadata set map_a` {*value*}		Name of an event metadata string you'd like visible in %Ea.
All	Mapping b	`metadata set map_b` {*value*}		Name of an event metadata string you'd like visible in %Eb.
All	Mapping c	`metadata set map_c` {*value*}		Name of an event metadata string you'd like visible in %Ec.
All	Mapping d	`metadata set map_d` {*value*}		Name of an event metadata string you'd like visible in %Ed.
All	Mapping e	`metadata set map_e` {*value*}		Name of an event metadata string you'd like visible in %Ee.
All	Mapping f	`metadata set map_f` {*value*}		Name of an event metadata string you'd like visible in %Ef.
All	Mapping g	`metadata set map_g` {*value*}		Name of an event metadata string you'd like visible in %Eg.

Platforms	Name	Command	Default Value	Description
All	Mapping h	`metadata set map_h {value}`		Name of an event metadata string you'd like visible in %Eh.
All	Mapping i	`metadata set map_i {value}`		Name of an event metadata string you'd like visible in %Ei.
All	Mapping j	`metadata set map_j {value}`		Name of an event metadata string you'd like visible in %Ej.
All	Mapping k	`metadata set map_k {value}`		Name of an event metadata string you'd like visible in %Ek.
All	Mapping l	`metadata set map_l {value}`		Name of an event metadata string you'd like visible in %El.
All	Mapping m	`metadata set map_m {value}`		Name of an event metadata string you'd like visible in %Em.
All	Mapping n	`metadata set map_n {value}`		Name of an event metadata string you'd like visible in %En.
All	Mapping o	`metadata set map_o {value}`		Name of an event metadata string you'd like visible in %Eo.
All	Mapping p	`metadata set map_p {value}`		Name of an event metadata string you'd like visible in %Ep.
All	Mapping q	`metadata set map_q {value}`		Name of an event metadata string you'd like visible in %Eq.
All	Mapping r	`metadata set map_r {value}`		Name of an event metadata string you'd like visible in %Er.
All	Mapping s	`metadata set map_s {value}`		Name of an event metadata string you'd like visible in %Es.
All	Mapping t	`metadata set map_t {value}`		Name of an event metadata string you'd like visible in %Et.
All	Mapping u	`metadata set map_u {value}`		Name of an event metadata string you'd like visible in %Eu.
All	Mapping v	`metadata set map_v {value}`		Name of an event metadata string you'd like visible in %Ev.
All	Mapping w	`metadata set map_w {value}`		Name of an event metadata string you'd like visible in %Ew.
All	Mapping x	`metadata set map_x {value}`		Name of an event metadata string you'd like visible in %Ex.
All	Mapping y	`metadata set map_y {value}`		Name of an event metadata string you'd like visible in %Ey.
All	Mapping z	`metadata set map_z {value}`		Name of an event metadata string you'd like visible in %Ez.
All	String a	`metadata set string_a {value}`		A string, access in format strings as %Ma.
All	String b	`metadata set string_b {value}`		A string, access in format strings as %Mb.
All	String c	`metadata set string_c {value}`		A string, access in format strings as %Mc.
All	String d	`metadata set string_d {value}`		A string, access in format strings as %Md.

Platforms	Name	Command	Default Value	Description
All	String e	`metadata set string_e {value}`		A string, access in format strings as %Me.
All	String f	`metadata set string_f {value}`		A string, access in format strings as %Mf.
All	String g	`metadata set string_g {value}`		A string, access in format strings as %Mg.
All	String h	`metadata set string_h {value}`		A string, access in format strings as %Mh.
All	String i	`metadata set string_i {value}`		A string, access in format strings as %Mi.
All	String j	`metadata set string_j {value}`		A string, access in format strings as %Mj.
All	String k	`metadata set string_k {value}`		A string, access in format strings as %Mk.
All	String l	`metadata set string_l {value}`		A string, access in format strings as %Ml.
All	String m	`metadata set string_m {value}`		A string, access in format strings as %Mm.
All	String n	`metadata set string_n {value}`		A string, access in format strings as %Mn.
All	String o	`metadata set string_o {value}`		A string, access in format strings as %Mo.
All	String p	`metadata set string_p {value}`		A string, access in format strings as %Mp.
All	String q	`metadata set string_q {value}`		A string, access in format strings as %Mq.
All	String r	`metadata set string_r {value}`		A string, access in format strings as %Mr.
All	String s	`metadata set string_s {value}`		A string, access in format strings as %Ms.
All	String t	`metadata set string_t {value}`		A string, access in format strings as %Mt.
All	String u	`metadata set string_u {value}`		A string, access in format strings as %Mu.
All	String v	`metadata set string_v {value}`		A string, access in format strings as %Mv.
All	String w	`metadata set string_w {value}`		A string, access in format strings as %Mw.
All	String x	`metadata set string_x {value}`		A string, access in format strings as %Mx.
All	String y	`metadata set string_y {value}`		A string, access in format strings as %My.

Platforms	Name	Command	Default Value	Description
All	String z	`metadata set string_z {value}`		A string, access in format strings as %Mz.

OEM Modules (modules)

Available on platforms: All

Allows the specification of the supported OEM module types

Platforms	Name	Command	Default Value	Description
All	Number of ACS	`modules set num_acs {value}`	1	Number of ACS modules. Any change will require a restart to take effect. Set to 0 if you dont need ACS. If set to 1, will be called simply acs. If>1 will be called acs1, acs2 etc.
All	Number of BOF 2	`modules set num_bof2 {value}`	0	Number of BOF 2.2 Delivery modules. Any change will require a restart to take effect. Set to 0 if you dont need the Relay Output. Otherwise set to 1. Only a single Relay Output module is allowed.
All	Number of JTMS	`modules set num_jtms {value}`	1	Number of JTMS modules. Any change will require a restart to take effect. Set to 0 if you dont need JTMS. Otherwise set to 1. Only a single JTMS module allowed. .
All	Number of Relay Output	`modules set num_relayOut {value}`	0	Number of Relay Output modules. Any change will require a restart to take effect. Set to 0 if you dont need the Relay Output. Otherwise set to 1. Only a single Relay Output module is allowed.
All	Number of SAP	`modules set num_sap {value}`	0	Number of SAP modules. Any change will require a restart to take effect. Set to 0 if you dont need SAP. Otherwise set to 1. Only a single sap module allowed.
All	Number of UTMC	`modules set num_utmc {value}`	0	Number of UTMC modules. Any change will require a restart to take effect. Set to 0 if you dont need UTMC.

Platforms	Name	Command	Default Value	Description
				Otherwise set to 1. Only a single UTMC module allowed.
All	Number of UTMCV12	`modules set num_utmcv12 {value}`	0	Number of UTMC Version 1.2 modules. Any change will require a restart to take effect. Set to 0 if you dont need UTMC Version 1.2. Otherwise set to 1. Only a single UTMC Version 1.2 module allowed.
All	Number of VES	`modules set num_ves {value}`	1	Number of VES modules. Any change will require a restart to take effect. Set to 0 if you dont need VES. Otherwise set to 1. Only a single ves module allowed.

Network user interface manager (netuis)

Available on platforms: All

The manager for the network user interfaces. These are the interfaces which the web and shell connect to.

Platforms	Name	Command	Default Value	Description
All	To enable/disable the generation of exceptions	`netuis set exceptions {value}`	false	If true, will transmit an exception when a control connection is made. Will only count the first control connection and will only clear the condition when there have been no connections for 5 minutes

- `netuis status`

  Current status. Platforms: All.

  Display the status of the NetUI servers, how many are in use.

Network user interface (netuis netui1)

Available on platforms: All

Network user interface instance which communicates with users

Platforms	Name	Command	Default Value	Description
All	Print line/file	`netuis netui1 set lineFilePrint {value}`	true	Print Linenumber and Filename for logging messages
All	Print time	`netuis netui1 set timePrint {value}`	true	Print time for logging messages
All	Disconnect timeout	`netuis netui1 set timeout {value}`	300	Disconnect timeout in seconds, for when the interface is inactive

NTP Monitor (ntpMonitor)

Available on platforms: All

Monitors NTP status and generates exceptions if any issues detected.

Platforms	Name	Command	Default Value	Description
All	Allowed missed polls	`ntpMonitor set allowed_missed_polls {value}`	8	Number of allowed consecutive missed polls of NTP server before an exception is flagged. The NTP daemon itself flags after 8 missed polls, so that will always generate an exception. However, 8 polls may take quite some time to complete (hours). While system time should be stable and accurate during this period, some might prefer to know sooner if the NTP server has not been reached. This value is also for consecutive missed polls. Set this to between 0 and 8.

Licence options (options)

Available on platforms: All

Management of the licence file

- `options display`

  Display Licence. Platforms: All.

  Display current licence information

- `options load`

  Read Licence file. Platforms: All.

  Load a new licence file from /storage/options.txt, and install's to system licence information

- `options test {on_off}`

  Set System in test mode. Platforms: All.

  Enable test mode, allows 100 Reads before marking number plate unreadable

#	Name	Parameter	Description
1	Test Mode	on_off	Test mode enable / disable

Patch Overlay Control (patchoverlay)

Available on platforms: All

Specify whether the plateread patch has an overlay, and what its contents should be.

Platforms	Name	Command	Default Value	Description
All	Overlay Text Enable	`patchoverlay set enabled {value}`	false	Enables additional text on the Image
All	Text	`patchoverlay set text {value}`		The format string for the overlayed text. This has limitations

Platforms	Name	Command	Default Value	Description
			%Iy04d/%Io02d/%Id02d_%Ih02d:%Im02d:%Is02d\n%Shs_%Pps_%Pc02d	

PCI Camera Source (pciSource)

Available on platforms: All

The internal camera subsystem, connected via PCI to the processor. These controls are mostly for diagnostics.

- `pciSource clear`

  Reset interrupt latency statistics. Platforms: All.

  Reset counts of interrupts from the PCI camera.

- `pciSource irbufs`

  Dump IR Bufs in use. Platforms: All.

  Dump IR Bufs in use

- `pciSource latency`

  Display interrupt latency statistics. Platforms: All.

  Display details and counts of interrupts from the PCI camera.

PIXI Contexts (pixicontexts)

Available on platforms: All

Manages PIXI contexts

- `pixicontexts list`

  List PIXI Contexts. Platforms: All.

  List existing PIXI persistent LIFOS as well as their lengths.

Power Manager (power)

Available on platforms: All

Power Management subsystem, monitoring the power coming into the system and dealing with power down when the power is cut.

Relay Out (relayOut)

Available on platforms: All

Controls the relay according to plate read events

Platforms	Name	Command	Default Value	Description
All	Relay Action	`relayOut set action {value}`	close	

Platforms	Name	Command	Default Value	Description
All	Enabled	`relayOut set enabled` {*value*}	false	
All	Relay Pulse Period	`relayOut set period` {*value*}	250	
All	Tag Match Regular Expression	`relayOut set tag_regex` {*value*}	.*	

SAP - Serial Application Port (sap)

Available on platforms: All

Simple serial port output

Platforms	Name	Command	Default Value	Description
All	Serial Baud Rate	`sap set baud` {*value*}	9600	The serial port baud rate. For changes to take effect, disable then re-enable. Valid values 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400
All	Enabled	`sap set enabled` {*value*}	false	Allows the SAP system to be enabled and disabled. Disable it unless you are using it.
All	Message contents	`sap set msg_contents` {*value*}	%Pps\n	A format string specifying the message content. The default gives you the plate-read text followed by newline.

Vehicle Image Selector (selector)

Available on platforms: All

Selects images from the hardware platefinder for further analysis and ANPR by the rest of the software.

Platforms	Name	Command	Default Value	Description
All	Previous trigger frame	`selector set pre_trigger_frame` {*value*}	true	Allow the camera to select the frame before the trigger was recieved if it has a lower time proximity to the trigger than the event after
All	Selector queue length	`selector set queueLength` {*value*}	5	Do not chnge this without good reason. By Changing the length of the queue it may change the latency to delivery, but is very likely to affect the read rate
All	Trigger Overview	`selector set triggerOview` {*value*}	false	If this is set *when triggered* the overview will be coincident with the trigger start. If this is not set or the vehicle was not triggered then the overview image will be taken at the same time as the IR image.
All	Triggers Only	`selector set triggersOnly` {*value*}	false	If this is set we will only detect vehicles during the trigger period, otherwise we'll auto detect

Platforms	Name	Command	Default Value	Description
				vehicles all the time but explicitly pass them on when triggered

- `selector statistics`

  Cumulative statistics. Platforms: All.

  Provides cumulative statistics of longterm vehicle processing

Hardware Monitoring sensors (sensors)

Available on platforms: All

This module periodically polls the sensor values

- `sensors dump`

  Dump Current readings. Platforms: All.

  Displays the current readings of the sensors

Console Logger (stdout)

Available on platforms: All

The logger which reports information to the standard out (stdout) device (usually the console). This is probably of no use to you as you probably aren't looking at it.

Platforms	Name	Command	Default Value	Description
All	Print line/file	`stdout set lineFilePrint {`*`value`*`}`	true	Print Linenumber and Filename for logging messages
All	Print time	`stdout set timePrint {`*`value`*`}`	true	Print time for logging messages

System Details (system)

Available on platforms: All

An object for collecting lists of system details and objects.

Platforms	Name	Command	Default Value	Description
All	P392 Bracket Location	`system set bracketBottom {`*`value`*`}`	true	P392 mounted with bracket at the bottom is true otherwise the variable should be false
All	COM2 serial use	`system set com2 {`*`value`*`}`	disabled	This settings determines what the com2 second user available serial port is used for. Options are: 'trig_serial' - generic serial triggering with regex matching and variable baud rate. 'sap' - Serial text output of vehicle plateread events. 'vestrigger' - 19.2k STX delimited trigger messages for VES.

Platforms	Name	Command	Default Value	Description
				'gps' - GPS unit talking NMEA at 4.8k. 'disabled' - not in use.
All	Coordinates Valid	`system set coord_valid {value}`	false	A flag indicating whether these coordinates are valid or not
All	East (not West)	`system set east {value}`	true	Flag indicating whether the longitude value is East or West. 1->East, 0->West
All	North Degrees	`system set latitude {value}`	0	This is the latitude coordinate of this camera, and this is the degree portion of the coordinate. If you have a GPS system attached and working this will be automatically updated everytime we have a lock, otherwise it is manually enterable.
All	North Microdegrees	`system set latitude_micro {value}`	0	This is the latitude coordinate of this camera, and this is the microdegree portion of the coordinate. If you have a GPS system attached and working this will be automatically updated everytime we have a lock, otherwise it is manually enterable.
All	East Degrees	`system set longitude {value}`	0	This is the longitude coordinate of this camera, and this is the degree portion of the coordinate. If you have a GPS system attached and working this will be automatically updated everytime we have a lock, otherwise it is manually enterable.
All	East Microdegrees	`system set longitude_micro {value}`	0	This is the longitude coordinate of this camera, and this is the microdegree portion of the coordinate. If you have a GPS system attached and working this will be automatically updated everytime we have a lock, otherwise it is manually enterable.
All	North (not south)	`system set north {value}`	true	Flag indicating whether the latitude value is North or South. 1->North, 0->South
All	Relay output use	`system set relay {value}`	disabled	This setting determines what the relay input is used for. Options are: 'gpspower' - for use in switching on and off a gps unit (only usable with the serial port com2 also connected to the gps). 'disabled' - not in use.
All	Trigger input use	`system set trigger {value}`	disabled	This setting determines what the trigger input is used for. Options are: 'hwtrigger' - for a triggering vehicles detection. 'gpspps' - for the pulse per second signal from a gps unit (only useable with the serial port com2 also connected to the gps). 'exception' - generate exceptions when the line changes state. 'script' - run a user script on line state change. 'anpr_enable' - only perform anpr when trigger input circiut is completed. 'disabled' - not in use.

- `system crc`

  Display CRCs. Platforms: All.

Display CRCs of the system and configuration

- `system info`

  Display information. Platforms: All.

  Display general information about this camera. Always useful as a debugging aid.

- `system queues`

  Queues. Platforms: All.

  List all queues and their state

- `system reboot`

  Reboot camera. Platforms: All.

  Reboot the camera now unconditionally.

- `system relay`

  Toggle Relay. Platforms: All.

  Change the state of the relay

- `system relay_close`

  Close Relay. Platforms: All.

  Set the state of the relay to closed

- `system relay_open`

  Open Relay. Platforms: All.

  Set the state of the relay to open.

- `system relay_pulse` {*`closed`*} {*`period`*}

  Pulse Relay. Platforms: All.

  Set the relay to a specified state for a period

#	Name	Parameter	Description
1	Pulse Closed	closed	true to set relay closed, then, after period, open. Otherwise relay will open and, after period, close
2	Pulse Period	period	The relay pulse period in milliseconds

- `system restart`

  Restart application. Platforms: All.

  Attempt to restart the application without rebooting. May reboot camera under some circumstances.

Trigger Control (trig)

Available on platforms: All

External trigger control, for when you have wired an external vehicle detector into the camera. To use this you must set the Vehicle Image Selector filter to triggered rather than auto.

Platforms	Name	Command	Default Value	Description
All	Forward All Payloads	`trig set forward_all_payloads {value}`	false	For an already open gate, subsequent trigger stimuli will be processed for payload (while the gate is open). This will for example allow the hardware trigger to cause the gate to open and a TCP trigger (while the gate is open) could provide the payload. Please note that timing is important. If the payload-providing-trigger is late (arrives after the gate has closed) it will generate a new trigger rather than a payload to a current open trigger. See also the trigger payload format specifiers.
All	Trigger Latency	`trig set latency {value}`	0	Sets configurable delay from electrical signal edge to when we regard the trigger to have occurred.
All	Gate open period	`trig set open_period {value}`	250	Sets period during which we enable image processing for the triggering vehicle.
All	Appends the trigger id to all trigger acknowledgement messages	`trig set reply_with_trigger_id {value}`	false	
All	Simulated trigger period	`trig set simulated_period {value}`	1000	Sets the period between simulated triggers. Not for use in a production system.
All	Simulation Mode	`trig set simulation_mode {value}`	false	Enabling simulation mode causes software triggers to be generated at the rate determined by the simulated period
All	Variable Gate Open Period	`trig set variable_period {value}`	false	For an already open gate, the open period will be extended if further stimulus received (e.g. motion detection, physical trigger, TCP trigger). Under this mechanism the gate will always stay open for a minimum of the configured Gate Open Period and for no longer than 2 seconds.
All	Wait period	`trig set wait_period {value}`	700	Sets period after latency expires before we will accept another trigger. Can be used to prevent noisy triggers causing problems.

- `trig message {msg}`

  Single Simulated Trigger with content. Platforms: All.

Generates a single simulated trigger. Note, this will be generated regardless of whether simulation mode is enabled. It takes an argument which will populate the OEM trigger data field for the vehicle. How you next see this information is dependant upon your output mechanism.

#	Name	Parameter	Description
1	Message Content	msg	The OEM trigger data field.

- `trig oneshot`

  Single Simulated Trigger. Platforms: All.

  Generates a single simulated trigger. Note, this will be generated regardless of whether simulation mode is enabled.

- `trig statistics`

  Cumulative statistics. Platforms: All.

  Provides cumulative statistics of longterm trigger processing

Hardware Trigger (trig hw)

Available on platforms: All

This module manages the external trigger input on the rear of the camera. You must connect this up to a 12V external trigger input such as a loop or other vehicle detector for this to be of any use. To use this you must assign the trigger to be 'hwtrigger' in the system parameters.

Platforms	Name	Command	Default Value	Description
All	Debounce time	`trig hw set debounce {value}`	1	Number of milliseconds for which a trigger has to be stable before it is accepted by the system. Increasing this will remove false short triggers from the system at the expense of the same amount of latency in the trigger. It could also miss triggers if your trigger system produces very short pulses and you set it too high. This debounce parameter is applied for all uses of the trigger input, including scripts and exceptions.
All	Falling Edge	`trig hw set falling_edge {value}`	false	This chooses which edge of the signal will be used to trigger on, if unselected you will trigger on the rising edge of the signal. You will need to refer to the manual for your trigger source to determine which it produces when a vehicle enters the field of view.

- `trig hw clearcount`

  Clear Hardware trigger count. Platforms: All.

  Resets the count of number of hardware triggers recorded to 0

- `trig hw count`

  Hardware trigger count. Platforms: All.

Provides a count of number of hardware triggers recorded

- `trig hw status`

  Current trigger status. Platforms: All.

  Gets the current status of the trigger input signal

Serial Trigger (trig serial)

Available on platforms: All

This module manages Serial Triggers. These may be sent into com2.

Platforms	Name	Command	Default Value	Description
All	Acknowledge	`trig serial set ack_enabled` {*value*}	true	To enable/disable the generation of acks. If enabled the whole message as sent will be echoed back to you.
All	Serial Baud Rate	`trig serial set baud` {*value*}	115200	The serial port baud rate. For changes to take effect, disable then re-enable. Valid values 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400
All	Serial triggers enabled	`trig serial set enabled` {*value*}	false	If true, will detect and propogate triggers from com2.
All	Heartbeat Regular Expression	`trig serial set heartbeat_regex` {*value*}	disabled	If the string arriving on the trigger port matches this regex, it will NOT generate a trigger, it will simply echo the pattern back exactly as received. Notes: To disable it, set it to the string disabled. Heartbeat will work regardless of the ack_enabled setting
All	Trigger Regular Expression	`trig serial set trig_regex` {*value*}	(.*)\n	A regular expression (matching the Perl Regular Expression Syntax) that the incoming string must match in order for a trigger to be generated. The trigger payload will be the concatination of those parts of the incoming string that match any subexpressions in the regex, as specified by ()'s. If no ()'s are present in the trig_regex, then the entire incoming string, that matches the regex, will be used as the trigger payload. Note: A trigger payload may only contain XML legal ASCII. If it contains any illegal characters, no trigger will be generated.

TCP Trigger (trig tcp)

Available on platforms: All

This module manages TCP Triggers. These are sent in to a server socket on port 3820.

Platforms	Name	Command	Default Value	Description
All	Acknowledge	`trig tcp set ack_enabled {value}`	true	To enable/disable the generation of acks. If enabled the whole message, exactly as sent, will be echoed back to you.
All	TCP triggers enabled	`trig tcp set enabled {value}`	true	If true, will detect and propogate TCP Socket triggers.
All	Heartbeat Regular Expression	`trig tcp set heartbeat_regex {value}`	disabled	If the string arriving on the trigger port matches this regex, it will NOT generate a trigger, it will simply echo the pattern back exactly as received. Notes: To disable it, set it to the string disabled. Heartbeat will work regardless of the ack_enabled setting
All	Trigger Regular Expression	`trig tcp set trig_regex {value}`	(.*)\n	A regular expression (matching the Perl Regular Expression Syntax) that the incoming string must match in order for a trigger to be generated. The trigger payload will be the concatination of those parts of the incoming string that match any subexpressions in the regex, as specified by ()'s. If no ()'s are present in the trig_regex, then the entire incoming string, that matches the regex, will be used as the trigger payload. Note: A trigger payload may only contain XML legal ASCII. If it contains any illegal characters, no trigger will be generated.

Trigger Script (trigScript)

Available on platforms: All

This module will run a unix binary when the trigger input changes state. You must connect this up to an external trigger input for this to be of any use. To use this modules you must assign the trigger to 'script' in the system parameters. Note, each script must finish running before we will run the next script if the scripts take time to execute and the trigger makes fast transitions. The use of this feature is obviously unsupportable as you can cause anything to run which could cause the system to become unstable. It is suggested you get your script verified by PIPS if you do require support. These scripts will run a maximum of once every 5 seconds.

Platforms	Name	Command	Default Value	Description
All	Falling Edge	`trigScript set falling {value}`		This is the full path to a binary (usually a unix shell script) will be run on the falling edge of the trigger. If this is left blank or an invalid binary nothing will happen. This script will be run at bootup if the trigger input is low at bootup.

Platforms	Name	Command	Default Value	Description
All	Rising Edge	`trigScript set rising {value}`		This is the full path to a binary (usually a unix shell script) will be run on the rising edge of the trigger. If this is left blank or an invalid binary nothing will happen. This script will be run at bootup if the trigger input is high at bootup.

UTMC Delivery Module (utmc)

Available on platforms: All

The UTMC module is a delivery module which sends vehicle event data to an external computer (instation) using the UTMC protocol.

Platforms	Name	Command	Default Value	Description
All	Authenticate using username and password	`utmc set authenticate {value}`	false	authenticate
All	UTMC Camera ID	`utmc set cameraID {value}`	0	The UTMC camera ID
All	Minimum Samples for Diagnostics	`utmc set diagnostic_min_samples {value}`	10	Certain types of diagnostics (e.g. mean values or ratios) are only considered valid after a certain number of samples.
All	Diagnostic period	`utmc set diagnostic_period {value}`	20	Period in minutes between diagnostic updates
All	Diagnostics and Exceptions Enabled	`utmc set diagnostics_exceptions_enabled {value}`	false	Send diagnostics and exceptions.
All	Timeout (in seconds) for DNS caching	`utmc set dnsCacheTimeout {value}`	60	Selectable option to change the timeout used by the DNS cache within libCURL. 60 to maintain backwards compatability, or 0 to completely disable DNS caching.
All	Enabled	`utmc set enabled {value}`	false	Allows the UTMC system to be enabled and disabled. Disable it unless you are using it.
All	Minimum Samples for Exceptions	`utmc set exception_min_samples {value}`	20	Certain types of exceptions (e.g. mean values or ratios) are only considered valid after a certain number of samples.
All	Exception Period	`utmc set exception_period {value}`	5	Period in minutes between (non-realtime) exception updates
All	Host	`utmc set host {value}`	192.168.1.1:8080	IP address and port of the instation which will receive the UTMC data.
All	Maximum number of vehicles in a batch	`utmc set maxBatchSize {value}`	100	The Maximum number of vehicles that can be in a batch, if the number of vehicles becomes larger than this number we will send out a batch
All	Merge Characters	`utmc set mergechars {value}`	true	

Platforms	Name	Command	Default Value	Description
				Enable merging of possible ambiguous characters such as 8 and B prior to transmission (for tags only)
All	Maximum Files	`utmc set nlog {value}`	100	The maximum number of files which will be stored on the local drive if it is not possible to contact the instation. Once this number has been stored, the oldest will be overwritten. Warning, arbitrarily setting this to a high value may fill up the device on which you are storing the files and then the system will lose the wrong data or perform badly (or not at all).
All	Password for transport	`utmc set password {value}`		Password
All	Path	`utmc set path {value}`	utmc	The path on the http url.
All	Tag Period	`utmc set period {value}`	5	The number of minutes between sending tag messages
All	Send Tag	`utmc set sendTag {value}`	true	Send hashed plates
All	Send VRN	`utmc set sendVRN {value}`	false	Send raw plates (VRNs)
All	Time Slot	`utmc set time_slot {value}`	0	Time slot which is used by this system for transmission. Use this to spread the network load of your outstations. This is a percentage value and is used as an offset from the beginning of the time which could be used for transmission verses the end of that transmission slot - e.g. 0 it will transmit at the very beginning of the slot, at 100 at the very end.
All	ACK Timeout	`utmc set timeout {value}`	60	Number of seconds to wait for an ACK (if ACKs are enabled). Set to zero to disable
All	UTMC transport	`utmc set transport {value}`	HTTP	HTTP or HTTPS
All	Use Gzip	`utmc set useGzip {value}`	true	Encode with gzip to save bandwidth
All	Use SOAP	`utmc set useSOAP {value}`	true	Wrap with SOAP envelope
All	Username for transport	`utmc set username {value}`		Username

- `utmc clearstats`

  Clear statistics. Platforms: All.

  Reset the statistics for this module

- `utmc stats`

  Statistics. Platforms: All.

Display statistics from this module

UTMC V1.2 Delivery Module (utmcv12)

Available on platforms: All

The UTMC module is a delivery module which sends vehicle event data to an external computer (instation) using version 1.2 of the UTMC protocol.

Platforms	Name	Command	Default Value	Description
All	Authenticate using username and password	`utmcv12 set authenticate {value}`	false	authenticate
All	UTMCV1_2 Camera ID	`utmcv12 set cameraID {value}`	0	The UTMCV1_2 camera ID
All	Timeout (in seconds) for DNS caching	`utmcv12 set dnsCacheTimeout {value}`	60	Selectable option to change the timeout used by the DNS cache within libCURL. 60 to maintain backwards compatability, or 0 to completely disable DNS caching.
All	Enabled	`utmcv12 set enabled {value}`	false	Allows the UTMCV1_2 system to be enabled and disabled. Disable it unless you are using it.
All	Host	`utmcv12 set host {value}`	192.168.1.1:8080	The IP address and port of the instation which will receive the UTMCV1_2 data.
All	Merge Characters	`utmcv12 set mergechars {value}`	true	Enable merging of possible ambiguous characters such as 8 and B prior to transmission (for tags only)
All	Maximum Files	`utmcv12 set nlog {value}`	100	The maximum number of files which will be stored on the local drive if it is not possible to contact the instation. Once this number has been stored, the oldest will be overwritten. Warning, arbitrarily setting this to a high value may fill up the device on which you are storing the files and then the system will lose the wrong data or perform badly (or not at all).
All	Password for transport	`utmcv12 set password {value}`		Password
All	Path	`utmcv12 set path {value}`	utmc	The path on the http url.
All	Send ANPR Image	`utmcv12 set sendANPRImage {value}`	true	Send the ANPR Image (the image used for the ANPR.)
All	Send Asynchronous Payload	`utmcv12 set sendAsyncPayload {value}`	false	Manufacturer Specific. Will send the asynchrounous payload within the UTMC ManufacturerSpecific area.
All	Send Overview Image	`utmcv12 set sendOverviewImage {value}`	true	Send the overview image
All	Send Plate Patch Image	`utmcv12 set sendPlatePatch {value}`	true	Send patch Image

Platforms	Name	Command	Default Value	Description
All	Send Tag	`utmcv12 set sendTag {value}`	false	Send hashed plates
All	Send VRN	`utmcv12 set sendVRN {value}`	true	Send raw plates (VRNs)
All	ACK Timeout	`utmcv12 set timeout {value}`	60	Number of seconds to wait for an ACK (if ACKs are enabled). Set to zero to disable
All	UTMCV1_2 transport	`utmcv12 set transport {value}`	HTTP	HTTP or HTTPS
All	Use Gzip	`utmcv12 set useGzip {value}`	true	Encode with gzip to save bandwidth
All	Use SOAP	`utmcv12 set useSOAP {value}`	true	Wrap with SOAP envelope
All	Username for transport	`utmcv12 set username {value}`		Username
All	Async. Payload is XML	`utmcv12 set xmlPayload {value}`	false	Manufacturer Specific. The async payload contains further XML tags within the ManufacturerSpecific area.

- `utmcv12 clearstats`

  Clear statistics. Platforms: All.

  Reset the statistics for this module

- `utmcv12 stats`

  Statistics. Platforms: All.

  Display statistics from this module

VES - Violation Enforcement System (ves)

Available on platforms: All

Highly configurable system with many options. Please refer to VES Software Interface Specification

Platforms	Name	Command	Default Value	Description
All	Enable Ack	`ves set ack_enable {value}`	0	When set require ack from instation on summary and/or evidential records. Retry on ack failure. 0x01 - ack required on evidential records (ERs) 0x02 - ack required on individual summary records (SRs) 0x04 - ack required on diagnostics 0x08 - ack required on exceptions 0x10 - ack required when transferring a record from spikestore to instation

Platforms	Name	Command	Default Value	Description
				0x20 - ack required on batched summary records (BSRs)
All	Retry attempts	`ves set ack_retry {value}`	3	Retry transfers this many times before giving up
All	ack timeout	`ves set ack_timeout {value}`	500	Time to wait for an ack (mS). This timeout is used for longg transfer events. Specifically full ERs. On a system connected by hi speed links, system overhead may dominate so this and the short timeout may be identical. Where comms is slow, a separate timeout is beneficial.
All	Alternate Host	`ves set alt_host {value}`	10.1.1.1	Sets the IP address of the alternate instation.
All	Enforcement area	`ves set area {value}`	WEZ	The name of the enforcement zone. This is expected to be a three character field. However up to seven characters are accepted.
All	batched SR interval	`ves set bsr_interval {value}`	300	Interval (seconds) over which SRs are accumulated to build a batch. If no data is collected during the interval, then no batch is generated. The current batch is skipped.
All	batched SR max batches	`ves set bsr_nlog {value}`	12	Maximum number of historic SR batches which may be stored on the camera. When this number is exceeded the oldest batch will be overwritten.
All	batched SR port	`ves set bsr_port {value}`	10007	Port for transfer of batched SRs. This may be the same port as used by standard SRs.
All	Cabinet controller	`ves set cabinet {value}`		Sets the IP address the cabinet controller if present. Used to monitor the cabling and link to detect intrusions or failures.
All	cf age limit	`ves set cf_age_limit {value}`	48	Maximum time (hours) an evidential record may be retained on camera. Records older than this will be deleted.
All	No. of context images	`ves set context_count {value}`	2	Specify the number of supporting context images which must be captured. The permissable range is 0-8. The number must be even. If an odd number is entered, it will be interpreted as the next lower even number.
All	Context image offset	`ves set context_offset {value}`	250	Specify the approximate interval (mS) between context images.
All	Context image order	`ves set context_order {value}`	0	Specify whether context images are split equally before/after the event, all before the event or all after the event.
All	Country Code standard	`ves set country_code {value}`	0	Determines the standard used for country codes. 0 - PIPS ANPR Standard

Platforms	Name	Command	Default Value	Description
				2 - ISO 3166-1 Alpha 2 3 - ISO 3166-1 Alpha 3
All	D&E debug	`ves set de_debug {value}`	0	set debug flags for diagnostic and exceptions module
All	D&E Ping wait time	`ves set de_ping_wait {value}`	15000	Applicable to diagnistics & exceptions only. Amount of time the system should wait for a ping acknowledge message before giving up. The system usually pings the instation before connecting to it. Set to zero to disable these pre-transmission pings.
All	VES Debug	`ves set debug {value}`	0	Bit field specifying which code modules genetate debug information 0x00000001 - main VES process 0x00000002 - summary record transmission 0x00000004 - image (blob) record transmission 0x00000008 - session & initial key exchange 0x00000010 - message port 0x00000020 - heartbeat system 0x00000040 - DSRC trigger system 0x00000080 - NVT control port 0x00000100 - PING events 0x00000200 - show ping replies 0x00000400 - transmission of records from file buffer 0x00000800 - local file index management 0x00001000 - blob generation 0x00002000 - system timing 0x00004000 - match slots 0x00008000 - data cleanup 0x00010000 - encryption 0x00020000 - key exchange 0x00040000 - diagnostics

Platforms	Name	Command	Default Value	Description
				0x00080000 - oem specific 0x00100000 - oem specific 0x00200000 - context capture 0x00400000 - pull archtecture 0x00800000 - image synchronisation 0x01000000 - radar interface 0x02000000 - trajectory computations 0x04000000 - spikestore interface 0x08000000 - batch summary records 0x10000000 - clock drifts 0x20000000 - audit trail 0x40000000 - oem data record
All	Local Directory	`ves set directory {value}`	/ves	Directory where diagnostic and exception files will be created and stored locally on the system before transfer to the host.
All	VES Enabled	`ves set enabled {value}`	false	Enables/Disables VES. If enabled is false on camera startup, VES will not load. To get VES to load, set enabled to true and restart the camera. Once VES is loaded the enable flag has the effect of enabling/disabling the flow of events into VES.
All	Max ER file size	`ves set file_size {value}`	256	Size in kbytes to be preallocated for storage of ERs. Also sets the storage allocation on the Compact Flash device. ERs larger than this size will be discarded.
All	Heartbeat Port	`ves set hb_port {value}`	10005	The TCP/IP port number used for heartbeat messages.
All	Heartbeat period	`ves set heart_beat {value}`	0	The period in seconds between heart beat (hb) messages. If set to 0, no heart beat messages will be sent.
All	Host	`ves set host {value}`	10.1.1.1	Sets the IP address of the instation.
All	Image port	`ves set image_port {value}`	10000	port on host server expecting image data
All	Image port (background)	`ves set image_port_b {value}`	10000	port on host server expecting image data from background process. This may - and usually will - be exactly the same port as the foreground process.
All	Image Timeout	`ves set image_timeout {value}`	5	Timeout in seconds after which a camera as marked as having a possible problem
All	Switch overview to monochrome	`ves set jpeg_mono {value}`	0	Set to force overview image to monochrome

Platforms	Name	Command	Default Value	Description
All	Colour image scale factor	`ves set jpeg_scale {value}`	0	Set Colour image jpeg scale factor. Only applies to systems equiped with hardware jpeg accelerator. 0 - not scaled 1 - 360x288 2 - 180x144
All	Colour image file size	`ves set jpeg_size {value}`	22	Set Colour image jpeg file size (kbytes). Default is 22k. Only applies to systems equiped with hardware jpeg accelerator
All	Key Exchange port	`ves set key_port {value}`	10003	port on camera listening for session start and key exchange requests
All	Lane Name	`ves set lane {value}`	1	short machine name for this ANPR system. Format TBD.
All	Link Timeout	`ves set link_timeout {value}`	20	Timeout in seconds after which image or summary ports will be closed when inactive.
All	VES Site Location	`ves set location {value}`	test site description	A site specific location string. If using pipsshell and the string contains spaces, then quote the whole string with "".
All	Event match window	`ves set match_window {value}`	700	Only applicable to externally triggered systems. This window (mS) specifies the maximum time window between a trigger event and the matching image set. Alternatively, this window may be used when other events must be matched to an image event.
All	Enable trigger match	`ves set matched_trig {value}`	0	Set this parameter to configure the system to use lane controller messages 0-subsystem disabled 1-A message triggers the camera. The message is not retained. 2-A message must be assocciated with a plate event. Any plate event without an assocciated message is disgarded 3-A message triggers the camera and is subsequently associated with the plate event

Platforms	Name	Command	Default Value	Description
				Messages may arrive on either designated tcp/ip connection or on the serial port. However note that trigger events received via tcp/ip are subject to latencies beyond the control of the system and may be unusable in many circumstances
All	batched SR max count	`ves set max_batch_size {value}`	100	Maximum number of records in a SR batch. When this number is reached, the batch will be queued for transmission even if the interval has not expired.
All	Message Port	`ves set msg_port {value}`	10004	The TCP/IP port number used for messages.
All	Message Timeout	`ves set msg_timeout {value}`	60	Timeout in seconds after which the message port will be closed when inactive.
All	Camera Name	`ves set name {value}`	lane	short machine name for this ANPR system. Format TBD.
All	Number of Files	`ves set nlog {value}`	200	Number of image files to store on local disk.
All	Not Alive Counter	`ves set not_alive {value}`	10	If the heart beat process is running (heartbeat period>0) then if the heart beat fails to send its message (i.e. unable to establish a connection for this many attempts), then the system will attempt recovery action.
All	NVT control mode	`ves set nvt_mode {value}`	0	set nvt control channel mode
All	NVT port	`ves set nvt_port {value}`	10002	port on camera listening for NVT control connection
All	NVT channel timeout	`ves set nvt_timeout {value}`	5	Timeout in seconds after which the NVT port will be closed when inactive.
All	OEM contents	`ves set oem_contents {value}`	%PTs	A format string specifying how to construct the data you would like in the OEM field. NB: The OEM field is limited to 64 bytes. Excess data will be truncated.
All	Camera Direction	`ves set orientation {value}`	0	Set camera orientation according to cardinal compass point ie N, NW, W etc.
All	Ping Interval	`ves set ping_interval {value}`	300	Number of seconds interval between ping requests. These ping requests are used to establish whether and which server is online.
All	Ping Port	`ves set ping_port {value}`	10010	Selects the port on which UDP pings will be sent.
All	Ping Wait Time	`ves set ping_wait {value}`	100	Number of milliseconds to wait for a response to a ping request. Ping requests are sent before opening a connection to the host system.

Platforms	Name	Command	Default Value	Description
All	Reference image file	`ves set ref_file {value}`	mem:/ dummy.bin	The name of a file containing a set of reference jpeg images used to prepare dummy records.
All	Remote Network Router	`ves set router {value}`		Sets the IP address of the remote network router. May be used to monitor the cabling and link to detect failures.
All	Session control rules	`ves set rules {value}`	0xffff	Set the rules which specify which items will be checked before a session may be started. This may be hard coded in shipping systems but can be set to facilitate testing. Not all rules may apply to all system builds. 0x001 - check time sync 0x002 - check config crc 0x004 - check tamper switch 0x008 - check equipment 0x010 - only set secret from serial port 0x020 - terminate on network hack 0x040 - terminate on multiple password fail 0x080 - terminate on restart 0x100 - terminate on network tamper.
All	Disk Buffer scan interval	`ves set scan_interval {value}`	30	Interval in seconds between scans of disk buffer system to check for any oustanding files to transfer to host
All	ER transfer throttle	`ves set scan_throttle {value}`	500	throttle background transfer of ERs to approximately one record per this many mS. Set to 0 to disable the throttle
All	security level	`ves set security {value}`	3	This setting defines the security level used by the system 0x00 - no security 0x01 - HMAC - ERs will have an HMAC applied but are sent in clear text 0x02 - ERs are encrypted (AES256 with CBC) 0x04 - ERs are transferred with rolling keys 0x80 - Diagnostics and exceptions are encrypted NB: Batched SRs are always encryypted

Platforms	Name	Command	Default Value	Description
All	SER transfer throttle	`ves set ser_throttle {value}`	500	throttle background transfer of SERs to approximately one record per this many mS. Set to 0 to disable the throttle
All	Enable serial trigger	`ves set serial_trig {value}`	0	Set to enable serial trigger input. This will of course only be meaningfull if the hardware has a serial input available.
All	session options	`ves set session_opts {value}`	0	Set the session security level in use 0x00 - No sessions - no session security 0x01 - Sessions enabled, session control must pass CHAP 0x02 - Sessions enabled, session control is encrypted
All	short ack timeout	`ves set short_ack_timeout {value}`	500	Time to wait for an ack (mS) This timeout is used for short events. Specifically SRs SERs. On systems with slows comms benefit is gained by setting this to a more appropriate value.
All	Slot age limit	`ves set slot_age_limit {value}`	30	Maximum time (seconds) an event (summary and/or evidential record) will spend in ram before being transferred to Compact Flash store (or deleted if no CF store in use)
All	Media Source	`ves set source {value}`	NULL	The name of the media source type. This is expected to be a four character field. However up to seven characters are accepted.
All	SPIKEstore Account	`ves set store_account {value}`	vesstore	Username used for transfer of ERs to SPIKEstore.
All	SPIKEstore enable	`ves set store_enable {value}`	0	When a record is deleted from Compact Flash or ram buffers either through a specific delete request or through age expiry, an option exists to transfer the record to SPIKEstore. This store can provide very long term historical storage of records. Set this option to enable transfer to this store. NB: No facility exists to transfer these records to the host system. It is expected that this and any other housekeeping required will be the direct responsibility of the host system.
All	SPIKEstore Host IP	`ves set store_host {value}`	10.1.1.1	Sets the IP address of the SPIKEstore module.

Platforms	Name	Command	Default Value	Description
All	SPIKEstore Password	`ves set store_password {value}`	vesstore	Password used for transfer of ERs to SPIKEstore.
All	SPIKEstore Path	`ves set store_path {value}`		sub path in which files will be created on SPIKEstore server. NB: This path is NOT created on the host system by the camera software. It is assumed to exist. Transfers will fail if this path does not exist. The path, if set, should terminate in / or \ as appropriate for the SPIKEstore system. This path is used as a prefix to directories and files when they are created on the host.
All	Summary port	`ves set summary_port {value}`	10001	port on host server expecting summary data
All	Summary port (background)	`ves set summary_port_b {value}`	10001	port on host server expecting summary data from background process. This may - and usually will - be exactly the same port as the foreground process.
All	summary rate threshold	`ves set summary_rate {value}`	0	Set a control on transfer of summary records based on the outstanding count of evidential records. Set to zero to disable this control. Minimum active value:10 When set, if there are more outstanding ERs than this count, then transfer of summary records from backing store will be suspended. A hysteresis of 10% is applied.
All	Conf threshold	`ves set threshold {value}`	35	When transfer on threshold set, only ANPR reads with a threshold higher than this will be transferred to the host system.
All	Time slot	`ves set time_slot {value}`	0	Time slot which is used by this system for transmission of diagnostics & exceptions. Use this to spread the network load of your outstations. This is a percentage value and is used as an offset from the beginning of the time which could be used for transmission verses the end of that transmission slot - e.g. 0 it will transmit at the very beginning of the slot, at 100 at the very end.
All	Timeout	`ves set timeout {value}`	300	If no plate image is received on a camera for this many seconds, then a bit will be set in the status register. This may indicate a possible system failure e.g. camera fault or may indicate that a lane is closed.
All	Transfer	`ves set transfer {value}`	0x09f7	Bit field specifying which data must be transferred 0x00001 - transfer patch

Platforms	Name	Command	Default Value	Description
				0x00002 - transfer full IR 0x00004 - transfer scene 0x00008 - transfer context images 0x00010 - explicit delete required on PULL protocol 0x00020 - add text to patch & IR images 0x00040 - discard events below threshold 0x00080 - transfer ERs only on request (PULL protocol) 0x00100 - on tx failure buffer data to local disk 0x00200 - send M001 message 0x00400 - send M002 message 0x00800 - send WARNing messages 0x01000 - send ERRor messages 0x02000 - transfer Hearbeat as H001 messag 0x04000 - transfer session state messages 0x08000 - transfer summary records 0x10000 - create short evidential record 0x20000 - transfer batched summary records 0x40000 - Always transfer ERs via CF and background channel
All	TCPIP trigger port	`ves set trig_port {value}`	10006	TCP/IP Port on camera listening trigger messages. The protocol accepted on this port may be OEM specific.

- `ves aes`

  . Platforms: All.

- `ves clear`

  . Platforms: All.

- `ves delete`

  . Platforms: All.

- `ves init`

. Platforms: All.

- `ves list`

  . Platforms: All.

- `ves ping`

  . Platforms: All.

- `ves rebuild`

  . Platforms: All.

- `ves remove`

  . Platforms: All.

- `ves secret`

  . Platforms: All.

- `ves send`

  . Platforms: All.

- `ves statistics`

  VES Statistics. Platforms: All.

- `ves test`

  . Platforms: All.

- `ves trigger`

  . Platforms: All.

Vehicle Event Database (vfeDB)

Available on platforms: All

Platforms	Name	Command	Default Value	Description
All	Enabled	`vfeDB set enabled` {*value*}	false	Enables the storage capability within the vfeDB
All	Maximum Age	`vfeDB set max_age` {*value*}	0	The Maximum age records are allowed to be specified in minutes. Set to 0 for no time restriction
All	Store Analysis Images	`vfeDB set store_analysis_images` {*value*}	true	This parameter is used to control if analysis images are stored
All	Store Context Images	`vfeDB set store_context_images` {*value*}	true	This parameter is used to control if context images are stored
All	Store Overview Images	`vfeDB set store_overview_images` {*value*}	true	This parameter is used to control if overview images are stored

Platforms	Name	Command	Default Value	Description
All	Store Patch Images	`vfeDB set store_patch_images {value}`	true	This parameter is used to control if patch images are stored
All	Store Supplementary Images	`vfeDB set store_supplementary_images {value}`	true	This parameter is used to control if supplementary images are stored

- `vfeDB statistics`

  Cumulative statistics. Platforms: All.

  Provides cumulative statistics

Logging bits

These commands can be used to turn on and off real time messages from the camera about its status. These are implemented for debugging purposes in the main, and may not be meaningful at all. Turning too many of these on may adversely impact the performance of the camera. It is recommended that you use a pipsshell over SSH to watch logging, rather than serial, as the serial port can become overloaded if you turn too many messages on.

Platforms	Command	Description
All	`log acs bufferdisk_append {on/off}`	Appends to buffer disk queue
All	`log acs bufferdisk_remove {on/off}`	Removals from buffer disk queue
All	`log acs disk {on/off}`	Disk interactions
All	`log acs events {on/off}`	ACS events
All	`log acs filenames {on/off}`	Filename details
All	`log acs images {on/off}`	Image aquisition status
All	`log acs inevents {on/off}`	Incoming events
All	`log acs overviews {on/off}`	Overview aquisition status
All	`log acs transfer {on/off}`	Transfer messages
All	`log anpr allreads {on/off}`	Reports all vehicle read events, may be very noisy
All	`log anpr colour {on/off}`	Reports on colour full screen retries
All	`log anpr laneId {on/off}`	Reports information for debugging and varifiying the lane identification system - Only works on supported platforms
All	`log anpr latency {on/off}`	Reports age of departing ImageRecords associated with events
All	`log anpr noreads {on/off}`	Reports vehicle noread events
All	`log anpr patches {on/off}`	Reports on patches and full screen retries
All	`log anpr performance {on/off}`	Reports time taken by AnprLib_run
All	`log anpr reads {on/off}`	Reports vehicle read events
All	`log asyncp incoming {on/off}`	Incoming vehicle events
All	`log asyncp matches {on/off}`	Reports on Matches made between the async payloads and vehicle events. Also reports failures to match
All	`log asyncpStore payloads {on/off}`	Reports payloads added to store
All	`log bof2 incoming {on/off}`	Incoming Events

Platforms	Command	Description
All	`log bof2 messages` {*on/off*}	BOF2.2 Message Log
All	`log bof2 verbose` {*on/off*}	Display error message from the BOF2.2 instation
All	`log cam2exposure brightness` {*on/off*}	Exposure process debugging
All	`log cam2exposure settings` {*on/off*}	Shutter and gain settings debugging
All	`log client connections` {*on/off*}	Connection events
All	`log client latency` {*on/off*}	Reports age of departing ImageRecords associated with events
All	`log client overviews` {*on/off*}	Overview aquisition status
All	`log client vehicles` {*on/off*}	Vehicle events
All	`log dbmatcher incoming` {*on/off*}	Incoming vehicle events
All	`log dbmatcher matches` {*on/off*}	Matches made by the duplicate matcher
All	`log dbmatcher notification` {*on/off*}	Reasons for passing on this image
All	`log diskDB deletes` {*on/off*}	log when an entity is deleted
All	`log exposure brightness` {*on/off*}	Brightness controller actions
All	`log exposure processing` {*on/off*}	Exposure process debugging
All	`log exposure statistics` {*on/off*}	Collect some data for analysis.
All	`log exposure vehicles` {*on/off*}	Number of vehicles checks
All	`log exposure voting` {*on/off*}	Voting by the exposure subsystem on getting brighter or dimmer
All	`log fusion best` {*on/off*}	Choices made by the best plate chooser
All	`log fusion hazard` {*on/off*}	Hazard Processing
All	`log fusion incoming` {*on/off*}	Incoming vehicle events
All	`log fusion latency` {*on/off*}	Latency of events through the system
All	`log fusion matches` {*on/off*}	Matches made by the duplicate matcher
All	`log fusion noread` {*on/off*}	Noread Processing
All	`log fusion notify` {*on/off*}	Reasons for passing on this image
All	`log fusion resetting` {*on/off*}	Resetting a vehicle
All	`log fusion supplementary` {*on/off*}	Supplementary Image Processing
All	`log fusion timers` {*on/off*}	Event timer details
All	`log fusion traj` {*on/off*}	Trajectory of vehicle
All	`log gps controller` {*on/off*}	GPS Controller status reported at poll interval
All	`log gps sentences` {*on/off*}	Echo GPS sentences
All	`log gps time` {*on/off*}	Time Management status reported at poll interval
All	`log heartbeat incoming` {*on/off*}	Incoming vehicle events
All	`log hwtrigger latency` {*on/off*}	Latency of triggers through the system
All	`log ifo outputName` {*on/off*}	Filenames of output
All	`log jpegService performance` {*on/off*}	Performance measurements on the JPEG system
All	`log jpegService retries` {*on/off*}	Report whether we are having to retry JPEG compressions to fit into the buffers
All	`log jpegService type` {*on/off*}	Reports whether JPEG processing is performed in hardware, or software and what type
All	`log jtms connection` {*on/off*}	Connection issues

Platforms	Command	Description
All	`log jtms incoming` {*on/off*}	Incoming events
All	`log jtms messages` {*on/off*}	See outgoing messages, (Text format only)
All	`log jtms outgoing` {*on/off*}	Outgoing events
All	`log jtms timing` {*on/off*}	Timing information
All	`log ntp peers` {*on/off*}	Logs extracted Peers values as stored internally.
All	`log ntp raw` {*on/off*}	Logs raw unparsed data as received from the ntpq script.
All	`log ntp reach` {*on/off*}	Logs NTP reach processing.
All	`log ntp values` {*on/off*}	Logs extracted NTP values.
All	`log pciSource capIR` {*on/off*}	Outputs periodic updates of IR capture count
All	`log pciSource capOview` {*on/off*}	Outputs periodic updates of overview capture count
All	`log pciSource initialisation` {*on/off*}	Initialisation of the cameras
All	`log platefinder groups` {*on/off*}	Groups process debugging
All	`log platefinder hwoutput` {*on/off*}	FPGA output debugging
All	`log platefinder plates` {*on/off*}	Found plates debugging
All	`log platefinder searchgroups` {*on/off*}	Search group debugging
All	`log platewidth processing` {*on/off*}	PlateWidth process debugging
All	`log platewidth samples` {*on/off*}	PlateWidth collected samples debugging
All	`log platewidth shape` {*on/off*}	PlateWidth plate shape debugging
All	`log power state` {*on/off*}	Power state changes
All	`log relayOut incoming` {*on/off*}	Incoming events
All	`log relayOut outgoing` {*on/off*}	Outgoing events
All	`log sap incoming` {*on/off*}	Incoming events
All	`log sap outgoing` {*on/off*}	Outgoing events
All	`log selector detects` {*on/off*}	Reports generated vehicle detect events
All	`log selector indrops` {*on/off*}	Drops on the input queue
All	`log selector latency` {*on/off*}	Reports generated vehicle detect events associated ImageRecord age
All	`log selector multi` {*on/off*}	Show how many vehicles were detected in each image
All	`log selector notify` {*on/off*}	Notification from selector
All	`log selector performance` {*on/off*}	Reports the time taken to do the software portion of platefinding, the tracking algorithm and disposal algorithm
All	`log selector platefinder` {*on/off*}	Platefinder output
All	`log selector queue` {*on/off*}	Show the internal queue adds and deletes
All	`log selector score` {*on/off*}	Show how vehicles are scored and dropped from the internal queue
All	`log selector score_detail` {*on/off*}	Show details on scoring
All	`log selector tracking` {*on/off*}	Show details of the vehicle tracking
All	`log sensors changes` {*on/off*}	Reports changes in sensor values - currently just voltage, but may be extended to temperature etc. in the future

Platforms	Command	Description
All	`log system crcs` {*on/off*}	Reports changes in CRCs
All	`log transport_2acs failure` {*on/off*}	Brief failure details
All	`log transport_2acs items` {*on/off*}	Items being transferred
All	`log transport_2acs verbose` {*on/off*}	Verbose transfer details
All	`log transport_acs failure` {*on/off*}	Brief failure details
All	`log transport_acs items` {*on/off*}	Items being transferred
All	`log transport_acs verbose` {*on/off*}	Verbose transfer details
All	`log transport_bof2 failure` {*on/off*}	Brief failure details
All	`log transport_bof2 items` {*on/off*}	Items being transferred
All	`log transport_bof2 verbose` {*on/off*}	Verbose transfer details
All	`log transport_utmc failure` {*on/off*}	Brief failure details
All	`log transport_utmc items` {*on/off*}	Items being transferred
All	`log transport_utmc verbose` {*on/off*}	Verbose transfer details
All	`log transport_utmcv12 failure` {*on/off*}	Brief failure details
All	`log transport_utmcv12 items` {*on/off*}	Items being transferred
All	`log transport_utmcv12 verbose` {*on/off*}	Verbose transfer details
All	`log trig events` {*on/off*}	Instruments the triggers events
All	`log trig timers` {*on/off*}	Instruments the trigger timers, probably not of much interest
All	`log trigScript script` {*on/off*}	Show the running of scripts.
All	`log utmc connection` {*on/off*}	Connection issues
All	`log utmc incoming` {*on/off*}	Incoming events
All	`log utmc messages` {*on/off*}	See outgoing messages, (Text format only)
All	`log utmc outgoing` {*on/off*}	Outgoing events
All	`log utmc timing` {*on/off*}	Timing information
All	`log vfeDB deletes` {*on/off*}	Log when database records are deleted
All	`log vfeDB incoming` {*on/off*}	Incoming vehicle events
All	`log vfeDB notification` {*on/off*}	Reasons for passing on this image
All	`log vfeDB overviews` {*on/off*}	Log Overview information
All	`log vfeDB retrievals` {*on/off*}	Log when database objects are retrieved
All	`log videoStore fails` {*on/off*}	Retrieval failures
All	`log videoStore requests` {*on/off*}	Retrieval requests
All	`log viewfinder connections` {*on/off*}	Connection events
All	`log viewfinder sessions` {*on/off*}	Session events

Notifications

These commands can be used to turn on and off real time notifications from the camera. These notifications may be seen via pipsshell or via file logging, but the most useful way to use these notifications is via PIXI. To turn the notifications on/off via pipshell, use the command 'notification <source> <type> [on/off]'.

Platforms	Source	Type	Description
All	acs	datasetComplete	Provides notification of the successful transfer of an entire data-set via ACS. This notification has an

Platforms	Source	Type	Description
			additional property of 'eventId' which identifies the event the data transferred relates to.
All	acs	fileComplete	Provides notification of the successful completion of the transfer of an individual file via ACS. The notification will have an additional 'eventId' property which indicates the event that the file relates to. The property 'destpath' includes the full destination URL of the file which has now been transferred.

Chapter 7. Format strings

Format strings are a powerful tool for configuring the output from the camera. Spend some time studying this chapter to understand how they work if you want to change them. They can be used to configure file names and the format of outputted data in many places. Familiarity with the C (or other languages which have copied it) *printf* command will help in understanding what is going on here.

Only configuration parameters which specify that they are a format string may use this syntax. Please notify us if you think we should make a string into a format string.

Caution

Beware, you can configure the system incorrectly so that you get bad filenames which then cannot transfer. Be especially careful of the characters : / \ and . in your filename strings. Also, most systems won't accept filenames with control characters in them.

A format string consists of any number of parts, but essentially there are three different types of data you can put in it.

- Ordinary characters: which will just be output as is. This is the simplest type of entry. For example: if you want your filename to end in .txt, then just put .txt in the format string at the end. Note, you cannot put a \ or % in the string this way, you need to use a control character to do this.
- Control characters: which are used for unprintable characters which you can't simply enter into your string, such as **\n** for end of line. There is more detail on these in the section called “Control Characters” [84].
- Replacement specifiers: these are completely replaced by other text or numbers which are dependant upon the current item the string is working with. For example **%Pps** would be replaced by the read number plate. This is where the real power of the format strings lies. There is more detail on these in the section called “Replacement specifier” [85].

Control Characters

Each one of these will be replaced by a single control character in the output. These do *not* make sense for filenames, and are likely to cause problems with filesystems and FTP if you try to use them. They are of most use in file contents where you may want to add carriage returns or tabs.

- **\a** Alert (bell) (not often used)
- **\b** Backspace (not often used)
- **\f** Form feed, or new page (not often used)
- **\r** Carriage return. Combined with \n this is the DOS style end of line marker (e.g. **\r\n**.
- **\n** New line. This is the unix style end of line marker.
- **\t** Tab (horizontal)
- **\v** Vertical Tab (not often used)
- **** Gives a single \. Remember to put in two of these when you only want one in the output
- _ Gives a single space. You can use space directly on the P382, P392+ and P492 but this is for compatiblilty with the P357/P372. You cannot currently enter spaces in the shell, only on the web pages, so you'll need to use this from pipsshell.
- **\%** Gives a single %. Otherwise we think the % is the start of a replacement specifier

This paragraph can be skipped if you do not understand it. The escape character is ****, and can be followed by a character to cause various outputs, see above. **\octal-number** as in **\077** and **\hex-number** as in **\x3f** are also supported to output other ascii values - both of those will give a question mark character in ASCII.

Replacement specifier

The real power of format strings is in these. They all start with a % sign and there are a multitude of options for formatting the value. You then specify what the value is you want, and then how you want it presented.

Note

The format differs from printf, in that we must say what we are trying to display in the % as well as how to display it. The minimum length for a replacement specifier is 4 characters, including the % sign

The format goes as follows:

%{*replacement value*}[*format detail*]{*format*}

- *%* indicates the start of a replacement specifier
- *replacement value* is a two character string indicating what it is we wish to display here
- *format detail* is an optional string indicating more detail on how we wish to display it
- *format* is a single character indicating how we wish to display the value, e.g. as a decimal or hexadecimal number. Some values only make sense when displayed with a certain format

Format

The following characters are valid as the format in the replacement specifiers. Not all printf formats are valid.

Table 7.1. Format characters

Character	Desrciption
c	A single character
d	A signed decimal integer
i	A signed decimal integer (the same as d)
o	An octal integer
s	A string
u	An unsigned decimal integer
x	A hexadecimal integer with lower case letters
X	A hexadecimal integer with upper case letters
t	Treat the entry as numeric, and convert it to a string using the asctime() call to give something like 'Wed Jun 30 21:49:08 1993'. Trailing carriage return will be stripped.

Format Detail

An integer value placed here will ensure that the output is at least that many characters long. It will be padded with spaces. If you precede the integer with a 0 then it will pad with zeros instead. This is totally optional.

For example **The plate is %Pp8s\n** Will pad the plate string with spaces so outputting for a plate N7CTR

```
The plate is    N7CTR
```

with 4 spaces between the s and the N.

List of replacement values

Format value C

The camera detail of the plate the vehicle was read on

Platforms	Detail	Data Type	Description
All	Ce	Number	The shutter setting used for this image
All	Cg	Number	The gain setting used for this image
All	Cn	Number	The camera number (starting at zero)
All	CN	Number	The camera number (starting at one)
All	Cs	Number	The sequence setting (starting at zero)
All	CS	Number	The sequence setting (starting at one)

Format value D

The camera detail of the hazard plate the vehicle was read on

Platforms	Detail	Data Type	Description
All	De	Number	The shutter setting used for this image
All	Dg	Number	The gain setting used for this image
All	Dn	Number	The camera number (starting at zero)
All	DN	Number	The camera number (starting at one)
All	Ds	Number	The sequence setting (starting at zero)
All	DS	Number	The sequence setting (starting at one)

Format value E

Unique information about delivery event, Not usable under all circumstances

Platforms	Detail	Data Type	Description
All	Ei	Number	The Event id, which uniquly identifies the event

Format value F

Associated file. Not useable under all circumstances. Primarily for use in ACS's LPR files.

Platforms	Detail	Data Type	Description
All	F1	String	The filename of context image 1
All	F2	String	The filename of context image 2
All	F3	String	The filename of context image 3
All	F4	String	The filename of context image 4
All	F5	String	The filename of context image 5
All	F6	String	The filename of context image 6
All	F7	String	The filename of context image 7
All	F8	String	The filename of context image 8
All	Fl	String	The lpr text filename
All	Fn	String	The IR image filename

Platforms	Detail	Data Type	Description
All	FN	String	The hazard IR image filename
All	Fp	String	The patch image filename
All	FP	String	The hazard patch image filename
All	Ft	String	The transfer path (which is not prepended to the other filenames)
All	Fw	String	The wide angle, overview image filename
All	FW	String	The hazard wide angle, overview image filename

Format value H

The read hazard plate from the vehicle

Platforms	Detail	Data Type	Description
All	Ha	Number	The anpr classification (not useful with many ANPR engines)
All	HA	String	The OEM asynchronous payload. Asynchronous messages injected via serial (or TCP) will be associated with messages based on a closest match within a window. Otherwise an empty string.
All	Hc	Number	The confidence of the hazard plate read
All	HC	Number	The confidence category of the hazard plate read
All	Hf	Number	The confidence of the hardware platefinder
All	HF	Number	The field number
All	Hn	Number	The nationality code (not generally useful, see HN which is)
All	HN	String	The nationality (country and state) of origin of this plate if known
All	Ho	Number	The time offset between the trigger time and the image associated with this read (milliseconds). If not triggered, will be 0
All	Hp	String	The text of the hazard plate
All	Hr	Number	The total number of reads associated with the trigger that caused this plateread (A single trigger can lead to >1 plateread event). For a NOREAD the value will still be 1.
All	Hs	Number	The syntax confidence of the hazard plate read. This is a measure of how confident we are that the hazard plate matched the syntax of the reported country or state.
All	Ht	String	The plate tag, as extracted from the vehicle filter database. Will be blank if no tag entered, the plate is not matched, or the filter is off
All	HT	String	The OEM trigger payload. If you are using serial (or TCP/IP) triggers, this will be the OEM content of those, otherwise it will be boring. Text 'auto' will be returned if not triggered
All	Hx	Number	The x position of the plate's left edge in pixels
All	HX	Number	The width of the plate in pixels
All	Hy	Number	The y position of the plate's top edge in pixels
All	HY	Number	The height of the plate in pixels

Format value h

The camera heartbeat delivery

Platforms	Detail	Data Type	Description
All	hc	Number	The count of heartbeat delivery attempts.

Platforms	Detail	Data Type	Description
All	hf	Number	The count of heartbeat delivery failures.
All	hs	Number	A camera status bitfield (legacy).

Format value l

The image timestamp, the moment the image for the vehicle was captured.

This is a local time and accounts for timezone and daylight saving

Platforms	Detail	Data Type	Description
All	la	String	The string am for the morning, pm for the afternoon
All	lc	Number	Seconds since midnight 1st of January 1970 (commonly known as C time). This is UTC always, included for completeness.
All	ld	Number	The day of the month
All	lD	Number	The day of the year, with January the 1st as zero
All	lh	Number	The hour, 24 hour clock
All	lH	Number	The hour, 12 hour clock
All	li	Number	Milliseconds
All	ll	Number	Indicates if time is locked via NTP
All	lL	String	Indicates if time is locked via NTP as a string
All	lm	Number	Minutes past the hour
All	lM	Number	Tens of minutes past the hour
All	lo	Number	Month of the year (January as one)
All	lO	String	Month of the year as a word, in English
All	lP	String	Month of the year as three letter shortened word, in English
All	ls	Number	Seconds past the minute
All	lt	Number	Tenths of seconds
All	lu	Number	Hundredths of seconds
All	lv	Number	One if daylight saving is in effect, zero otherwise
All	lw	Number	The day of the week as a number, with zero being Sunday
All	lW	String	The day of the week as a word, in English
All	lX	String	The day of the week as a three letter shortened word, in English
All	ly	Number	The year
All	lY	Number	The last two digits of the year

Format value i

The image timestamp, the moment the image for the vehicle was captured.

This is UTC time (like GMT)

Platforms	Detail	Data Type	Description
All	ia	String	The string am for the morning, pm for the afternoon
All	ic	Number	Seconds since midnight 1st of January 1970 (commonly known as C time)
All	id	Number	The day of the month

Platforms	Detail	Data Type	Description
All	iD	Number	The day of the year, with January the 1st as zero
All	ih	Number	The hour, 24 hour clock
All	iH	Number	The hour, 12 hour clock
All	ii	Number	Milliseconds
All	il	Number	Indicates if time is locked via NTP
All	iL	String	Indicates if time is locked via NTP as a string
All	im	Number	Minutes past the hour
All	iM	Number	Tens of minutes past the hour
All	io	Number	Month of the year (January as one)
All	iO	String	Month of the year as a word, in English
All	iP	String	Month of the year as three letter shortened word, in English
All	is	Number	Seconds past the minute
All	it	Number	Tenths of seconds
All	iu	Number	Hundredths of seconds
All	iv	Number	One if daylight saving is in effect, zero otherwise
All	iw	Number	The day of the week as a number, with zero being Sunday
All	iW	String	The day of the week as a word, in English
All	iX	String	The day of the week as a three letter shortened word, in English
All	iy	Number	The year
All	iY	Number	The last two digits of the year

Format value J

JPEG data. Not useable under all circumstances. Primarily for use in output filenames to distinguish between them.

Platforms	Detail	Data Type	Description
All	Jt	Character	The file type. Will be p for a patch, n for an IR image, and w for an overview wide angle image. Context images will be 1 (for context 1), 2 (for context 2). Currently up to 8 context images are supported.

Format value L

The location of the camera

Platforms	Detail	Data Type	Description
All	Ld	Number	The whole number of degrees of latitude (north or south). Will always be positive.
All	LD	Number	The whole number of degrees of longitude (east or west). Will always be positive.
All	Le	Number	The whole number of degrees north we are. Will be negative if we are south.
All	LE	Number	The whole number of degrees east we are. Will be negative if we are west.
All	Lf	Number	The number of millidegrees of latitude we are away from the nearest degree.
All	LF	Number	The number of millidegrees of longitude we are away from the nearest degree.
All	Lg	Number	The number of microdegrees of latitude we are away from the nearest degree.

Platforms	Detail	Data Type	Description
All	LG	Number	The number of microdegrees of longitude we are away from the nearest degree.
All	Ll	Character	A character for latitude, N (north) or S (south) depending upon which hemisphere the location represents.
All	LL	Character	A character for longitude, E (east) or W (west) depending upon which side of the meridian the location represents.
All	Lm	Number	The number of minutes of latitude (north or south) that we are away from the nearest whole degree. Will always be positive.
All	LM	Number	The number of minutes of longitude (east or west) that we are away from the nearest whole degree. Will always be positive.
All	Ln	Number	The number of minutes of latitude (north or south) that we are away from the equator. Will always be positive.
All	LN	Number	The number of minutes of longitude (east or west) that we are away from the equator. Will always be positive.
All	Lo	Number	The number of minutes north that we are away from the equator. Will be negative if we are south.
All	LO	Number	The number of minutes east that we are away from the equator. Will be negative if we are south.
All	Lp	Number	The number of milliminutes of latitude we are away from the nearest minute.
All	LP	Number	The number of milliminutes of longitude we are away from the nearest minute.
All	Lq	Number	The number of microminutes of latitude we are away from the nearest minute.
All	LQ	Number	The number of microminutes of longitude we are away from the nearest minute.
All	LV	String	The string Valid or Invalid depending upon whether the location is deemed good.

Format value M

Metadata strings from the Metadata object. This is purely here so you can have the same format strings on all sites, and just change the metadata in this store

Platforms	Detail	Data Type	Description
All	Ma	String	Metadata string a
All	Mb	String	Metadata string b
All	Mc	String	Metadata string c
All	Md	String	Metadata string d
All	Me	String	Metadata string e
All	Mf	String	Metadata string f
All	Mg	String	Metadata string g
All	Mh	String	Metadata string h
All	Mi	String	Metadata string i
All	Mj	String	Metadata string j
All	Mk	String	Metadata string k
All	Ml	String	Metadata string l
All	Mm	String	Metadata string m
All	Mn	String	Metadata string n
All	Mo	String	Metadata string o

Platforms	Detail	Data Type	Description
All	Mp	String	Metadata string p
All	Mq	String	Metadata string q
All	Mr	String	Metadata string r
All	Ms	String	Metadata string s
All	Mt	String	Metadata string t
All	Mu	String	Metadata string u
All	Mv	String	Metadata string v
All	Mw	String	Metadata string w
All	Mx	String	Metadata string x
All	My	String	Metadata string y
All	Mz	String	Metadata string z

Format value o

The time offsets of overview context images

Platforms	Detail	Data Type	Description
All	o1	Number	The offset (in milliseconds) of context image 1 measured from the vehicle event timestamp
All	o2	Number	The offset (in milliseconds) of context image 2 measured from the vehicle event timestamp
All	o3	Number	The offset (in milliseconds) of context image 3 measured from the vehicle event timestamp
All	o4	Number	The offset (in milliseconds) of context image 4 measured from the vehicle event timestamp
All	o5	Number	The offset (in milliseconds) of context image 5 measured from the vehicle event timestamp
All	o6	Number	The offset (in milliseconds) of context image 6 measured from the vehicle event timestamp
All	o7	Number	The offset (in milliseconds) of context image 7 measured from the vehicle event timestamp
All	o8	Number	The offset (in milliseconds) of context image 8 measured from the vehicle event timestamp

Format value P

The read number plate from the vehicle

Platforms	Detail	Data Type	Description
All	P2	String	The 2-character nationality of origin of this plate if known, as defined by ISO 3166-1
All	P3	String	The 3-character nationality of origin of this plate if known, as defined by ISO 3166-1
All	Pa	Number	The anpr classification (not useful with many ANPR engines)
All	PA	String	The OEM asynchronous payload. Asynchronous messages injected via serial (or TCP) will be associated with messages based on a closest match within a window. Otherwise an empty string.

Platforms	Detail	Data Type	Description
All	Pc	Number	The confidence of the plate read
All	PC	Number	The confidence category of the plate read
All	Pd	String	The direction of travel of the plate read. This will be one of the following strings: AWAY, TOWARD, NOTSET. If NOTSET it indicates the direction could not be determined.
All	PD	String	The subdivision of origin of this plate if known, as defined by ISO 3166-2
All	Pf	Number	The confidence of the hardware platefinder
All	PF	Number	The field number
All	Pg	String	The source of OEM trigger
All	Pi	String	The OEM trigger payload from the first TCP/IP trigger
All	PI	Number	The trigger identifier.
All	PL	String	The lane in which the plate is located.
All	Pn	Number	The nationality code (not generally useful, see PN which is)
All	PN	String	The nationality (country and state) of origin of this plate if known
All	Po	Number	The time offset between the trigger time and the image associated with this read (milliseconds). If not triggered, will be 0
All	Pp	String	The text of the plate
All	Pr	Number	The total number of reads associated with the trigger that caused this plateread (A single trigger can lead to >1 plateread event). For a NOREAD the value will still be 1.
All	Ps	Number	The syntax confidence of the plate read. This is a measure of how confident we are that the plate matched the syntax of the reported country or state.
All	PS	String	The OEM trigger payload from the first Serial trigger
All	Pt	String	The plate tag, as extracted from the vehicle filter database. Will be blank if no tag entered, the plate is not matched, or the filter is off
All	PT	String	The OEM trigger payload. If you are using serial (or TCP/IP) triggers, this will be the OEM content of those, otherwise it will be boring. Text 'auto' will be returned if not triggered
All	Px	Number	The x position of the plate's left edge in pixels
All	PX	Number	The width of the plate in pixels
All	Py	Number	The y position of the plate's top edge in pixels
All	PY	Number	The height of the plate in pixels

Format value R

The trigger timestamp, the moment the trigger started. You should probably be using T instead of this, as if the event was not a triggered one you will not get anything in the string with R.

This is a local time and accounts for timezone and daylight saving

Platforms	Detail	Data Type	Description
All	Ra	String	The string am for the morning, pm for the afternoon
All	Rc	Number	Seconds since midnight 1st of January 1970 (commonly known as C time). This is UTC always, included for completeness.
All	Rd	Number	The day of the month
All	RD	Number	The day of the year, with January the 1st as zero

Platforms	Detail	Data Type	Description
All	Rh	Number	The hour, 24 hour clock
All	RH	Number	The hour, 12 hour clock
All	Ri	Number	Milliseconds
All	Rm	Number	Minutes past the hour
All	RM	Number	Tens of minutes past the hour
All	Ro	Number	Month of the year (January as one)
All	RO	String	Month of the year as a word, in English
All	RP	String	Month of the year as three letter shortened word, in English
All	Rs	Number	Seconds past the minute
All	Rt	Number	Tenths of seconds
All	Ru	Number	Hundredths of seconds
All	Rv	Number	One if daylight saving is in effect, zero otherwise
All	Rw	Number	The day of the week as a number, with zero being Sunday
All	RW	String	The day of the week as a word, in English
All	RX	String	The day of the week as a three letter shortened word, in English
All	Ry	Number	The year
All	RY	Number	The last two digits of the year

Format value r

The trigger timestamp, the moment the trigger started. You should probably be using t instead of this, as if the event was not a triggered one you will not get anything in the string with r.

This is UTC time (like GMT)

Platforms	Detail	Data Type	Description
All	ra	String	The string am for the morning, pm for the afternoon
All	rc	Number	Seconds since midnight 1st of January 1970 (commonly known as C time)
All	rd	Number	The day of the month
All	rD	Number	The day of the year, with January the 1st as zero
All	rh	Number	The hour, 24 hour clock
All	rH	Number	The hour, 12 hour clock
All	ri	Number	Milliseconds
All	rm	Number	Minutes past the hour
All	rM	Number	Tens of minutes past the hour
All	ro	Number	Month of the year (January as one)
All	rO	String	Month of the year as a word, in English
All	rP	String	Month of the year as three letter shortened word, in English
All	rs	Number	Seconds past the minute
All	rt	Number	Tenths of seconds
All	ru	Number	Hundredths of seconds
All	rv	Number	One if daylight saving is in effect, zero otherwise
All	rw	Number	The day of the week as a number, with zero being Sunday

Platforms	Detail	Data Type	Description
All	rW	String	The day of the week as a word, in English
All	rX	String	The day of the week as a three letter shortened word, in English
All	ry	Number	The year
All	rY	Number	The last two digits of the year

Format value S

The site details for this unit

Platforms	Detail	Data Type	Description
All	Sh	String	The site's hostname, the recommended way of identifying a site
All	Sl	Number	The system's library version number
All	Sn	Number	The system's serial number
All	Sv	Number	The system's application version number

Format value s

The supplementary images details

Platforms	Detail	Data Type	Description
All	s1	Number	The offset (in milliseconds) of supplementary image 1 measured from the vehicle event timestamp
All	s2	Number	The offset (in milliseconds) of supplementary image 2 measured from the vehicle event timestamp
All	s3	Number	Supplementary image 1 sequence setting (starting at one)
All	s4	Number	Supplementary image 2 sequence setting (starting at one)
All	s5	Number	Supplementary image 1 shutter setting
All	s6	Number	Supplementary image 2 shutter setting
All	s7	Number	Supplementary image 1 gain setting
All	s8	Number	Supplementary image 2 gain setting

Format value T

The timestamp for the vehicle, which is the trigger timestamp if the vehicle was triggered (see R), or the image timestamp if it was not (see I).

This is a local time and accounts for timezone and daylight saving

Platforms	Detail	Data Type	Description
All	Ta	String	The string am for the morning, pm for the afternoon
All	Tc	Number	Seconds since midnight 1st of January 1970 (commonly known as C time). This is UTC always, included for completeness.
All	Td	Number	The day of the month
All	TD	Number	The day of the year, with January the 1st as zero
All	Th	Number	The hour, 24 hour clock
All	TH	Number	The hour, 12 hour clock

Platforms	Detail	Data Type	Description
All	Ti	Number	Milliseconds
All	Tm	Number	Minutes past the hour
All	TM	Number	Tens of minutes past the hour
All	To	Number	Month of the year (January as one)
All	TO	String	Month of the year as a word, in English
All	TP	String	Month of the year as three letter shortened word, in English
All	Ts	Number	Seconds past the minute
All	Tt	Number	Tenths of seconds
All	Tu	Number	Hundredths of seconds
All	Tv	Number	One if daylight saving is in effect, zero otherwise
All	Tw	Number	The day of the week as a number, with zero being Sunday
All	TW	String	The day of the week as a word, in English
All	TX	String	The day of the week as a three letter shortened word, in English
All	Ty	Number	The year
All	TY	Number	The last two digits of the year

Format value t

The timestamp for the vehicle, which is the trigger timestamp if the vehicle was triggered (see r), or the image timestamp if it was not (see i).

This is UTC time (like GMT)

Platforms	Detail	Data Type	Description
All	ta	String	The string am for the morning, pm for the afternoon
All	tc	Number	Seconds since midnight 1st of January 1970 (commonly known as C time)
All	td	Number	The day of the month
All	tD	Number	The day of the year, with January the 1st as zero
All	th	Number	The hour, 24 hour clock
All	tH	Number	The hour, 12 hour clock
All	ti	Number	Milliseconds
All	tm	Number	Minutes past the hour
All	tM	Number	Tens of minutes past the hour
All	to	Number	Month of the year (January as one)
All	tO	String	Month of the year as a word, in English
All	tP	String	Month of the year as three letter shortened word, in English
All	ts	Number	Seconds past the minute
All	tt	Number	Tenths of seconds
All	tu	Number	Hundredths of seconds
All	tv	Number	One if daylight saving is in effect, zero otherwise
All	tw	Number	The day of the week as a number, with zero being Sunday
All	tW	String	The day of the week as a word, in English
All	tX	String	The day of the week as a three letter shortened word, in English
All	ty	Number	The year

Platforms	Detail	Data Type	Description
All	tY	Number	The last two digits of the year

Examples

Here are a few example format specifiers which might help you concoct your own. All the example output assumes a plate of RG51BTV has been read with confidence 96, on shutter 50/gain 9 at 15:34:30.2234 on 2008/03/27 in the eastern european timezone (GMT+2) on hostname "testsite" and that we're looking at the IR image, and the system is not triggered.

%Shs/

Input	%Shs	/
Output	testsite	/

(example result `testsite/`) This is the default ACS transfer path, just putting the hostname into the path.

acs/%Shs/

Input	acs/	%Shs	/
Output	acs/	testsite	/

(example result `acs/testsite/`) Now we have shifted to putting it into an acs subdirectory, followed by a site dependant hostname.

acs\\%Shs

Input	acs\\	%Shs	\\
Output	acs\	testsite	\

(example result `acs\testsite\`) And this version uses windows style directory separators, which is necessary for some broken windows FTP servers. Note we need to escape the \ by putting \\ in the path.

%Shs/%Iy04d%Io02d%Id02d/%Ih02d%IMd0/

Input	%Shs	/	%Iy04d	%Io02d	%Id02d	/	%Ih02d	%Idm	0/
Output	testsite	/	2008	03	27	/	12	3	0/

(example result `acs/20080327/1230/`) And now we are storing the files in time and date subdirectories, with 10 minutes worth of files per directory. Note the use of %IMd0 at the end which gives us the digit for each of the ten minutes, followed by a 0 which is copied through unchanged.

%Jtc%Id02u%Io02u%Iy04u,%Ih02u%Im02u%Is02u%Iu02u,%Pps,%Pc02u.jpg

Input	%Jtc	%Id02u	%Io02u	%Iy04u	,	%Ih02u	%Im02u	%Is02u	%Iu02u
Output	n	27	03	2008	,	12	34	30	22

Input	,	%Pps	,	%Pc02u	.jpg
Output	,	RG51BTV	,	96	.jpg

(example result `n27032008,12343022,RG51BTV,96.jpg`) This is the default image filename for ACS images. It produces a string starting with a character to identify which type of image it is. Followed by the date in DDMMYYYY format, followed by the time with hundredths of seconds, follwed by the plate and then the confidence. All of these are separated by commas.

`%Jtc%Iy04u%Io02u%Id02u_%Ih02u%Im02u%Is02u%Iu02u_%Pps_%Pc02u.jpg`

Input	%Jtc	%Iy04u	%Io02u	%Id02u	_	%Ih02u	%Im02u	%Is02u	%Iu02u
Output	n	2008	03	27	_	12	34	30	22

Input	_	%Pps	_	%Pc02u	.jpg
Output	_	RG51BTV	_	96	.jpg

(example result `n20080327_12343022_RG51BTV_96.jpg`) Now we have changed the commas to underscores, and swapped the date around to be YYYYMMDD.

`%Jtc%ty04u%to02u%td02u%th02u%tm02u%ts02u%tu02u,%Pps,%Pc02u,%Ced,%Cgd.jpg`

Input	%Jtc	%td02u	%to02u	%ty04u	%th02u	%tm02u	%ts02u	%tu02u
Output	n	27	03	2008	10	34	30	22

Input	,	%Pps	,	%Pc02u	,	%Ced	,	%Cgd	.jpg
Output	,	RG51BTV	,	96	,	50	,	9	.jpg

(example result `n2703200810343022,RG51BTV,96,50,9.jpg`) This time we are using GMT trigger time if the system is triggered, instead of local time of the image. We're also putting the shutter and gain settings for the read into the plate. We have also gone back to commas, loosing the separator between the date and time.

Chapter 8. PIXI Protocol

Note

PIXI was formerly known as NetUI, but has been renamed as it has been extended and the old name became inappropriate for the functions delivered.

This is a highly technical appendix describing the raw protocol you can use to communicate with and control the camera. This is of no interest unless you want to do that.

Using this protocol you can implement anything that the pipsshell, web interface to the camera application or manual generation tools can do. It is able to query application parameters, set them, issue commands, watch logging parameters and find out other details from the camera application. You can also get the camera to push images and event data to you, and collect image and event data (pull) from the camera.

Protocol

This protocol is run over TCP/IP to the camera, on port 3382. On OS release version 8 or later this port is firewalled off from the outside world, you will have to add a firewall rule to allow your remote application to access the camera. The protocol is a simple encapsulation of XML documents within a couple of boundaries. The XML must be correctly formed, if it is not then nothing in the message will be processed. The messages are not compressed, nor are they encrypted in any way.

Warning

Opening this port up may be a security risk to the camera.

The suggested way of working is to set up an ssh tunnel into the camera which will provide a way around the firewall without compromising it, and requires zero setup. This will also encrypt the data on the wire.

The XML may refer to some extra binary data which will follow the XML data.

The basic packet format is

Table 8.1. PIXI Packet Format

Name	Bytes	Content
Head	2	1. 0x0000 if there are no binary blobs in this data 2. 0x0001 if there are one or more binary blobs in the data
Length	2	XML Document length in bytes, as 2 byte, big endian value. Maximum length that the camera will accept is 16k. This is only the XML document portion.
Data	as required	Fully formed XML document adhering to schema below
Binary Length	0 or 4	Length of the binary blob if marked as present by the header.
Binary Data	0 or as required	Zero or more binary blobs. The position and size of the individual may be determined from the XML content.
End	4	0xffffffff

The link observes the following:

1. Multiple documents can be passed down the same link.

2. The link will stay open for a period of time, the camera will close it after 5 minutes of inactivity. To prevent this happening you can send heartbeat message which will be echoed back to you to show the camera is alive.

3. Either end can send a message unsolicited.

4. The camera responds to messages in the order in which the messages were received. This is on a per-connection basis, each connection can execute in parallel with others.

5. The camera will allow a maximum of 5 links at once.

Figure 8.1. Link with no heartbeat, camera will close when no command has been received for 5 minutes.

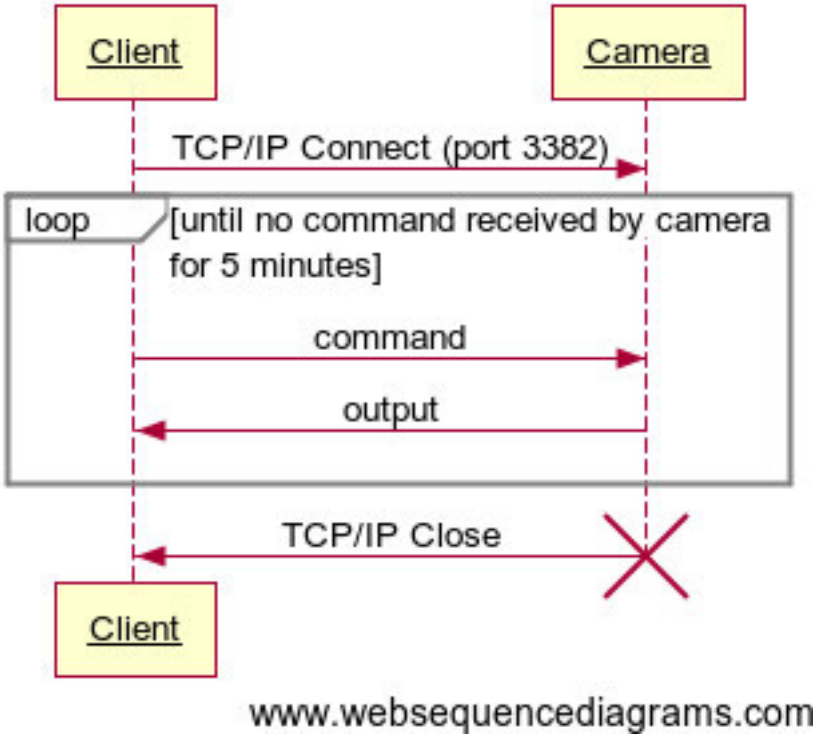
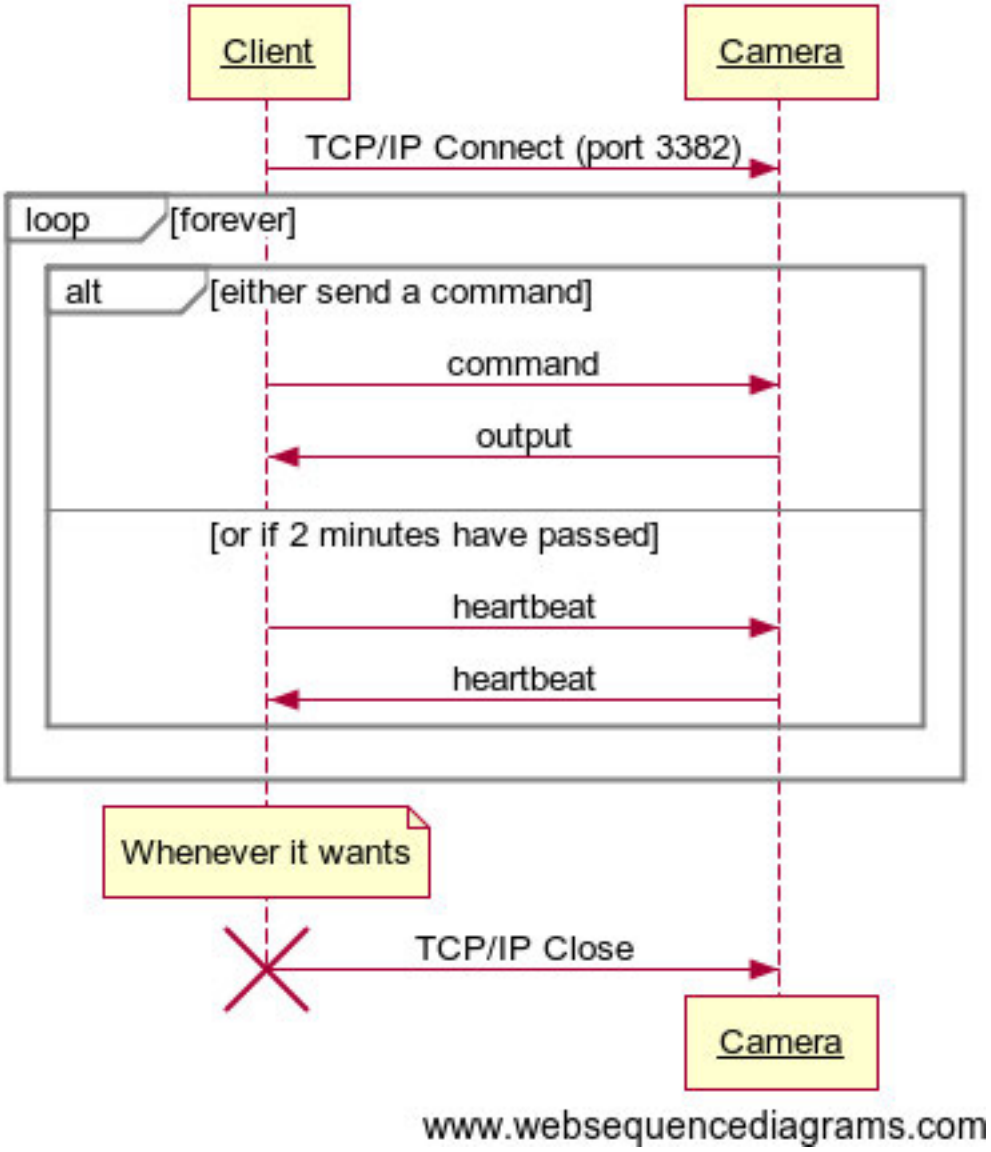


Figure 8.2. Link with heartbeat, client chooses when to end by closing the link.



Example documents

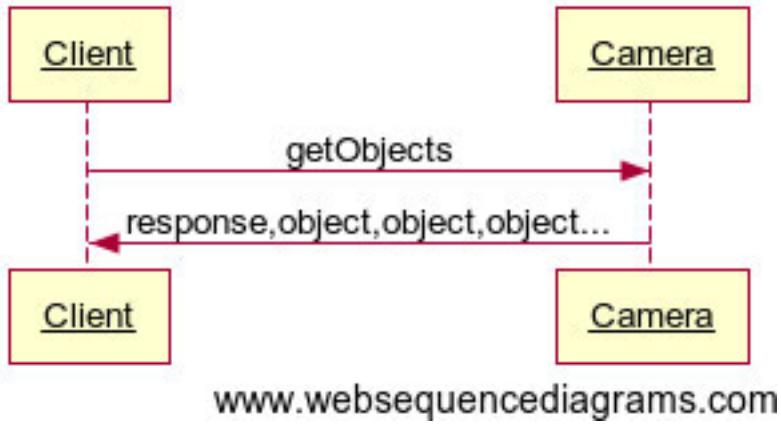
Here are few example documents to help you with composing your own messages and developing an application. In each case the PC/Instation/Handheld/other device is referred to as the Client, and the end that is implemented in the P382, P392+ and P492 is the Camera.

Note

All examples are "pretty printed" with space and formatting to make them easier to read. The camera will actually respond with documents without formatting, and for efficiency reasons I would suggest also sending unformatted documents.

Root objects

Figure 8.3. Get Root Objects - a list of all configureable objects is collected, some may have subobjects



This command to gets the root objects from the camera:

```
<?xml version="1.0"?>
<commands>
  <getObjects name=""/>
</commands>
```

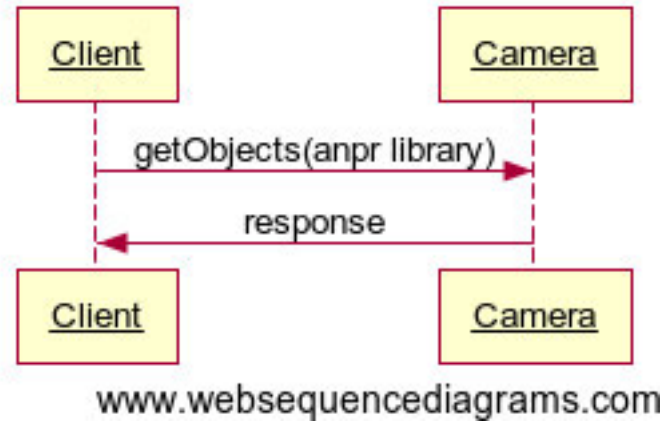
And the reply with the root objects

```
<?xml version="1.0"?>
<output>
  <response name="getObjects">
    <object/>
    <success>true</success>
  </response>
  <object name="acs">
    <longName>ACS - Access Control System</longName>
    <help>The Access Control System is an output module which sends vehicle details to an external computer for processing via the FTP protocol. It will ou
    <typeName/>
  </object>
  <object name="anpr">
    <longName>ANPR Vehicle Analyser</longName>
    <help>This module processes images to read the number plates in them.</help>
    <typeName/>
  </object>
  <object name="cam1">
    <longName>IR Camera</longName>
    <help>Controls for managing the camera and images that it takes</help>
    <typeName/>
  </object>
  <object name="cam2">
    <longName>Colour Camera</longName>
    <help>Controls for managing the camera and images that it takes</help>
    <typeName/>
  </object>
  <object name="client">
    <longName>Client vehicle event reporter</longName>
    <help>Reports individual vehicle events over the network to a client for live monitoring and diagnostics. Using the PIPS ClientView application you can
    <typeName/>
  </object>
  <object name="filter">
    <longName>Vehicle Filter</longName>
    <help>The filter system allows the system to look up number plates in a database. It is possible to filter out plates based on whether they are found o
    <typeName/>
  </object>
  <object name="fusion">
    <longName>Vehicle Fusion</longName>
    <help>The system may read multiple images of any given vehicle, and this subsystem merges those multiple vehicle reads into a single coherant result fo
    <typeName/>
  </object>
  <object name="imageFileOutput">
    <longName>Image File Outputter</longName>
    <help>Stores the images from the camera onto disk. These are just periodic images from the selected camera, like a video stream, not ones of particular
    <typeName/>
  </object>
  <object name="jpegService">
    <longName>JPEG Service</longName>
    <help>Controls the generation of JPEG images</help>
    <typeName/>
  </object>
  <object name="jtms">
    <longName>JTMS - Journey Time Measurement System</longName>
```

```
    <help>A system for delivering numberplates using very low bandwidth specifically for journey time measurement. Only minimal information is transmitted
    <typeName/>
  </object>
  <object name="metadata">
    <longName>Metadata store</longName>
    <help>This is purely an object for storing site metadata. The information stored in here is NOT used by the system, and is just for you to use when crea
    <typeName/>
  </object>
  <object name="netuis">
    <longName>Network user interface manager</longName>
    <help>The manager for the network user interfaces. These are the interfaces which the web and shell connect to.</help>
    <typeName/>
  </object>
  <object name="pci">
    <longName>PCI Interface to the cameras</longName>
    <help>Low level controls for the PCI interface talking to the cameras. This is for debugging and testing only, you can break your camera by playing.</he
    <typeName/>
  </object>
  <object name="pciSource">
    <longName>PCI Camera Source</longName>
    <help>The internal camera subsystem, connected via PCI to the processor. These controls are mostly for diagnostics.</help>
    <typeName/>
  </object>
  <object name="power">
    <longName>Power Manager</longName>
    <help>Power Management subsystem, monitoring the power coming into the system and dealing with power down when the power is cut.</help>
    <typeName/>
  </object>
  <object name="selector">
    <longName>Vehicle Image Selector</longName>
    <help>Selects images from the hardware platefinder for further analysis and ANPR by the rest of the software.</help>
    <typeName/>
  </object>
  <object name="sensors">
    <longName>Hardware Monitoring sensors</longName>
    <help>This module periodically polls the sensor values</help>
    <typeName/>
  </object>
  <object name="stdout">
    <longName>Console Logger</longName>
    <help>The logger which reports information to the standard out (stdout) device (usually the console). This is probably of no use to you as you probably
    <typeName/>
  </object>
  <object name="system">
    <longName>System Lists</longName>
    <help>A debugging object for collecting lists of objects and finding out their details</help>
    <typeName/>
  </object>
  <object name="trig">
    <longName>Trigger Control</longName>
    <help>External trigger control, for when you have wired an external vehicle detector into the camera.</help>
    <typeName/>
  </object>
  <object name="ves">
    <longName>VES - Violation Enforcement System</longName>
    <help>Highly configurable system with many options. Please refer to VES Software Interface Specification</help>
    <typeName/>
  </object>
</output>
```

Subobjects

Figure 8.4. Get subobjects of an object - a list of all subobjects is collected, some may have subobjects. The list may be empty, as in the example



A command to get a subobject's objects

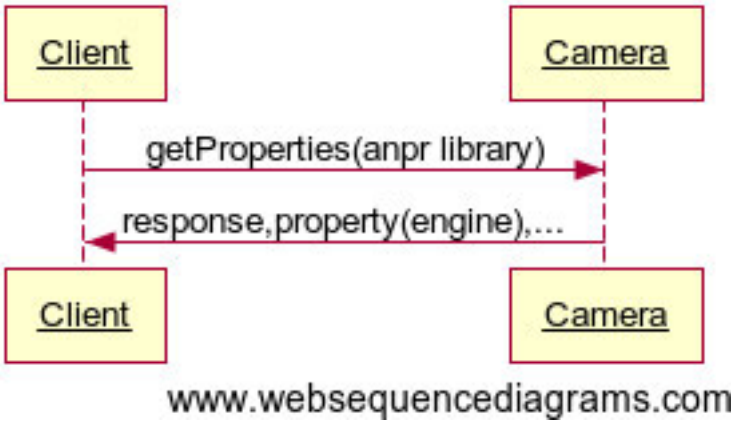
```
<?xml version="1.0"?>
<commands>
  <getObjects name="anpr library"/>
</commands>
```

And the reply, with no subobjects

```
<?xml version="1.0"?>
<output>
  <response name="getObjects">
    <object>anpr library</object>
    <success>false</success>
  </response>
</output>
```

Properties

Figure 8.5. Get properties of an object - a list of all the properties of an object. The list may be empty.



And now getting the properties of an object

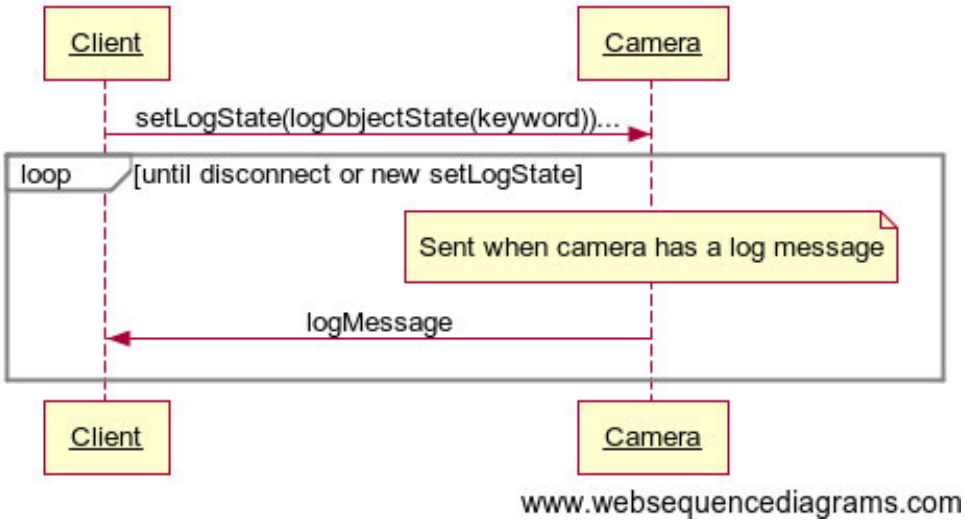
```
<?xml version="1.0"?>
<commands>
  <getProperties name="anpr library"/>
</commands>
```

And the reply, with just one property

```
<?xml version="1.0"?>
<output>
  <response name="getProperties">
    <object>anpr library</object>
    <success>true</success>
  </response>
  <property name="engine">
    <longName>Plate Reading Engine</longName>
    <default>none</default>
    <type>6</type>
    <current>libcardet.p382.so.1.2212.UK_IE</current>
    <help>The filename of the libcardet plate reading engine in use</help>
    <qualifier/>
  </property>
</output>
```

Logging

Figure 8.6. Start some logging. Asynchronous messages will be sent back by the Camera containing the log messages



Now setting up logging (note, no immediate reply)

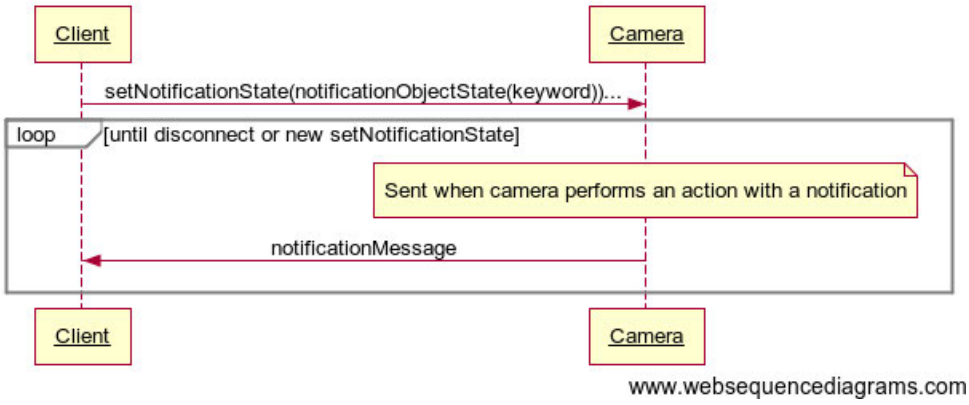
```
<?xml version="1.0"?>
<commands>
  <setLogState name="stdout">
    <logObjectState name="acs">
      <keywordState name="disk">
        <onoff>on</onoff>
      </keywordState>
      <keywordState name="events">
        <onoff>off</onoff>
      </keywordState>
      <keywordState name="filenames">
        <onoff>off</onoff>
      </keywordState>
      <keywordState name="ftp">
        <onoff>off</onoff>
      </keywordState>
      <keywordState name="inevents">
        <onoff>off</onoff>
      </keywordState>
      <keywordState name="overviews">
        <onoff>off</onoff>
      </keywordState>
    </logObjectState>
    <logObjectState name="anpr">
      <keywordState name="latency">
        <onoff>off</onoff>
      </keywordState>
      <keywordState name="noreads">
        <onoff>off</onoff>
      </keywordState>
      <keywordState name="patches">
        <onoff>off</onoff>
      </keywordState>
      <keywordState name="performance">
        <onoff>on</onoff>
      </keywordState>
      <keywordState name="reads">
        <onoff>on</onoff>
      </keywordState>
    </logObjectState>
    <logObjectState name="cam1exposure">
      <keywordState name="averages">
        <onoff>off</onoff>
      </keywordState>
      <keywordState name="brightness">
        <onoff>off</onoff>
      </keywordState>
      <keywordState name="processing">
        <onoff>off</onoff>
      </keywordState>
      <keywordState name="vehicles">
        <onoff>off</onoff>
      </keywordState>
      <keywordState name="voting">
        <onoff>off</onoff>
      </keywordState>
```

```
</logObjectState>
<logObjectState name="client">
  <keywordState name="connections">
    <onoff>off</onoff>
  </keywordState>
  <keywordState name="latency">
    <onoff>off</onoff>
  </keywordState>
  <keywordState name="overviews">
    <onoff>off</onoff>
  </keywordState>
  <keywordState name="vehicles">
    <onoff>off</onoff>
  </keywordState>
</logObjectState>
<logObjectState name="filter">
  <keywordState name="incoming">
    <onoff>off</onoff>
  </keywordState>
  <keywordState name="matches">
    <onoff>off</onoff>
  </keywordState>
  <keywordState name="notification">
    <onoff>off</onoff>
  </keywordState>
</logObjectState>
<logObjectState name="fusion">
  <keywordState name="best">
    <onoff>off</onoff>
  </keywordState>
  <keywordState name="incoming">
    <onoff>off</onoff>
  </keywordState>
  <keywordState name="latency">
    <onoff>off</onoff>
  </keywordState>
  <keywordState name="matches">
    <onoff>off</onoff>
  </keywordState>
  <keywordState name="notification">
    <onoff>off</onoff>
  </keywordState>
  <keywordState name="resetting">
    <onoff>off</onoff>
  </keywordState>
  <keywordState name="timers">
    <onoff>off</onoff>
  </keywordState>
</logObjectState>
<logObjectState name="hwtrigger">
  <keywordState name="latency">
    <onoff>off</onoff>
  </keywordState>
</logObjectState>
<logObjectState name="imageFileOutput">
  <keywordState name="outputName">
    <onoff>off</onoff>
  </keywordState>
</logObjectState>
<logObjectState name="jpegService">
  <keywordState name="HWorSW">
    <onoff>off</onoff>
  </keywordState>
</logObjectState>
<logObjectState name="jtms">
  <keywordState name="connection">
    <onoff>off</onoff>
  </keywordState>
  <keywordState name="disk">
    <onoff>off</onoff>
  </keywordState>
  <keywordState name="incoming">
    <onoff>off</onoff>
  </keywordState>
  <keywordState name="timing">
    <onoff>off</onoff>
  </keywordState>
</logObjectState>
<logObjectState name="pciInterface">
  <keywordState name="setup">
    <onoff>off</onoff>
  </keywordState>
</logObjectState>
<logObjectState name="pciSource">
  <keywordState name="capColour">
    <onoff>off</onoff>
  </keywordState>
  <keywordState name="capIR">
    <onoff>on</onoff>
  </keywordState>
  <keywordState name="initialisation">
    <onoff>off</onoff>
  </keywordState>
</logObjectState>
<logObjectState name="power">
  <keywordState name="state">
```

```
        <onoff>off</onoff>
      </keywordState>
    </logObjectState>
    <logObjectState name="selector">
      <keywordState name="detects">
        <onoff>off</onoff>
      </keywordState>
      <keywordState name="latency">
        <onoff>off</onoff>
      </keywordState>
      <keywordState name="multi">
        <onoff>off</onoff>
      </keywordState>
    </logObjectState>
    <logObjectState name="videoStore">
      <keywordState name="fails">
        <onoff>off</onoff>
      </keywordState>
    </logObjectState>
    <logObjectState name="viewfinder">
      <keywordState name="connections">
        <onoff>off</onoff>
      </keywordState>
      <keywordState name="sessions">
        <onoff>off</onoff>
      </keywordState>
    </logObjectState>
  </setLogState>
</commands>
```

Notifications

Figure 8.7. Start notification messages. Asynchronous messages will be sent back by the Camera containing the notification messages of the requested events



To enable notifications, send a setNotificationState message listing the notifications that you wish to enable. Note that there will not be an immediate reply from this message.

```
<?xml version="1.0"?>
<commands>
 <setNotificationState name="self">
  <notificationObjectState name="acs">
   <keywordState name="fileComplete">
    <onoff>on</onoff>
   </keywordState>
   <keywordState name="datasetComplete">
    <onoff>on</onoff>
   </keywordState>
  </notificationObjectState>
 </setNotificationState>
</commands>
```

When an event for which you have registered a notification occurs, you will now receive an unsolicited notificationMessage

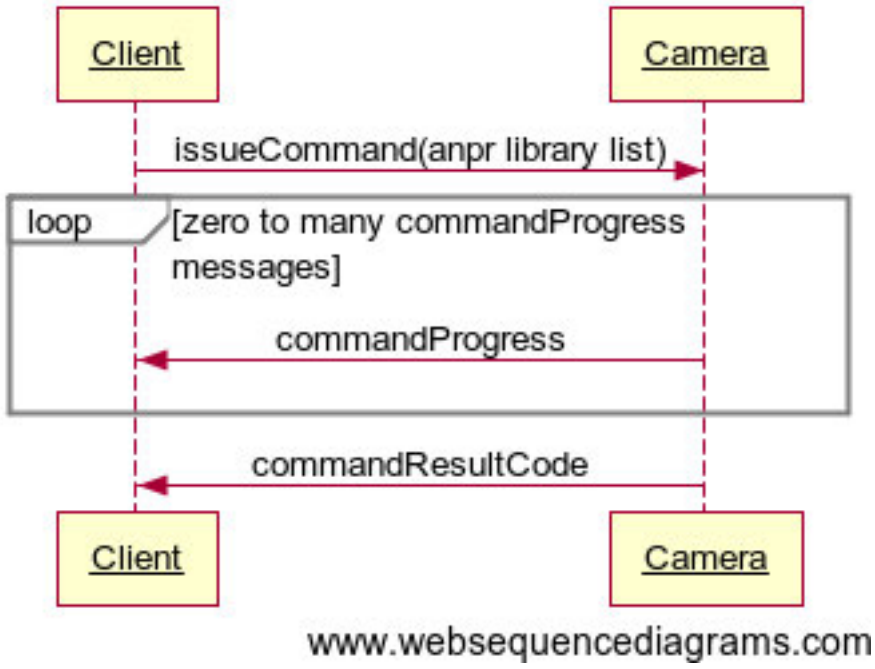
```
<?xml version="1.0"?>
<output>
 <notificationMessage>
  <source>acs</source>
  <type>fileComplete</type>
  <timeDate>2013-03-11T13:36:51.989154</timeDate>
  <destpath>ftp://10.20.13.120/11662/0008764A.lpr</destpath>
  <eventId>513dddf20008764a</eventId>
 </notificationMessage>
</output>
```

All notifications will have the source, type, and timeDate values, indicating when the notification was triggered, and what triggered it. Each notification type may have additional properties that are specific to that notification type. The available notifications are:

Platforms	Source	Type	Description
All	acs	datasetComplete	Provides notification of the successful transfer of an entire data-set via ACS. This notification has an additional property of 'eventId' which identifies the event the data transferred relates to.
All	acs	fileComplete	Provides notification of the successful completion of the transfer of an individual file via ACS. The notification will have an additional 'eventId' property which indicates the event that the file relates to. The property 'destpath' includes the full destination URL of the file which has now been transferred.

Issue Command

Figure 8.8. Issue a command and receive the responses.



A command, which has 3 replies. Note: issueCommand will probably be deprecated in the future

```
<?xml version="1.0"?>
<commands>
  <issueCommand>anpr library list</issueCommand>
</commands>
```

The output, as the command is processed

```
<?xml version="1.0"?>
<output>
  <commandProgress>Available cardet libraries</commandProgress>
</output>

<?xml version="1.0"?>
<output>
  <commandProgress>UK, Ireland, France (version 2212) - libcardet.p382.so.1.2212.UK_IE</commandProgress>
</output>
```

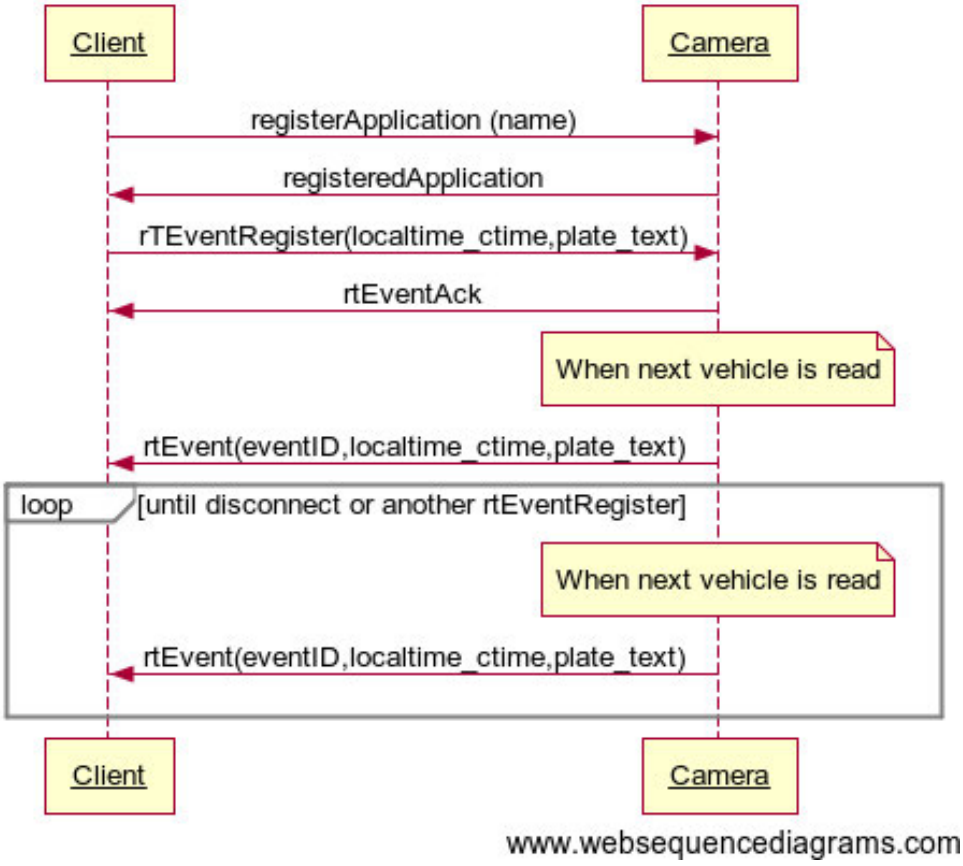
Then the result, one (and only one) of which is guaranteed to arrive

```
<?xml version="1.0"?>
<output>
  <commandResultCode>OK</commandResultCode>
```

```
</output>
```

Event data

Figure 8.9. Connect to the camera and get events as it reads vehicles.



Here we need to register the application, prior to setting up and receiving events as they occur. We are receiving minimal information, just what would be required for say a journey time measurement system. You can request as much data as you like in the rtEventRegister, and it will all be sent on every event.

First we register the application.

```
<?xml version="1.0"?>
<commands>
  <registerApplication name="test">
    <description>A test application</description>
  </registerApplication>
</commands>
```

and receive a success response

```
<?xml version="1.0"?>
<output>
  <response name="registerApplication">
    <object>test</object>
    <success>true</success>
  </response>
  <registeredApplication/>
</output>
```

And then we request real time events

```
<?xml version="1.0"?>
<commands>
  <rtEventRegister>
    <eventDetail>localtime_ctime</eventDetail>
    <eventDetail>plate_text</eventDetail>
  </rtEventRegister>
</commands>
```

Which come back like follows when they occur. Note the details *are not* in the same order as when they were requested.

```
<?xml version="1.0"?>
```

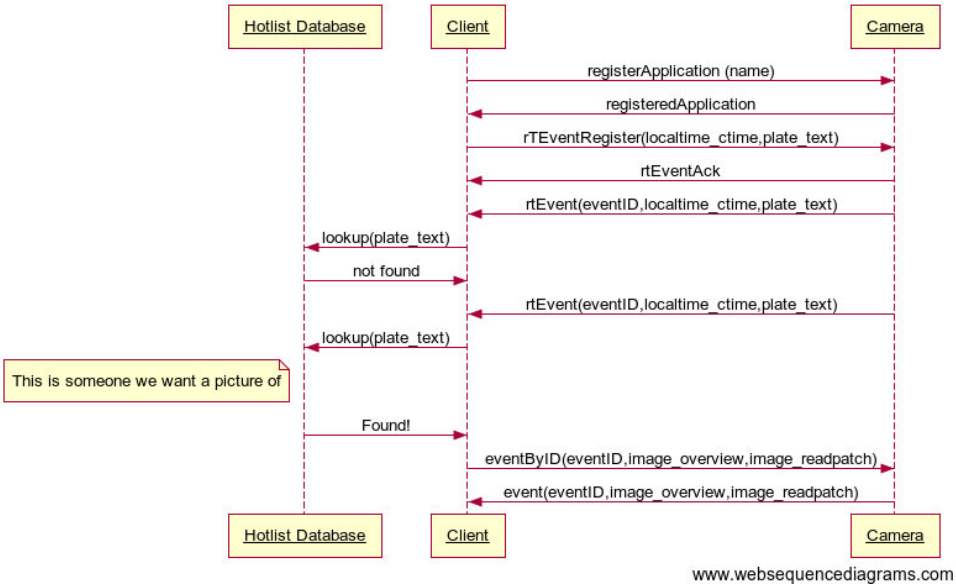
```
<output>
  <rtEvent>
    <eventID>4df5ee07000d6ae9</eventID>
    <eventData name="plate_text">
      <data>FJ05PKV</data>
    </eventData>
    <eventData name="localtime_ctime">
      <data>1308219250</data>
    </eventData>
  </rtEvent>
</output>
```

Alternatively, when registering to receive events you can specify an nlog parameter. This specifies a maximum number of events to buffer on the camera if the client application is not currently connected. This can be used to prevent data-loss should client applications disconnect.

```
<xi:include></xi:include>
```

Event data with pull

Figure 8.10. Here we are collecting (pulling) certain vehicle details when a particular vehicle is found.



As an extension to the section called “Event data” [109], here we have a database of vehicles we are particularly interested in and are requesting images for just particular vehicles. This will save bandwidth over pulling data for all vehicles.

The new message is an event request

```
<?xml version="1.0"?>
<commands>
  <eventByID>
    <eventID>4df5ee07000d6ae9</eventID>
    <eventDetail>image_overview</eventDetail>
    <eventDetail>image_readpatch</eventDetail>
  </eventByID>
</commands>
```

which gets a response indicating two binary data blobs are following the XML which can be extracted into JPEG files (JFIF).

```
<?xml version="1.0"?>
<output>
  <rtEvent>
    <eventID>4df5ee07000d6ae9</eventID>
    <eventData name="image_overview">
      <length>30412</length>
      <offset>0</offset>
    </eventData>
    <eventData name="image_readpatch">
      <length>4972</length>
      <offset>30412</offset>
    </eventData>
  </rtEvent>
</output>
```

PIXI Documents

The documents you can send across the link are in XML, as defined by the following schemas. You can send documents from the command.xsd schema, and expect to receive documents from the output.xsd schema. The definitive versions of the schemas are found on the camera under the following URLs:

1. `https://`*`camera.ip.address`*`/spikeapp/commands.xsd` - for commands to send to the camera

2. `https://`*`camera.ip.address`*`/spikeapp/output.xsd` - for output from the camera

3. `https://`*`camera.ip.address`*`/spikeapp/common.xsd` - a common file, included by both the other files

These are the definitive versions of these files, and should always be used, not any other versions. They are not generated on the fly, and will only change when software on the camera is changed.

The schemas *will* change between releases of the camera software and are not currently written as extensible. Adding the necessary text into the xsds to make them extensible also makes them confusing, so we have left it out, but consider that they will always be extended in logical ways - for example new parameters, result fields or command. We will maintain backwards compatibility, but rigid checks against historic schemas will fail.

There are a lot of correctly formed documents according to the schemas that are error conditions. For example asking for a non-existant object... for example it is required that you ask the camera for it's objects to verify that the object you want to talk about does exist.

commands.xsd

```
<?xml version="1.0" encoding="UTF-8" ?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <xsd:include schemaLocation="common.xsd"/>
  <xsd:element name="commands" type="commands"/>
  <xsd:complexType name="commands">
    <xsd:sequence minOccurs="1" maxOccurs="unbounded">
      <xsd:choice>
 <xsd:element name="heartbeat" type="heartbeat"/>
 <xsd:element name="getObjects" type="getObjects"/>
 <xsd:element name="getProperties" type="getProperties"/>
 <xsd:element name="getCommands" type="getCommands"/>
 <xsd:element name="setProperties" type="setProperties"/>
 <xsd:element name="issueCommand" type="issueCommand"/>
 <xsd:element name="getSystemInfo" type="getSystemInfo"/>
 <xsd:element name="getFormatStringTops" type="getFormatStringTops"/>
 <xsd:element name="getFormatStringDetails" type="getFormatStringDetails"/>
 <xsd:element name="getLogObjects" type="getLogObjects"/>
 <xsd:element name="getLogKeywords" type="getLogKeywords"/>
 <xsd:element name="getNotificationKeywords" type="getNotificationKeywords"/>
 <xsd:element name="getLogListeners" type="getLogListeners"/>
 <xsd:element name="getLogState" type="getLogState"/>
 <xsd:element name="setLogState" type="setLogState"/>
 <xsd:element name="getNotificationState" type="getNotificationState"/>
 <xsd:element name="setNotificationState" type="setNotificationState"/>
 <xsd:element name="registerApplication" type="registerApplication"/>
 <xsd:element name="rtEventRegister" type="rtEventRegister"/>
 <xsd:element name="eventByID" type="eventByID"/>
 <xsd:element name="listDiagnostics" type="listDiagnostics"/>
 <xsd:element name="listExceptions" type="listExceptions"/>
 <xsd:element name="getDiagnostics" type="getDiagnostics"/>
 <xsd:element name="getExceptions" type="getExceptions"/>
      </xsd:choice>
    </xsd:sequence>
  </xsd:complexType>

  <!-- ** The commands ** -->

  <xsd:complexType name="heartbeat"/>
  <!-- Response is one heartbeat message -->

  <xsd:complexType name="getObjects">
    <!-- Gets a list of the subobjects of this object. Pass objectname of "" for the base objects -->
    <!-- Response is one message containing zero or more object entities-->
    <xsd:attribute name="name" type="objectName" use="required"/>
  </xsd:complexType>

  <xsd:complexType name="getProperties">
    <!-- Objects have properties - you can get a list with this command -->
    <!-- Response is one message containing zero or more property entities-->
    <xsd:attribute name="name" type="objectName" use="required"/>
    <xsd:attribute name="currentOnly" type="xsd:boolean"/>
  </xsd:complexType>

  <xsd:complexType name="getCommands">
    <!-- Objects have commands - you can get a list with this command -->
    <!-- Response is one message containing zero or more command entities-->
```

```
    <xsd:attribute name="name" type="objectName" use="required"/>
  </xsd:complexType>

  <xsd:complexType name="setProperties">
    <!-- Objects have properties - you can attempt to set these with this command -->
    <!-- Response is one message containing the properties set -->
    <xsd:sequence>
      <xsd:element minOccurs="1" maxOccurs="unbounded"  name="property" type="property"/>
    </xsd:sequence>
    <xsd:attribute name="name" type="objectName" use="required"/>
  </xsd:complexType>
  <xsd:complexType name="property">
    <xsd:simpleContent>
      <xsd:extension base="xsd:string">
<xsd:attribute name="name" type="propertyName" use="required"/>
      </xsd:extension>
    </xsd:simpleContent>
  </xsd:complexType>

  <xsd:complexType name="issueCommand">
    <!-- This is currently how you issue the command. It will be deprecated when a replacement is made available -->
    <!-- Response is zero or more commandProgress followed by a resultCode -->
    <xsd:simpleContent>
      <xsd:extension base="xsd:string"/>
      <!-- Place the object, command & parameters in that order, space seperated here -->
    </xsd:simpleContent>
  </xsd:complexType>

  <xsd:complexType name="getSystemInfo"/>
  <!-- Gets a set of information about the system -->
  <!-- Response is one systemInfo message -->

  <xsd:complexType name="getFormatStringTops"/>
  <!-- Gets a list of all format string initial characters -->
  <!-- Response is zero or more formatStringTop entities -->

  <xsd:complexType name="getFormatStringDetails">
    <!-- Gets a list of format strings with a given intial character -->
    <xsd:attribute name="name" type="formatStringTopName" use="required"/>
  </xsd:complexType>

  <xsd:complexType name="getLogObjects"/>
  <!-- Gets a list of loggingObjects which can produce logging. NOT the same as property/command objects. Also no nesting here -->
  <!-- Response is one or more logObject entities -->

  <xsd:complexType name="getLogKeywords">
    <!-- Gets a list of  keywords for the given logging object -->
    <!-- Response is zero or more logKeywords -->
    <xsd:attribute name="name" type="logObjectName" use="required"/>
  </xsd:complexType>

  <xsd:complexType name="getNotificationKeywords">
    <!-- Gets a list of  keywords for the given logging object -->
    <!-- Response is zero or more logKeywords -->
    <xsd:attribute name="name" type="logObjectName" use="required"/>
  </xsd:complexType>

  <xsd:complexType name="getLogListeners"/>
  <!-- Get a list of objects that can receive log messages -->
  <!-- Response is zero or more logListener -->

  <xsd:complexType name="getLogState">
    <!-- Get the current state of the logging for a log receiver -->
    <!-- Response is one or more logObjectState messages -->
    <xsd:attribute name="name" type="logListenerName" use="required"/>
  </xsd:complexType>

  <xsd:complexType name="getNotificationState">
    <!-- Get the current state of the notifications for a log receiver -->
    <!-- Response is one or more notificationObjectState messages -->
    <xsd:attribute name="name" type="logListenerName" use="required"/>
  </xsd:complexType>

  <xsd:complexType name="setLogState">
    <!-- Set the state of logging for a log receiver -->
    <!-- THERE IS CURRENTLY NO REPLY TO THIS MESSAGE -->
    <xsd:sequence>
      <xsd:choice maxOccurs="unbounded" minOccurs="1">
<xsd:element name="logObjectState" type="logObjectState"/>
      </xsd:choice>
    </xsd:sequence>
    <xsd:attribute name="name" type="logListenerName" use="required"/>
  </xsd:complexType>

  <xsd:complexType name="setNotificationState">
    <!-- Set the state of notifications for a log receiver -->
    <!-- THERE IS CURRENTLY NO REPLY TO THIS MESSAGE -->
    <xsd:sequence>
      <xsd:choice maxOccurs="unbounded" minOccurs="1">
<xsd:element name="notificationObjectState" type="notificationObjectState"/>
      </xsd:choice>
    </xsd:sequence>
    <xsd:attribute name="name" type="logListenerName" use="required"/>
  </xsd:complexType>

  <xsd:complexType name="registerApplication">
```

```
    <!-- Registers an application so that other commands which require an application registration can be used -->
    <!-- Response is one registeredApplication message - wait for it being accepted before using any of those other commands -->
    <!-- Requires the appropriate software options enabled -->
    <xsd:sequence>
      <xsd:element name="description" type="xsd:string"/> <!-- A human readable description of the application -->
    </xsd:sequence>
    <xsd:attribute name="name" type="applicationName" use="required"/> <!-- Note that if multiple PIXI clients connect to the camera, each must connect with
  </xsd:complexType>

<xsd:complexType name="getRegisteredApplications/">
    <!-- Requests the names of all of the currently registered applications currently connected to the camera. -->
    <!-- Response is 0 or more registeredApplicationName elements, listing the names of all of the currently registered applications. -->
    <!-- Requires the appropriate software options enabled -->


  <xsd:complexType name="rtEventRegister">
    <!-- Requires a successful registerApplication prior to use -->
    <!-- Response is one rtEventAck message - subsequent rTEvents will contain the new descriptions -->
    <!-- The description used will REPLACE any previous calls -->
    <!-- Once you have the response to this you are guaranteed to receive all events in sequence up until the last one you receive. The sequence used is "ev
    <!-- Real time events may not arrive in precise time order. This is not a bug. -->
    <!-- It it deliberate that you cannot request previous eventID here. Next eventID would not make sense -->
    <xsd:sequence>
      <xsd:sequence maxOccurs="unbounded" minOccurs="0"> <!-- The use of zero entries disables further notification -->
 <xsd:element name="eventDetail" type="eventDetail"/>
      </xsd:sequence>
      <xsd:sequence maxOccurs="unbounded" minOccurs="0">
 <xsd:element name="nlog" type="nonNegativeInteger"/>
      </xsd:sequence>
    </xsd:sequence>
  </xsd:complexType>

 <xsd:simpleType name="nonNegativeInteger" id="nonNegativeInteger">
   <xsd:restriction base="xsd:integer">
    <xsd:minInclusive value="0"/>
   </xsd:restriction>
 </xsd:simpleType>

  <xsd:complexType name="eventByID">
    <!-- Requires a successful registerApplication prior to use -->
    <!-- Response is one event message -->
    <!-- It is required that you store or cache this result in your application rather than recalling regularly for any reason -->
    <xsd:sequence>
      <xsd:element name="eventID" type="eventID"/><!-- Only if you're requesting a previous or next event, you may get the first by using eventID 0 with pre
      <xsd:element name="prevNext" type="prevNext" minOccurs="0" maxOccurs="1"/> <!-- You will receive the previous or next event's id as well as the curren
      <xsd:sequence maxOccurs="unbounded" minOccurs="1">
 <xsd:element name="eventDetail" type="eventDetail"/>
      </xsd:sequence>
    </xsd:sequence>
  </xsd:complexType>

  <xsd:complexType name="listDiagnostics">
  <!-- Get a list of diagnostic entries -->
  <!-- Response is zero or more diagnosticList -->
    <xsd:sequence>
      <xsd:element name="helpIncluded" type="xsd:boolean"/> <!-- Whether the replies should include help -->
    </xsd:sequence>
  </xsd:complexType>

  <xsd:complexType name="listExceptions">
  <!-- Get a list of exceptions entries -->
  <!-- Response is zero or more exceptionList -->
    <xsd:sequence>
      <xsd:element name="helpIncluded" type="xsd:boolean"/> <!-- Whether the replies should include help -->
    </xsd:sequence>
  </xsd:complexType>

  <xsd:complexType name="getDiagnostics">
    <!-- Requires a successful registerApplication prior to use -->
    <!-- Response is one diagnosticData message containing values for the diagnostics requested -->
    <!-- These is not yet defined properly, do not base anything around this message as we want to change it -->
    <xsd:sequence>
      <xsd:choice maxOccurs="unbounded" minOccurs="0"> <!-- The use of zero entries disabled further notification -->
 <xsd:element name="diagnosticName" type="diagnosticName"/>
      </xsd:choice>
    </xsd:sequence>
  </xsd:complexType>

  <xsd:complexType name="getExceptions">
    <!-- Requires a successful registerApplication prior to use -->
    <!-- Registers this application to receive the exceptions requested -->
    <!-- Response will be a getExceptionsAck and then list of excptionData, delivered when it is generated -->
    <!-- The list used will REPLACE any previous calls -->
    <xsd:sequence>
      <xsd:choice maxOccurs="unbounded" minOccurs="0"> <!-- The use of zero entries disabled further notification -->
 <xsd:element name="exceptionName" type="exceptionName"/>
      </xsd:choice>
    </xsd:sequence>
  </xsd:complexType>
</xsd:schema>
```

output.xsd

```
<?xml version="1.0" encoding="UTF-8" ?>
<xsd:schema  xmlns:xsd="http://www.w3.org/2001/XMLSchema">
```

```
 <xsd:include schemaLocation="common.xsd"/>
 <xsd:element name="output" type="output"/>
 <xsd:complexType name="output">
   <xsd:sequence minOccurs="1" maxOccurs="unbounded">
     <xsd:element minOccurs="0" maxOccurs="1" name="response" type="response"/>
     <xsd:choice>
<xsd:element name="heartbeat" type="heartbeat"/>
<xsd:group ref="objectSequence"/>
<xsd:group ref="propertySequence"/>
<xsd:group ref="commandSequence"/>
<xsd:group ref="setPropertySequence"/>
<xsd:element name="commandProgress" type="commandProgress"/>
<xsd:element name="commandResultCode" type="commandResultCode"/>
<xsd:element name="systemInfo" type="systemInfo"/>
<xsd:element maxOccurs="unbounded" minOccurs="1" name="formatStringTop" type="formatStringTop"/>
<xsd:group ref="formatStringDetailSequence"/>
<xsd:group ref="logObjectSequence"/>
<xsd:group ref="logKeywordSequence"/>
<xsd:group ref="notificationKeywordSequence"/>
<xsd:element maxOccurs="unbounded" minOccurs="1" name="logListener" type="logListener"/>
<xsd:element maxOccurs="unbounded" minOccurs="1" name="logObjectState" type="logObjectState"/>
<!-- This next message is unsolicited -->
<xsd:element name="logMessage" type="logMessage"/>
<!-- This next message is unsolicited -->
<xsd:element name="notificationMessage" type="notificationMessage"/>

<xsd:group ref="registeredApplicationNameSequence"/>
<xsd:element name="registeredApplication" type="registeredApplication"/>
<xsd:element name="rtEventAck" type="rtEventAck"/>
<!-- This next message is unsolicited -->
<xsd:element name="rtEvent" type="event"/>
<xsd:element name="event" type="event"/>
<xsd:element maxOccurs="unbounded" minOccurs="1" name="diagnosticEntry" type="diagnosticEntry"/>
<xsd:element maxOccurs="unbounded" minOccurs="1" name="exceptionEntry" type="exceptionEntry"/>
<xsd:element maxOccurs="unbounded" minOccurs="1" name="diagnosticData" type="diagnosticData"/>
<!-- This next message is unsolicited -->
<xsd:element maxOccurs="unbounded" minOccurs="1" name="exceptionData" type="exceptionData"/>
     </xsd:choice>
   </xsd:sequence>
 </xsd:complexType>

 <!-- ** Output messages ** -->

 <!-- Generic Response header -->
 <xsd:complexType name="response">
   <xsd:sequence>
     <xsd:element name="object" minOccurs="0" maxOccurs="1" type="internalNameBlank"/> <!-- Context dependant - should be obvious -->
     <xsd:element name="success" type="xsd:boolean"/>
     <xsd:element name="errorText" minOccurs="0" maxOccurs="1" type="xsd:string"/> <!-- May appear if success=false - english text describing failure -->
   </xsd:sequence>
   <xsd:attribute name="name" type="xsd:token" use="required"/> <!-- The name of the command that initiated this response -->
 </xsd:complexType>

 <xsd:complexType name="heartbeat"/>
 <!-- Sent in response to a heartbeat message -->

 <xsd:group name="objectSequence">
   <!-- Sent in response to a getObjects message -->
   <xsd:sequence>
     <xsd:element maxOccurs="unbounded" minOccurs="0" name="object" type="object"/>
   </xsd:sequence>
 </xsd:group>
 <xsd:complexType name="object">
   <xsd:sequence>
     <xsd:element name="longName" type="xsd:token"/>
     <xsd:element name="help" type="xsd:string"/>
     <xsd:element name="typeName" type="xsd:string"/>
   </xsd:sequence>
   <xsd:attribute name="name" type="objectName" use="required"/>
 </xsd:complexType>


 <xsd:group name="propertySequence">
   <!-- Sent in response to a getProperties message -->
   <xsd:sequence>
     <xsd:element maxOccurs="unbounded" minOccurs="1" name="property" type="property"/>
   </xsd:sequence>
 </xsd:group>
 <xsd:complexType name="property">
   <xsd:sequence>
     <xsd:element minOccurs="0" maxOccurs="1" name="longName" type="xsd:token"/>
     <xsd:element minOccurs="0" maxOccurs="1" name="default" type="xsd:string"/>
     <xsd:element minOccurs="0" maxOccurs="1" name="type" type="typeid"/>
     <xsd:element name="current" type="xsd:string"/> <!-- Will be the only thing present if currentOnly is true -->
     <xsd:element minOccurs="0" maxOccurs="1" name="help" type="xsd:string"/>
     <xsd:element minOccurs="0" maxOccurs="1" name="qualifier" type="xsd:string"/>
   </xsd:sequence>
   <xsd:attribute name="name" type="propertyName" use="required"/>
 </xsd:complexType>

 <xsd:group name="commandSequence">
   <!-- Sent in response to a getCommands message -->
   <xsd:sequence>
     <xsd:element maxOccurs="unbounded" minOccurs="0" name="command" type="command"/>
   </xsd:sequence>
 </xsd:group>
```

```
 <xsd:complexType name="command">
   <xsd:sequence>
     <xsd:element name="longName" type="xsd:token"/>
     <xsd:element name="help" type="xsd:string"/>
     <xsd:element maxOccurs="unbounded" minOccurs="0" name="parameter" type="parameter"/>
   </xsd:sequence>
   <xsd:attribute name="name" type="commandName" use="required"/>
 </xsd:complexType>
 <xsd:complexType name="parameter">
   <xsd:sequence>
     <xsd:element name="longName" type="xsd:token"/>
     <xsd:element name="default" type="xsd:string"/>
     <xsd:element name="type" type="xsd:token"/>
     <xsd:element name="help" type="xsd:string"/>
     <xsd:element name="qualifier" type="xsd:string"/>
   </xsd:sequence>
   <xsd:attribute name="name" type="parameterName" use="required"/>
 </xsd:complexType>

 <xsd:group name="setPropertySequence">
   <!-- Sent in response to a setProperties message -->
   <!-- Only valid properties will be returned here -->
   <xsd:sequence>
     <xsd:element minOccurs="1" maxOccurs="unbounded" name="setProperty" type="setProperty"/>
   </xsd:sequence>
 </xsd:group>
 <xsd:complexType name="setProperty">
   <xsd:sequence>
     <xsd:element name="requestedValue" type="xsd:string"/>
     <xsd:element name="success" type="xsd:boolean"/>
     <xsd:element name="newValue" type="xsd:string"/>
   </xsd:sequence>
   <xsd:attribute name="name" type="propertyName" use="required"/>
 </xsd:complexType>

 <xsd:complexType name="commandProgress">
   <!-- Zero or more of these will be emitted as a command is executed, which may take some time to complete -->
   <xsd:simpleContent>
     <xsd:extension base="xsd:string"/>
   </xsd:simpleContent>
 </xsd:complexType>

 <xsd:complexType name="commandResultCode">
   <!-- One of these will be emitted once the command is completed, which may take some time to complete -->
   <xsd:simpleContent>
     <xsd:extension base="commandResults"/>
   </xsd:simpleContent>
 </xsd:complexType>


 <xsd:complexType name="systemInfo">
   <!-- Sent in response to a getSystemInfo message -->
   <xsd:sequence minOccurs="1" maxOccurs="unbounded">
     <xsd:element name="infoElement" type="infoElement"/>
   </xsd:sequence>
 </xsd:complexType>
 <xsd:complexType name="infoElement">
   <xsd:simpleContent>
     <xsd:extension base="xsd:string">
<xsd:attribute name="name" type="internalName" use="required"/>
     </xsd:extension>
   </xsd:simpleContent>
 </xsd:complexType>

 <xsd:complexType name="formatStringTop">
   <!-- Sent in response to a getFormatStringTops message -->
   <xsd:sequence>
     <xsd:element name="help" type="xsd:string"/>
     <xsd:element name="xml" type="eventTop"/>
   </xsd:sequence>
   <xsd:attribute name="name" type="formatStringTopName" use="required"/>
 </xsd:complexType>

 <xsd:group name="formatStringDetailSequence">
   <!-- Sent in response to a getFormatStringDetails message -->
   <xsd:sequence>
     <xsd:element maxOccurs="unbounded" minOccurs="1" name="formatStringDetail" type="formatStringDetail"/>
   </xsd:sequence>
 </xsd:group>
 <xsd:complexType name="formatStringDetail">
   <xsd:sequence>
     <xsd:element name="help" type="xsd:string"/>
     <xsd:element name="type" type="xsd:token"/>
     <xsd:element name="xml" type="eventDetail"/>
   </xsd:sequence>
   <xsd:attribute name="name" type="formatStringDetailName" use="required"/>
 </xsd:complexType>

 <xsd:group name="logObjectSequence">
   <!-- Sent in response to a getLogObjects message -->
   <xsd:sequence>
     <xsd:element maxOccurs="unbounded" minOccurs="1" name="logObject" type="logObject"/>
   </xsd:sequence>
 </xsd:group>
 <xsd:complexType name="logObject">
   <!-- NOT the same as property/command objects. Also no nesting here -->
```

```
    <xsd:attribute name="name" type="objectName" use="required"/>
  </xsd:complexType>

  <xsd:group name="logKeywordSequence">
    <xsd:sequence>
      <xsd:element maxOccurs="unbounded" minOccurs="1" name="logKeyword" type="logKeyword"/>
    </xsd:sequence>
  </xsd:group>
  <xsd:complexType name="logKeyword">
    <xsd:sequence>
      <xsd:element name="help" type="xsd:token"/>
    </xsd:sequence>
    <xsd:attribute name="name" type="logKeywordName" use="required"/>
  </xsd:complexType>

  <xsd:group name="notificationKeywordSequence">
    <xsd:sequence>
      <xsd:element maxOccurs="unbounded" minOccurs="1" name="notificationKeyword" type="notificationKeyword"/>
    </xsd:sequence>
  </xsd:group>
  <xsd:complexType name="notificationKeyword">
    <xsd:sequence>
      <xsd:element name="help" type="xsd:token"/>
    </xsd:sequence>
    <xsd:attribute name="name" type="notificationKeywordName" use="required"/>
  </xsd:complexType>

  <xsd:complexType name="resultCode">
    <xsd:simpleContent>
      <xsd:extension base="xsd:token"/>
    </xsd:simpleContent>
  </xsd:complexType>

  <xsd:complexType name="logListener">
    <xsd:attribute name="name" type="logListenerName" use="required"/>
  </xsd:complexType>

  <xsd:complexType name="logMessage">
    <!-- An unsolicted logMessage, sent as and when logging events occur -->
    <xsd:sequence>
      <xsd:element name="timeDate" minOccurs="0" maxOccurs="1" type="xsd:string"/>
      <xsd:element name="file" minOccurs="0" maxOccurs="1" type="xsd:token"/>
      <xsd:element name="lineNumber" minOccurs="0" maxOccurs="1" type="xsd:positiveInteger"/>
      <xsd:element name="text" type="xsd:string"/>
    </xsd:sequence>
  </xsd:complexType>

  <xsd:complexType name="notificationMessage">
    <!-- An unsolicted notificationMessage, sent as and when notification events occur. Additional elements are added dependent upon the specific notificati
    <xsd:sequence>
      <xsd:element name="source" minOccurs="1" maxOccurs="1" type="xsd:string"/>
      <xsd:element name="type" minOccurs="1" maxOccurs="1" type="xsd:string"/>
      <xsd:element name="timeDate" minOccurs="1" maxOccurs="1" type="xsd:dateTime"/>
      <xsd:any minOccurs="0" maxOccurs="unbounded" processContents="lax"/>
    </xsd:sequence>
  </xsd:complexType>

  <xsd:group name="registeredApplicationNameSequence">
    <!-- Sent in response to a getRegisteredApplications message -->
    <xsd:sequence>
      <xsd:element maxOccurs="unbounded" minOccurs="1" name="registeredApplicationName" type="xsd:string"/>
    </xsd:sequence>
  </xsd:group>

  <xsd:complexType name="registeredApplication">
    <!-- Object name will be name from request -->
    <xsd:attribute name="reason" type="xsd:string"/> <!-- If the request failed, an english human readable response will be given here-->
  </xsd:complexType>

  <xsd:complexType name="rtEventAck"/>

  <xsd:complexType name="eventData">
    <xsd:choice>
      <xsd:element name="data" type="xsd:string"/> <!-- This is for all non-image data -->
      <xsd:sequence> <!-- This is for image data in the trailing binary section -->
<xsd:element name="length" type="xsd:positiveInteger"/>
<xsd:element name="offset" type="xsd:nonNegativeInteger"/>
<xsd:element name="timeoffset" minOccurs="0" maxOccurs="1" type="xsd:integer"/>
      </xsd:sequence>
    </xsd:choice>
    <xsd:attribute name="name" type="eventDetail" use="required"/>
  </xsd:complexType>

  <xsd:complexType name="event">
    <xsd:sequence>
      <xsd:element name="eventID" type="eventID"/>
      <xsd:element name="previousEventID" minOccurs="0" maxOccurs="1" type="eventID"/> <!-- Previous event id in sequence, only if requested -->
      <xsd:element name="nextEventID" minOccurs="0" maxOccurs="1" type="eventID"/> <!-- Next event id in sequence, only if requested -->
      <xsd:element name="eventData" minOccurs="0" maxOccurs="unbounded" type="eventData"/>
    </xsd:sequence>
  </xsd:complexType>

  <xsd:complexType name="diagnosticEntry">
    <xsd:sequence>
      <xsd:element name="type" type="diagnosticType"/>
      <xsd:element name="resettable" type="xsd:boolean"/>
```

```
      <xsd:element name="lowerLimit" type="xsd:integer"/>
      <xsd:element name="upperLimit" type="xsd:integer"/>
      <xsd:element name="minDiagnosticSamples" type="xsd:positiveInteger"/>
      <xsd:element name="minExceptionSamples" type="xsd:positiveInteger"/>
      <xsd:element name="hysteresis" type="xsd:boolean"/>
      <xsd:element name="units" type="diagnosticUnits"/>
      <xsd:element name="help" minOccurs="0" maxOccurs="1" type="xsd:string"/>
    </xsd:sequence>
    <xsd:attribute name="name" type="diagnosticName" use="required"/>
  </xsd:complexType>

  <xsd:complexType name="exceptionEntry">
    <xsd:sequence>
      <xsd:element name="type" type="exceptionType"/>
      <xsd:element name="state" minOccurs="0" maxOccurs="1" type="xsd:boolean"/> <!-- Included for boolean exceptions to show current state -->
      <xsd:element name="help" minOccurs="0" maxOccurs="1" type="xsd:string"/>
    </xsd:sequence>
    <xsd:attribute name="name" type="exceptionName" use="required"/>
  </xsd:complexType>

  <xsd:complexType name="getExceptionsAck"/>

  <xsd:complexType name="diagnosticData">
    <xsd:sequence>
      <xsd:element name="value" type="xsd:float"/>
    </xsd:sequence>
    <xsd:attribute name="name" type="diagnosticName"  use="required"/>
  </xsd:complexType>

  <xsd:complexType name="exceptionData">
    <xsd:sequence>
      <xsd:element name="value" type="xsd:boolean" minOccurs="0" maxOccurs="1"/> <!-- Only present for boolean exceptions -->
    </xsd:sequence>
    <xsd:attribute name="name" type="exceptionName"  use="required"/>
  </xsd:complexType>
</xsd:schema>
```

common.xsd

```
<?xml version="1.0" encoding="UTF-8" ?>
<xsd:schema  xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <!-- Descriptive types -->
  <xsd:simpleType name="objectName">
    <xsd:restriction base="internalNameBlank"/>
  </xsd:simpleType>
  <xsd:simpleType name="propertyName">
    <xsd:restriction base="internalName"/>
  </xsd:simpleType>
  <xsd:simpleType name="logObjectName">
    <xsd:restriction base="internalName"/>
  </xsd:simpleType>
  <xsd:simpleType name="logListenerName">
    <xsd:restriction base="internalName"/> <!-- Can be "self" for the PIXI that you are using_-->
  </xsd:simpleType>
  <xsd:simpleType name="logKeywordName">
    <xsd:restriction base="internalName"/>
  </xsd:simpleType>
  <xsd:simpleType name="notificationKeywordName">
    <xsd:restriction base="internalName"/>
  </xsd:simpleType>
  <xsd:simpleType name="commandName">
    <xsd:restriction base="internalNameBlank"/>
  </xsd:simpleType>
  <xsd:simpleType name="parameterName">
    <xsd:restriction base="internalNameBlank"/>
  </xsd:simpleType>
  <xsd:simpleType name="applicationName">
    <xsd:restriction base="internalName"/>
  </xsd:simpleType>
  <xsd:simpleType name="eventID">
    <xsd:restriction base="xsd:hexBinary"/>
  </xsd:simpleType>
  <xsd:simpleType name="diagnosticName">
    <xsd:restriction base="internalName"/>
  </xsd:simpleType>
  <xsd:simpleType name="exceptionName">
    <xsd:restriction base="internalName"/>
  </xsd:simpleType>
  <xsd:simpleType name="eventTop">
    <xsd:restriction base="internalNameNoSpace"/>
  </xsd:simpleType>
  <xsd:simpleType name="eventDetail">
    <!-- A list of these is in the camera manual -->
    <xsd:restriction base="internalNameNoSpace"/> <!-- Every detail name will start with the top name -->
  </xsd:simpleType>

  <!-- Types -->
  <xsd:simpleType name="internalName">
    <xsd:restriction base="xsd:string">
      <xsd:pattern value="[a-zA-Z]{1}([a-zA-Z0-9_ ])*"/>
    </xsd:restriction>
  </xsd:simpleType>

  <xsd:simpleType name="internalNameNoSpace">
    <xsd:restriction base="xsd:string">
```

```
    <xsd:pattern value="[a-zA-Z]{1}([a-zA-Z0-9_])*"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="internalNameBlank">
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="[a-zA-Z]{0,1}([a-zA-Z0-9_ ])*"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="formatStringTopName">
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="([a-zA-Z]){1}"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="formatStringDetailName">
  <xsd:restriction base="xsd:string">
    <xsd:pattern value="([a-zA-Z]){2}"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="commandResults">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="Invalid"/>
    <xsd:enumeration value="OK"/>
    <xsd:enumeration value="Failed"/>
    <xsd:enumeration value="OK (save)"/> <!-- Indicates that the result should be saved, should never be seen as you cannot initate the save anyway -->
    <xsd:enumeration value="Invalid Parameters"/>
    <xsd:enumeration value="Unknown Result"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="yesNo">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="yes"/>
    <xsd:enumeration value="no"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="typeid">
  <xsd:restriction base="xsd:token">
    <xsd:enumeration value="bool"/>
    <xsd:enumeration value="schar"/>
    <xsd:enumeration value="uchar"/>
    <xsd:enumeration value="short"/>
    <xsd:enumeration value="ushort"/>
    <xsd:enumeration value="int"/>
    <xsd:enumeration value="uint"/>
    <xsd:enumeration value="long"/>
    <xsd:enumeration value="ulong"/>
    <xsd:enumeration value="longlong"/>
    <xsd:enumeration value="ulonglong"/>
    <xsd:enumeration value="float"/>
    <xsd:enumeration value="double"/>
    <xsd:enumeration value="string"/>
    <xsd:enumeration value="ibuffer_sp"/> <!-- Should never be presented externally, an internal type -->
    <xsd:enumeration value="invalid"/> <!-- Should never be visible externally, if it appears this is a bug -->
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="diagnosticType">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="value"/>
    <xsd:enumeration value="counter"/>
    <xsd:enumeration value="minmax"/>
    <xsd:enumeration value="ratio"/>
    <xsd:enumeration value="rate"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="diagnosticUnits">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="millisecond"/>
    <xsd:enumeration value="second"/>
    <xsd:enumeration value="minute"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="prevNext">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="previous"/>
    <xsd:enumeration value="next"/>
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="exceptionType">
  <xsd:restriction base="xsd:string">
    <xsd:enumeration value="instant"/>
    <xsd:enumeration value="boolean"/>
  </xsd:restriction>
</xsd:simpleType>

<!-- Complex structures -->
<xsd:complexType name="logObjectState">
  <xsd:sequence>
```

```
      <xsd:element minOccurs="1" maxOccurs="unbounded" name="keywordState" type="keywordState"/>
    </xsd:sequence>
    <xsd:attribute name="name" type="logObjectName"/>
  </xsd:complexType>
  <xsd:complexType name="keywordState">
    <xsd:sequence>
      <xsd:element name="onoff" type="xsd:token"/>
    </xsd:sequence>
    <xsd:attribute name="name" type="logKeywordName"/>
  </xsd:complexType>

  <xsd:complexType name="notificationObjectState">
    <xsd:sequence>
      <xsd:element minOccurs="1" maxOccurs="unbounded" name="keywordState" type="keywordState"/>
    </xsd:sequence>
    <xsd:attribute name="name" type="notificationKeywordName"/>
  </xsd:complexType>

  <xsd:simpleType name="onoff">
    <xsd:restriction base="xsd:string">
      <xsd:enumeration value="on"/>
      <xsd:enumeration value="off"/>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:schema>
```

List of PIXI values

This is a list of all the eventDetails available on the camera and a description of them. The "image" types will return a length and offset, whereas the other types return data.

PIXI values image_*

The images from the cameras. Not all images are always available in all circumstances.

Platforms	Name	Type	Description
All	image_overview	image	The image from the overview taken at the same time as the plate was read, or at the same time as the trigger depending upon settings.
All	image_analysis	image	The full image from the camera from which the number plate was read. Usually this will be an infrared image.
All	image_readpatch	image	The image of the number plate, cropped so that the number plate is all that is visible.
All	image_hazoverview	image	The image from the overview taken at the same time as the hazard plate was read, or at the same time as the trigger depending upon settings.
All	image_hazanalysis	image	The full image from the camera from which the hazard plate was read. Usually this will be an infrared image.
All	image_hazreadpatch	image	The image of the hazard plate, cropped so that the hazard plate is all that is visible.

PIXI values cam_*

The camera detail of the plate the vehicle was read on

Platforms	Name	Type	Description
All	cam_shutter	xsd:integer	The shutter setting used for this image
All	cam_gain	xsd:integer	The gain setting used for this image
All	cam_cam0	xsd:integer	The camera number (starting at zero)

Platforms	Name	Type	Description
All	cam_cam1	xsd:integer	The camera number (starting at one)
All	cam_seq0	xsd:integer	The sequence setting (starting at zero)
All	cam_seq1	xsd:integer	The sequence setting (starting at one)

PIXI values hazcam_*

The camera detail of the hazard plate the vehicle was read on

Platforms	Name	Type	Description
All	hazcam_shutter	xsd:integer	The shutter setting used for this image
All	hazcam_gain	xsd:integer	The gain setting used for this image
All	hazcam_cam0	xsd:integer	The camera number (starting at zero)
All	hazcam_cam1	xsd:integer	The camera number (starting at one)
All	hazcam_seq0	xsd:integer	The sequence setting (starting at zero)
All	hazcam_seq1	xsd:integer	The sequence setting (starting at one)

PIXI values event_*

Unique information about delivery event, Not usable under all circumstances

Platforms	Name	Type	Description
All	event_id	xsd:integer	The Event id, which uniquly identifies the event

PIXI values file_*

Associated file. Not useable under all circumstances. Primarily for use in ACS's LPR files.

Platforms	Name	Type	Description
All	file_context1_file	xsd:string	The filename of context image 1
All	file_context2_file	xsd:string	The filename of context image 2
All	file_context3_file	xsd:string	The filename of context image 3
All	file_context4_file	xsd:string	The filename of context image 4
All	file_context5_file	xsd:string	The filename of context image 5
All	file_context6_file	xsd:string	The filename of context image 6
All	file_context7_file	xsd:string	The filename of context image 7
All	file_context8_file	xsd:string	The filename of context image 8
All	file_lpr	xsd:string	The lpr text filename
All	file_ir	xsd:string	The IR image filename
All	file_hazir	xsd:string	The hazard IR image filename
All	file_patch	xsd:string	The patch image filename
All	file_hazpatch	xsd:string	The hazard patch image filename
All	file_path	xsd:string	The transfer path (which is not prepended to the other filenames)
All	file_overview	xsd:string	The wide angle, overview image filename

Platforms	Name	Type	Description
All	file_hazoverview	xsd:string	The hazard wide angle, overview image filename

PIXI values hazard_*

The read hazard plate from the vehicle

Platforms	Name	Type	Description
All	hazard_classification	xsd:integer	The anpr classification (not useful with many ANPR engines)
All	hazard_asyncpayload	xsd:string	The OEM asynchronous payload. Asynchronous messages injected via serial (or TCP) will be associated with messages based on a closest match within a window. Otherwise an empty string.
All	hazard_readconfidence	xsd:integer	The confidence of the hazard plate read
All	hazard_readconfidencecat	xsd:integer	The confidence category of the hazard plate read
All	hazard_platefinderconfidence	xsd:integer	The confidence of the hardware platefinder
All	hazard_fieldnum	xsd:integer	The field number
All	hazard_natcode	xsd:integer	The nationality code (not generally useful, see HN which is)
All	hazard_nationality	xsd:string	The nationality (country and state) of origin of this plate if known
All	hazard_tiggeroffset	xsd:integer	The time offset between the trigger time and the image associated with this read (milliseconds). If not triggered, will be 0
All	hazard_text	xsd:string	The text of the hazard plate
All	hazard_numreads	xsd:integer	The total number of reads associated with the trigger that caused this plateread (A single trigger can lead to >1 plateread event). For a NOREAD the value will still be 1.
All	hazard_syntaxconfidence	xsd:integer	The syntax confidence of the hazard plate read. This is a measure of how confident we are that the hazard plate matched the syntax of the reported country or state.
All	hazard_tag	xsd:string	The plate tag, as extracted from the vehicle filter database. Will be blank if no tag entered, the plate is not matched, or the filter is off
All	hazard_triggerpayload	xsd:string	The OEM trigger payload. If you are using serial (or TCP/IP) triggers, this will be the OEM content of those, otherwise it will be boring. Text 'auto' will be returned if not triggered
All	hazard_xpos	xsd:integer	The x position of the plate's left edge in pixels
All	hazard_width	xsd:integer	The width of the plate in pixels
All	hazard_ypos	xsd:integer	The y position of the plate's top edge in pixels
All	hazard_height	xsd:integer	The height of the plate in pixels

PIXI values heartbeat_*

The camera heartbeat delivery

Platforms	Name	Type	Description
All	heartbeat_attemptcount	xsd:integer	The count of heartbeat delivery attempts.
All	heartbeat_failurecount	xsd:integer	The count of heartbeat delivery failures.
All	heartbeat_statusbits	xsd:integer	A camera status bitfield (legacy).

PIXI values imglocaltime_*

The image timestamp, the moment the image for the vehicle was captured.

This is a local time and accounts for timezone and daylight saving

Platforms	Name	Type	Description
All	imglocaltime_ampm	xsd:string	The string am for the morning, pm for the afternoon
All	imglocaltime_ctime	xsd:integer	Seconds since midnight 1st of January 1970 (commonly known as C time). This is UTC always, included for completeness.
All	imglocaltime_day	xsd:integer	The day of the month
All	imglocaltime_dayyear	xsd:integer	The day of the year, with January the 1st as zero
All	imglocaltime_hour	xsd:integer	The hour, 24 hour clock
All	imglocaltime_hour12	xsd:integer	The hour, 12 hour clock
All	imglocaltime_millisecond	xsd:integer	Milliseconds
All	imglocaltime_locked	xsd:integer	Indicates if time is locked via NTP
All	imglocaltime_locked_text	xsd:string	Indicates if time is locked via NTP as a string
All	imglocaltime_minute	xsd:integer	Minutes past the hour
All	imglocaltime_tenmin	xsd:integer	Tens of minutes past the hour
All	imglocaltime_month	xsd:integer	Month of the year (January as one)
All	imglocaltime_monthname	xsd:string	Month of the year as a word, in English
All	imglocaltime_monthnamesh	xsd:string	Month of the year as three letter shortened word, in English
All	imglocaltime_second	xsd:integer	Seconds past the minute
All	imglocaltime_tenthsecond	xsd:integer	Tenths of seconds
All	imglocaltime_hundredthsecond	xsd:integer	Hundredths of seconds
All	imglocaltime_daylight	xsd:integer	One if daylight saving is in effect, zero otherwise
All	imglocaltime_dayweek	xsd:integer	The day of the week as a number, with zero being Sunday
All	imglocaltime_dayweekname	xsd:string	The day of the week as a word, in English
All	imglocaltime_dayweeknamesh	xsd:string	The day of the week as a three letter shortened word, in English
All	imglocaltime_year	xsd:integer	The year
All	imglocaltime_year2	xsd:integer	The last two digits of the year

PIXI values imgutctime_*

The image timestamp, the moment the image for the vehicle was captured.

This is UTC time (like GMT)

Platforms	Name	Type	Description
All	imgutctime_ampm	xsd:string	The string am for the morning, pm for the afternoon
All	imgutctime_ctime	xsd:integer	Seconds since midnight 1st of January 1970 (commonly known as C time)
All	imgutctime_day	xsd:integer	The day of the month
All	imgutctime_dayyear	xsd:integer	The day of the year, with January the 1st as zero
All	imgutctime_hour	xsd:integer	The hour, 24 hour clock
All	imgutctime_hour12	xsd:integer	The hour, 12 hour clock
All	imgutctime_millisecond	xsd:integer	Milliseconds
All	imgutctime_locked	xsd:integer	Indicates if time is locked via NTP
All	imgutctime_locked_text	xsd:string	Indicates if time is locked via NTP as a string
All	imgutctime_minute	xsd:integer	Minutes past the hour
All	imgutctime_tenmin	xsd:integer	Tens of minutes past the hour
All	imgutctime_month	xsd:integer	Month of the year (January as one)
All	imgutctime_monthname	xsd:string	Month of the year as a word, in English
All	imgutctime_monthnamesh	xsd:string	Month of the year as three letter shortened word, in English
All	imgutctime_second	xsd:integer	Seconds past the minute
All	imgutctime_tenthsecond	xsd:integer	Tenths of seconds
All	imgutctime_hundredthsecond	xsd:integer	Hundredths of seconds
All	imgutctime_daylight	xsd:integer	One if daylight saving is in effect, zero otherwise
All	imgutctime_dayweek	xsd:integer	The day of the week as a number, with zero being Sunday
All	imgutctime_dayweekname	xsd:string	The day of the week as a word, in English
All	imgutctime_dayweeknamesh	xsd:string	The day of the week as a three letter shortened word, in English
All	imgutctime_year	xsd:integer	The year
All	imgutctime_year2	xsd:integer	The last two digits of the year

PIXI values jpeg_*

JPEG data. Not useable under all circumstances. Primarily for use in output filenames to distinguish between them.

Platforms	Name	Type	Description
All	jpeg_type	xsd:string length='1'	The file type. Will be p for a patch, n for an IR image, and w for an overview wide angle image. Context images will be 1 (for context 1), 2 (for context 2). Currently up to 8 context images are supported.

PIXI values location_*

The location of the camera

Platforms	Name	Type	Description
All	location_latitude	xsd:integer	The whole number of degrees of latitude (north or south). Will always be positive.

Platforms	Name	Type	Description
All	location_longitude	xsd:integer	The whole number of degrees of longitude (east or west). Will always be positive.
All	location_north	xsd:integer	The whole number of degrees north we are. Will be negative if we are south.
All	location_east	xsd:integer	The whole number of degrees east we are. Will be negative if we are west.
All	location_millideglat	xsd:integer	The number of millidegrees of latitude we are away from the nearest degree.
All	location_millideglong	xsd:integer	The number of millidegrees of longitude we are away from the nearest degree.
All	location_microdeglat	xsd:integer	The number of microdegrees of latitude we are away from the nearest degree.
All	location_microdeglong	xsd:integer	The number of microdegrees of longitude we are away from the nearest degree.
All	location_ns	xsd:string length='1'	A character for latitude, N (north) or S (south) depending upon which hemisphere the location represents.
All	location_ew	xsd:string length='1'	A character for longitude, E (east) or W (west) depending upon which side of the meridian the location represents.
All	location_minlatitude	xsd:integer	The number of minutes of latitude (north or south) that we are away from the nearest whole degree. Will always be positive.
All	location_minlongitude	xsd:integer	The number of minutes of longitude (east or west) that we are away from the nearest whole degree. Will always be positive.
All	location_minlatitudetotal	xsd:integer	The number of minutes of latitude (north or south) that we are away from the equator. Will always be positive.
All	location_minlongitudetotal	xsd:integer	The number of minutes of longitude (east or west) that we are away from the equator. Will always be positive.
All	location_minnorthtotal	xsd:integer	The number of minutes north that we are away from the equator. Will be negative if we are south.
All	location_mineasttotal	xsd:integer	The number of minutes east that we are away from the equator. Will be negative if we are south.
All	location_milliminuteslat	xsd:integer	The number of milliminutes of latitude we are away from the nearest minute.
All	location_milliminuteslong	xsd:integer	The number of milliminutes of longitude we are away from the nearest minute.
All	location_microminuteslat	xsd:integer	The number of microminutes of latitude we are away from the nearest minute.
All	location_microminuteslong	xsd:integer	The number of microminutes of longitude we are away from the nearest minute.
All	location_validity	xsd:string	The string Valid or Invalid depending upon whether the location is deemed good.

PIXI values globalmeta_*

Metadata strings from the Metadata object. This is purely here so you can have the same format strings on all sites, and just change the metadata in this store

Platforms	Name	Type	Description
All	globalmeta_a	xsd:string	Metadata string a
All	globalmeta_b	xsd:string	Metadata string b
All	globalmeta_c	xsd:string	Metadata string c
All	globalmeta_d	xsd:string	Metadata string d
All	globalmeta_e	xsd:string	Metadata string e
All	globalmeta_f	xsd:string	Metadata string f
All	globalmeta_g	xsd:string	Metadata string g
All	globalmeta_h	xsd:string	Metadata string h
All	globalmeta_i	xsd:string	Metadata string i
All	globalmeta_j	xsd:string	Metadata string j
All	globalmeta_k	xsd:string	Metadata string k
All	globalmeta_l	xsd:string	Metadata string l
All	globalmeta_m	xsd:string	Metadata string m
All	globalmeta_n	xsd:string	Metadata string n
All	globalmeta_o	xsd:string	Metadata string o
All	globalmeta_p	xsd:string	Metadata string p
All	globalmeta_q	xsd:string	Metadata string q
All	globalmeta_r	xsd:string	Metadata string r
All	globalmeta_s	xsd:string	Metadata string s
All	globalmeta_t	xsd:string	Metadata string t
All	globalmeta_u	xsd:string	Metadata string u
All	globalmeta_v	xsd:string	Metadata string v
All	globalmeta_w	xsd:string	Metadata string w
All	globalmeta_x	xsd:string	Metadata string x
All	globalmeta_y	xsd:string	Metadata string y
All	globalmeta_z	xsd:string	Metadata string z

PIXI values timeoffset_*

The time offsets of overview context images

Platforms	Name	Type	Description
All	timeoffset_context1	xsd:integer	The offset (in milliseconds) of context image 1 measured from the vehicle event timestamp
All	timeoffset_context2	xsd:integer	The offset (in milliseconds) of context image 2 measured from the vehicle event timestamp
All	timeoffset_context3	xsd:integer	The offset (in milliseconds) of context image 3 measured from the vehicle event timestamp
All	timeoffset_context4	xsd:integer	The offset (in milliseconds) of context image 4 measured from the vehicle event timestamp
All	timeoffset_context5	xsd:integer	The offset (in milliseconds) of context image 5 measured from the vehicle event timestamp
All	timeoffset_context6	xsd:integer	The offset (in milliseconds) of context image 6 measured from the vehicle event timestamp

Platforms	Name	Type	Description
All	timeoffset_context7	xsd:integer	The offset (in milliseconds) of context image 7 measured from the vehicle event timestamp
All	timeoffset_context8	xsd:integer	The offset (in milliseconds) of context image 8 measured from the vehicle event timestamp

PIXI values plate_*

The read number plate from the vehicle

Platforms	Name	Type	Description
All	plate_isoalpha2	xsd:string	The 2-character nationality of origin of this plate if known, as defined by ISO 3166-1
All	plate_isoalpha3	xsd:string	The 3-character nationality of origin of this plate if known, as defined by ISO 3166-1
All	plate_classification	xsd:integer	The anpr classification (not useful with many ANPR engines)
All	plate_asyncpayload	xsd:string	The OEM asynchronous payload. Asynchronous messages injected via serial (or TCP) will be associated with messages based on a closest match within a window. Otherwise an empty string.
All	plate_readconfidence	xsd:integer	The confidence of the plate read
All	plate_readconfidencecat	xsd:integer	The confidence category of the plate read
All	plate_direction	xsd:string	The direction of travel of the plate read. This will be one of the following strings: AWAY, TOWARD, NOTSET. If NOTSET it indicates the direction could not be determined.
All	plate_isosubdivision	xsd:string	The subdivision of origin of this plate if known, as defined by ISO 3166-2
All	plate_platefinderconfidence	xsd:integer	The confidence of the hardware platefinder
All	plate_fieldnum	xsd:integer	The field number
All	plate_trigsource	xsd:string	The source of OEM trigger
All	plate_tcppayload	xsd:string	The OEM trigger payload from the first TCP/IP trigger
All	plate_triggerId	xsd:integer	The trigger identifier.
All	plate_laneId	xsd:string	The lane in which the plate is located.
All	plate_natcode	xsd:integer	The nationality code (not generally useful, see PN which is)
All	plate_nationality	xsd:string	The nationality (country and state) of origin of this plate if known
All	plate_triggeroffset	xsd:integer	The time offset between the trigger time and the image associated with this read (milliseconds). If not triggered, will be 0
All	plate_text	xsd:string	The text of the plate
All	plate_numreads	xsd:integer	The total number of reads associated with the trigger that caused this plateread (A single trigger can lead to >1 plateread event). For a NOREAD the value will still be 1.
All	plate_syntaxconfidence	xsd:integer	

Platforms	Name	Type	Description
			The syntax confidence of the plate read. This is a measure of how confident we are that the plate matched the syntax of the reported country or state.
All	plate_serialpayload	xsd:string	The OEM trigger payload from the first Serial trigger
All	plate_tag	xsd:string	The plate tag, as extracted from the vehicle filter database. Will be blank if no tag entered, the plate is not matched, or the filter is off
All	plate_triggerpayload	xsd:string	The OEM trigger payload. If you are using serial (or TCP/IP) triggers, this will be the OEM content of those, otherwise it will be boring. Text 'auto' will be returned if not triggered
All	plate_xpos	xsd:integer	The x position of the plate's left edge in pixels
All	plate_width	xsd:integer	The width of the plate in pixels
All	plate_ypos	xsd:integer	The y position of the plate's top edge in pixels
All	plate_height	xsd:integer	The height of the plate in pixels

PIXI values triglocaltime_*

The trigger timestamp, the moment the trigger started. You should probably be using T instead of this, as if the event was not a triggered one you will not get anything in the string with R.

This is a local time and accounts for timezone and daylight saving

Platforms	Name	Type	Description
All	triglocaltime_ampm	xsd:string	The string am for the morning, pm for the afternoon
All	triglocaltime_ctime	xsd:integer	Seconds since midnight 1st of January 1970 (commonly known as C time). This is UTC always, included for completeness.
All	triglocaltime_day	xsd:integer	The day of the month
All	triglocaltime_dayyear	xsd:integer	The day of the year, with January the 1st as zero
All	triglocaltime_hour	xsd:integer	The hour, 24 hour clock
All	triglocaltime_hour12	xsd:integer	The hour, 12 hour clock
All	triglocaltime_millisecond	xsd:integer	Milliseconds
All	triglocaltime_minute	xsd:integer	Minutes past the hour
All	triglocaltime_tenmin	xsd:integer	Tens of minutes past the hour
All	triglocaltime_month	xsd:integer	Month of the year (January as one)
All	triglocaltime_monthname	xsd:string	Month of the year as a word, in English
All	triglocaltime_monthnamesh	xsd:string	Month of the year as three letter shortened word, in English
All	triglocaltime_second	xsd:integer	Seconds past the minute
All	triglocaltime_tenthsecond	xsd:integer	Tenths of seconds
All	triglocaltime_hundredthsecond	xsd:integer	Hundredths of seconds
All	triglocaltime_daylight	xsd:integer	One if daylight saving is in effect, zero otherwise
All	triglocaltime_dayweek	xsd:integer	The day of the week as a number, with zero being Sunday
All	triglocaltime_dayweekname	xsd:string	The day of the week as a word, in English

Platforms	Name	Type	Description
All	triglocaltime_dayweeknamesh	xsd:string	The day of the week as a three letter shortened word, in English
All	triglocaltime_year	xsd:integer	The year
All	triglocaltime_year2	xsd:integer	The last two digits of the year

PIXI values trigutctime_*

The trigger timestamp, the moment the trigger started. You should probably be using t instead of this, as if the event was not a triggered one you will not get anything in the string with r.

This is UTC time (like GMT)

Platforms	Name	Type	Description
All	trigutctime_ampm	xsd:string	The string am for the morning, pm for the afternoon
All	trigutctime_ctime	xsd:integer	Seconds since midnight 1st of January 1970 (commonly known as C time)
All	trigutctime_day	xsd:integer	The day of the month
All	trigutctime_dayyear	xsd:integer	The day of the year, with January the 1st as zero
All	trigutctime_hour	xsd:integer	The hour, 24 hour clock
All	trigutctime_hour12	xsd:integer	The hour, 12 hour clock
All	trigutctime_millisecond	xsd:integer	Milliseconds
All	trigutctime_minute	xsd:integer	Minutes past the hour
All	trigutctime_tenmin	xsd:integer	Tens of minutes past the hour
All	trigutctime_month	xsd:integer	Month of the year (January as one)
All	trigutctime_monthname	xsd:string	Month of the year as a word, in English
All	trigutctime_monthnamesh	xsd:string	Month of the year as three letter shortened word, in English
All	trigutctime_second	xsd:integer	Seconds past the minute
All	trigutctime_tenthsecond	xsd:integer	Tenths of seconds
All	trigutctime_hundredthsecond	xsd:integer	Hundredths of seconds
All	trigutctime_daylight	xsd:integer	One if daylight saving is in effect, zero otherwise
All	trigutctime_dayweek	xsd:integer	The day of the week as a number, with zero being Sunday
All	trigutctime_dayweekname	xsd:string	The day of the week as a word, in English
All	trigutctime_dayweeknamesh	xsd:string	The day of the week as a three letter shortened word, in English
All	trigutctime_year	xsd:integer	The year
All	trigutctime_year2	xsd:integer	The last two digits of the year

PIXI values site_*

The site details for this unit

Platforms	Name	Type	Description
All	site_hostname	xsd:string	The site's hostname, the recommended way of identifying a site

Platforms	Name	Type	Description
All	site_libver	xsd:integer	The system's library version number
All	site_serialnumber	xsd:integer	The system's serial number
All	site_appver	xsd:integer	The system's application version number

PIXI values supplementary_*

The supplementary images details

Platforms	Name	Type	Description
All	supplementary_1_offset	xsd:integer	The offset (in milliseconds) of supplementary image 1 measured from the vehicle event timestamp
All	supplementary_2_offset	xsd:integer	The offset (in milliseconds) of supplementary image 2 measured from the vehicle event timestamp
All	supplementary_1_seq1	xsd:integer	Supplementary image 1 sequence setting (starting at one)
All	supplementary_2_seq1	xsd:integer	Supplementary image 2 sequence setting (starting at one)
All	supplementary_1_shutter	xsd:integer	Supplementary image 1 shutter setting
All	supplementary_2_shutter	xsd:integer	Supplementary image 2 shutter setting
All	supplementary_1_gain	xsd:integer	Supplementary image 1 gain setting
All	supplementary_2_gain	xsd:integer	Supplementary image 2 gain setting

PIXI values localtime_*

The timestamp for the vehicle, which is the trigger timestamp if the vehicle was triggered (see R), or the image timestamp if it was not (see I).

This is a local time and accounts for timezone and daylight saving

Platforms	Name	Type	Description
All	localtime_ampm	xsd:string	The string am for the morning, pm for the afternoon
All	localtime_ctime	xsd:integer	Seconds since midnight 1st of January 1970 (commonly known as C time). This is UTC always, included for completeness.
All	localtime_day	xsd:integer	The day of the month
All	localtime_dayyear	xsd:integer	The day of the year, with January the 1st as zero
All	localtime_hour	xsd:integer	The hour, 24 hour clock
All	localtime_hour12	xsd:integer	The hour, 12 hour clock
All	localtime_millisecond	xsd:integer	Milliseconds
All	localtime_minute	xsd:integer	Minutes past the hour
All	localtime_tenmin	xsd:integer	Tens of minutes past the hour
All	localtime_month	xsd:integer	Month of the year (January as one)
All	localtime_monthname	xsd:string	Month of the year as a word, in English
All	localtime_monthnamesh	xsd:string	Month of the year as three letter shortened word, in English
All	localtime_second	xsd:integer	Seconds past the minute

Platforms	Name	Type	Description
All	localtime_tenthsecond	xsd:integer	Tenths of seconds
All	localtime_hundredthsecond	xsd:integer	Hundredths of seconds
All	localtime_daylight	xsd:integer	One if daylight saving is in effect, zero otherwise
All	localtime_dayweek	xsd:integer	The day of the week as a number, with zero being Sunday
All	localtime_dayweekname	xsd:string	The day of the week as a word, in English
All	localtime_dayweeknamesh	xsd:string	The day of the week as a three letter shortened word, in English
All	localtime_year	xsd:integer	The year
All	localtime_year2	xsd:integer	The last two digits of the year

PIXI values utctime_*

The timestamp for the vehicle, which is the trigger timestamp if the vehicle was triggered (see r), or the image timestamp if it was not (see i).

This is UTC time (like GMT)

Platforms	Name	Type	Description
All	utctime_ampm	xsd:string	The string am for the morning, pm for the afternoon
All	utctime_ctime	xsd:integer	Seconds since midnight 1st of January 1970 (commonly known as C time)
All	utctime_day	xsd:integer	The day of the month
All	utctime_dayyear	xsd:integer	The day of the year, with January the 1st as zero
All	utctime_hour	xsd:integer	The hour, 24 hour clock
All	utctime_hour12	xsd:integer	The hour, 12 hour clock
All	utctime_millisecond	xsd:integer	Milliseconds
All	utctime_minute	xsd:integer	Minutes past the hour
All	utctime_tenmin	xsd:integer	Tens of minutes past the hour
All	utctime_month	xsd:integer	Month of the year (January as one)
All	utctime_monthname	xsd:string	Month of the year as a word, in English
All	utctime_monthnamesh	xsd:string	Month of the year as three letter shortened word, in English
All	utctime_second	xsd:integer	Seconds past the minute
All	utctime_tenthsecond	xsd:integer	Tenths of seconds
All	utctime_hundredthsecond	xsd:integer	Hundredths of seconds
All	utctime_daylight	xsd:integer	One if daylight saving is in effect, zero otherwise
All	utctime_dayweek	xsd:integer	The day of the week as a number, with zero being Sunday
All	utctime_dayweekname	xsd:string	The day of the week as a word, in English
All	utctime_dayweeknamesh	xsd:string	The day of the week as a three letter shortened word, in English
All	utctime_year	xsd:integer	The year
All	utctime_year2	xsd:integer	The last two digits of the year

Appendix A. Technical Details

Communication

Console Serial RS-232

The console runs at a fixed line speed of 38,400 bits per second with 8 bits of data, no parity and 1 stop bit. This is often abbreviated to 38,400 8N1. Hardware flow control is not supported, Xon/Xoff can be used, but no flow control also works.

Ethernet

The ethernet port is wired to the four Ethernet wires.

The ethernet port is 100BASE-TX autosensing 10/100 Mbit/s and full/half duplex over twisted pair. You must use Category 5e cable to make full use of the bandwidth of the connection, and are limited to 100metres total cable length from the camera to the receiver. If you are having problems with the ethernet link being intermittent or unreliable do ensure your cable meets full Cat 5e specification. The camera will work with a hub or switch with a "straight through" cable (pin 1 to 1, pin 2 to 2) or with a "cross-over" cable directly into the back of a PC. The camera will *not* autosense the RX and TX pairs so you must use the correct cable type for the far end unless that will autosense.

Although the camera is capable of 100Base-TX Full Duplex and will often negotiate to that given an appropriate other end point, sometimes the cable in between is not up to Cat 5e standards and running over long distances will drop packets. It is possible to force the camera to slow down or change to half duplex using a linux command called mii-tool.

`mii-tool` {-F} {*`10baseT-HD`*}
will force set it to 10 Mbit/s and half duplex. mii-tool has many other options, which are detailed below in the manual page for it.

If you need to make a permanent change to the speed of the camera's ethernet link you can put the command into `/etc/conf.d/local.start`, either using nano or by going to the System → Bootup and Shutdown page of webmin where you can edit the same file.

mii-tool

view, manipulate media-independent interface status

`mii-tool` [-v, --verbose] [-V, --version] [-R, --reset] [-r, --restart] [-w, --watch] [-l, --log] [-A, --advertise=*`media,`* ...] [-F, --force=*`media`*] [*`interface`*...]

This utility checks or sets the status of a network interface's Media Independent Interface (MII) unit. Most fast ethernet adapters use an MII to autonegotiate link speed and duplex setting.

Most intelligent network devices use an autonegotiation protocol to communicate what media technologies they support, and then select the fastest mutually supported media technology. The `-A` or `--advertise` options can be used to tell the MII to only advertise a subset of its capabilities. Some passive devices, such as single-speed hubs, are unable to autonegotiate. To handle such devices, the MII protocol also allows for establishing a link by simply detecting either a 10baseT or 100baseT link beat. The `-F` or `--force` options can be used to force the MII to operate in one mode, instead of autonegotiating. The `-A` and `-F` options are mutually exclusive.

The default short output reports the negotiated link speed and link status for each interface. If an interface or interfaces are not specified on the command line, then **mii-tool** will check any available interfaces from *eth0* through *eth7*.

`-v`, `--verbose`	Display more detailed MII status information. If used twice, also display raw MII register contents.

`-V`, `--version`	Display program version information.
`-R`, `--reset`	Reset the MII to its default configuration.
`-r`, `--restart`	Restart autonegotiation.
`-w`, `--watch`	Watch interface(s) and report changes in link status. The MII interfaces are polled at one second intervals.
`-l`, `--log`	Used with `-w`, records link status changes in the system log instead of printing on standard output.
`-F` *media*, `--force=`*media*	Disable autonegotiation, and force the MII to either *100baseTx-FD*, *100baseTx-HD*, *10baseT-FD*, or *10baseT-HD* operation.
`-A` *media,...*, `--advertise=`*media,...*	Enable and restart autonegotiation, and advertise only the specified media technologies. Multiple technologies should be separated by commas. Valid media are *100baseT4*, *100baseTx-FD*, *100baseTx-HD*, *10baseT-FD*, and *10baseT-HD*.

Diagnostics

SIOCGMIIPHY on 'eth?' failed: Invalid argument	If the interface is not running (up), kernel will refuse to report its link state.
SIOCGMIIPHY on 'eth?' failed: Operation not permitted	Most kernels restrict access to root.
SIOCGMIIPHY on 'eth?' failed: No such device	This error is shown, if the kernel does not know about the named device.
SIOCGMIIPHY on 'eth?' failed: Operation not supported	The interface in question does not support MII queries. Most likely, it does not have MII transceivers, at all.

Network details

The P382, P392+ and P492 are network capable cameras which make extensive use of TCP/IP and UDP/IP. They also use raw ethernet packets with type 0xAC01 for local configuration of the IP address details (sometimes known as IP Discovery or Remote IP Configuration). In case you need to pass TCP/IP or UDP/IP through a firewall or network translation device this table lists the appropriate ports.

Table A.1. TCP/IP and UDP/IP Port numbers

Port used for	Port type	Port number
SSH Shell	TCP/IP Server	22
Webmin secure HTTP	TCP/IP Server	443
Viewfinder	TCP/IP Server	9000
Client	TCP/IP Server	3570
PIXI (Unsecured, recommend an SSH tunnel to access). Usually firewalled on camera.	TCP/IP Server	3382
ACS	when FTP Client	21 plus ephemeral data ports
ACS	when SCP/SSH Client	22
NTP (where used)	UDP Client	123
Portmapper (where used for NFS)	UDP and TCP Server	111
NFS (where used)	UDP and TCP	2049
VES	TCP Server	Configurable, defaults [redacted] through [redacted] inclusive)
UDP Ping (may be used by VES)	UDP	10010
Ping	ICMP	No port for ICMP
TCP Trigger	TCP	3820
UTMC	TCP Server	Configurable

Filesystem layout

As you may well discover, the camera's root filesystem is mounted read-only to prevent accidental corruption. This section of the manual documents how the file system is layed out, and what goes where. A base knowledge of linux filesystems, disks, partitions and nomeclature for these is expected to be able to read this section.

There are flash devices within the camera, the internal flash, and the compact flash/SD card (not user removable). The internal flash is no longer used. The other flash card may vary in size, but only any space over 512Mb is available for user storage. It is a build to order option to have storage space in the camera.

On the P382 The flash is `/dev/hda` and on the P392+/P492 is `/dev/mmcblk0` and is partitioned into 5 sections as follows:

- 1 - This is the boot device. On the P382 it contains GRUB, the bootloader and the kernels. On the P392+/P492 it doesn't contain very much - all the boot data is held in NOR flash which is not accessible from linux. It is vital for booting, and there is no alternative. It is not usually mounted, so should be safe from damage. When mounted it exists as `/boot`
- 2 - This is the root filesystem. It is normally mounted as `/` *read only*.
- 5 - It is mounted as `/var` and is used for storing logging information and other run time data.
- 6 - It is mounted as `/opt` and is used for storing the PIPS application, libraries and configuration information. `/opt/pips` contains the ANPR reading engine, the application, the shell and other application files. `/opt/config/current` is a symbolic link to the current configuration of the camera including the usual `/etc`. You should back up `/opt/config/current` to preserve the state of a camera.
- 7 - It is mounted as `/storage` and is used for storing PIPS application data. All output from the camera application goes into this directory. If you have not purchased a larger than 512Mb compact flash this area will be small and should not be used for storage. You can (and should if you want to do this) mount a network filesystem under this directory to store files off camera.

Partition 1 on disk hda is known as `/dev/hda1` and on disk mmcblk0 it is known as `/dev/mmcblk0p1`.

Most of the filesystem is “normal linux” and adheres to the Linux Filesystem Standard (see http://tldp.org/LDP/Linux-Filesystem-Hierarchy/html/). Here are a few highlights and P382, P392+ and P492 specifics:

- `/etc` contains system specific configuration.
  - `fstab` mounted filesystems, included those mounted at boot. You can manipulate this in webmin, see the section called “Mounting network disks” [13]
  - `init.d/` several startup scripts, including those used to start the application and network
- `/opt/pips` contains the PIPS specific code including the applications.
  - `camera_app` the camera application which does ANPR and runs all the output modules
  - `libpipslinux.so.*` the shared library written by PIPS, used by all our applications on the camera
  - `libcardet*` are the ANPR libraries for reading plates. See the section called “Camera control” [13] to manipluate these.
  - `s2driver*` the kernel module (think of it like a windows device driver) for the PCI interface to the cameras and platefinder.
  - `ipconfigd` the IPDiscovery responder, this is what you're using when you use IP Discovery. This is started from `/etc/conf.d/local.start`
  - `modempulse` simple application which assists in turning the modem (where fitted) on and off.
  - `*.msc, *.isc, xcf08p_vo_48_1532.bsd, prog_prom*, jdrive, instfpga.pl` Files for setting up the FPGA. `instfpga.pl` uses the other files appropriately to reprogram the FPGA. Once the FPGA is programmed the camera will need rebooting.
  - `pipsshell` is the camera application's shell, see Chapter 6, *PIPS ANPR Shell* [15].
  - `uid.pl` generates a unique ID for this camera for use in VES.
  - `netmon.pl` manages the network and NTP on the camera.
- `/opt/config` contains all local configuration.
  - `current` is a symbolic link to the current configuration. You can use this to quickly switch configurations if you understand how to maniplate symbolic links.
  - `current/state.xml` is the camera script, containing all the configuration used by the camera application. This is XML, and must be correct or we will discard it. Hand edits are possible, but do take care. You can check it with **`xmllint`**
  - `current/netmon.xml` is the network configuration script. This is XML, and must be correct or we will discard it. Hand edits are possible, but do take care. You can check it with **`xmllint`**
  - `current/etc` is the actual `/etc` which is linked to here
- `/var` writable area used by linux. In particular contains linux's log files, see `log/messages` in particular. Equivalent of the event log on the P372.
- `/storage` writable area used by our application. This is user storage and all paths you enter in the application are relative to this directory, so entering `foo` as a directory will store the files in `/storage/foo`. This will contain the compact flash storage size minus 500Mb.

Backup

On the P392+ and P492 cameras (and only these models) should have the /backup.pl script run from the command line after any change - once that change is determined to be satisfactory. Changes include:

- New OS and application installations
- Application upgrades, Cardet upgrades
- Configuration changes

Appendix B. Software installation and upgrades

This appendix covers software maintenance of the camera which you may need to do, including upgrading or changing the software installed on the camera.

The camera software has a version numbering scheme to help you decide what action to take when new versions become available. The format of a version number is *major.minor.revision*. The "revision" will be an increasing "revision" number, always larger for later releases. For bug fixes, "revision" will increase. For minor enhancements, "minor" will increase. For major new features, or architectural changes, "major" will increase.

Optionally we may append the characters 'a', 'b' or "rc" to indicate alpha, beta or release candidate.

If only the revision number is increased, backward compatibility is guaranteed without any config changes.

If the minor number is increased, backward compatibility *may* be affected if deemed absolutely necessary. This will be clearly highlighted in the release note.

If the major number is increased, backward compatibility *may* be affected if deemed necessary or desirable. This will be clearly highlighted in the release note.

In general we will always try to maintain backward compatibility where it makes sense. Always refer to the release notes for more details on the changes that have occurred.

The old mechanisms of manual installation and web based installation are no longer possible nor supported. All software installation is managed via the PIPS ANPR Toolkit which is documented in Chapter 3, *PIPS ANPR Toolkit* [8].

Appendix C. Factory Defaults

On the P382 the password for the root user is *382*

On the P392+/P492 the password for the root user is *392*

The default network configuration stored in(`/opt/config/current/netmon.xml`) is

Table C.1. Default IP configuration

IP address	`10.20.xxx.yy`
Network mask	`255.255.0.0`
Default gateway	`10.20.100.1`

where `xxx` are the first three digits of the serial number of the camera, and `yy` are the last two. The serial number is printed on a sticker on the rear of the P382, P392+ and P492

Caution

It is important to note any changes which you make to these parameters. Without these details it may be impossible to maintain the camera and it may have to be returned to Neology for servicing

Appendix D. File transfers

This section describes how to transfer files to or from the camera by various means. You can pick which of these you want to try, although not all are suitable for all situations.

SFTP

SFTP stands for Secure File Transfer Protocol. It is an encrypted protocol, and is a partner to SSH. Like you can log onto a system using SSH, you can use SFTP to transfer files in both directions. It is simple to use if you are familiar with the ubiquitous FTP, and plenty of front ends make it's use trivial. It is the recommended way of transferring files, requiring little setup to use.

Multiplatform — The filezilla program (see the section called “Filezilla” [142]) provides a two window commander style interface for accessing the camera via sftp.

Windows — The WinSCP program (see the section called “WinSCP” [142]) provides an explorer or commander style interface for accessing the camera via scp and sftp.

To use SFTP I recommend a graphical browser unless you're happy to train yourself in the use of a command line version.

SCP

SCP stands for Secure CoPy. It is an encrypted protocol, and is also a partner to SSH. Like you can log onto a system using SSH, you can use SCP to transfer files in both directions. It is simple to use, but does not provide directory listings or any other features you might expect - you will need to use SSH for directory listings as a partner to SCP. As SCP is available on most operating systems as a built in, and is also available on the camera for camera-to-camera copies it is useful to understand.

Windows — The WinSCP program (see the section called “WinSCP” [142]) provides an explorer style interface for accessing the camera via scp and sftp.

Windows — The PuTTY project (see the section called “PuTTY” [142]) also provides PSCP for Windows. If you want to use it, put it on your path, or current directory, and use **pscp** instead of **scp** in the command examples.

Mac OS X — scp is a built in command.

Linux — scp is provided if you have ssh installed, which you most likely will do.

SCP is used like the standard DOS or Unix copy commands. You specify a source and target file to transfer, just one of them happens to be on a remote computer.

- `scp {`*`SourceFile`*`} {`*`user@host:directory/TargetFile`*`}`
  to copy a file to the remote computer
- `scp {`*`user@host:directory/SourceFile`*`} {`*`TargetFile`*`}`
  to copy a file from the remote computer

Note

SCP can be used from on the camera too; if you have a computer with an SSH server you can scp out from the camera, or from one camera to another.

FTP

FTP stands for File Transfer Protocol. It is a simple open protocol, and is purely for transferring files. To use it you will need an FTP server installed on a PC accessible via the network from the camera. There are various options available

for each operating system. FTP is not recommended, but included here as people familiar with our older cameras will be familiar with FTP. This is a quick introduction to FTP, not a complete guide. There are books available on the subject, or guides on the internet.

Windows	For Windows we recommend the free FileZilla server, which is a download from http://filezilla-project.org/. This is simple to setup and enable users without requiring rights to add users to the PC.
Windows (alternative)	For Windows you can also use the FTP server which comes with the OS as part of IIS. You can install this from Start → Settings → Control Panel+Add/Remove Programs. It is tricky to set up correctly, and requires that you create a Windows user, and assign them correct permissions to work right. I do not recommend it as FileZilla is easier to use.
Mac OS X	MacOS X comes with an FTP server which can be enabled using the Sharing Pane.
Linux	Different distributions of Linux come with different FTP servers which are probably not installed or enabled by default. I recommend the ProFTPd software, but any FTP server should work correctly.

If you now connect to the camera's shell you should be able to ftp from the camera and transfer files. A typical session is shown below.

Note

The use of the bin command to enable all binary transfers may be necessary otherwise binary files may get corrupted, and does no harm so always do it.

```
pole ~ # ftp 80.177.196.175
Connected to 80.177.196.175 (80.177.196.175).
220 ProFTPD 1.3.1rc3 Server (Alan's ProFTPD) [::ffff:80.177.196.175]
Name (80.177.196.175:root): ftp_boot
500 AUTH not understood
SSL not available
331 Password required for ftp_boot
Password:
230 User ftp_boot logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> bin
200 Type set to I
ftp> lcd /opt/config/current
Local directory now /opt/config/released
ftp> put state.xml
local: state.xml remote: state.xml
200 PORT command successful
150 Opening BINARY mode data connection for state.xml
226 Transfer complete
8089 bytes sent in 0.000208 secs (3.8e+04 Kbytes/sec)
ftp> cd 382
250 CWD command successful
ftp> lcd /storage
Local directory now /storage
ftp> get instapp.pl
local: instapp.pl remote: instapp.pl
200 PORT command successful
150 Opening BINARY mode data connection for instapp.pl (3132 bytes)
226 Transfer complete
3132 bytes received in 0.00201 secs (1.5e+03 Kbytes/sec)
ftp> cd app
250 CWD command successful
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
drwxr-xr-x   2 alan     alan         4096 Jul 23 23:00 254
drwxr-xr-x   2 alan     alan         4096 Sep 10 13:33 384
drwxr-xr-x   2 alan     alan         4096 Sep 25 11:39 435
drwxr-xr-x   2 alan     alan         4096 Oct 24 16:04 540
226 Transfer complete
ftp> cd 540
250 CWD command successful
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
-rw-r--r--   1 alan     alan      4553379 Oct 24 16:04 distrib.tbz2
226 Transfer complete
ftp> get distrib.tbz2
local: distrib.tbz2 remote: distrib.tbz2
200 PORT command successful
150 Opening BINARY mode data connection for distrib.tbz2 (4553379 bytes)
226 Transfer complete
```

```
4553379 bytes received in 0.741 secs (6e+03 Kbytes/sec)
ftp> quit
221 Goodbye.
pole ~ #
```

The **put** and **get** commands actually transfer files. **lcd** changes *local* directory, **cd** changes remote directory. **ls** will list files

Note

You cannot FTP from a remote computer into the P382, P392+ and P492

NFS

NFS stands for Network File System. This is an open protocol for sharing filesystems between computers. Unlike FTP and SCP this allows the camera to see remote files as if they were local files, rather than actually needing room to store them on its local storage. NFS is quite paranoid and must have all permissions correct before it will work. When it fails it doesn't usually give a helpful error message.

Windows see the section called “NFS Server on Windows” [142] to install nfs.

Mac OS X nfs is built in, but needs enabling.

Linux an nfs server is available for linux, see your distribution documentation to find out how to install it.

Setting up NFS involves editing /etc/exports and restarting the nfs server to pick up those changes. Once this is done you should be able to mount the exported filesystem from Webmin, as described in the section called “Mounting network disks” [13]. I'd suggest mounting the file system under /storage. Once this is done you should be able to list and access files on the remote PC as if they were local, using the standard **cd**, **ls** and **cp** commands.

CIFS/Samba (Windows shares)

CIFS is the latest version of Windows networking. It is available as samba for Linux and MacOS X, but it doesn't make as much sense as using NFS for those OSes.

Once you have a windows share set up you can mount the directories using webmin.

Transfer troubleshooting

A complete troubleshooting guide is beyond the scope of this manual, but I hope to give some hints and tips. Most problems boil down to one of two things, networking or permissions.

Network problems

- Can you ping the camera from the PC? If not then check your ethernet is correctly connected, networking settings are correct, and there is no firewall?
- Can you ping the PC from the camera? Both directions should work.
- Can you access the service on the PC from itself (not appropriate for all transfer types)? e.g. Can you FTP to the PC from itself?
- Is there a firewall running on the PC?
- Is there a second or third firewall running?
- Is there a firewall on the network in between?
- Or how about a NAT (network address translation) device?

- What happens if you telnet from either end to the service's port number? You should at least connect...

Permissions

- Do you have permissions to access the file you are trying to access? Can you read it locally on that machine?
- Do you have permissions to write to the file you are trying to write to?
- How about the directory that it is in?
- Do you have write permissions granted by the transport (e.g. FTP write permissions)? Or read permissions? *These permissions are separate from the permissions on the files... this often catches people out*
- Does the particular pairing of camera and PC allowed, lots of these services can restrict by IP address?

Appendix E. Software tools

This appendix lists some useful software tools you may wish to use with your camera

PIPS ANPR Toolkit

The PIPS ANPR Toolkit (P374) is available from PIPS. It consists of various software applications to install, diagnose and maintain PIPS cameras, including the P382, P392+ and P492. It is available as a package for Microsoft Windows 7.

Windows 7

To install the applications just double click on the installer executable and select the options you require.

PuTTY

PuTTY is a free terminal client. It can connect to the P382, P392+ and P492 via both the serial port and via SSH. It also provides the pscp SCP program. It is available from http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html and is highly recommended. A version of PuTTY is installed with the PIPS ANPR Toolkit.

Filezilla

Filezilla is a commander like file transfer program for many platforms suitable for using with the camera. It is available from http://filezilla-project.org/.

WinSCP

WinSCP is an explorer like file transfer program for Windows suitable for using with the camera. It is available from http://winscp.net/.

NFS Server on Windows

Windows does not come with an NFS server, however one is available for free as part of the cygwin project, and it is compatible with the P382, P392+ and P492. To install it

1. Download setup.exe from http://www.cygwin.com.
2. You should run this and select the **`nfs-server`** and **`cygrunsrv`** components.
3. Start the shell that is installed to Start → Cygwin → Cygwin Bash Shell and run **`nfs-server-config`**.
4. Now edit *`CYGWIN_DIR`*`/etc/exports` to add a directory to export. Full documentation of the exports file format is available online, but an example would be

   ```
   /cygdrive/d/workspace      80.177.196.176(rw,async,no_root_squash,insecure,no_subtree_check)
   /cygdrive/c/workdir/fish   80.177.196.0/24(ro,async,no_root_squash,insecure,no_subtree_check)
   ```

   which will export `d:\workspace` and the camera at 80.177.196.176 and `c:\workdir\fish` to all 80.177.196.* read-only.
5. Now start the **`Cygwin nfsd`** and **`Cygwin mountd`** services from Start → Settings → Control Panel+Administrative Tools → Services. You will need to restart them if you change the `exports` file.

Appendix F. Nano - text editor

This is a short guide to using the recommended text editor on the P382, P392+ and P492 *nano*. More detailed documentation is available on the web at http://www.nano-editor.org/docs.php

Opening and creating files

Opening and creating files is simple in nano, simply type:

nano {*filename*}
You can start typing immediately to insert text, and move around with the cursor keys.

Saving and exiting

If you want to save the changes you've made, press **Ctrl**+**O**. To exit nano, type **Ctrl**+**C**. If you ask nano to exit from a modified file, it will ask you if you want to save it. Just press **N** in case you don't, or **Y** in case you do. It will then ask you for a filename. Just type it in and press **Enter**.

If you accidentally confirmed that you want to save the file but you actually don't, you can always cancel by pressing **Ctrl**+**C** when you're prompted for a filename.

Cutting and pasting

To cut a single line, you use **Ctrl**+**K**. The line disappears. To paste it, you simply move the cursor to where you want to paste it and punch **Ctrl**+**U**. The line reappears. To move multiple lines, simply cut them with several **Ctrl**+**K**s in a row, then paste them with a single **Ctrl**+**U**. The whole paragraph appears wherever you want it.

If you need a little more fine-grained control, then you have to mark the text. Move the cursor to the beginning of the text you want to cut. Hit **Ctrl**+**6** (or **Alt**+**A**). Now move your cursor to the end of the text you want to cut: the marked text gets highlighted. If you need to cancel your text marking, simply hit **Ctrl**+**6** again. Press **Ctrl**+**K** to cut the marked text. Use **Ctrl**+**U** to paste it.

Searching for text

Searching for a string is easy as long as you think "WhereIs" instead of "Search". Simply hit **Ctrl**+**W**, type in your search string, and press Enter. To search for the same string again, hit **Alt**+**W**.

Note

Note: In nano's help texts the **Ctrl**-key is represented by a caret (^), so **Ctrl**+**W** is shown as ^W, and so on. The Alt-key is represented by an M (from "Meta"), so **Alt**+**W** is shown as M-W.

Appendix G. rc-update

This is a short guide on how to use *rc-update*

Introduction

rc-update is a script for adding/removing/listing available scripts to the boot, default and nonetwork run levels of your computer. these scripts allow you to run programs at your computers boot time.

rc-update is very useful and can be used to start anything from your network card to your login manager.

rc-update commands

adding a script to a runlevel

rc-update add script runlevel

will add a script to that runlevel of your computer.

removing a script from a runlevel

rc-update del script runlevel

will remove a script from the runlevel.

list available scripts and their current runlevel

rc-update show

will show all available scripts and their currently set runlevel(s) if any.

runlevels

boot

default

nonetwork

more runlevels may be added to /etc/runlevels/

Examples

rc-update add pips_app default

This will start the camera application at the default runlevel

rc-update del pips_app default

This will remove the camera application at the default runlevel

Other information

rc update uses scripts in the /etc/init.d/ directory exclusively

Appendix H. Viewfinder Protocol

The Viewfinder Protocol is a method for accessing the camera's video stream. The Viewfinder can be accessed via TCP port 9000.

There are several protocol versions available on the cameras, versions 1, 2, 3 and 4. By default the Viewfinder will be configured to use version 1

To initiate a Viewfinder session, you need to connect to the viewfinder port, to end the session just disconnect.

The viewfinder protocol constantly sends images, but when a session is first opened the camera needs to be set before any data will be sent, this is done by using the VF run command. Data will only stop being sent once the session is closed. The VF run command can be used to change the data that is sent, there may also be a small amount of lag before the changeover happens.

Viewfinder commands

Command	Description
VF set version *`version`*\n	Sets the version specified by *`version`* The viewfinder protocol does not respond
VF get channels\n	Gets information on the channels. See example below for output. (Viewfinder Protocol Version 2 or above must be used) The Viewfinder protocol responds with an xml type response
VF run camera *`camera`* seq *`sequence`* interval *`interval`* quality *`quality`* scale *`scale`*	Initiates the video stream. camera: The camera which is used to stream video from, required sequence: The sequence which is to be viewed, must be 0 for colour camera, default = 0, optional interval: The time between each frame, specified in ms, default = 2000, optional quality: Not used, optional scale: Not used, optional Viewfinder protocol responds with an image type response

Note

Camera 0 = cam1 in user interface = IR Camera

Camera 1 = cam2 in user interface = Colour Camera

Note

sequence 0 = seq1 in user interface

sequence 1 = seq2 in user interface

sequence 2 = seq3 in user interface

sequence 3 = seq4 in user interface

sequence 4 = seq5 in user interface

sequence 5 = seq6 in user interface

sequence 6 = seq7 in user interface

sequence 7 = seq8 in user interface

Viewfinder messages

This section contains information about the responses from the Viewfinder server

Version 1

In version 1 VF run is the only command that can be used. The following example I will configure the run command to the the IR camera and sequence 0 with 2 frames per second

`VF run camera 0 sequence 0 interval 500\n`

The response from the camera will be the following:

```
VF 1 0 0 11000\n[binary-jpeg-data]
```

Note

The [binary_jpeg_data] is a standalone JFIF (JPEG file interchange format), the specification can be found here, http://www.w3.org/Graphics/JPEG/jfif3.pdf

Note

This will be repeated every 500ms

VF *`version camera sequence jpeg_length`*

Version 2

In version 2 VF run and VF get can be used.

The response from version 2 is as follows

VF *`version type data`*

`VF set version 2`

`VF run camera 0 sequence 0 interval 500\n`

```
VF 2 image 0 0 5265846397017522284 11008\n[binary_jpeg_data]
```

Note

The [binary_jpeg_data] is a standalone JFIF (JPEG file interchange format), the specification can be found here, http://www.w3.org/Graphics/JPEG/jfif3.pdf

The above example gives a type of image which can be decoded as follows

VF *`version`* image *`camera sequence 64Bit_TimeStamp jpeg_length\n[binary_jpeg_data]`*

The 64bit Time Stamp can be decoded as follows, [Upper 32 bit Time stamp].[Lower 32 bit Time stamp].

The upper 32 bit Time stamp is a normal UTC time stamp indicating the number of seconds since 00:00:00 1st January 1970

The lower 32 bit Time stamp is the number milliseconds since the start of the current second

The second example

VF set version 2

VF get channels

```
VF 2 xml 367
<?xml version="1.0"?>
<channels model="P382" count="2">
 <channel0 num_sequence_entries="1">
  <format raw_type="mono" rate="50" quality="fixed" resolution="fixed" pixel_width="1" pixel_height="1"/>
 </channel0>
 <channel1 num_sequence_entries="1">
  <format raw_type="colour" rate="50" quality="fixed" resolution="fixed" pixel_width="2" pixel_height="1"/>
 </channel1>
</channels>
```

Note

The above example has been formatted for readability

The above example give an xml type which can be decoded as follows

VF *version* xml *xml_length*\n[xml_file]

<channels model="P382" count="2">indicates that the camera we are using is a P382 and that there are two possible image sources.

<channel0 num_sequence_entries="1"> indicates on the first channel has only one sequence available

<format raw_type="colour" rate="50" quality="fixed" resolution="fixed" pixel_width="2" pixel_height="1"/>

raw_type indicates that this channel is in colour, this can also be mono, or unknown

rate is not used, and is fixed at 50

quality is fixed so this cannot be changed, if it could this would be a number between 1 and 99

resolution is fixed which means it cannot be changed otherwise it would be a number such as 1, 2 or 4 which would be a defined resolution

pixel_width and pixel_height if pixel_width and pixel_height are the same then no adjustment of the image needs to take place, if they are different i.e. pixel_width = 2 and pixel_height = 1 means that each pixel needs to be made half the width, to view the image correctly.

Version 3

In version 3 VF run and VF get can be used.

The response from version 3 is as follows

VF *version type data*

VF set version 3

VF run camera 0 sequence 0 interval 500\n

```
VF 3 image 0 2 6129809915063042098 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1107 201 252 72 895 602 252 72 1023 92 252 72 93504\n[binary_jpeg_data]
```

Note

The [binary_jpeg_data] is a standalone JFIF (JPEG file interchange format), the specification can be found here, http://www.w3.org/Graphics/JPEG/jfif3.pdf

The above example gives a type of image which can be decoded as follows

VF *version* image *camera sequence 64Bit_TimeStamp PlateFindData jpeg_length\n[binary_jpeg_data]*

The 64bit Time Stamp can be decoded as follows, [Upper 32 bit Time stamp].[Lower 32 bit Time stamp].

The upper 32 bit Time stamp is a normal UTC time stamp indicating the number of seconds since 00:00:00 1st January 1970

The lower 32 bit Time stamp is the number milliseconds since the start of the current second

16 zeroes for future enhancement.

The plate find data describes up to 4 number plates found in the image. For each plate the x and y co-ordinates, width and height are displayed. This gives 16 data items in total.

Version 4

In version 4 VF run and VF get can be used.

The response from version 2 is as follows

VF *version type data*

VF set version 4

VF run camera 0 sequence 0 interval 500\n

```
VF 4 image 0 2 6129809915063042098 0 0 0 0 0 0 0 1107 201 252 72 5352 0 0 895 602 252 72 6737 0 0 1023 92 252 72 8941 0 0 93504\n[binary_jpeg_data]
```

Note

The [binary_jpeg_data] is a standalone JFIF (JPEG file interchange format), the specification can be found here, http://www.w3.org/Graphics/JPEG/jfif3.pdf

The above example gives a type of image which can be decoded as follows

VF *version* image *camera sequence 64Bit_TimeStamp PlateFindData jpeg_length\n[binary_jpeg_data]*

The 64bit Time Stamp can be decoded as follows, [Upper 32 bit Time stamp].[Lower 32 bit Time stamp].

The upper 32 bit Time stamp is a normal UTC time stamp indicating the number of seconds since 00:00:00 1st January 1970

The lower 32 bit Time stamp is the number milliseconds since the start of the current second

The plate find data describes up to 4 number plates found in the image. For each plate the x and y co-ordinates, width and height, plate find confidence, shape and clipped flag are displayed. This gives 28 data items in total.

The shape parameters indicate whether the plate is a number plate (0), a square number plate (1), a hazard plate (2) or a blank hazard plate (3).

The clipped flag indicates that the number plate may be partly obscured.

Appendix I. Vehicle Event Viewer Protocol

This section describes the PIPS Vehicle Event Viewer (aka "Client") protocol. It describes version 3 of the protocol as implemented by the cameras. The Vehicle Events can be accessed via TCP port 3570.

The Vehicle Event Viewer service runs on the camera and will be referred to as the "service". The service provides a stream of Vehicle Plate Read records (containing image and other data) for each vehicle plate read event created by the camera.

To initiate a Viewfinder session, you need to connect to the viewfinder port, to end the session just disconnect.

Entities may use TCP to connect to the camera and monitor this data stream. Any entity connecting to the "service" will be referred to as a "client".

Vehicle Event Viewer commands

Commands are sent to the service in ASCII text delimited by a Carriage Return character ('\r').

Currently, only a single command is recognised and this would normally only be issued once. The command (to select the version) is a string:

"vers[v]\r"

where v is the version "number", a single character in the ranges '1' to '9' or 'a' to 'z'.

The latest version supported on the cameras is 4 although it defaults to 2. If you connect to the service and issue no command, you will receive version 2 data. To switch to version 4, immediately on connection completion, the client should send the following string to the service: "vers4\r"

Vehicle Event Viewer data

The service starts streaming binary data to the client immediately on connection. It does not wait for anything from the client.

The data streamed from the service is binary. The binary data is streamed as a BLOB as follows:

1. Firstly a header structure which begins with a "start of block" pattern followed by information about the event, such as the plate string. It also contains information (lengths in bytes) allowing the end of the header and the start/endings of the subsequent jpeg images to be computed.

2. The header is immediately followed by the patch jpeg image - the length of which is contained in the header. The jpeg data is in JFIF format.

3. The patch jpeg is immediately followed by the colour overview jpeg image - the length of which is contained in the header. The jpeg data is in JFIF format.

Header Format

The header is a packed structure. Currently the cameras default to version 2, so the client must be able to recognise version 2 headers too. Since there is actually little difference between the versions, it is not difficult to support both.

Even if the client switches to version 3 immediately on connection, it is possible that one or more version 2 headers will be received first. Version 2 data may be used or ignored.

The difference between the version 2 and version 3 headers is that the version 3 header has two extra fields appended on the end - namely: utc_timestamp_s and utc_timestamp_ms.

The difference between the version 3 and version 4 headers is that the version 4 header has one extra field appended on the end - namely: m_plate.

The jpeg fields, if present, follow immediately after the header. Their location may be determined by the respective size fields in the header. The jpeg data is in JFIF format.

The version 3 header is shown below:

Note

Entries commented

```
//Not Used
```

are not currently used on the P382. It is possible that at some time in the future they may be used without causing a version number change. It will always be safe to ignore them).

```
struct PTFMPlateHeaderV3
{
 unsigned start; // start of message block indicator
 unsigned header_size; // size of header
 unsigned patch_size; // patch length
 unsigned overview_size; // overview length
 unsigned sum; //Not Used
 unsigned camera; //Not Used
 unsigned flash; //Not Used
 unsigned gain;
 unsigned shutter;
 unsigned seq; // exposure sequence number 0 - 2
 unsigned threshold; //Not Used
 unsigned platefinder_confidence;
 unsigned plateread_confidence;
 unsigned id; //Not Used
 unsigned ticks; // system tick counter at exposure time (ms)
 unsigned location; //Not Used
 unsigned mseq; //Not Used
 unsigned exp[3]; //Not Used
 unsigned event_count[4]; //Not Used
 char  plate_str[16];
 unsigned  utc_timestamp_s;
 unsigned  utc_timestamp_ms;
 char   m_plate[40];
};
```

Each field will be described below:

Note

All integer fields are transmitted in network byte order and will need to be converted back to host byte order before interpretation.

- *start:* A 4 byte pattern which identifies the start of the header. This will be 0x50544632 for version 2, 0x50544633 for version 3 and 0x50544634 for version 4.
- *header_size:* The size of the header (and only the header) in bytes. This will be different between versions. This value may be used to determine where the jpeg data begins.
- *patch_size:* The size in bytes of the patch jpeg. If this is non-zero, then this data begins immediately after the last header byte. (The patch jpeg is in jfif format).
- *overview_size:* The size in bytes of the overview jpeg. If this is non zero, this data begins immediately after the last byte of patch data. (The overview jpeg is in jfif format)
- *sum:*Currently unused
- *camera:* Currently unused
- *flash:* Currently unused. The flash period is equal to the shutter period.
- *gain:* The gain setting for this plate read event

- *shutter:* The shutter setting for this plate read event. A reported value of 0 indicates a shutter period 10us. The maximum value is 31 and indicates a shutter period of 1ms. In order to deduce in-between shutter period's note that there is a linear relationship between these reported values and actual shutter period.
- *seq:*The exposure sequence number, typically a number from 0 to 2 indicating which in a sequence of exposures was used to give this plate read event.
- *threshold:*Currently unused
- *platefinder_confidence:* The platefinder confidence value. This is not normally of much interest to an end user.
- *plateread_confidence:* The confidence of the plate read expressed as a number less than a 100 (where 100 would indicate absolute confidence).
- *id:*Currently unused
- *ticks:* A system monotonic tick count in milliseconds indicating the time of exposure. Has no meaning as an absolute time, but can be useful in relative terms - for example to measure elapsed time between two consecutive events. The tick value is strictly monotonic and therefore is unaffected by changes to the system time.
- *location:*Currently unused
- *mseq:* Currently unused
- *exp:* Currently unused
- *event_count:* Currently unused
- *plate_str:* Number plate string. Null terminated character string.
- *utc_timestamp_s:* (Version 3 and 4 only) UTC Timestamp of plate read image set (seconds). May be used together with utc_timestamp_ms (see below) to provide accurate UTC time.
- *utc_timestamp_ms:* (Version 3 and 4 only) UTC Timestamp of plate read image set (milliseconds)
- *m_plate:* (Version 4 only) The text read from the plate

Appendix J. Legal Notices

English

Copyright Notice

The information within this handbook is authorised for distribution to customers, authorised service centre personnel, and distributors of Neology. Every effort has been made to supply information within this handbook that is correct. However, Neology assumes neither responsibility for its use, nor any infringements of patents or other rights of third parties which would result. No licence is granted by the manufacturer under any patent or patent rights. The manufacturer reserves the right to modify and update the equipment at any time without prior notice.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means to a third party without the prior consent of the copyright holder.

The manufacturer's warranty will be invalidated if untrained personnel operate the equipment or if any attempt is made to service the equipment by untrained personnel.

Warranty

Neology warrants products and spare parts of its own manufacture against faulty materials and workmanship for a period of 12 months, or as modified by the contract, from the date of purchase or on site acceptance, if installed by Neology authorised personnel.

The warranty excludes consumable materials and parts with an inherently limited life and excludes faults arising from misuse, neglect or vandalism.

Neology will replace or repair at its option and at no cost to the purchaser any faulty items reported to it within the warranty period.

Service

Service of this equipment by replacement of parts, on site repair or routine maintenance inspections is available. Please contact Neology for a quotation. There are no user serviceable parts inside the camera.

Technical Support

Should you require technical support, please contact Neology.

Users finding errors or omissions in this document are requested to advise Neology.

Write or telephone:

Neology United Kingdom plc
17 Bartley Wood Business Park
Hook
Hampshire
RG27 9XA
United Kingdom
Telephone: +44 (0)
Email: <anprsupportous@uk.neology.net>

If you telephone please have the following information available:

product name and version number
operating system and version number

Design Changes

Neology reserves the right to change the design of any product from time to time without notice and with no obligation to make corresponding changes in products previously manufactured.

Trademarks

Windows and Windows XP are registered trademarks of Microsoft Corporation.

FCC Declaration

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Français

Notification de Copyright

L'information dans ce manuel est autorisée pour la distribution aux clients, au personnel des services de maintenance autorisés, et aux distributeurs de Neology (ci-après dénommée "La compagnie") Tout effort a été fait pour que l'information dans ce manuel soit correcte. Cependant, "La compagnie" n'assume ni la responsabilité pour son usage, ni aucune infraction à des brevets ou à d'autres droites des tiers qui résulteraient de son utilisation. "La compagnie" n'accorde aucune licence sous aucun brevet ou propriété industrielle. "La compagnie" se réserve le droit de modifier et mettre à jour le matériel à tout moment sans préavis.

Aucune partie de cette publication ne peut être reprise, reproduite ou enregistrée sous quelque forme que ce soit sans l'accord écrit préalable de "La compagnie".

La garantie de "La compagnie" sera infirmée si le matériel est utilisé ou si n'importe quelle tentative est faite de le réparer par un personnel non formé par "La compagnie".

Garantie

Cette garantie s'étend aux produits et pièces de rechange fabriquées par "La compagnie" contre les matériaux défectueux et l'exécution défectueuses pendant une période de 12 mois ou comme modifiée par le contrat, de la date de l'achat ou sur l'acceptation de site, si le matériel est installé par "La compagnie" ou un personnel autorisé.

La garantie exclut les matériaux consommables et les parties avec une durée de vie limitée et exclut des défauts redevant de l'abus, de la négligence ou du vandalisme.

"La compagnie" substituera ou réparera, à son option, et à aucun coût à l'acheteur tous les éléments défectueux reportés au cours de la période de garantie.

Service

Le service de ce matériel par le remplacement des parties, par des inspections de maintenance ou de réparation sur de site est disponible. Prière de contacter "La compagnie" pour la liste des coûts.

Support Technique

Pour tout support technique, prière de contacter "La compagnie" au Royaume-Uni.

Si vous trouvez des erreurs ou des omissions dans ce document prière d'informer "La compagnie"

Écrivez ou téléphonez:

Neology United Kingdom plc
17 Bartley Wood Business Park
Hook
Hampshire
RG27 9XA
United Kingdom
Telephone: +44 (0)
Email: <anprsupportous@uk.neology.net>

Si vous téléphonez, prière d’avoir l'information suivante disponible:

nom de produit et nombre de version
système d'exploitation et nombre de version

Changements de Conception

"La compagnie" se réserve le droit de changer la conception de n'importe quel produit de temps # autre sans communication préalable et sans l'obligation de faire les changements correspondants des produits construits antérieurement.

Marques Déposées

Windows et Windows XP sont des marques déposées de Microsoft Corporation.

Appendix K. Contact information

Table K.1. Contact Information

United Kingdom	USA
Neology United Kingdom plc 17 Bartley Wood Business Park Hook Hampshire RG27 9XA United Kingdom Telephone: +44 (0) Email: <anprsupportous@uk.neology.net>	Neology 12760 Danielson Ct., Suite A Poway CA USA Telephone: +1 (0) 858-391-0260 Fax:+1 (0) 858-391-0264
Web site:http://www.neology.net/	

SAFEWARE®

Safeware Catalog Price List

Combined Systems

Effective: March 1, 2020

Item ID	Description	Extended Description	Safeware List	Discount	Net Price	UOM
CTS 0300	Smoke (Inert) Formulation Fog, Quart		$ 59.55	41%	$ 35.13	EA
CTS 0311	Smoke (Inert) Formulation Fog, Gallon		$ 138.31	41%	$ 81.60	EA
CTS 0330	CS Formulation Fog, Quart		$ 75.48	41%	$ 44.53	EA
CTS 0340	Flush Fog Formulation, Quart		$ 46.89	41%	$ 27.67	EA
CTS 0340G	Flush Fog Formulation, Gallon		$ 138.31	41%	$ 81.60	EA
CTS 0431	OC Fog Formulation, Quart		$ 75.48	41%	$ 44.53	EA
CTS 0431G	OC Fog Formulation, Gallon		$ 209.49	41%	$ 123.60	EA
CTS 1101R	MK-21 Inert Refill 21 OZ		$ 57.74	41%	$ 34.07	EA
CTS 1101T	Titan Inert Stream 20 OZ	Case of 6	$ 433.22	41%	$ 255.60	CS
CTS 1108T	Titan Inert Stream 17.6 OZ	Case of 6	$ 433.22	41%	$ 255.60	CS
CTS 1111R	MK-21 Level 1 OC Refill 21 OZ		$ 95.48	41%	$ 56.33	EA
CTS 1121R	MK-21 Level 2 OC Refill 21 OZ		$ 95.48	41%	$ 56.33	EA
CTS 1131R	MK-21 Level 3 OC Refill 21 OZ		$ 95.48	41%	$ 56.33	EA
CTS 1131T	Titan Level 3 OC Stream 20 OZ	Case of 6	$ 475.25	41%	$ 280.40	CS
CTS 1132T	Titan Level 3 OC Foam 19.4 OZ	Case of 6	$ 488.14	41%	$ 288.00	CS
CTS 1133T	Titan Level 3 OC Fog 19.4 OZ	Case of 6	$ 488.14	41%	$ 288.00	CS
CTS 1134T	Titan Level 3 OC Gel 16.75 OZ	Case of 6	$ 488.14	41%	$ 288.00	CS
CTS 1138T	Titan Level 3 OC Omni-Stream™ 17.6 OZ, 360° Performance	Case of 6	$ 505.08	41%	$ 298.00	CS
CTS 1141R	MK-21 OC/CS Refill 21 OZ		$ 95.48	41%	$ 56.33	EA
CTS 1201R	MK-46 Inert Refill 46 OZ		$ 77.85	41%	$ 45.93	EA
CTS 1201V	MK-21 Vertical Dispenser 21 OZ		$ 429.81	41%	$ 253.59	EA
CTS 1203A	MK-21/46 Recharge Set - Regulator, Hose w/ Threaded Schraeder Valve Adapter, Funnel, O-Rings, Lubricant		$ 747.46	41%	$ 441.00	ST
CTS 1204A	MK-21/46 Hose & Wand		$ 73.22	41%	$ 43.20	EA
CTS 1211R	MK-46 Level 1 OC Refill 46 OZ		$ 150.85	41%	$ 89.00	EA
CTS 1221R	MK-46 Level 2 OC Refill 46 OZ		$ 150.85	41%	$ 89.00	EA
CTS 1231R	MK-46 Level 3 OC Refill 46 OZ		$ 150.85	41%	$ 89.00	EA
CTS 1241R	MK-46 OC/CS Refill 46 OZ		$ 150.85	41%	$ 89.00	EA
CTS 1301	MK-3 Inert Stream 1.5 OZ	Case of 25	$ 358.76	41%	$ 211.67	CS
CTS 1302	MK-3 Inert Foam 2.1 OZ	Case of 25	$ 395.48	41%	$ 233.33	CS
CTS 1303	MK-3 Inert Fog 2.1 OZ	Case of 25	$ 381.36	41%	$ 225.00	CS
CTS 1304	MK-3 Inert Gel 1.5 OZ	Case of 25	$ 358.76	41%	$ 211.67	CS
CTS 1307	Inert Grenade 2 OZ	Case of 25	$ 576.27	41%	$ 340.00	CS
CTS 1308	MK-3 Inert 1.2 OZ, Omni-Stream™, 360° Performance	Case of 25	$ 395.48	41%	$ 233.33	CS
CTS 1311	MK-3 Level 1 OC Stream 1.5 OZ	Case of 25	$ 480.09	41%	$ 283.25	CS
CTS 1318	MK-3 Level 1 Omni-Stream™ - 360° Performance		$ 14.66	41%	$ 8.65	EA
CTS 1321	MK-3 Level 2 OC Stream 1.5 OZ	Case of 25	$ 491.73	41%	$ 290.12	CS
CTS 1322	MK-3 Level 2 OC Foam 1.5 OZ	Case of 25	$ 485.88	41%	$ 286.67	CS
CTS 1323	MK-3 Level 2 OC Fog 1.5 OZ	Case of 25	$ 502.82	41%	$ 296.66	CS

CONFIDENTIAL

Item ID	Description	Extended Description	Safeware List	Discount	Net Price	UOM
CTS 1324	MK-3 Level 2 OC Gel 1.5 OZ	Case of 25	$ 480.09	41%	$ 283.25	CS
CTS 1328	MK-3 Level 2 OC Omni-Stream™ 1.2 OZ, 360° Performance	Case of 25	$ 485.88	41%	$ 286.67	CS
CTS 1331	MK-3 Level 3 OC Stream 1.5 OZ	Case of 25	$ 477.18	41%	$ 281.54	CS
CTS 1332	MK-3 Level 3 OC Foam 2.1 OZ	Case of 25	$ 480.23	41%	$ 283.34	CS
CTS 1333	MK-3 Level 3 OC Fog 2.1 OZ	Case of 25	$ 480.23	41%	$ 283.34	CS
CTS 1334	MK-3 Level 3 OC Gel 1.5 OZ	Case of 25	$ 480.23	41%	$ 283.34	CS
CTS 1337	OC Grenade 2 OZ	Case of 25	$ 624.73	41%	$ 368.59	CS
CTS 1338	MK-3 Level 3 OC Omni-Stream™ 1.2 OZ, 360° Performance	Case of 25	$ 485.88	41%	$ 286.67	CS
CTS 1341	MK-3 OC/CS Stream 1.5 OZ	Case of 25	$ 483.01	41%	$ 284.98	CS
CTS 1347	MK-3 Level 2 OC Vapor 1.5 OZ	Case of 25	$ 519.77	41%	$ 306.66	CS
CTS 1395	Decontamination Spray 1.5 OZ		$ 15.14	41%	$ 8.93	EA
CTS 1401	MK-4 Inert Stream 3.75 OZ	Case of 25	$ 418.08	41%	$ 246.67	CS
CTS 1401A	Nitrogen Refill Cartridge		$ 27.71	41%	$ 16.35	EA
CTS 1401A-6	Nitrogen Refill Cartridge, 6 Pack		$ 166.23	41%	$ 98.08	PK
CTS 1401H	MK-46 Horizontal Dispenser 46 OZ		$ 687.20	41%	$ 405.45	EA
CTS 1401HE	MK-46 Rapid Recharge Cylinder w/ Nozzle Head & Sling (Nitrogen Cartridge & Refill Solution Not Included)		$ 1,313.56	41%	$ 775.00	EA
CTS 1401HV	Nozzle Assembly for 1401HE		$ 1,015.65	41%	$ 599.23	EA
CTS 1401V	MK-46 Vertical Dispenser 46 OZ		$ 615.49	41%	$ 363.14	EA
CTS 1402	MK-4 Inert Foam 3.5 OZ	Case of 25	$ 393.85	41%	$ 232.37	CS
CTS 1403	MK-4 Inert Fog 3.5 OZ	Case of 25	$ 457.63	41%	$ 270.00	CS
CTS 1404	MK-4 Inert Gel 2.8 OZ	Case of 25	$ 446.33	41%	$ 263.33	CS
CTS 1408	MK-4 Inert 2.99 OZ, Omni-Stream™, 360° Performance	Case of 25	$ 393.85	41%	$ 232.37	CS
CTS 1411	MK-4 Level 1 OC Stream 3.75 OZ	Case of 25	$ 525.42	41%	$ 310.00	CS
CTS 1418	MK-4 Level 1 Omni-Stream™ - 360° Performance		$ 15.76	41%	$ 9.30	EA
CTS 1421	MK-4 Level 2 OC Stream 3.75 OZ	Case of 25	$ 542.37	41%	$ 320.00	CS
CTS 1422	MK-4 Level 2 OC Foam 3.75 OZ	Case of 25	$ 663.84	41%	$ 391.67	CS
CTS 1423	MK-4 Level 2 OC Fog 3.75 OZ	Case of 25	$ 584.75	41%	$ 345.00	CS
CTS 1424	MK-4 Level 2 OC Gel 3.75 OZ	Case of 25	$ 525.42	41%	$ 310.00	CS
CTS 1428	MK-4 Level 2 OC Omni-Stream™ 2.99 OZ, 360° Performance	Case of 25	$ 525.42	41%	$ 310.00	CS
CTS 1431	MK-4 Level 3 OC Stream 3.75 OZ	Case of 25	$ 533.90	41%	$ 315.00	CS
CTS 1432	MK-4 Level 3 OC Foam 3.5 OZ	Case of 25	$ 525.42	41%	$ 310.00	CS
CTS 1433	MK-4 Level 3 OC Fog 3.5 OZ	Case of 25	$ 525.42	41%	$ 310.00	CS
CTS 1434	MK-4 Level 3 OC Gel 2.8 OZ	Case of 25	$ 525.42	41%	$ 310.00	CS
CTS 1438	MK-4 Level 3 OC Omni-Stream™ 2.99 OZ, 360° Performance	Case of 25	$ 525.42	41%	$ 310.00	CS
CTS 1441	MK-4 OC/CS Stream 3.75 OZ	Case of 25	$ 542.37	41%	$ 320.00	CS
CTS 1447	MK-4 Level 2 OC Vapor 3.75 OZ	Case of 25	$ 649.17	41%	$ 383.01	CS
CTS 1601	MK-6 Inert Stream 0.75 OZ	Case of 25	$ 437.85	41%	$ 258.33	CS
CTS 1604	MK-6 Inert Gel 0.75 OZ	Case of 25	$ 418.08	41%	$ 246.67	CS
CTS 1611	MK-6 Level 1 OC Stream 0.75 OZ	Case of 25	$ 426.55	41%	$ 251.66	CS
CTS 1621	MK-6 Level 2 OC Stream 0.75 OZ	Case of 25	$ 437.85	41%	$ 258.33	CS
CTS 1624	MK-6 Level 2 OC Gel 0.75 OZ	Case of 25	$ 463.28	41%	$ 273.34	CS
CTS 1631	MK-6 Level 3 OC Stream 0.75 OZ	Case of 25	$ 443.50	41%	$ 261.67	CS
CTS 1901	MK-9 Inert Stream 12.5 OZ	Case of 6	$ 271.86	41%	$ 160.40	CS

CONFIDENTIAL

Item ID	Description	Extended Description	Safeware List	Discount	Net Price	UOM
CTS 1901A	MK-9 Hose & Wand - Hose and Wand Only - Only adapts to 1947 OC Vapor		$ 70.62	41%	$ 41.67	EA
CTS 1901T	MK-9 Training Dispenser 16 OZ		$ 234.68	41%	$ 138.46	EA
CTS 1902	MK-9 Inert Foam 14 OZ	Case of 6	$ 296.61	41%	$ 175.00	CS
CTS 1903	MK-9 Inert Fog 13 OZ	Case of 6	$ 366.10	41%	$ 216.00	CS
CTS 1904	MK-9 Inert Gel 13 OZ	Case of 6	$ 321.36	41%	$ 189.60	CS
CTS 1908	MK-9 Inert 12.9 OZ Omni-Stream™, 360° Performance	Case of 6	$ 296.61	41%	$ 175.00	CS
CTS 1911	MK-9 Level 1 OC Stream 12.5 OZ	Case of 6	$ 399.32	41%	$ 235.60	CS
CTS 1918	MK-9 Level 1 Omni-Stream™ - 360° Performance		$ 43.74	41%	$ 25.81	EA
CTS 1921	MK-9 Level 2 OC Stream 12.5 OZ	Case of 6	$ 416.27	41%	$ 245.60	CS
CTS 1922	MK-9 Level 2 OC Foam 12.5 OZ	Case of 6	$ 437.29	41%	$ 258.00	CS
CTS 1923	MK-9 Level 2 OC Fog 12.5 OZ	Case of 6	$ 483.39	41%	$ 285.20	CS
CTS 1924	MK-9 Level 2 OC Gel 12.5 OZ	Case of 6	$ 418.98	41%	$ 247.20	CS
CTS 1928	MK-9 Level 2 OC Omni-Stream™ 12.9 OZ, 360° Performance	Case of 6	$ 406.10	41%	$ 239.60	CS
CTS 1931	MK-9 Level 3 OC Stream 12.5 OZ	Case of 6	$ 433.22	41%	$ 255.60	CS
CTS 1932	MK-9 Level 3 OC Foam 14 OZ	Case of 6	$ 406.10	41%	$ 239.60	CS
CTS 1933	MK-9 Level 3 OC Fog 13 OZ	Case of 6	$ 406.10	41%	$ 239.60	CS
CTS 1934	MK-9 Level 3 OC Gel 13 OZ	Case of 6	$ 406.10	41%	$ 239.60	CS
CTS 1938	MK-9 Level 3 OC Omni-Stream™ 12.9 OZ, 360° Performance	Case of 6	$ 406.10	41%	$ 239.60	CS
CTS 1941	MK-9 OC/CS Stream 12.5 OZ	Case of 6	$ 414.92	41%	$ 244.80	CS
CTS 1947	MK-9 Level 2 OC Vapor 9.4 OZ	Case of 6	$ 509.83	41%	$ 300.80	CS
CTS 201FB	Flash-Bang Reload Training Fuze - Blue	Must order Quantities of 35	$ 893.79	41%	$ 527.34	CS
CTS 201SB	Sting-Ball Reload Training Fuze - Blue (3 Sec +/- .3 Delay)		$ 24.55	41%	$ 14.48	EA
CTS 201TF	5 & 8 Series Grenade Training Fuze RH Thread		$ 24.99	41%	$ 14.74	EA
CTS 2300	12GA Inert Liquid Barricade	Must order Quantities of 5	$ 61.39	41%	$ 36.22	CS
CTS 2330	12GA CS Liquid Barricade	Must order Quantities of 5	$ 65.19	41%	$ 38.46	CS
CTS 2340	12GA OC Liquid Barricade	Must order Quantities of 5	$ 65.19	41%	$ 38.46	CS
CTS 2400	12GA Powder Projectile, Training	Must order Quantities of 5	$ 61.39	41%	$ 36.22	CS
CTS 2430	12GA CS Powder Projectile	Must order Quantities of 5	$ 65.19	41%	$ 38.46	CS
CTS 2440	12GA OC Powder Projectile	Must order Quantities of 5	$ 65.19	41%	$ 38.46	CS
CTS 2550	12GA Single Rubber Baton- Sabot	Must order Quantities of 5	$ 43.50	41%	$ 25.67	CS
CTS 2551	12GA Fin Stabilized	Must order Quantities of 5	$ 46.89	41%	$ 27.67	CS
CTS 2552	12GA .31Cal Sting-Balls	Must order Quantities of 5	$ 43.50	41%	$ 25.67	CS
CTS 2553	12GA .31 Cal High Velocity Sting-Balls	Must order Quantities of 5	$ 43.50	41%	$ 25.67	CS
CTS 2555	12GA (3) .60 Cal Sting-Balls	Must order Quantities of 5	$ 43.50	41%	$ 25.67	CS
CTS 2570	12GA Door Breacher	Must order Quantities of 5	$ 49.72	41%	$ 29.33	CS
CTS 2577	12GA Heavy Door Breacher (Non Toxic)		$ 18.53	41%	$ 10.93	EA
CTS 2581	12GA Super-Sock® Bean Bag	Must order Quantities of 5	$ 49.15	41%	$ 29.00	CS
CTS 2581B	12GA Super-Sock® Bean Bag- Blue Marking Powder	Must order Quantities of 5	$ 63.84	41%	$ 37.67	CS
CTS 2581G	12GA Super-Sock® Bean Bag - Green Marking Powder	Must order Quantities of 5	$ 63.84	41%	$ 37.67	CS
CTS 2581R	12GA Super-Sock® Bean Bag - Red Marking Powder	Must order Quantities of 5	$ 63.84	41%	$ 37.67	CS
CTS 2581Y	12GA Super-Sock® Bean Bag - Yellow Marking Powder	Must order Quantities of 5	$ 63.84	41%	$ 37.67	CS
CTS 2595	12GA Muzzle Bang	Must order Quantities of 25	$ 322.03	41%	$ 190.00	CS
CTS 2600	12GA Launching Cartridge	Must order Quantities of 5	$ 42.37	41%	$ 25.00	CS

CONFIDENTIAL

Item ID	Description	Extended Description	Safeware List	Discount	Net Price	UOM
CTS 3210	37MM Short Range Smoke, Pyro, 4.9" Long		$ 32.77	41%	$ 19.33	EA
CTS 3211	37MM Long Range Smoke, Pyro, 4.9" Long		$ 33.22	41%	$ 19.60	EA
CTS 3213	37MM Multi 3 Smoke, Pyro, 4.9" Long		$ 43.50	41%	$ 25.67	EA
CTS 3215	37MM Multi 5 Smoke, Pyro, 8" Long		$ 44.29	41%	$ 26.13	EA
CTS 3230	37MM CS Short Range, Pyro, 4.9" Long		$ 36.16	41%	$ 21.33	EA
CTS 3231	37MM CS Long Range, Pyro, 4.9" Long		$ 38.68	41%	$ 22.82	EA
CTS 3233	37MM CS Multi 3, Pyro, 4.9" Long		$ 43.62	41%	$ 25.74	EA
CTS 3235	37MM CS Multi 5, Pyro, 8" Long		$ 47.23	41%	$ 27.87	EA
CTS 3300	37MM Liquid Barricade, Smokeless, 5.45" Long		$ 30.85	41%	$ 18.20	EA
CTS 3330	37MM CS Liquid Barricade, Smokeless, 5.45" Long		$ 34.92	41%	$ 20.60	EA
CTS 3340	37MM OC Liquid Barricade, Smokeless, 5.45" Long		$ 35.48	41%	$ 20.93	EA
CTS 3400	37MM Muzzle Blast, 8" Long		$ 30.51	41%	$ 18.00	EA
CTS 3401	37MM Powder Barricade, Smokeless, 5.45" Long		$ 33.90	41%	$ 20.00	EA
CTS 3430	37MM CS Muzzle Blast, 8" Long		$ 36.05	41%	$ 21.27	EA
CTS 3431	37MM CS Powder Barricade, Smokeless, 5.45" Long		$ 38.98	41%	$ 23.00	EA
CTS 3440	37MM OC Muzzle Blast, 8" Long		$ 38.87	41%	$ 22.93	EA
CTS 3441	37MM OC Powder Barricade, Smokeless, 5.45" Long		$ 38.98	41%	$ 23.00	EA
CTS 3551	37MM Multi 3 Foam Baton, 4.9" Long		$ 41.24	41%	$ 24.33	EA
CTS 3553	37MM .31Cal Sting-Balls, 4.9" Long		$ 33.33	41%	$ 19.66	EA
CTS 3555	37MM Multi 5 Foam Baton, 8" Long		$ 40.11	41%	$ 23.66	EA
CTS 3555R	37MM Multi 5 Rubber Baton, 8" Long		$ 36.27	41%	$ 21.40	EA
CTS 3556	37MM .31Cal Sting-Ball, 8" Long		$ 28.14	41%	$ 16.60	EA
CTS 3558	37MM .60Cal Sting-Balls, 4.9" Long		$ 36.84	41%	$ 21.74	EA
CTS 3559	37MM .60Cal Sting-Ball, 8" Long		$ 32.77	41%	$ 19.33	EA
CTS 3561	37MM Multi 3 Wood Baton, 4.9" Long		$ 33.33	41%	$ 19.66	EA
CTS 3565	37MM Multi 5 Wood Baton, 8" Long		$ 32.32	41%	$ 19.07	EA
CTS 3581	37MM Super-Sock® Bean Bag 4.9" Long		$ 45.08	41%	$ 26.60	EA
CTS 3582	37MM Flexible Baton Close Range 4.9" Long, Close Range (Green)		$ 44.29	41%	$ 26.13	EA
CTS 3583	37MM Nylon-Flex Bean Bag 4.9" Long, Low Impact (Yellow)		$ 44.29	41%	$ 26.13	EA
CTS 3584	37MM Flexible Baton Standard 4.9" Long, Standard (Red)		$ 44.29	41%	$ 26.13	EA
CTS 3585	37MM Flexible Baton Standard 4.9" Long, Long Range (Black)		$ 44.29	41%	$ 26.13	EA
CTS 3600	37MM Launching Cartridge		$ 18.31	41%	$ 10.80	EA
CTS 405016	40MM .60Cal Sting-Balls, Smokeless,	4.8" Long	$ 47.05	41%	$ 27.76	EA
CTS 405077	40MM Sponge, Smokeless,	Spin Stabilized, 4in long	$ 42.98	41%	$ 25.36	EA
CTS 4090-1	40MM Aerial Flash-Bang, 100 Meter Warning Signal		$ 65.73	41%	$ 38.78	EA
CTS 4090-2	40MM Aerial Flash-Bang, 200 Meter Warning Signal		$ 65.73	41%	$ 38.78	EA
CTS 4090-3	40MM Aerial Flash-Bang, 300 Meter Warning Signal		$ 65.73	41%	$ 38.78	EA
CTS 4090-50	40MM Aerial Flash-Bang, 50 Meter Warning Signal		$ 65.73	41%	$ 38.78	EA
CTS 4094	Venom® Multi (4) Flash-Bang Round	Must order Quantities of 60	$ 10,474.58	41%	$ 6,180.00	CS
CTS 4210	40MM White Smoke, Pyro, 4.8" Long		$ 32.77	41%	$ 19.33	EA
CTS 4210G	40MM Green Smoke, Pyro, 4.8" Long		$ 51.53	41%	$ 30.40	EA
CTS 4210R	40MM Red Smoke, Pyro, 4.8" Long		$ 51.53	41%	$ 30.40	EA
CTS 4210Y	40MM Yellow Smoke, Pyro, 4.8" Long		$ 51.53	41%	$ 30.40	EA
CTS 4213	40MM Multi 3 Smoke, 4.8" Long		$ 47.46	41%	$ 28.00	EA

CONFIDENTIAL

Item ID	Description	Extended Description	Safeware List	Discount	Net Price	UOM
CTS 4217	Venom® Multi (7) Smoke Round / Min	Must order Quantities of 60	$ 6,705.08	41%	$ 3,956.00	CS
CTS 4230	40MM CS Smoke, Pyro, 4.8" Long		$ 33.33	41%	$ 19.66	EA
CTS 4233	40MM CS Multi 3 Smoke, 4.8" Long		$ 51.19	41%	$ 30.20	EA
CTS 4237	Venom® Multi Smoke Cs	Must order Quantities of 60	$ 6,705.08	41%	$ 3,956.00	CS
CTS 4300	40MM Inert Liquid Barricade, Spin Stabilized, 4.1" Long		$ 39.11	41%	$ 23.07	EA
CTS 4330	40MM CS Liquid Barricade, Spin Stabilized, 4.1" Long		$ 40.20	41%	$ 23.72	EA
CTS 4340	40MM OC Liquid Barricade, Spin Stabilized, 4.1" Long		$ 41.07	41%	$ 24.23	EA
CTS 4401	40MM Inert Powder Barricade, Spin Stabilized, 4.1" Long		$ 39.11	41%	$ 23.07	EA
CTS 4431	40MM CS Powder Barricade, Spin Stabilized, 4.1" Long		$ 40.63	41%	$ 23.97	EA
CTS 4441	40MM OC Powder Barricade, Spin Stabilized, 4.1" Long		$ 40.63	41%	$ 23.97	EA
CTS 4500	40MM 4557 Reload Kit - 24 Shot Practice Only - 24 Cases, 8 Bands And 5 Noses		$ 562.71	41%	$ 332.00	KT
CTS 4502	40MM 4557 Reload Kit - 72 Shot Practice Only - 72 Cases, 24 Bands And 15 Noses		$ 1,511.86	41%	$ 892.00	KT
CTS 4504	40MM 4557 Reload Kit - 120 Shot Practice Only - 120 Cases, 40 Bands And 25 Noses		$ 2,237.29	41%	$ 1,320.00	KT
CTS 4505	40MM 4557 Reload Kit - 250 Shot Practice Only - 250 Inserts, 25 Cases, 30 Bands And 30 Noses - Press Needed		$ 2,288.14	41%	$ 1,350.00	KT
CTS 4510	40MM Frangible Impact - Inert Powder		$ 43.50	41%	$ 25.67	EA
CTS 4530	40MM Frangible Impact - CS Powder		$ 48.47	41%	$ 28.60	EA
CTS 4550	40MM Frangible Impact - Orange Marking Powder		$ 48.47	41%	$ 28.60	EA
CTS 4551	40MM Multi 3 Foam Baton, Smokeless, 4.8" Long		$ 38.08	41%	$ 22.47	EA
CTS 4553	40MM .31Cal Sting-Balls, Smokeless, 4.8" Long		$ 35.14	41%	$ 20.73	EA
CTS 4555R	40MM Multi 3 Rubber Baton, 4.8" Long		$ 35.14	41%	$ 20.73	EA
CTS 4556	40MM Frangible Impact - OC Powder		$ 48.47	41%	$ 28.60	EA
CTS 4557	40MM Sponge, Smokeless, Spin Stabilized, 3.9" Long		$ 35.82	41%	$ 21.13	EA
CTS 4557-01	40MM Insert		$ 5.54	41%	$ 3.27	EA
CTS 4557-01I	40MM 1,000 Inserts (Press Not Included)		$ 5,225.65	41%	$ 3,083.13	EA
CTS 4557-02	40MM Case W/O Insert		$ 7.68	41%	$ 4.53	EA
CTS 4557-03	40MM Driving Band		$ 4.29	41%	$ 2.53	EA
CTS 4557-04	40MM Nose/Ogive		$ 7.57	41%	$ 4.47	EA
CTS 4557HV	40MM Sponge, Smokeless, Spin Stabilized, High Velocity, 3.9" Long		$ 38.98	41%	$ 23.00	EA
CTS 4557RP	40MM Reload Press		$ 640.11	41%	$ 377.66	EA
CTS 4558	40MM .60Cal Sting-Balls, Smokeless, 4.8" Long		$ 39.21	41%	$ 23.13	EA
CTS 4561	40MM Multi 3 Wood Baton, Smokeless, 4.8" Long		$ 35.25	41%	$ 20.80	EA
CTS 4581	40MM Super-Sock® Bean Bag 4.8" Long		$ 39.44	41%	$ 23.27	EA
CTS 4600	40MM Inert Muzzle Blast		$ 33.33	41%	$ 19.66	EA
CTS 4630	40MM CS Muzzle Blast		$ 35.20	41%	$ 20.77	EA
CTS 4640	40MM OC Muzzle Blast		$ 39.66	41%	$ 23.40	EA
CTS 5200T	5 Series Canister Grenade Training Body		$ 74.53	41%	$ 43.97	EA
CTS 5210	White Smoke Canister Grenade		$ 48.24	41%	$ 28.46	EA
CTS 5210B	Smoke Baffled Canister Grenade, Pyro, Low Flame Potential		$ 65.54	41%	$ 38.67	EA
CTS 5210JL	Smoke Jet-Lite Canister Grenade, Pyro		$ 63.62	41%	$ 37.54	EA
CTS 5211	White Smoke Triple-Phaser® Canister Grenade		$ 66.10	41%	$ 39.00	EA

CONFIDENTIAL

Item ID	Description	Extended Description	Safeware List	Discount	Net Price	UOM
CTS 5230	CS Canister Grenade		$ 52.43	41%	$ 30.93	EA
CTS 5230B	CS Baffled Canister Grenade, Pyro, Low Flame Potential		$ 67.80	41%	$ 40.00	EA
CTS 5230JL	CS Jet-Lite Canister Grenade, Pyro		$ 65.20	41%	$ 38.47	EA
CTS 5231	CS Triple-Phaser® Canister Grenade		$ 73.33	41%	$ 43.26	EA
CTS 5300	CS Training Pellets (50 Per Can)		$ 72.32	41%	$ 42.67	EA
CTS 5400	Inert Flameless Expulsion Canister Grenade		$ 69.38	41%	$ 40.93	EA
CTS 5430	CS Flameless Expulsion Canister Grenade		$ 71.75	41%	$ 42.33	EA
CTS 5440	OC Flameless Expulsion Canister Grenade		$ 71.75	41%	$ 42.33	EA
CTS 6210	White Smoke Canister Grenade		$ 50.28	41%	$ 29.67	EA
CTS 6210B	Blue Smoke Canister Grenade		$ 70.62	41%	$ 41.67	EA
CTS 6210G	Green Smoke Canister Grenade		$ 70.62	41%	$ 41.67	EA
CTS 6210HC	Hexachlorothane (HC) Smoke		$ 60.23	41%	$ 35.54	EA
CTS 6210K	Black Smoke Canister Grenade		$ 70.62	41%	$ 41.67	EA
CTS 6210O	Orange Smoke Canister Grenade		$ 70.62	41%	$ 41.67	EA
CTS 6210R	Red Smoke Canister Grenade		$ 70.62	41%	$ 41.67	EA
CTS 6210V	Violet Smoke Canister Grenade		$ 70.62	41%	$ 41.67	EA
CTS 6210Y	Yellow Smoke Canister Grenade		$ 70.62	41%	$ 41.67	EA
CTS 6214	Thermite Incendiary Grenade (2.34" / 59MM Diameter)		$ 90.40	41%	$ 53.34	EA
CTS 6230	CS Canister Grenade		$ 48.59	41%	$ 28.67	EA
CTS 6300	Inert Vapor Grenade		$ 63.28	41%	$ 37.34	EA
CTS 6330	CS Vapor Grenade		$ 68.93	41%	$ 40.67	EA
CTS 6340	OC Vapor Grenade		$ 68.93	41%	$ 40.67	EA
CTS 6343	OC-CS Vapor Grenade		$ 68.93	41%	$ 40.67	EA
CTS 7200	Flash-Bang Training Kit - 70 Reload Trng Fuzes and 1 Free Body		$ 1,715.56	41%	$ 1,012.18	KT
CTS 7200M	Mini-Bang® Training Kit - 70 Reload Trng Fuzes And 1 Free Body		$ 1,715.56	41%	$ 1,012.18	KT
CTS 7290	Flash-Bang - Steel Body	Must order Quantities of 12	$ 901.69	41%	$ 532.00	CS
CTS 7290-2	Flash-Bang, Aluminum Body, Low Roll DoubleBang™	Must order Quantities of 12	$ 1,069.10	41%	$ 630.77	CS
CTS 7290-3	Flash-Bang, Aluminum Body, 3 Bang	Must order Quantities of 12	$ 1,956.61	41%	$ 1,154.40	CS
CTS 7290-5	Flash-Bang, Aluminum Body, 5 Bang	Must order Quantities of 12	$ 2,244.07	41%	$ 1,324.00	CS
CTS 7290-7	Flash-Bang, Aluminum Body, 7 Bang	Must order Quantities of 12	$ 2,503.05	41%	$ 1,476.80	CS
CTS 7290-9	Flash-Bang, Aluminum Body, 9 Bang	Must order Quantities of 12	$ 2,733.56	41%	$ 1,612.80	CS
CTS 7290-CI	Flash-Bang - Command Initiated	Must order Quantities of 12	$ 1,040.42	41%	$ 613.85	CS
CTS 7290I	Initiator		$ 258.47	41%	$ 152.50	EA
CTS 7290KT	Training Kit, Flash-Bang (7290T, 7290Mt) Sting-Ball (9590T) Hard Case W/ Fuze Capacity		$ 209.49	41%	$ 123.60	KT
CTS 7290M	Mini-Bang® - Steel Body	Must order Quantities of 12	$ 847.46	41%	$ 500.00	CS
CTS 7290M-CI	Mini-Bang® - Command Initiated	Must order Quantities of 12	$ 1,040.42	41%	$ 613.85	CS
CTS 7290ML	Mini-Bang - Aluminum Body, Reduced Weight	Must order Quantities of 12	$ 1,069.10	41%	$ 630.77	CS
CTS 7290MT	Mini-Bang® Training Body - Blue With Left Hand Thread		$ 77.97	41%	$ 46.00	EA
CTS 7290NE	Non El (2500Ft Spool Shock Tube)		$ 861.69	41%	$ 508.40	SP
CTS 7290S	Splicers - Qty 30		$ 17.28	41%	$ 10.20	PK
CTS 7290T	Flash-Bang Training Body - Blue With Left Hand Thread		$ 80.23	41%	$ 47.34	EA
CTS 8200T	8 Series Canister Grenade Training Body		$ 71.75	41%	$ 42.33	EA
CTS 8210	White Smoke Tactical Canister Grenade		$ 36.05	41%	$ 21.27	EA

CONFIDENTIAL

Item ID	Description	Extended Description	Safeware List	Discount	Net Price	UOM
CTS 8210G	Green Smoke Tactical Canister Grenade		$ 55.66	41%	$ 32.84	EA
CTS 8210R	Red Smoke Tactical Canister Grenade		$ 55.66	41%	$ 32.84	EA
CTS 8210Y	Yellow Smoke Tactical Canister Grenade		$ 55.66	41%	$ 32.84	EA
CTS 8230	CS Tactical Canister Grenade		$ 37.51	41%	$ 22.13	EA
CTS 9210	Smoke Jet-Lite Rubber Ball Grenade, Pyro		$ 53.67	41%	$ 31.67	EA
CTS 922038	9430 - GRND., BLASTING, CS, LABELED		$ 97.63	41%	$ 57.60	EA
CTS 9230	CS Jet-Lite Rubber Ball Grenade, Pyro		$ 55.37	41%	$ 32.67	EA
CTS 925006	9590 Grnd, Sting Ball .314 labeled CTS		$ 94.92	41%	$ 56.00	EA
CTS 9410	Inert Tear Ball Grenade	Must order Quantities of 12	$ 935.59	41%	$ 552.00	CS
CTS 9430	CS Tear Ball Grenade	Must order Quantities of 12	$ 976.27	41%	$ 576.00	CS
CTS 9440	OC Tear Ball Grenade	Must order Quantities of 12	$ 976.27	41%	$ 576.00	CS
CTS 9500	Sting-Ball Training Kit - 70 Reload Trng Fuzes And 1 Free Body		$ 1,715.56	41%	$ 1,012.18	KT
CTS 9590	No Irritant Sting-Ball Grenade	Must order Quantities of 12	$ 949.15	41%	$ 560.00	CS
CTS 9590T	Sting-Ball Training Body - Blue With Left Handed Thread	Must order Quantities of 35	$ 2,507.34	41%	$ 1,479.33	CS
CTS 9593	CS Sting-Ball Grenade - Approx. 105 Rubber Balls	Must order Quantities of 12	$ 947.80	41%	$ 559.20	CS
CTS 9594	OC Sting-Ball Grenade - Approx. 105 Rubber Balls	Must order Quantities of 12	$ 947.80	41%	$ 559.20	CS
CTS 9690	No Irritant Sting-Ball Grenade .61 Caliber	Must order Quantities of 12	$ 949.15	41%	$ 560.00	CS
CTS A402	11" RAIL ADJ. GHOST RING FRONT SIGHT, PRE-DRILLED		$ 271.19	41%	$ 160.00	EA
CTS A403	11" RAIL ADJ. GHOST RING FRONT SIGHT, PRE-DRILLED, ADDED BRACKET FOR MONOBLOCK		$ 271.19	41%	$ 160.00	EA
CTS A404	BRACKET MOUNTED ON COMBO RAIL W/ TWO 3" PICATINNY TYPE RAILS		$ 110.17	41%	$ 65.00	EA
CTS A405	5" PICATINNY RAIL, MOUNTS TO TOP FRONT OF MULTI-LAUNCHER FRAME		$ 114.41	41%	$ 67.50	EA
CTS A406	5" PICATINNY RAIL, MOUNTS TO MONO BLOCK OF SINGLE SHOT LAUNCHER		$ 220.34	41%	$ 130.00	EA
CTS A407	RING W/ 2 SIDE RAILS, MOUNTS TO 40MM GL-6, GL-65, GL-1 LAUNCHERS		$ 163.14	41%	$ 96.25	EA
CTS A408	RING W/ 2 SIDE & 1 UNDER RAIL MOUNTS TO 40MM SINGLE SHOT LAUNCHERS		$ 180.08	41%	$ 106.25	EA
CTS A410	40MM RETRO-FIT RAIL SYSTEM W/ BARREL PROTECTOR		$ 400.42	41%	$ 236.25	EA
CTS H137-0	UNDER MOUNT LAUNCHER w/ MOUNTING BRACKET (HL-1 37)		$ 1,487.29	41%	$ 877.50	EA
CTS H140-0	UNDER MOUNT LAUNCHER w/ MOUNTING BRACKET (HGL-1 40)		$ 1,769.07	41%	$ 1,043.75	EA
CTS HC1003C [COLOR]	Color Gorcote® OS Handcuff *NIJ*	Colors: Red, yellow, orange, pink, blue, purple, black, green; OS = Oversize, 17% Larger than 1010 Standard Handcuff, Includes 2 universal handcuff keys; ***MINIMUM PURCHASE Qty of 30	$ 63.62	41%	$ 37.54	EA
CTS HC1003NIC	OS Chain Style Handcuff *NIJ*	OS = Oversize, 17% Larger than 1010 Standard Handcuff, Includes 2 universal handcuff keys	$ 47.80	41%	$ 28.20	EA
CTS HC1008C [COLOR]	Color Gorcote® TRI-MAX™ Pick Resistant Handcuff - Pat Pend *NIJ*	Colors: Red, yellow, orange, pink, blue, purple, black, green; Include 2 universal handcuff keys; ***MINIMUM PURCHASE Qty of 30	$ 68.93	41%	$ 40.67	EA
CTS HC1008NIC	TRI-MAX™ Pick Resistant Handcuff - Patent Pending *NIJ*	Includes 2 universal handcuff keys	$ 53.11	41%	$ 31.33	EA

CONFIDENTIAL

Item ID	Description	Extended Description	Safeware List	Discount	Net Price	UOM
CTS HC10109000AR	AR Set 1010 Handcuffs Attached to 9000 Leg Cuffs by 30" Chain	Transport restraints with handcuffs include 2 universal handcuff keys.	$ 145.76	41%	$ 86.00	EA
CTS HC10109000H	H Style Design for Transport 56" #7000 Waist Chain Separated	1010 Handcuffs Connected to 9000 Leg Cuff by 30" Chain	$ 161.81	41%	$ 95.47	EA
CTS HC1010C [COLOR]	Color Gorcote® Standard Handcuff - *NIJ*	Colors: Red, yellow, orange, pink, blue, purple, black, green; Include 2 universal handcuff keys; ***MINIMUM PURCHASE Qty of 30	$ 60.34	41%	$ 35.60	EA
CTS HC1010NIC	Standard Handcuff Set - *NIJ*	Includes 2 universal handcuff keys	$ 43.50	41%	$ 25.67	EA
CTS HC1054C [COLOR]	Color Gorcote® OS Hinged Handcuffs - *NIJ*	Colors: Red, yellow, orange, pink, blue, purple, black, green; OS = Oversize, 17% Larger than 1010 Standard Handcuff, Includes 2 universal handcuff keys; ***MINIMUM PURCHASE Qty of 30	$ 68.14	41%	$ 40.20	EA
CTS HC1054NIC	OS Hinged Handcuffs - *NIJ*	OS = Oversize, 17% Larger than 1010 Standard Handcuff, Includes 2 universal handcuff keys	$ 55.82	41%	$ 32.93	EA
CTS HC1058C [COLOR]	Color Gorcote® Tri-Max™ OS Hinged Handcuffs *NIJ*	Colors: Red, yellow, orange, pink, blue, purple, black, green; OS = Oversize, 17% Larger than 1010 Standard Handcuff, Includes 2 universal handcuff keys; ***MINIMUM PURCHASE Qty of 30	$ 71.98	41%	$ 42.47	EA
CTS HC1058NIC	Tri-Max™ OS Hinged Handcuffs - Patent Pending *NIJ*	OS = Oversize, 17% Larger than 1010 Standard Handcuff, Includes 2 universal handcuff keys	$ 56.16	41%	$ 33.13	EA
CTS HC1108C [COLOR]	Color Gorcote® OS TRI-MAX™ Pick Resistant Cuff - Pat. Pend *NIJ*	Colors: Red, yellow, orange, pink, blue, purple, black, green; OS = Oversize, 17% Larger than 1010 Standard Handcuff, Includes 2 universal handcuff keys; ***MINIMUM PURCHASE Qty of 30	$ 72.09	41%	$ 42.53	EA
CTS HC1108NIC	OS TRI-MAX™ Pick Resistant Handcuff - Pat Pend *NIJ*	OS = Oversize, 17% Larger than 1010 Standard Handcuff, Includes 2 universal handcuff keys	$ 56.27	41%	$ 33.20	EA
CTS HC5259NIC	Legcuff Over the Boot/XXLarge Size	Include 2 universal handcuff keys	$ 114.01	41%	$ 67.27	EA
CTS HC6000	Hardened Lead Chain, 1010 Handcuff Set on 60" Chain w/ 2" Ring Attached at end		$ 62.71	41%	$ 37.00	EA
CTS HC6010	Hardened Lead Chain, One 1010 Handcuff on 60" Chain w/ 2" Ring Attached at end		$ 58.19	41%	$ 34.33	EA
CTS HC70009010	Hardened Waist Chain w/ 9010 XOS Handcuff Set		$ 98.19	41%	$ 57.93	EA
CTS HC7000NIC	Hardened Waist Chain w/ 1010 Handcuffs Separated Left & Right Side		$ 64.18	41%	$ 37.87	EA
CTS HC7003NIC	Hardened Waist Chain w/ 1003 Handcuffs Separated Left & Right Side		$ 72.88	41%	$ 43.00	EA
CTS HC7008NIC	Hardened Waist Chain w/ 1008 Handcuffs Separated Left & Right Side		$ 82.82	41%	$ 48.86	EA
CTS HC7077	Hardened Waist Chain w/ Rectangular Link for use w/ Blue Box 60" Overall Length		$ 39.44	41%	$ 23.27	EA
CTS HC7078	Hardened Connector Chain for Handcuffs to Leg Cuffs		$ 27.01	41%	$ 15.94	EA

CONFIDENTIAL

Item ID	Description	Extended Description	Safeware List	Discount	Net Price	UOM
CTS HC7084	Blue Box for Chain Style Handcuffs, Safety Cover w/ Locking Clip		$ 26.89	41%	$ 15.87	EA
CTS HC7178	Hardened Waist Chain w/ Rectangular Link for use w/ Blue Box 78" Overall Length		$ 52.43	41%	$ 30.93	EA
CTS HC7196	Hardened Waist Chain w/ Rectangular Link for use w/ Blue Box 96" Overall Length		$ 67.46	41%	$ 39.80	EA
CTS HC8010	Universal Standard Handcuff Key, Fits Popular Brands, Single	All keys are sold individually	$ 1.24	41%	$ 0.73	EA
CTS HC9000C [COLOR]	Color Gorcote®Finish Legcuffs	Colors: Red, yellow, orange, pink, blue, purple, black, green; Include 2 universal handcuff keys; ***MINIMUM PURCHASE Qty of 30	$ 79.77	41%	$ 47.06	EA
CTS HC9000NIC	OS Legcuffs, Carbon Steel w/ Nickel Plating	Include 2 universal handcuff keys	$ 70.62	41%	$ 41.67	EA
CTS HC9008C [COLOR]	Color Gorcote®Carbon Steel Leg Cuff Tri-Max™ Pick Resistant	Colors: Red, yellow, orange, pink, blue, purple, black, green; Include 2 universal handcuff keys; ***MINIMUM PURCHASE Qty of 30	$ 113.90	41%	$ 67.20	EA
CTS HC9008NIC	Carbon Steel Leg Cuff Tri-Max™ Pick Resistant - Pat Pend	Include 2 universal handcuff keys	$ 104.75	41%	$ 61.80	EA
CTS HC9010C [COLOR]	Color Gorcote® XOS Handcuff or Hobbles	Colors: Red, yellow, orange, pink, blue, purple, black, green; XOS = Extra Oversize, 25% Larger than 1010 Standard Legcuff; Includes 2 universal handcuff keys; ***MINIMUM PURCHASE Qty of 30	$ 78.64	41%	$ 46.40	EA
CTS HC9010NIC	Carbon Steel XOS Handcuff or Hobbles	XOS = Extra Oversize, 25% Larger than 1010 Standard Legcuff; Includes 2 universal handcuff keys	$ 69.49	41%	$ 41.00	EA
CTS HC9108C [COLOR]	Color Gorcote® Tri-Max™ Carbon Steel XOS Handcuff or Hobbles	Colors: Red, yellow, orange, pink, blue, purple, black, green; XOS = Extra Oversize, 25% Larger than 1010 Standard Legcuff; Includes 2 universal handcuff keys; ***MINIMUM PURCHASE Qty of 30	$ 111.53	41%	$ 65.80	EA
CTS HC9108NIC	Tri-Max™ Carbon Steel XOS Handcuff or Hobbles	XOS = Extra Oversize, 25% Larger than 1010 Standard Legcuff; Includes 2 universal handcuff keys	$ 102.37	41%	$ 60.40	EA
CTS HCENGRAVE	Special Laser Engraving for 25+ Pieces - Priced Per Item		$ 2.26	41%	$ 1.33	EA
CTS HCGC1	3 to 10 Position, One 1010 Handcuff per Station 24" Between Stations		$ 34.92	41%	$ 20.60	EA
CTS HCGC2	3 to 10 Position, 1010 Handcuff Set per Station 24" Between Stations		$ 51.19	41%	$ 30.20	EA
CTS HCSK1	Popular Baton Style Handcuff Key, Black, Imprint Available	All keys are sold individually	$ 5.65	41%	$ 3.33	EA
CTS HCSK3	Magnetic Training Key, Fits All Popular Brands, Single	All keys are sold individually	$ 5.76	41%	$ 3.40	EA
CTS HCSK5	Deluxe STAINLESS STEEL, Heavy Duty, Long Reach Key	All keys are sold individually	$ 9.27	41%	$ 5.47	EA
CTS L137-1	SINGLE-LAUNCHER FIXED STOCK w/ IRON SIGHTS (L1 37)		$ 1,451.27	41%	$ 856.25	EA
CTS L137-1-PAS-CER-B	CERAKOTED SINGLE-LAUNCHER FIXED STOCK w/ IRON SIGHTS (L1 37)	Cerakote Finish, Blue	$ 1,800.85	41%	$ 1,062.50	EA
CTS L137-1-PAS-CER-GN	CERAKOTED SINGLE-LAUNCHER FIXED STOCK w/ IRON SIGHTS (L1 37)	Cerakote Finish, Green	$ 1,800.85	41%	$ 1,062.50	EA

CONFIDENTIAL

Item ID	Description	Extended Description	Safeware List	Discount	Net Price	UOM
CTS L137-1-PAS-CER-GY	CERAKOTED SINGLE-LAUNCHER FIXED STOCK w/ IRON SIGHTS (L1 37)	Cerakote Finish, Gray	$ 1,800.85	41%	$ 1,062.50	EA
CTS L137-1-PAS-CER-O	CERAKOTED SINGLE-LAUNCHER FIXED STOCK w/ IRON SIGHTS (L1 37)	Cerakote Finish, Orange	$ 1,800.85	41%	$ 1,062.50	EA
CTS L137-1-PAS-CER-OD	CERAKOTED SINGLE-LAUNCHER FIXED STOCK w/ IRON SIGHTS (L1 37)	Cerakote Finish, Od Green	$ 1,800.85	41%	$ 1,062.50	EA
CTS L137-1-PAS-CER-T	CERAKOTED SINGLE-LAUNCHER FIXED STOCK w/ IRON SIGHTS (L1 37)	Cerakote Finish, Tan	$ 1,800.85	41%	$ 1,062.50	EA
CTS L137-1-PAS-CER-Y	CERAKOTED SINGLE-LAUNCHER FIXED STOCK w/ IRON SIGHTS (L1 37)	Cerakote Finish, Yellow	$ 1,800.85	41%	$ 1,062.50	EA
CTS L137-3	SINGLE-LAUNCHER COLLAPSING STOCK w/ IRON SIGHTS (L1 37)		$ 1,451.27	41%	$ 856.25	EA
CTS L137-3-PAS-CER-B	CERAKOTED SINGLE-LAUNCHER COLLAPSING STOCK w/ IRON SIGHTS (L1 37)	Cerakote Finish, Blue	$ 1,800.85	41%	$ 1,062.50	EA
CTS L137-3-PAS-CER-GN	CERAKOTED SINGLE-LAUNCHER COLLAPSING STOCK w/ IRON SIGHTS (L1 37)	Cerakote Finish, Green	$ 1,800.85	41%	$ 1,062.50	EA
CTS L137-3-PAS-CER-GY	CERAKOTED SINGLE-LAUNCHER COLLAPSING STOCK w/ IRON SIGHTS (L1 37)	Cerakote Finish, Gray	$ 1,800.85	41%	$ 1,062.50	EA
CTS L137-3-PAS-CER-O	CERAKOTED SINGLE-LAUNCHER COLLAPSING STOCK w/ IRON SIGHTS (L1 37)	Cerakote Finish, Orange	$ 1,800.85	41%	$ 1,062.50	EA
CTS L137-3-PAS-CER-OD	CERAKOTED SINGLE-LAUNCHER COLLAPSING STOCK w/ IRON SIGHTS (L1 37)	Cerakote Finish, Od Green	$ 1,800.85	41%	$ 1,062.50	EA
CTS L137-3-PAS-CER-T	CERAKOTED SINGLE-LAUNCHER COLLAPSING STOCK w/ IRON SIGHTS (L1 37)	Cerakote Finish, Tan	$ 1,800.85	41%	$ 1,062.50	EA
CTS L137-3-PAS-CER-Y	CERAKOTED SINGLE-LAUNCHER COLLAPSING STOCK w/ IRON SIGHTS (L1 37)	Cerakote Finish, Yellow	$ 1,800.85	41%	$ 1,062.50	EA
CTS L137P	SINGLE LAUNCHER, FLARE PISTOL		$ 1,338.98	41%	$ 790.00	EA
CTS L137P-PAS-CER-B	CERAKOTED SINGLE LAUNCHER, FLARE PISTOL	Cerakote Finish, Blue	$ 1,726.69	41%	$ 1,018.75	EA
CTS L137P-PAS-CER-GN	CERAKOTED SINGLE LAUNCHER, FLARE PISTOL	Cerakote Finish, Green	$ 1,726.69	41%	$ 1,018.75	EA
CTS L137P-PAS-CER-GY	CERAKOTED SINGLE LAUNCHER, FLARE PISTOL	Cerakote Finish, Gray	$ 1,726.69	41%	$ 1,018.75	EA
CTS L137P-PAS-CER-O	CERAKOTED SINGLE LAUNCHER, FLARE PISTOL	Cerakote Finish, Orange	$ 1,726.69	41%	$ 1,018.75	EA
CTS L137P-PAS-CER-OD	CERAKOTED SINGLE LAUNCHER, FLARE PISTOL	Cerakote Finish, Od Green	$ 1,726.69	41%	$ 1,018.75	EA
CTS L137P-PAS-CER-T	CERAKOTED SINGLE LAUNCHER, FLARE PISTOL	Cerakote Finish, Tan	$ 1,726.69	41%	$ 1,018.75	EA
CTS L137P-PAS-CER-Y	CERAKOTED SINGLE LAUNCHER, FLARE PISTOL	Cerakote Finish, Yellow	$ 1,726.69	41%	$ 1,018.75	EA
CTS L140-1	SINGLE-LAUNCHER FIXED STOCK COMBO RAIL (GL-1 40)		$ 1,692.80	41%	$ 998.75	EA
CTS L140-1-PAS-CER-B	CERAKOTED SINGLE-LAUNCHER FIXED STOCK COMBO RAIL (GL-1 40)	Cerakote Finish, Blue	$ 2,042.37	41%	$ 1,205.00	EA
CTS L140-1-PAS-CER-GN	CERAKOTED SINGLE-LAUNCHER FIXED STOCK COMBO RAIL (GL-1 40)	Cerakote Finish, Green	$ 2,042.37	41%	$ 1,205.00	EA
CTS L140-1-PAS-CER-GY	CERAKOTED SINGLE-LAUNCHER FIXED STOCK COMBO RAIL (GL-1 40)	Cerakote Finish, Gray	$ 2,042.37	41%	$ 1,205.00	EA
CTS L140-1-PAS-CER-O	CERAKOTED SINGLE-LAUNCHER FIXED STOCK COMBO RAIL (GL-1 40)	Cerakote Finish, Orange	$ 2,042.37	41%	$ 1,205.00	EA
CTS L140-1-PAS-CER-OD	CERAKOTED SINGLE-LAUNCHER FIXED STOCK COMBO RAIL (GL-1 40)	Cerakote Finish, Od Green	$ 2,042.37	41%	$ 1,205.00	EA
CTS L140-1-PAS-CER-T	CERAKOTED SINGLE-LAUNCHER FIXED STOCK COMBO RAIL (GL-1 40)	Cerakote Finish, Tan	$ 2,042.37	41%	$ 1,205.00	EA
CTS L140-1-PAS-CER-Y	CERAKOTED SINGLE-LAUNCHER FIXED STOCK COMBO RAIL (GL-1 40)	Cerakote Finish, Yellow	$ 2,042.37	41%	$ 1,205.00	EA
CTS L140-3	SINGLE-LAUNCHER COLLAPSING STOCK COMBO RAIL (GL-1 40)		$ 1,692.80	41%	$ 998.75	EA
CTS L140-3-PAS-CER-B	CERAKOTED SINGLE-LAUNCHER COLLAPSING STOCK COMBO RAIL (GL-1 40)	Cerakote Finish, Blue	$ 2,042.37	41%	$ 1,205.00	EA

CONFIDENTIAL

Item ID	Description	Extended Description	Safeware List	Discount	Net Price	UOM
CTS L140-3-PAS-CER-GN	CERAKOTED SINGLE-LAUNCHER COLLAPSING STOCK COMBO RAIL (GL-1 40)	Cerakote Finish, Green	$ 2,042.37	41%	$ 1,205.00	EA
CTS L140-3-PAS-CER-GY	CERAKOTED SINGLE-LAUNCHER COLLAPSING STOCK COMBO RAIL (GL-1 40)	Cerakote Finish, Gray	$ 2,042.37	41%	$ 1,205.00	EA
CTS L140-3-PAS-CER-O	CERAKOTED SINGLE-LAUNCHER COLLAPSING STOCK COMBO RAIL (GL-1 40)	Cerakote Finish, Orange	$ 2,042.37	41%	$ 1,205.00	EA
CTS L140-3-PAS-CER-OD	CERAKOTED SINGLE-LAUNCHER COLLAPSING STOCK COMBO RAIL (GL-1 40)	Cerakote Finish, Od Green	$ 2,042.37	41%	$ 1,205.00	EA
CTS L140-3-PAS-CER-T	CERAKOTED SINGLE-LAUNCHER COLLAPSING STOCK COMBO RAIL (GL-1 40)	Cerakote Finish, Tan	$ 2,042.37	41%	$ 1,205.00	EA
CTS L140-3-PAS-CER-Y	CERAKOTED SINGLE-LAUNCHER COLLAPSING STOCK COMBO RAIL (GL-1 40)	Cerakote Finish, Yellow	$ 2,042.37	41%	$ 1,205.00	EA
CTS L140-4	SINGLE LAUNCHER COMPACT FOLDING STOCK & GRIP QUAD RAIL (GL1-COMPACT)		$ 2,116.53	41%	$ 1,248.75	EA
CTS L140-4-PAS-CER-B	CERAKOTED SINGLE LAUNCHER COMPACT FOLDING STOCK & GRIP QUAD RAIL (GL1-COMPACT)	Cerakote Finish, Blue	$ 2,466.10	41%	$ 1,455.00	EA
CTS L140-4-PAS-CER-GN	CERAKOTED SINGLE LAUNCHER COMPACT FOLDING STOCK & GRIP QUAD RAIL (GL1-COMPACT)	Cerakote Finish, Green	$ 2,466.10	41%	$ 1,455.00	EA
CTS L140-4-PAS-CER-GY	CERAKOTED SINGLE LAUNCHER COMPACT FOLDING STOCK & GRIP QUAD RAIL (GL1-COMPACT)	Cerakote Finish, Gray	$ 2,466.10	41%	$ 1,455.00	EA
CTS L140-4-PAS-CER-O	CERAKOTED SINGLE LAUNCHER COMPACT FOLDING STOCK & GRIP QUAD RAIL (GL1-COMPACT)	Cerakote Finish, Orange	$ 2,466.10	41%	$ 1,455.00	EA
CTS L140-4-PAS-CER-OD	CERAKOTED SINGLE LAUNCHER COMPACT FOLDING STOCK & GRIP QUAD RAIL (GL1-COMPACT)	Cerakote Finish, Od Green	$ 2,466.10	41%	$ 1,455.00	EA
CTS L140-4-PAS-CER-T	CERAKOTED SINGLE LAUNCHER COMPACT FOLDING STOCK & GRIP QUAD RAIL (GL1-COMPACT)	Cerakote Finish, Tan	$ 2,466.10	41%	$ 1,455.00	EA
CTS L140-4-PAS-CER-Y	CERAKOTED SINGLE LAUNCHER COMPACT FOLDING STOCK & GRIP QUAD RAIL (GL1-COMPACT)	Cerakote Finish, Yellow	$ 2,466.10	41%	$ 1,455.00	EA
CTS L540-1	MULTI-LAUNCHER 5" CYL. FIXED STOCK w/ COMBO RAIL (GL-65 40)		$ 5,405.13	41%	$ 3,189.03	EA
CTS L540-1-PAM-CER-B	CERAKOTED MULTI-LAUNCHER 5" CYL. FIXED STOCK w/ COMBO RAIL (GL-65 40)	Cerakote Finish, BLUE	$ 6,175.85	41%	$ 3,643.75	EA
CTS L540-1-PAM-CER-GN	CERAKOTED MULTI-LAUNCHER 5" CYL. FIXED STOCK w/ COMBO RAIL (GL-65 40)	Cerakote Finish, GREEN	$ 6,175.85	41%	$ 3,643.75	EA
CTS L540-1-PAM-CER-GY	CERAKOTED MULTI-LAUNCHER 5" CYL. FIXED STOCK w/ COMBO RAIL (GL-65 40)	Cerakote Finish, GRAY	$ 6,175.85	41%	$ 3,643.75	EA
CTS L540-1-PAM-CER-O	CERAKOTED MULTI-LAUNCHER 5" CYL. FIXED STOCK w/ COMBO RAIL (GL-65 40)	Cerakote Finish, ORANGE	$ 6,175.85	41%	$ 3,643.75	EA
CTS L540-1-PAM-CER-OD	CERAKOTED MULTI-LAUNCHER 5" CYL. FIXED STOCK w/ COMBO RAIL (GL-65 40)	Cerakote Finish, OD GREEN	$ 6,175.85	41%	$ 3,643.75	EA
CTS L540-1-PAM-CER-T	CERAKOTED MULTI-LAUNCHER 5" CYL. FIXED STOCK w/ COMBO RAIL (GL-65 40)	Cerakote Finish, TAN	$ 6,175.85	41%	$ 3,643.75	EA
CTS L540-1-PAM-CER-Y	CERAKOTED MULTI-LAUNCHER 5" CYL. FIXED STOCK w/ COMBO RAIL (GL-65 40)	Cerakote Finish, YELLOW	$ 6,175.85	41%	$ 3,643.75	EA

CONFIDENTIAL

Item ID	Description	Extended Description	Safeware List	Discount	Net Price	UOM
CTS L540-3	MULTI-LAUNCHER 5" CYL. COLLAPSING STOCK w/ COMBO RAIL (GL-65 40)		$ 5,405.13	41%	$ 3,189.03	EA
CTS L540-3-PAM-CER-B	CERAKOTED MULTI-LAUNCHER 5" CYL. COLLAPSING STOCK w/ COMBO RAIL (GL-65 40)	Cerakote Finish, BLUE	$ 6,175.85	41%	$ 3,643.75	EA
CTS L540-3-PAM-CER-GN	CERAKOTED MULTI-LAUNCHER 5" CYL. COLLAPSING STOCK w/ COMBO RAIL (GL-65 40)	Cerakote Finish, GREEN	$ 6,175.85	41%	$ 3,643.75	EA
CTS L540-3-PAM-CER-GY	CERAKOTED MULTI-LAUNCHER 5" CYL. COLLAPSING STOCK w/ COMBO RAIL (GL-65 40)	Cerakote Finish, GRAY	$ 6,175.85	41%	$ 3,643.75	EA
CTS L540-3-PAM-CER-O	CERAKOTED MULTI-LAUNCHER 5" CYL. COLLAPSING STOCK w/ COMBO RAIL (GL-65 40)	Cerakote Finish, ORANGE	$ 6,175.85	41%	$ 3,643.75	EA
CTS L540-3-PAM-CER-OD	CERAKOTED MULTI-LAUNCHER 5" CYL. COLLAPSING STOCK w/ COMBO RAIL (GL-65 40)	Cerakote Finish, OD GREEN	$ 6,175.85	41%	$ 3,643.75	EA
CTS L540-3-PAM-CER-T	CERAKOTED MULTI-LAUNCHER 5" CYL. COLLAPSING STOCK w/ COMBO RAIL (GL-65 40)	Cerakote Finish, TAN	$ 6,175.85	41%	$ 3,643.75	EA
CTS L540-3-PAM-CER-Y	CERAKOTED MULTI-LAUNCHER 5" CYL. COLLAPSING STOCK w/ COMBO RAIL (GL-65 40)	Cerakote Finish, YELLOW	$ 6,175.85	41%	$ 3,643.75	EA
CTS L637-1	MULTI-LAUNCHER 6" CYL. FIXED STOCK w/ IRON SIGHTS(L6 37)		$ 4,364.41	41%	$ 2,575.00	EA
CTS L637-1-PAM-CER-B	CERAKOTED MULTI-LAUNCHER 6" CYL. FIXED STOCK w/ IRON SIGHTS(L6 37)	Cerakote Finish, BLUE	$ 5,000.00	41%	$ 2,950.00	EA
CTS L637-1-PAM-CER-GN	CERAKOTED MULTI-LAUNCHER 6" CYL. FIXED STOCK w/ IRON SIGHTS(L6 37)	Cerakote Finish, GREEN	$ 5,000.00	41%	$ 2,950.00	EA
CTS L637-1-PAM-CER-GY	CERAKOTED MULTI-LAUNCHER 6" CYL. FIXED STOCK w/ IRON SIGHTS(L6 37)	Cerakote Finish, GRAY	$ 5,000.00	41%	$ 2,950.00	EA
CTS L637-1-PAM-CER-O	CERAKOTED MULTI-LAUNCHER 6" CYL. FIXED STOCK w/ IRON SIGHTS(L6 37)	Cerakote Finish, ORANGE	$ 5,000.00	41%	$ 2,950.00	EA
CTS L637-1-PAM-CER-OD	CERAKOTED MULTI-LAUNCHER 6" CYL. FIXED STOCK w/ IRON SIGHTS(L6 37)	Cerakote Finish, OD GREEN	$ 5,000.00	41%	$ 2,950.00	EA
CTS L637-1-PAM-CER-T	CERAKOTED MULTI-LAUNCHER 6" CYL. FIXED STOCK w/ IRON SIGHTS(L6 37)	Cerakote Finish, TAN	$ 5,000.00	41%	$ 2,950.00	EA
CTS L637-1-PAM-CER-Y	CERAKOTED MULTI-LAUNCHER 6" CYL. FIXED STOCK w/ IRON SIGHTS(L6 37)	Cerakote Finish, YELLOW	$ 5,000.00	41%	$ 2,950.00	EA
CTS L637-3	MULTI-LAUNCHER 6" CYL. COLLAPSING STOCK w/ IRON SIGHTS(L6 37)		$ 4,364.41	41%	$ 2,575.00	EA
CTS L637-3-PAM-CER-B	CERAKOTED MULTI-LAUNCHER 6" CYL. COLLAPSING STOCK w/ IRON SIGHTS(L6 37)	Cerakote Finish, BLUE	$ 5,000.00	41%	$ 2,950.00	EA
CTS L637-3-PAM-CER-GN	CERAKOTED MULTI-LAUNCHER 6" CYL. COLLAPSING STOCK w/ IRON SIGHTS(L6 37)	Cerakote Finish, GREEN	$ 5,000.00	41%	$ 2,950.00	EA
CTS L637-3-PAM-CER-GY	CERAKOTED MULTI-LAUNCHER 6" CYL. COLLAPSING STOCK w/ IRON SIGHTS(L6 37)	Cerakote Finish, GRAY	$ 5,000.00	41%	$ 2,950.00	EA
CTS L637-3-PAM-CER-O	CERAKOTED MULTI-LAUNCHER 6" CYL. COLLAPSING STOCK w/ IRON SIGHTS(L6 37)	Cerakote Finish, ORANGE	$ 5,000.00	41%	$ 2,950.00	EA
CTS L637-3-PAM-CER-OD	CERAKOTED MULTI-LAUNCHER 6" CYL. COLLAPSING STOCK w/ IRON SIGHTS(L6 37)	Cerakote Finish, OD GREEN	$ 5,000.00	41%	$ 2,950.00	EA

CONFIDENTIAL

Item ID	Description	Extended Description	Safeware List	Discount	Net Price	UOM
CTS L637-3-PAM-CER-T	CERAKOTED MULTI-LAUNCHER 6" CYL. COLLAPSING STOCK w/ IRON SIGHTS(L6 37)	Cerakote Finish, TAN	$ 5,000.00	41%	$ 2,950.00	EA
CTS L637-3-PAM-CER-Y	CERAKOTED MULTI-LAUNCHER 6" CYL. COLLAPSING STOCK w/ IRON SIGHTS(L6 37)	Cerakote Finish, YELLOW	$ 5,000.00	41%	$ 2,950.00	EA
CTS L640-1	MULTI-LAUNCHER 6.2" CYL., FIXED STOCK w/ COMBO RAIL (GL-6 40)		$ 5,405.13	41%	$ 3,189.03	EA
CTS L640-1-PAM-CER-B	CERAKOTED MULTI-LAUNCHER 6.2" CYL., FIXED STOCK w/ COMBO RAIL (GL-6 40)	Cerakote Finish, BLUE	$ 6,175.85	41%	$ 3,643.75	EA
CTS L640-1-PAM-CER-GN	CERAKOTED MULTI-LAUNCHER 6.2" CYL., FIXED STOCK w/ COMBO RAIL (GL-6 40)	Cerakote Finish, GREEN	$ 6,175.85	41%	$ 3,643.75	EA
CTS L640-1-PAM-CER-GY	CERAKOTED MULTI-LAUNCHER 6.2" CYL., FIXED STOCK w/ COMBO RAIL (GL-6 40)	Cerakote Finish, GRAY	$ 6,175.85	41%	$ 3,643.75	EA
CTS L640-1-PAM-CER-O	CERAKOTED MULTI-LAUNCHER 6.2" CYL., FIXED STOCK w/ COMBO RAIL (GL-6 40)	Cerakote Finish, ORANGE	$ 6,175.85	41%	$ 3,643.75	EA
CTS L640-1-PAM-CER-OD	CERAKOTED MULTI-LAUNCHER 6.2" CYL., FIXED STOCK w/ COMBO RAIL (GL-6 40)	Cerakote Finish, OD GREEN	$ 6,175.85	41%	$ 3,643.75	EA
CTS L640-1-PAM-CER-T	CERAKOTED MULTI-LAUNCHER 6.2" CYL., FIXED STOCK w/ COMBO RAIL (GL-6 40)	Cerakote Finish, TAN	$ 6,175.85	41%	$ 3,643.75	EA
CTS L640-1-PAM-CER-Y	CERAKOTED MULTI-LAUNCHER 6.2" CYL., FIXED STOCK w/ COMBO RAIL (GL-6 40)	Cerakote Finish, YELLOW	$ 6,175.85	41%	$ 3,643.75	EA
CTS L640-3	MULTI-LAUNCHER 6.2" CYL., COLLAPSING STOCK w/ COMBO RAIL (GL-6 40)		$ 5,405.13	41%	$ 3,189.03	EA
CTS L640-3-PAM-CER-B	CERAKOTED MULTI-LAUNCHER 6.2" CYL., COLLAPSING STOCK w/ COMBO RAIL (GL-6 40)	Cerakote Finish, BLUE	$ 6,175.85	41%	$ 3,643.75	EA
CTS L640-3-PAM-CER-GN	CERAKOTED MULTI-LAUNCHER 6.2" CYL., COLLAPSING STOCK w/ COMBO RAIL (GL-6 40)	Cerakote Finish, GREEN	$ 6,175.85	41%	$ 3,643.75	EA
CTS L640-3-PAM-CER-GY	CERAKOTED MULTI-LAUNCHER 6.2" CYL., COLLAPSING STOCK w/ COMBO RAIL (GL-6 40)	Cerakote Finish, GRAY	$ 6,175.85	41%	$ 3,643.75	EA
CTS L640-3-PAM-CER-O	CERAKOTED MULTI-LAUNCHER 6.2" CYL., COLLAPSING STOCK w/ COMBO RAIL (GL-6 40)	Cerakote Finish, ORANGE	$ 6,175.85	41%	$ 3,643.75	EA
CTS L640-3-PAM-CER-OD	CERAKOTED MULTI-LAUNCHER 6.2" CYL., COLLAPSING STOCK w/ COMBO RAIL (GL-6 40)	Cerakote Finish, OD GREEN	$ 6,175.85	41%	$ 3,643.75	EA
CTS L640-3-PAM-CER-T	CERAKOTED MULTI-LAUNCHER 6.2" CYL., COLLAPSING STOCK w/ COMBO RAIL (GL-6 40)	Cerakote Finish, TAN	$ 6,175.85	41%	$ 3,643.75	EA
CTS L640-3-PAM-CER-Y	CERAKOTED MULTI-LAUNCHER 6.2" CYL., COLLAPSING STOCK w/ COMBO RAIL (GL-6 40)	Cerakote Finish, YELLOW	$ 6,175.85	41%	$ 3,643.75	EA
CTS L837-1	MULTI-LAUNCHER 8" CYL. FIXED STOCK w/ IRON SIGHTS (L8 37)		$ 4,497.88	41%	$ 2,653.75	EA
CTS L837-1-PAM-CER-B	CERAKOTED MULTI-LAUNCHER 8" CYL. FIXED STOCK w/ IRON SIGHTS (L8 37)	Cerakote Finish, BLUE	$ 5,133.47	41%	$ 3,028.75	EA
CTS L837-1-PAM-CER-GN	CERAKOTED MULTI-LAUNCHER 8" CYL. FIXED STOCK w/ IRON SIGHTS (L8 37)	Cerakote Finish, GREEN	$ 5,133.47	41%	$ 3,028.75	EA
CTS L837-1-PAM-CER-GY	CERAKOTED MULTI-LAUNCHER 8" CYL. FIXED STOCK w/ IRON SIGHTS (L8 37)	Cerakote Finish, GRAY	$ 5,133.47	41%	$ 3,028.75	EA
CTS L837-1-PAM-CER-O	CERAKOTED MULTI-LAUNCHER 8" CYL. FIXED STOCK w/ IRON SIGHTS (L8 37)	Cerakote Finish, ORANGE	$ 5,133.47	41%	$ 3,028.75	EA

CONFIDENTIAL

Item ID	Description	Extended Description	Safeware List	Discount	Net Price	UOM
CTS L837-1-PAM-CER-OD	CERAKOTED MULTI-LAUNCHER 8" CYL. FIXED STOCK w/ IRON SIGHTS (L8 37)	Cerakote Finish, OD GREEN	$ 5,133.47	41%	$ 3,028.75	EA
CTS L837-1-PAM-CER-T	CERAKOTED MULTI-LAUNCHER 8" CYL. FIXED STOCK w/ IRON SIGHTS (L8 37)	Cerakote Finish, TAN	$ 5,133.47	41%	$ 3,028.75	EA
CTS L837-1-PAM-CER-Y	CERAKOTED MULTI-LAUNCHER 8" CYL. FIXED STOCK w/ IRON SIGHTS (L8 37)	Cerakote Finish, YELLOW	$ 5,133.47	41%	$ 3,028.75	EA
CTS L837-3	MULTI-LAUNCHER 8" CYL. COLLAPSING w/ IRON SIGHTS (L8 37)		$ 4,497.88	41%	$ 2,653.75	EA
CTS L837-3-PAM-CER-B	CERAKOTED MULTI-LAUNCHER 8" CYL. COLLAPSING w/ IRON SIGHTS (L8 37)	Cerakote Finish, BLUE	$ 5,133.47	41%	$ 3,028.75	EA
CTS L837-3-PAM-CER-GN	CERAKOTED MULTI-LAUNCHER 8" CYL. COLLAPSING w/ IRON SIGHTS (L8 37)	Cerakote Finish, GREEN	$ 5,133.47	41%	$ 3,028.75	EA
CTS L837-3-PAM-CER-GY	CERAKOTED MULTI-LAUNCHER 8" CYL. COLLAPSING w/ IRON SIGHTS (L8 37)	Cerakote Finish, GRAY	$ 5,133.47	41%	$ 3,028.75	EA
CTS L837-3-PAM-CER-O	CERAKOTED MULTI-LAUNCHER 8" CYL. COLLAPSING w/ IRON SIGHTS (L8 37)	Cerakote Finish, ORANGE	$ 5,133.47	41%	$ 3,028.75	EA
CTS L837-3-PAM-CER-OD	CERAKOTED MULTI-LAUNCHER 8" CYL. COLLAPSING w/ IRON SIGHTS (L8 37)	Cerakote Finish, OD GREEN	$ 5,133.47	41%	$ 3,028.75	EA
CTS L837-3-PAM-CER-T	CERAKOTED MULTI-LAUNCHER 8" CYL. COLLAPSING w/ IRON SIGHTS (L8 37)	Cerakote Finish, TAN	$ 5,133.47	41%	$ 3,028.75	EA
CTS L837-3-PAM-CER-Y	CERAKOTED MULTI-LAUNCHER 8" CYL. COLLAPSING w/ IRON SIGHTS (L8 37)	Cerakote Finish, YELLOW	$ 5,133.47	41%	$ 3,028.75	EA
CTS LC5	5 Series (52 Series Canister Grenades) Launching Cup		$ 497.18	41%	$ 293.34	EA
CTS LC6	6 Series (62 Series Canister Grenades) Launching Cup		$ 497.18	41%	$ 293.34	EA
CTS LC8	8 Series & Standoff Launching Cup	For 12 Gauge Shotgun	$ 497.18	41%	$ 293.34	EA
CTS LC9	9 Series (Jet-Lite & Sting-Ball) Launching Cup		$ 497.18	41%	$ 293.34	EA
CTS MG540-3	MULTI-LAUNCHER FOR MED VEL, 5" CYL COLLAPSIBLE STOCK		$ 6,141.95	41%	$ 3,623.75	EA
CTS MG540-3-PAM-CER-B	CERAKOTED MULTI-LAUNCHER FOR MED VEL, 5" CYL COLLAPSIBLE STOCK	Cerakote Finish, BLUE	$ 6,777.54	41%	$ 3,998.75	EA
CTS MG540-3-PAM-CER-GN	CERAKOTED MULTI-LAUNCHER FOR MED VEL, 5" CYL COLLAPSIBLE STOCK	Cerakote Finish, GREEN	$ 6,777.54	41%	$ 3,998.75	EA
CTS MG540-3-PAM-CER-GY	CERAKOTED MULTI-LAUNCHER FOR MED VEL, 5" CYL COLLAPSIBLE STOCK	Cerakote Finish, GRAY	$ 6,777.54	41%	$ 3,998.75	EA
CTS MG540-3-PAM-CER-O	CERAKOTED MULTI-LAUNCHER FOR MED VEL, 5" CYL COLLAPSIBLE STOCK	Cerakote Finish, ORANGE	$ 6,777.54	41%	$ 3,998.75	EA
CTS MG540-3-PAM-CER-OD	CERAKOTED MULTI-LAUNCHER FOR MED VEL, 5" CYL COLLAPSIBLE STOCK	Cerakote Finish, OD GREEN	$ 6,777.54	41%	$ 3,998.75	EA
CTS MG540-3-PAM-CER-T	CERAKOTED MULTI-LAUNCHER FOR MED VEL, 5" CYL COLLAPSIBLE STOCK	Cerakote Finish, TAN	$ 6,777.54	41%	$ 3,998.75	EA
CTS MG540-3-PAM-CER-Y	CERAKOTED MULTI-LAUNCHER FOR MED VEL, 5" CYL COLLAPSIBLE STOCK	Cerakote Finish, YELLOW	$ 6,777.54	41%	$ 3,998.75	EA
CTS P540-1	PUMP MULTI-LAUNCHER 5" CYL. FIXED STOCK w/ COMBO RAIL (PGL-65 40)		$ 5,298.73	41%	$ 3,126.25	EA
CTS P540-1-PAM-CER-B	CERAKOTED PUMP MULTI-LAUNCHER 5" CYL. FIXED STOCK w/ COMBO RAIL (PGL-65 40)	Cerakote Finish, BLUE	$ 5,934.32	41%	$ 3,501.25	EA

CONFIDENTIAL

Item ID	Description	Extended Description	Safeware List	Discount	Net Price	UOM
CTS P540-1-PAM-CER-GN	CERAKOTED PUMP MULTI-LAUNCHER 5" CYL. FIXED STOCK w/ COMBO RAIL (PGL-65 40)	Cerakote Finish, GREEN	$ 5,934.32	41%	$ 3,501.25	EA
CTS P540-1-PAM-CER-GY	CERAKOTED PUMP MULTI-LAUNCHER 5" CYL. FIXED STOCK w/ COMBO RAIL (PGL-65 40)	Cerakote Finish, GRAY	$ 5,934.32	41%	$ 3,501.25	EA
CTS P540-1-PAM-CER-O	CERAKOTED PUMP MULTI-LAUNCHER 5" CYL. FIXED STOCK w/ COMBO RAIL (PGL-65 40)	Cerakote Finish, ORANGE	$ 5,934.32	41%	$ 3,501.25	EA
CTS P540-1-PAM-CER-OD	CERAKOTED PUMP MULTI-LAUNCHER 5" CYL. FIXED STOCK w/ COMBO RAIL (PGL-65 40)	Cerakote Finish, OD GREEN	$ 5,934.32	41%	$ 3,501.25	EA
CTS P540-1-PAM-CER-T	CERAKOTED PUMP MULTI-LAUNCHER 5" CYL. FIXED STOCK w/ COMBO RAIL (PGL-65 40)	Cerakote Finish, TAN	$ 5,934.32	41%	$ 3,501.25	EA
CTS P540-1-PAM-CER-Y	CERAKOTED PUMP MULTI-LAUNCHER 5" CYL. FIXED STOCK w/ COMBO RAIL (PGL-65 40)	Cerakote Finish, YELLOW	$ 5,934.32	41%	$ 3,501.25	EA
CTS P540-3	PUMP MULTI-LAUNCHER 5" CYL. COLLAPSING STOCK w/ COMBO RAIL (PGL-65 40)		$ 5,298.73	41%	$ 3,126.25	EA
CTS P540-3-PAM-CER-B	CERAKOTED PUMP MULTI-LAUNCHER 5" CYL. COLLAPSING STOCK w/ COMBO RAIL (PGL-65 40)	Cerakote Finish, BLUE	$ 5,934.32	41%	$ 3,501.25	EA
CTS P540-3-PAM-CER-GN	CERAKOTED PUMP MULTI-LAUNCHER 5" CYL. COLLAPSING STOCK w/ COMBO RAIL (PGL-65 40)	Cerakote Finish, GREEN	$ 5,934.32	41%	$ 3,501.25	EA
CTS P540-3-PAM-CER-GY	CERAKOTED PUMP MULTI-LAUNCHER 5" CYL. COLLAPSING STOCK w/ COMBO RAIL (PGL-65 40)	Cerakote Finish, GRAY	$ 5,934.32	41%	$ 3,501.25	EA
CTS P540-3-PAM-CER-O	CERAKOTED PUMP MULTI-LAUNCHER 5" CYL. COLLAPSING STOCK w/ COMBO RAIL (PGL-65 40)	Cerakote Finish, ORANGE	$ 5,934.32	41%	$ 3,501.25	EA
CTS P540-3-PAM-CER-OD	CERAKOTED PUMP MULTI-LAUNCHER 5" CYL. COLLAPSING STOCK w/ COMBO RAIL (PGL-65 40)	Cerakote Finish, OD GREEN	$ 5,934.32	41%	$ 3,501.25	EA
CTS P540-3-PAM-CER-T	CERAKOTED PUMP MULTI-LAUNCHER 5" CYL. COLLAPSING STOCK w/ COMBO RAIL (PGL-65 40)	Cerakote Finish, TAN	$ 5,934.32	41%	$ 3,501.25	EA
CTS P540-3-PAM-CER-Y	CERAKOTED PUMP MULTI-LAUNCHER 5" CYL. COLLAPSING STOCK w/ COMBO RAIL (PGL-65 40)	Cerakote Finish, YELLOW	$ 5,934.32	41%	$ 3,501.25	EA
CTS P837-1	PUMP MULTI-LAUNCHER 8" CYL. FIXED STOCK COMBO RAIL (PL-8 37)		$ 4,627.12	41%	$ 2,730.00	EA
CTS P837-1-PAM-CER-B	CERAKOTED PUMP MULTI-LAUNCHER 8" CYL. FIXED STOCK COMBO RAIL (PL-8 37)	Cerakote Finish, BLUE	$ 5,262.71	41%	$ 3,105.00	EA
CTS P837-1-PAM-CER-GN	CERAKOTED PUMP MULTI-LAUNCHER 8" CYL. FIXED STOCK COMBO RAIL (PL-8 37)	Cerakote Finish, GREEN	$ 5,262.71	41%	$ 3,105.00	EA
CTS P837-1-PAM-CER-GY	CERAKOTED PUMP MULTI-LAUNCHER 8" CYL. FIXED STOCK COMBO RAIL (PL-8 37)	Cerakote Finish, GRAY	$ 5,262.71	41%	$ 3,105.00	EA
CTS P837-1-PAM-CER-O	CERAKOTED PUMP MULTI-LAUNCHER 8" CYL. FIXED STOCK COMBO RAIL (PL-8 37)	Cerakote Finish, ORANGE	$ 5,262.71	41%	$ 3,105.00	EA
CTS P837-1-PAM-CER-OD	CERAKOTED PUMP MULTI-LAUNCHER 8" CYL. FIXED STOCK COMBO RAIL (PL-8 37)	Cerakote Finish, OD GREEN	$ 5,262.71	41%	$ 3,105.00	EA
CTS P837-1-PAM-CER-T	CERAKOTED PUMP MULTI-LAUNCHER 8" CYL. FIXED STOCK COMBO RAIL (PL-8 37)	Cerakote Finish, TAN	$ 5,262.71	41%	$ 3,105.00	EA
CTS P837-1-PAM-CER-Y	CERAKOTED PUMP MULTI-LAUNCHER 8" CYL. FIXED STOCK COMBO RAIL (PL-8 37)	Cerakote Finish, YELLOW	$ 5,262.71	41%	$ 3,105.00	EA

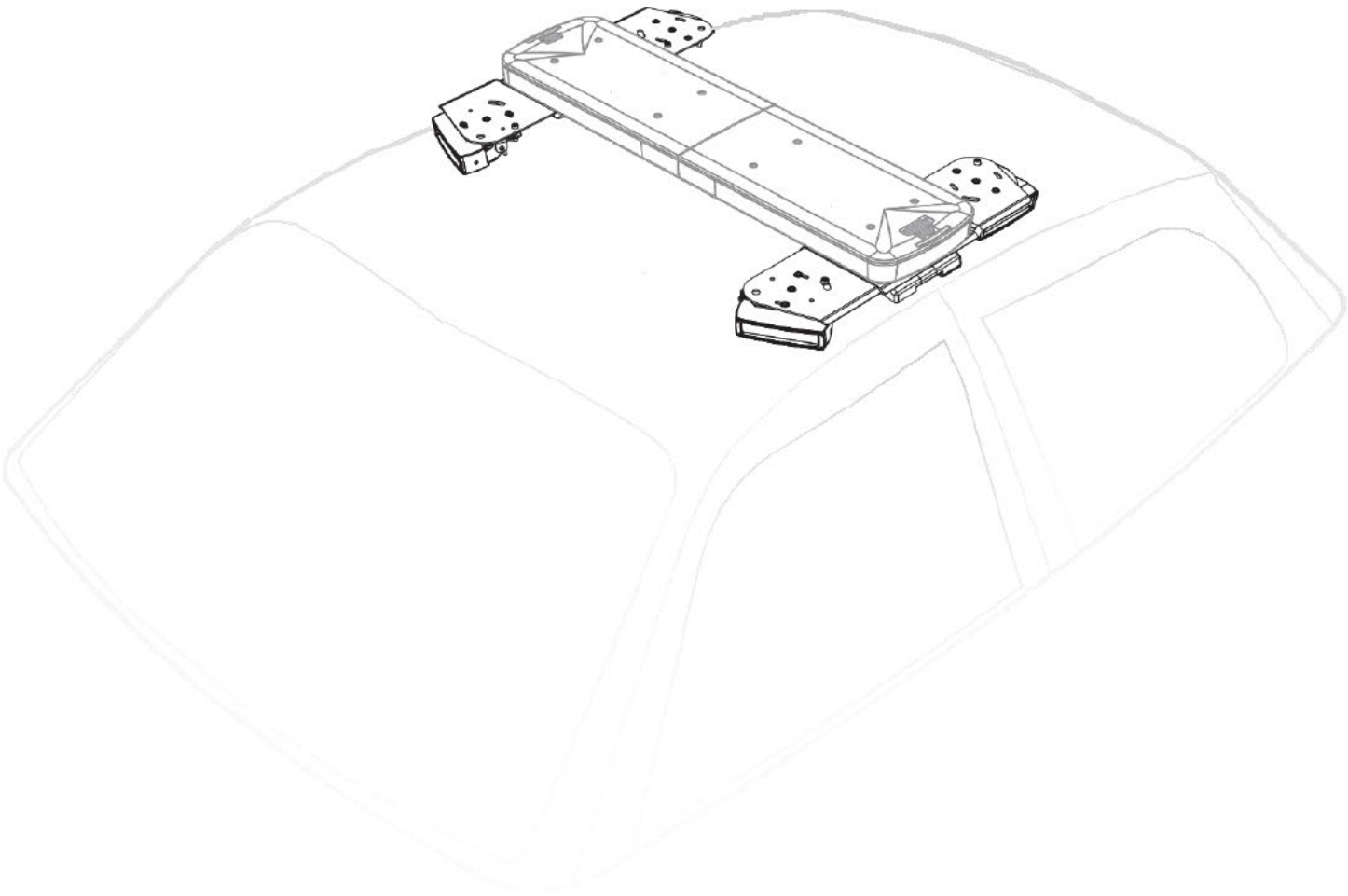
CONFIDENTIAL

Item ID	Description	Extended Description	Safeware List	Discount	Net Price	UOM
CTS P837-3	PUMP MULTI-LAUNCHER 8" CYL. COLLAPSING STOCK COMBO RAIL (PL-8 37)		$ 4,627.12	41%	$ 2,730.00	EA
CTS P837-3-PAM-CER-B	CERAKOTED PUMP MULTI-LAUNCHER 8" CYL. COLLAPSING STOCK COMBO RAIL (PL-8 37)	Cerakote Finish, BLUE	$ 5,262.71	41%	$ 3,105.00	EA
CTS P837-3-PAM-CER-GN	CERAKOTED PUMP MULTI-LAUNCHER 8" CYL. COLLAPSING STOCK COMBO RAIL (PL-8 37)	Cerakote Finish, GREEN	$ 5,262.71	41%	$ 3,105.00	EA
CTS P837-3-PAM-CER-GY	CERAKOTED PUMP MULTI-LAUNCHER 8" CYL. COLLAPSING STOCK COMBO RAIL (PL-8 37)	Cerakote Finish, GRAY	$ 5,262.71	41%	$ 3,105.00	EA
CTS P837-3-PAM-CER-O	CERAKOTED PUMP MULTI-LAUNCHER 8" CYL. COLLAPSING STOCK COMBO RAIL (PL-8 37)	Cerakote Finish, ORANGE	$ 5,262.71	41%	$ 3,105.00	EA
CTS P837-3-PAM-CER-OD	CERAKOTED PUMP MULTI-LAUNCHER 8" CYL. COLLAPSING STOCK COMBO RAIL (PL-8 37)	Cerakote Finish, OD GREEN	$ 5,262.71	41%	$ 3,105.00	EA
CTS P837-3-PAM-CER-T	CERAKOTED PUMP MULTI-LAUNCHER 8" CYL. COLLAPSING STOCK COMBO RAIL (PL-8 37)	Cerakote Finish, TAN	$ 5,262.71	41%	$ 3,105.00	EA
CTS P837-3-PAM-CER-Y	CERAKOTED PUMP MULTI-LAUNCHER 8" CYL. COLLAPSING STOCK COMBO RAIL (PL-8 37)	Cerakote Finish, YELLOW	$ 5,262.71	41%	$ 3,105.00	EA
CTS PAA200-600	ARMSON SIGHT W/TRITIUM DOT		$ 593.22	41%	$ 350.00	EA
CTS PAA-200-601	ARMSON SIGHT W/O TRITIUM GOT		$ 508.47	41%	$ 300.00	EA
CTS PG640-LR	PUMP MULTI-LAUNCHER FOR MED VEL , 6.2" CYL COLLAPSING STOCK		$ 6,565.68	41%	$ 3,873.75	EA
CTS PG640-LR-PAM-CER-B	CERAKOTED PUMP MULTI-LAUNCHER FOR MED VEL , 6.2" CYL COLLAPSING STOCK	Cerakote Finish, BLUE	$ 7,201.27	41%	$ 4,248.75	EA
CTS PG640-LR-PAM-CER-GN	CERAKOTED PUMP MULTI-LAUNCHER FOR MED VEL , 6.2" CYL COLLAPSING STOCK	Cerakote Finish, GREEN	$ 7,201.27	41%	$ 4,248.75	EA
CTS PG640-LR-PAM-CER-GY	CERAKOTED PUMP MULTI-LAUNCHER FOR MED VEL , 6.2" CYL COLLAPSING STOCK	Cerakote Finish, GRAY	$ 7,201.27	41%	$ 4,248.75	EA
CTS PG640-LR-PAM-CER-O	CERAKOTED PUMP MULTI-LAUNCHER FOR MED VEL , 6.2" CYL COLLAPSING STOCK	Cerakote Finish, ORANGE	$ 7,201.27	41%	$ 4,248.75	EA
CTS PG640-LR-PAM-CER-OD	CERAKOTED PUMP MULTI-LAUNCHER FOR MED VEL , 6.2" CYL COLLAPSING STOCK	Cerakote Finish, OD GREEN	$ 7,201.27	41%	$ 4,248.75	EA
CTS PG640-LR-PAM-CER-T	CERAKOTED PUMP MULTI-LAUNCHER FOR MED VEL , 6.2" CYL COLLAPSING STOCK	Cerakote Finish, TAN	$ 7,201.27	41%	$ 4,248.75	EA
CTS PG640-LR-PAM-CER-Y	CERAKOTED PUMP MULTI-LAUNCHER FOR MED VEL , 6.2" CYL COLLAPSING STOCK	Cerakote Finish, YELLOW	$ 7,201.27	41%	$ 4,248.75	EA
CTS T100	BORE BRUSH FOR 37MM LAUNCHER		$ 55.08	41%	$ 32.50	EA
CTS T101	BORE BRUSH FOR 40MM LAUNCHER		$ 55.08	41%	$ 32.50	EA
CTS T110	COMPLETE CLEANING KIT FOR 12GA, 37MM or 40MM LAUNCHERS		$ 137.71	41%	$ 81.25	EA
CTS T200	1" NYLON SLING		$ 23.31	41%	$ 13.75	EA
CTS T210	PADDED NYLON SLING		$ 46.61	41%	$ 27.50	EA
CTS T220	VERTICAL FOLDING-FRONT GRIP		$ 33.90	41%	$ 20.00	EA
CTS T220G	TACTICAL SLING 3 POINT OD GREEN		$ 63.35	41%	$ 37.38	EA
CTS T300	FULL TOOL KIT FOR PENN ARMS TRAINED ARMORERS		$ 1,514.83	41%	$ 893.75	EA
CTS T302	BARREL MAGAZINE ALIGNMENT GAUGE FOR 40MM MULTI-LAUNCHERS		$ 641.95	41%	$ 378.75	EA

CONFIDENTIAL

Item ID	Description	Extended Description	Safeware List	Discount	Net Price	UOM
CTS T500	HARD CASE - PGL65-40 PUMP MULTI-LAUNCHER		$ 752.12	41%	$ 443.75	EA
CTS T502	SOFT CASE - NYLON CORDURA GL-1 COMPACT, L-1 & GL-1 MODELS		$ 190.68	41%	$ 112.50	EA
CTS T506	SOFT CASE - NYLON CORDURA L-6, L-8, PGL-65, GL-65 MODELS		$ 190.68	41%	$ 112.50	EA
CTS T630	COLLAPSIBLE STOCK ASSEMBLY		$ 216.10	41%	$ 127.50	EA
CTS T650	COMPACT HINGE ASSEMBLY		$ 243.64	41%	$ 143.75	EA
CTS V3037	Venom® NL/TLMS Launcher		$ 54,237.29	41%	$ 32,000.00	EA

CONFIDENTIAL



PIPS MOBILE ALPR SOLUTION

Installation Guide

Revised: Nov 2019

SAFETY INFORMATION ____ *4*
Intended System Use ____ 4
RISK REDUCTION ____ *4*
Safety Prerequisites ____ 4
Component Installation ____ 4
Vehicle/Component Safety ____ 5
Maintenance ____ 5
General Safety Precautions ____ 5
PRODUCT OVERVIEW ____ *6*
Applications ____ 6
System Configurations ____ 6
ALPR System Vehicle Power Draw ____ 6
Inventory Lists ____ 7
PHYSICAL INSTALLATION ____ *8*
Unpacking the ALPR System ____ 8
Damaged or Missing Item ____ 8
Planning the ALPR System Installation ____ 8
Assess Existing On-Board Systems ____ 9
Assess Power Source ____ 9
Unpacking the Mobile Cameras ____ 10
Record Each Serial and Model Number ____ 10
Identify Each Camera ____ 10
General Camera Layout ____ 10
Preparing the Zero-Clearance Bracket ____ 11
Changing the Orientation of the Zero-Clearance Bracket ____ 12
Attaching the Zero-Clearance Bracket to the Camera ____ 13
Mobile ALPR Mounting Solutions ____ 14
Mounting the Camera Assembly to the Vehicle ____ 15
Attaching a Camera to Non-Lightbar Mounts ____ 16
Mounting the Mobile Processor ____ 17
WIRING AND CONNECTIONS ____ *18*
The Power Wiring ____ 18
The GPS Antenna ____ 19
The Mobile Camera Cables ____ 19
Connecting Camera Cables to the Processor ____ 19
Connecting the GPS Antenna to the Processor ____ 20

Connecting the Networking Elements to the Processor ____ **20**
Connecting the Power Cable to the Processor ____ **21**
Confirming the Power Status ____ **21**
ALIGNMENT ____ ***22***
ALIGNMENT PROCEDURE ____ ***22***
Alignment Requirements ____ **22**
Tools Required ____ **22**
Distance Marker Diagram ____ **22**
Aligning the Front Left Camera ____ **23**
Aligning the Front Right Camera ____ **23**
Aligning the Right Rear Parking Camera ____ **24**
Aligning the Left Rear Camera ____ **24**
CALIBRATING EXPOSURE TABLES ____ ***25***
Exposure Table Best Practices ____ **25**
Setting the Exposure Table/Plate Illumination ____ **25**
MAINTENANCE AND SERVICE ____ ***26***
Qualifications ____ **26**
Servicing Mobile ALPR Cameras ____ **26**
Cleaning Mobile ALPR Cameras ____ **26**
Servicing the Mobile ALPR Processor ____ **26**
Servicing the 10.4 inch Touchscreen Monitor ____ **26**
Cleaning the Vehicle ____ **26**
APPENDIX A – ALPR COMPONENTS ____ ***27***
APPENDIX B – WIRING DIAGRAM ____ ***28***
APPENDIX C – WIRING DIAGRAM ____ ***29***

SAFETY INFORMATION

Please read, understand, and follow all safety information contained in this guide prior to any attempts to Install or use the Mobile ALPR System. Retain these instructions for future reference.

Intended System Use

The Mobile ALPR System is intended to provide Automatic License Plate Recognition (ALPR) to users by automatically “reading” number plate or license plate characters. It is expected that all users be fully trained in the safe operation of this Mobile ALPR System. Use in any other application is not condoned, may immediately void all warranties, and may lead to an unsafe condition.

RISK REDUCTION

This section lists the recommended best practices to take prior to the installation, during installation, and during operation or maintenance of the Mobile Platform. Failure to adhere to these recommendations may result in hazardous voltages, fire, property damage, and equipment failure due to impact as well as potential injury to installers and users.

Safety Prerequisites

- Refer to the vehicle's service manuals when performing vehicle equipment installation and follow accepted automotive mechanical and electrical installation procedures.
- Review the manufacturer's vehicle wiring diagram prior to the Mobile ALPR System installation to ensure the installation does not affect vehicle operation or mandated safety functions or circuits.
- Installation to be performed only by authorized personnel or certified and/or trained installers.
- Service to be performed only by authorized personnel in compliance with all local, regional, and national applicable motor vehicle codes.

Component Installation

- Do not interact with ALPR system while driving or in hazardous conditions.
- Use only the Mobile ALPR Processor, brackets, and cabling provided.
- Ensure all external electrical connections are protected from the environment.
- Do not kink or pinch cables when routing through the vehicle as this could damage the cable/system.
- Do not get metal shavings inside the Processor. Use an ESD-approved cover if drilling near unit cannot be avoided. After mounting, inspect area and remove any metal shavings.
- Do not co-locate the SX Processor within 18 inches (45.7 cm) of a radio antenna or transmitter.
- Clear both sides of vehicle structure when drilling. Remove burrs from drilled holes and use grommets for wiring. Use care when installing mounting screws.
- Do not mount cameras or components in unapproved locations or mounting brackets. Doing so may immediately void warranty and/or service contract.
- After installation of a component, ensure it is securely attached to the vehicle.
- Avoid placing a magnetic mounting bracket or other magnetic component next to an electronic device.
- Verify all component mounts, power connections and wiring are properly connected prior to powering On the system after installation, maintenance, and/or service.

Vehicle/Component Safety

- After installation, test all vehicle functions, including horn operation, vehicle safety functions, and vehicle lighting systems, to ensure proper operation.
- Ensure the installation has not affected the vehicle operation or changed any vehicle safety function or circuit.
- Locate any ALPR system controls so the vehicle can be operated safely under all driving conditions.
- Do not install equipment or route wiring in the deployment path of an air bag.
- After deployment, inspect ALPR System periodically to ensure proper operation and attachment to vehicle.

Maintenance

- Replace Mobile ALPR System fuses with same size, type, and rating specified in installation guide.
- Always keep the Mobile ALPR Processor vent areas clear.
- Keep the Mobile ALPR Processer in a dry location.
- Do not use cleaning solutions such as strong detergents, solvents, or petroleum-, alcohol-, or ammonia-based products. Use only a soft cloth and a mild soap and water solution.
- The Agency is required to open the Mobile ALPR Processor case in order to remove the battery prior to disposal.

NOTE: Opening the case of the Mobile ALPR Processor will void the warranty. Opening the case may adversely affect any future operation of the processor. Never open the case of the Mobile ALPR Processor unless authorized by PIPS Support or when removing the battery for disposal. All disposal operations must be performed within local guidelines and laws. It is the responsibility of the processer owner to ensure all local and regional regulations are followed for proper disposal.

General Safety Precautions

- Follow safe workplace practices during installation and maintenance.
- The ALPR cameras are Class 1M LED products and emit LED radiation. Do not view directly with the eye or optical instruments.
- Dispose of all system components in accordance with applicable local and government regulations.
- Dispose of lithium-ion batteries and electronic components according to all applicable recycling or waste regulations.
- Ensure to keep all fingers and items clear when mounting magnetic camera brackets.

PRODUCT OVERVIEW

This section discusses the general application, configuration, and ALPR system information.

Applications

- Law Enforcement
- Parking Enforcement
- Community Service Vehicles
- Private Security Vehicles

System Configurations

The PIPS ALPR Mobile SX Processor can be configured in two distinct ways; Client/Server or Stand Alone.

Client/Server (VPRelay) Mode:
The Client/Server configuration consists of a Mobile ALPR Processor, up to four ALPR cameras with mounting brackets, and a network connection to a Mobile Data Computer (MDC)/laptop in the front of the vehicle. The ALPR processor collects images and data for license plate recognition and relays it to the MDC over a static network connection. The primary advantage of the Client/Server configuration is that it allows a user to be notified of "alerts" while operating the vehicle. This is done through mobile ALPR software called "PAGIS" running on the laptop/MDC and displaying the ALPR data inside the vehicle.

Stand-Alone Mode:
The Stand-Alone configuration consists of a Mobile ALPR Processor, up to four mounted ALPR cameras, and a touchscreen monitor. The self-contained system performs all plate recognition and runs its own copy of the PAGIS software. The primary advantage of the Stand-Alone configuration is its deployment flexibility as it does not require the agency to own and maintain MDCs/laptops. Some utilization examples are speed trailers, parked covert vehicles, or in manned patrol units (when equipped with touchscreen monitors and a hotspot/cellular data network).

ALPR System Vehicle Power Draw

When off, the ALPR system should draw around 20miliamps. The chart below shows the power draw when operational.

Component	Current Draw	Total Draw
SX Processor	3.5 A @ 12VDC	3.5 A @12VDC
Camera 1	1.0 A @ 12VDC	4.5 A @12VDC
Camera 2	1.0 A @ 12VDC	5.5 A @12VDC
Camera 3	1.0 A @ 12VDC	6.5 A @12VDC
Camera 4	1.0 A @ 12VDC	7.5 A @12VDC

NOTE: *These calculations do NOT include load from the MDC, Touchscreen monitor, or GPS antenna*

Inventory Lists

Below are the two most common system architectures.

Mobile Law Enforcement Package (Client/Server architecture):

- Mobile ALPR Camera(s) with appropriate infrared illumination
- Mobile ALPR Processor with camera, HDMI, Display Port, and USB 3.0 ports
- Mobile ALPR Processor power cable (three wire)
- Camera cables/connector(s)
- Accessory Kit including Antennas (when applicable)
- Garmin GPS Antenna (16x HVS)
- CAT 5E network cable (25ft.)
- ALPR/OCR Engine specifically for customer region inside the SX4e
- Lightbar Mounting Bracket(s) and Plate(s) for approved lightbar assemblies
- OPTIONAL – Mobile Mounting Bracket
- OPTIONAL – Garmin 16 GPS mount, trunk clip

NOTE: *Approved lightbar assemblies include Federal Signal, Whelen Liberty, Justice and Edge, Code3 Defender, Tomar, and other 13.25-inch and 16.25-inch bars. Non-approved lightbar mounting designs are available but may incur a design charge. Please check with your Sales representative.*

Mobile Law Enforcement Package (Stand-alone architecture):

- Mobile ALPR Camera(s) with appropriate infrared illumination
- Mobile ALPR Processor with camera, HDMI, Display Port, and USB 3.0 ports
- Mobile ALPR Processor Power cable (three wire)
- Camera cable/connector(s)
- Accessory Kit including Antennas (when applicable)
- Garmin GPS Antenna (16x HVS)
- 10.4 Inch Touch Screen Monitor with HDMI and two USB cables (25ft. ea)
- DC-DC power adapter for the touch screen monitor
- License Plate Capture Software (PAGIS) on the SX Processor
- ALPR/OCR Engine specifically for customer region on the SX Processor
- Lightbar Mounting Bracket(s) and Plate(s) for approved lightbar assemblies
- OPTIONAL – Mobile Mounting Bracket
- OPTIONAL – Third party mounting bracket for 10.4 inch monitor (based on vehicle)

NOTE: *Approved lightbar assemblies include Federal Signal, Whelen Liberty, Justice and Edge, Code3 Defender, Tomar, and other 13.25-inch and 16.25-inch bars. Non-approved lightbar mounting designs are available but may incur a design charge. Please check with your Sales representative.*

PHYSICAL INSTALLATION

This section discusses the aspects of the unboxing and physical installation of the ALPR system and its components.

Unpacking the ALPR System

Carefully unbox the ALPR platform, its components, as well as any other products included in the shipment. Inspect each item for any damage caused by shipping prior to installation.

Damaged or Missing Item

If an ordered product is missing, or was damaged during shipping, it cannot be used for installation. Immediately call ALPR Support at (833) 747-7577 Option 2 or email Support@PIPSTechnology.com to generate a support case (Please reference the order number).

Planning the ALPR System Installation

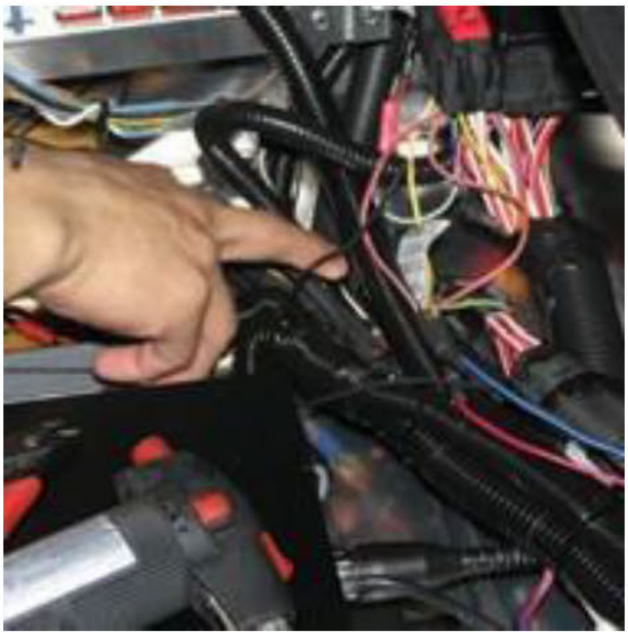
Be sure to assess the vehicle type before moving forward with any installation. Certain vehicle types may require variations of the installation process. For example, the lengths of wiring/cabling needed for an SUV are generally greater than what's needed for a sedan. Understanding these details ahead of time are highly recommended.



Shown - Ford Police Interceptor Utility and Police Interceptor Sedan. Photo courtesy of Ford Motor Company.

Assess Existing On-Board Systems

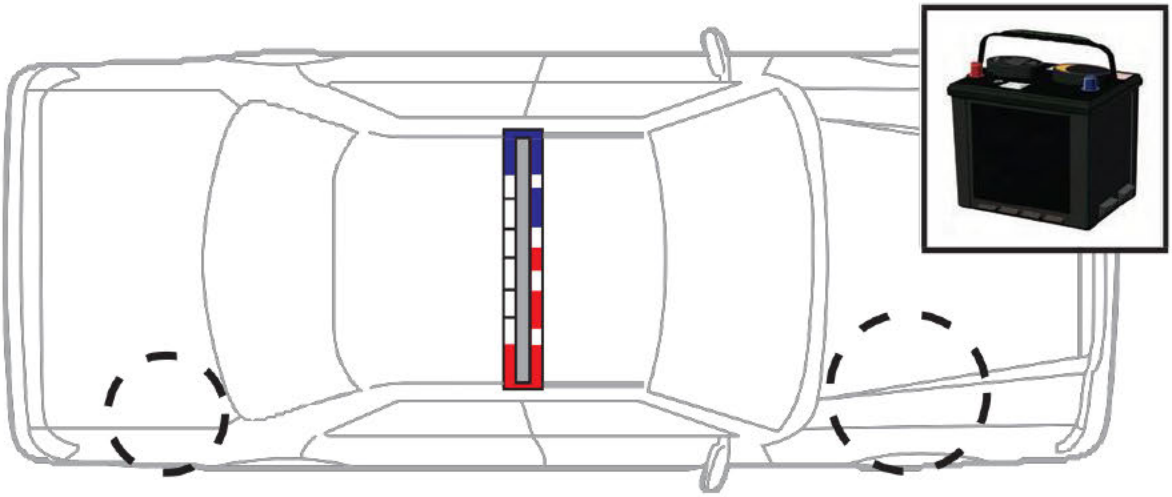
Before any installation steps, the installer should fully understand how each on-board system, radio, laptop, lightbar, etc., has been wired in the vehicle. He/she should then plan the Mobile ALPR Processor installation to take advantage of any existing power taps, wire runs, or other outfitter wiring systems. **NOTE**: To prevent malfunction or potential electrical damage, the installer should also take care to not overload any of the existing vehicle circuits.





Assess Power Source

Most police package vehicles have power distribution in the trunk or in the back of the vehicle. This is the preferred power source for the Mobile Processor. If a power tap is not found, the power must be run to the battery. Be sure to add an in-line fuse at the battery. **NOTE**: For more detail refer to Appendix B and C



Unpacking the Mobile Cameras

Each camera and mounting bracket are packaged individually. Best practice recommends the agency keep the shipping box of each bracket and camera in the unlikely event the unit needs to be returned. If it's not possible to temporarily save the shipping containers, they should be sent to an appropriate recycling center.

Record Each Serial and Model Number

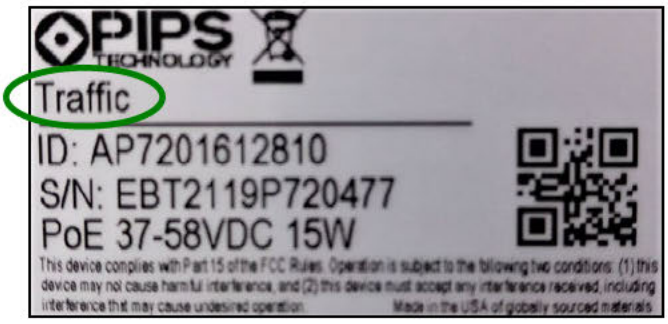
Note the serial and model numbers on the label of the product housing and record it for reference.
IMPORTANT: Please have the model and serial numbers available whenever Customer Support is contacted.

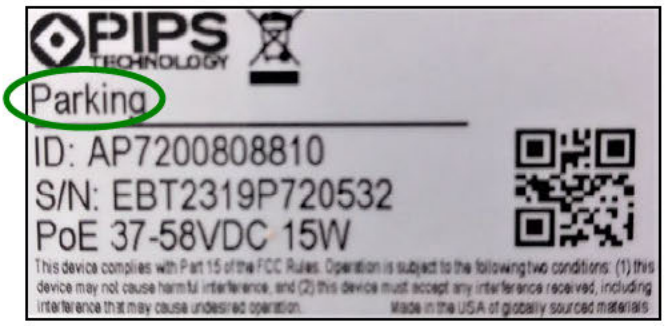
Identify Each Camera

Before mounting cameras to the vehicle, they should be checked for any damage, identified to confirm illumination uniformity, and assigned to the proper mounting locations based on lensing. The steps to identify the cameras and lensing are below:

1. Locate the Identification Label (Contains Serial and Model/ID Number)
2. The Label should say "Traffic" or "Parking"
    a. Traffic cameras are designed to view plates farther down the adjacent lanes
    b. Parking cameras are designed to view plates closer to the ALPR vehicle
3. Make note of the ID Number (This is the "Model Number")
4. Use ID/Model number information to select each camera position

How to Read the ID/Model Number: Example: AP7201612810
[Product: AP720] + [IR Lens: 16] + [OV Lens: 12] + [Illumination Wavelength: 810]





General Camera Layout

The proper mounting location is extremely important to overall function. Placing a camera in the wrong position on the vehicle will reduce the ALPR performance to almost zero. Below is the most common mounting layout:

1. The front left, and front right cameras are nearly always Traffic cameras.
2. The right rear side camera is nearly always a Parking camera and aimed perpendicular to the vehicle.
3. The left rear side camera can either be a second perpendicular parking camera or it can be a rear facing traffic camera.
    a. The advantage of the rear facing camera is its ability to capture rear plates of opposing traffic. This is especially useful in rear license plate only states.

For more detailed mounting information, refer to the alignment section.

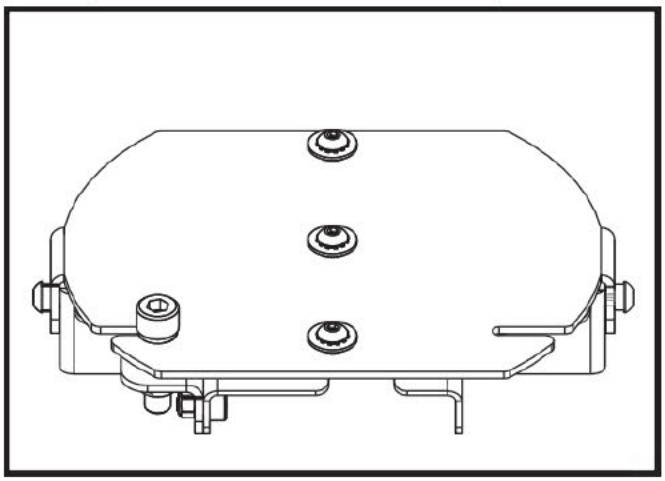
Preparing the Zero-Clearance Bracket

Once the proper camera configuration is determined for the vehicle, it's time to prepare the mounting brackets. There are two bracket configurations, a driver's side or left-handed bracket, and a passenger's side or right-handed bracket. When viewing the bracket from the rear and face up, the right-hand bracket will have the adjustment screw on the right. Since all brackets come this way, the installer will need to manually configure any required left-hand brackets.

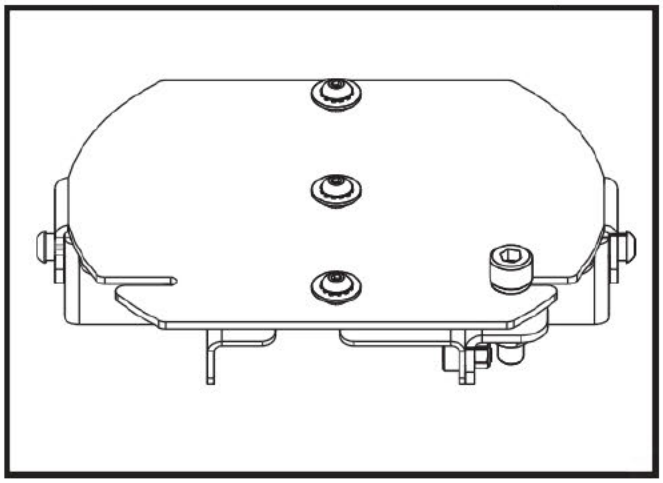
PRO-TIP: To assist with maintenance, PIPS recommends the use of an anti-seizing agent on all screws/bolts for the entire light bar and bracket system.

NOTICE: Zero-clearance brackets only ship with lightbar mounting configurations. Be sure to work with the Sales Department to procure the proper packages for each vehicle.

Left-Hand or Driver's Side Bracket



Right-Hand or Passenger's Side Bracket



Typical Camera and Bracket Configurations

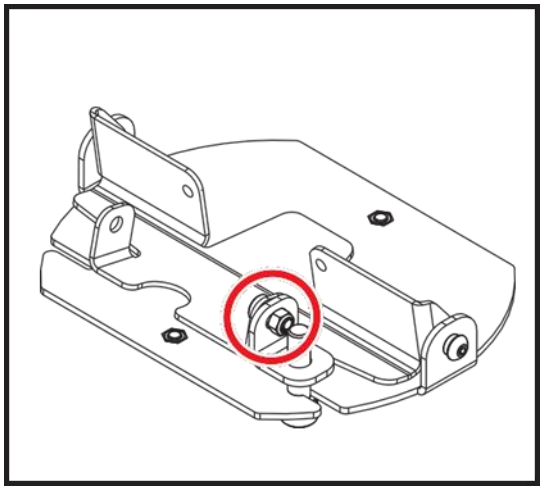
The chart below illustrates the combination of the camera position and the corresponding bracket configuration.

Camera location	Camera type	Bracket type	Camera number
Front/Left	Traffic	Left-hand	1
Front/Right	Traffic	Right-hand	2
Rear/Left	Traffic	Left-hand	3
Rear/Left	Parking	Left-hand	3
Rear/Right	Parking	Right-hand	4

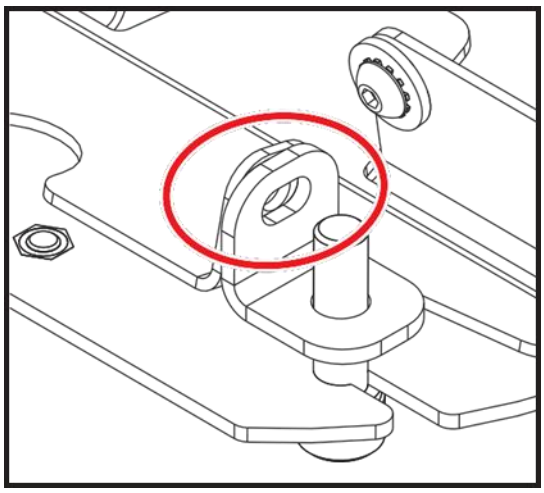
Changing the Orientation of the Zero-Clearance Bracket

In order to convert one or more of the right-hand brackets to left-hand brackets, follow the steps below:

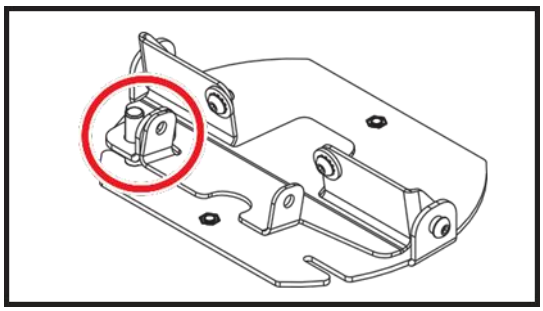
1. Locate the pivot screw on the bracket



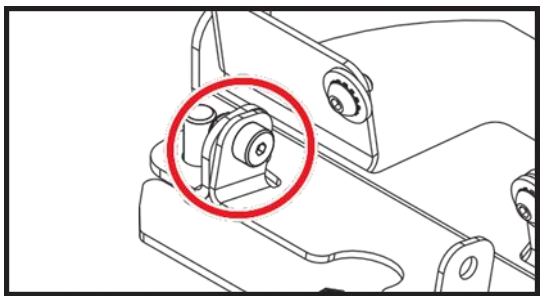
2. Remove the pivot screw from the bracket



3. Slide the pivot screw bracket from the slot and move it to the opposite side of the assembly

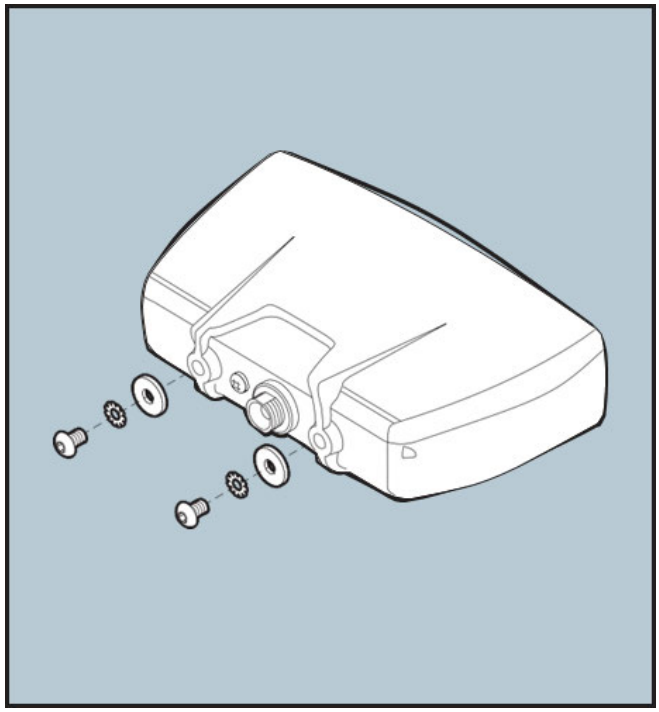


4. Reattach the pivot screw to complete the conversion



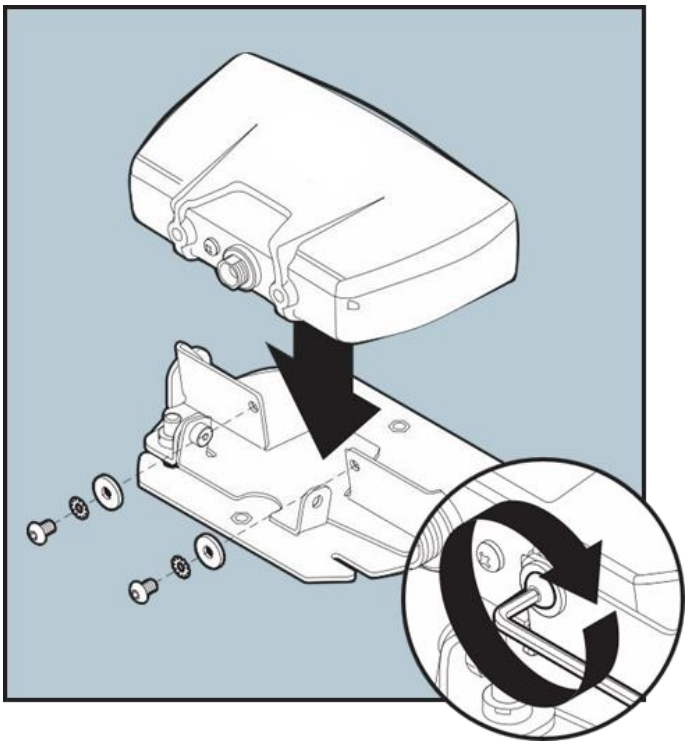
Attaching the Zero-Clearance Bracket to the Camera

Once all the brackets are assembled, the mobile cameras should be mounted to the brackets.



1. Remove the screws, star washers, and flat washers from the mounting holes at the rear of the camera.

2. With the camera and bracket upside down, install the zero-clearance bracket by sliding the bracket tongue into the camera groove. The camera groove is located on the top rear of the camera.



3. When the tongue is fully seated in the groove, place the star washers and flat washers on the screws. Tighten the screws in the mounting holes.

Mobile ALPR Mounting Solutions

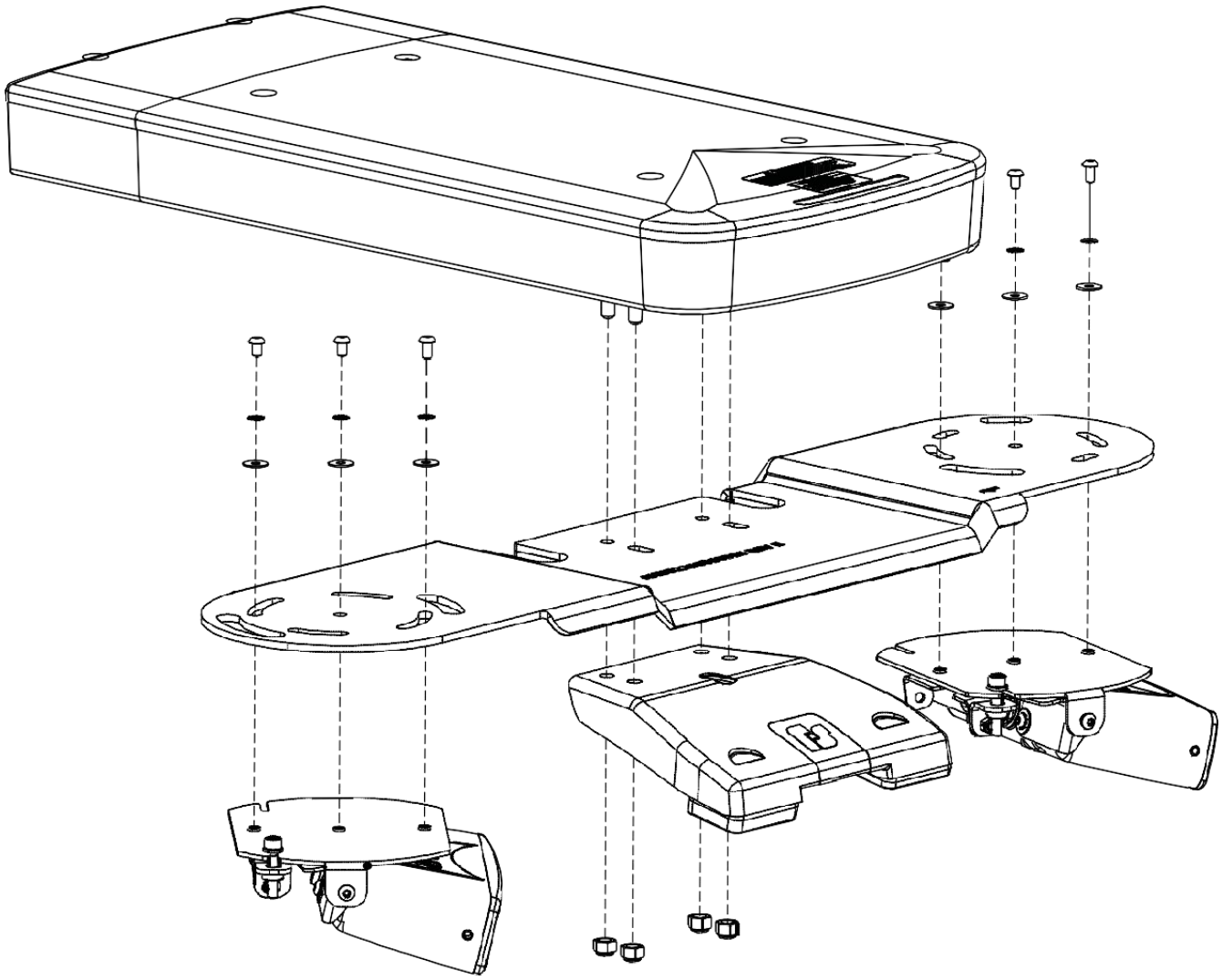
Below are examples of some of the mounting options available.

Supported Lightbar Mounting Options (Manufacturers):

- Federal Signal: Legend, Integrity, Argent, Vista, Raydian, Valor, Vision
- Code3: Defender 13.25 inch & 18 inch wide models
- Whelen: Edge, Justice, Liberty, Legacy, Freedom
- Tomar lightbars
- Unmarked Vehicle lightbar, Federal Signal product

Supported Non-Lightbar Mounting Options:

- Trunk Mount, Single or Dual Options
- Magnet Mounts (supports most vehicles with metallic/ferrous panels)
- Gutter Mounts (support Ford Police Interceptor models and Chevy Tahoe)



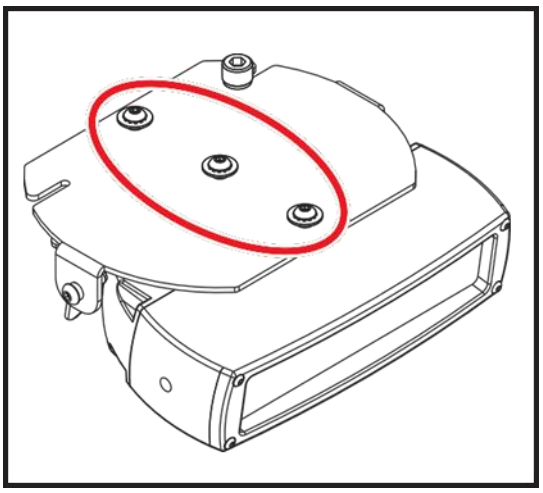
Shown - Classic Lightbar Bracket (Federal Signal "LEGEND")

Mounting the Camera Assembly to the Vehicle

The camera mounting assembly is then installed to the mounting plate attached to the lightbar.

NOTE: Due to the large number of variations between lightbars and mounting plates, this document only illustrates how to attach the camera mounting assembly to an existing mounting plate

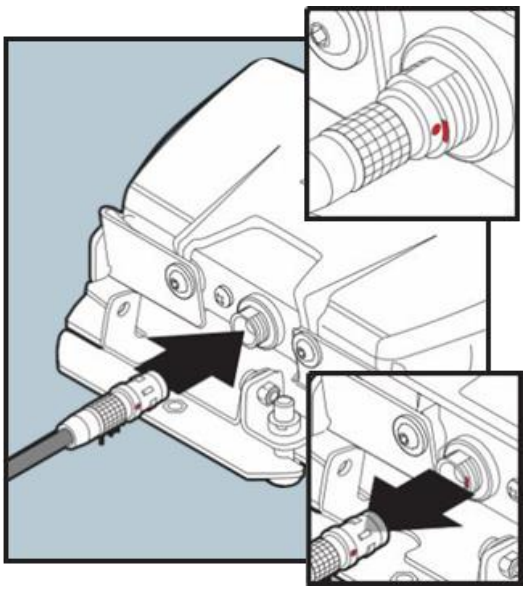
1. With the camera bracket attached to the camera, remove the three screws, star washers, and flat washers.



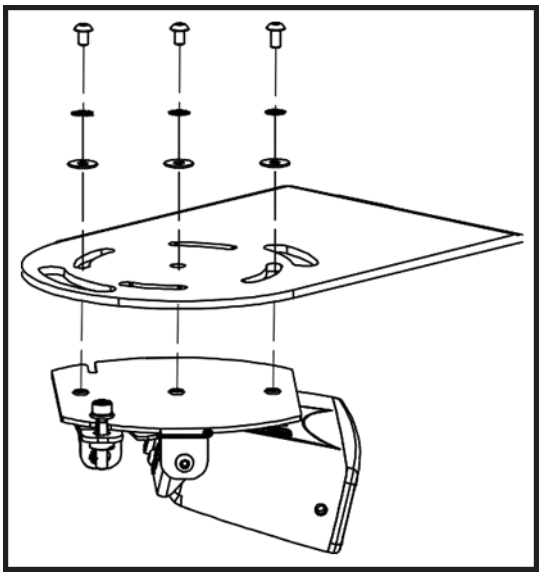
2. Connect the camera cable to the camera:
Align the red dot on connector with red mark on the port and connect using minimal force.

DO NOT FORCE OR TWIST THE CONNECTION. If the connector does not snap in easily, pull the connector out and realign.

PRO-TIP: PIPS recommends use of a bit of di-electric grease in and on the cable connectors.

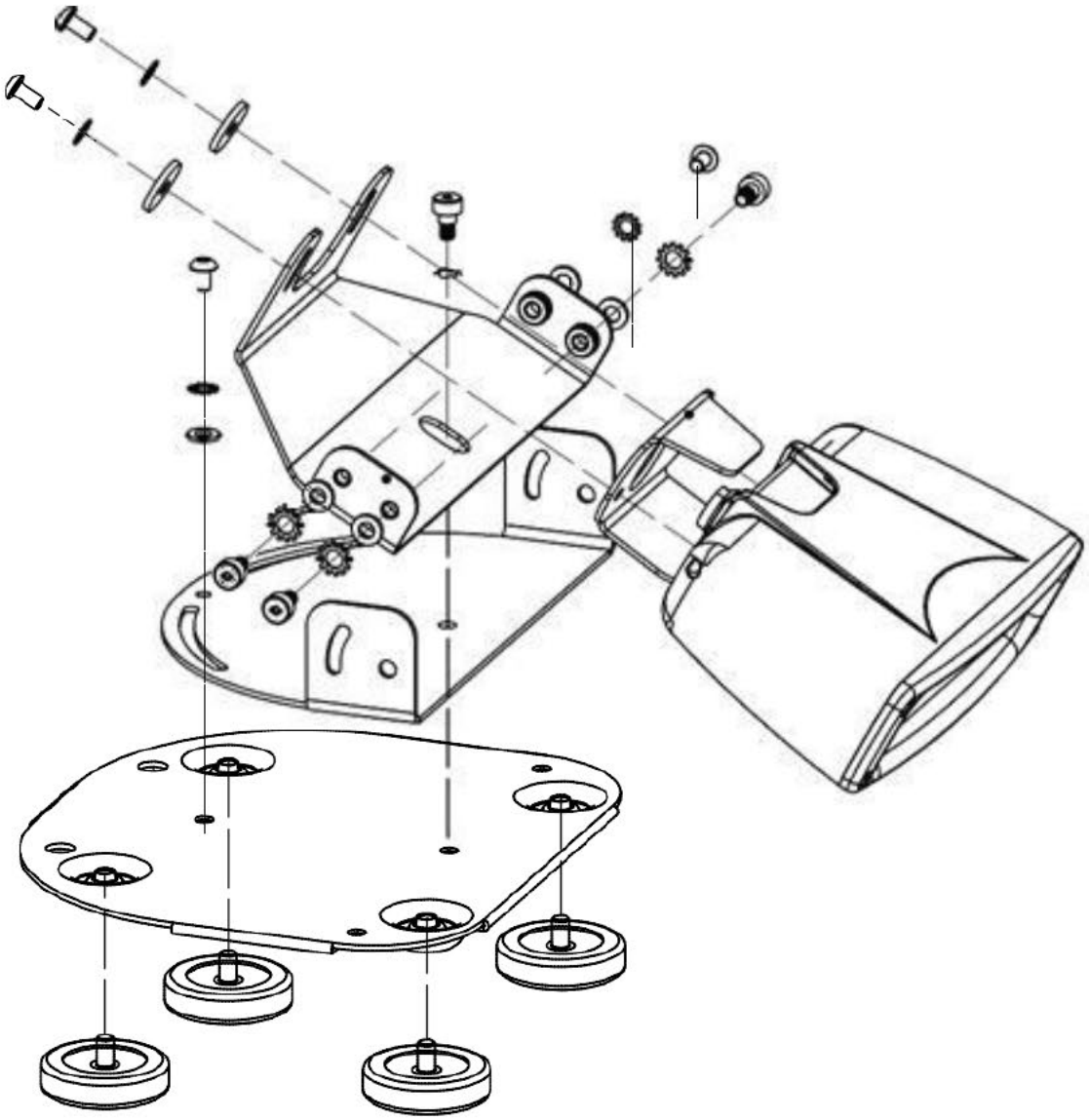


3. Attach the camera mounting assembly/plate to the lightbar bracket. **NOTE**: If the camera isn't perfectly secure, use the stabilizing foot included with the bracket to provide additional stability.



Attaching a Camera to Non-Lightbar Mounts

All Non-Lightbar mounting solutions utilize the Auxiliary 3 axis mounting plate. Once the camera is securely attached to the Aux mounting plate, attach it to the base plate of your bracket.



Shown – Magnet Mount

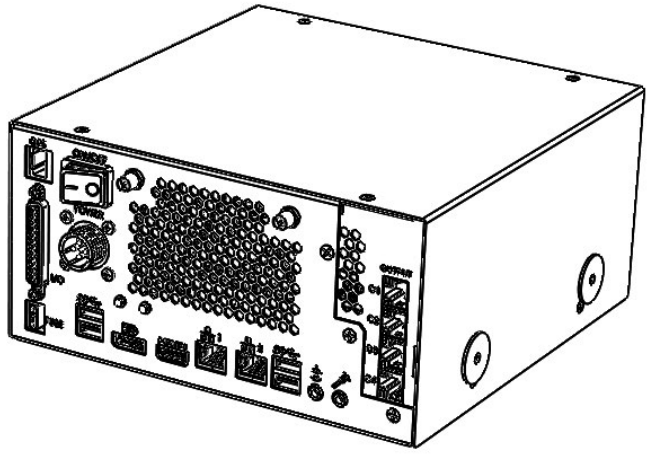
Mounting the Mobile Processor

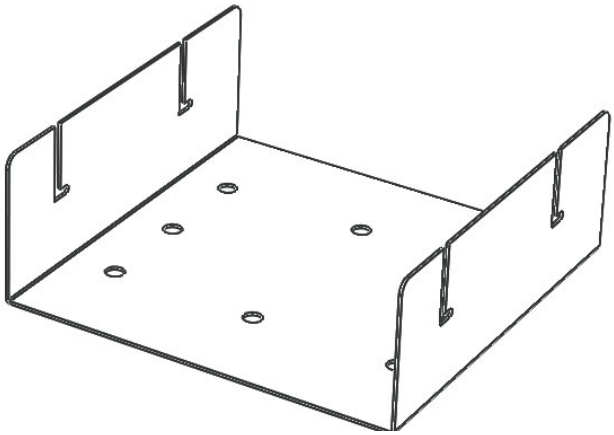
Understanding the vehicle and its current systems is a must when selecting the mounting location of the SupeRex (SX) Processor. Below are the key considerations:

- If the vehicle does not have a utility drawer/tray, be certain of all vehicle systems before drilling or mounting.
- The SX Processor and its bracket can be safely mounted in any orientation.
- Mount the unit with easy access to the rear panel and cables for maintenance/service.
- Be sure to leave adequate room for ventilation, cabling, and any maintenance needs.
- If the vehicle has a utility drawer/tray, mount the SX with enough clearance for ventilation, cabling, and service.
- Before mounting, physically place the SX in the mounting space to properly assess clearance or any dangers.
- Mount the bracket first, then secure the Mobile Processor to the bracket.

Additional Mounting Bracket Considerations:

- The Mobile Processor bracket comes with eight pre-drilled holes (0.375 in dia.). Use at least four of them to mount the bracket to the utility tray or trunk surface.
- For utility tray mounting, secure the unit using at least four 1/4-20UFC-2A bolts with appropriate washers and lock nuts. Hardware not provided.
- For direct trunk surface mounting, secure the unit using at least four #14 (or #16) sheet metal screws with appropriate washers. Hardware not provided.





WIRING AND CONNECTIONS

This section discusses the proper wiring and physical connections to the Mobile Processor. PIPS highly recommends the agency review the owner's manual of the ALPR vehicle to be certain of how to safely run cables and avoid vehicle/equipment damage. The agency is also responsible to fully understand how to safely tie into the on-board electrical systems in the vehicle.

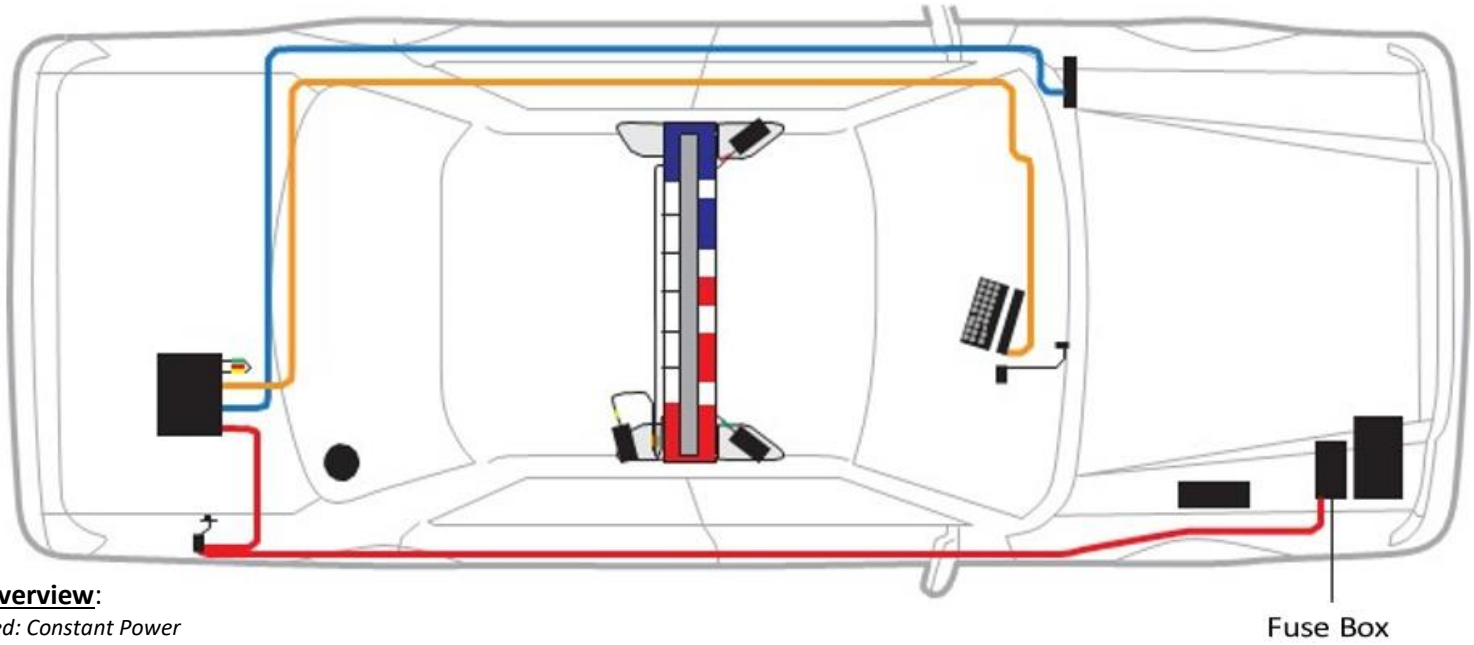
NOTE: Failure to adhere to this recommendation may immediately void all warranties and maintenance agreements.

The Power Wiring

The power cable provided with the Mobile Processor is a 3-wire connector. **NOTE**: The provided length of cable may not fit all vehicles. If wires must be extended, use 14 gauge or heavier. Min draw on 1 Cam system= 4.5AMPS, Max draw on 4 Cam system is 7.5AMPS.

1. Route the red wire (positive) from processor to a constant battery source. For example, a fused connection to the battery or to a vehicle power terminal block. Recommended fuse 20 amps.
2. Route the black wire (ground) from processor to vehicle ground tap.
3. Route the blue wire (remote) from processor to vehicle's ignition (key) source in the fuse panel or police packaging wiring harness. Recommended fuse 5 amps.





Overview:

Red: Constant Power
Blue: Remote/Ignition source
Black: Ground (barely visible off side of Processor)
Gold: Network (CAT5) to laptop or HDMI cable to front touchscreen

The GPS Antenna

The included GARMIN GPS antenna is a powerful omnidirectional receiver that can be mounted in any location with a line of sight to the sky.

1. Locate a position in, or on, the ALPR vehicle with a line of sight to the sky. Common zones are front dash, rear dash, rear window ledge, or on top of the vehicle.

2. Attach the hook side of hook-and-loop take to the underside of the GPS module.

3. Mount the antenna and route the GPS cable to the SX Processor.



GPS 16xHVS: Black PVC-jacketed, 5-meter, foil-shielded, 8-conductor 28 AWG with RJ-45 termination is waterproof up to 1m. Standby Current: < 10 microAmps

The Mobile Camera Cables

As mentioned previously, it's extremely important to review the vehicle manual when running the mobile camera cables.

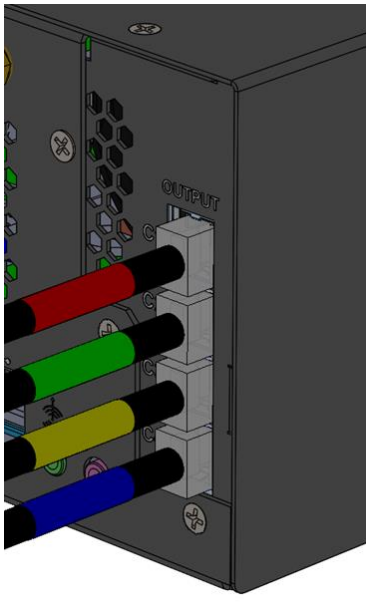
1. Locate the colored indicator rings that came with the Mobile Processor shipment.
2. Band and layout the camera cables to ensure the proper cables are going to the correct camera locations.
3. When run through the vehicle, be certain the cables do not get pinched or impede any of the vehicle airbags.

Color Coded Cable Rings:
Red: Front Left Camera
Green: Front Right Camera
Yellow: Rear Left Camera
Blue: Rear Right Camera

Connecting Camera Cables to the Processor

Connecting the P720 camera cables to the Mobile Processor is straight forward and as easy as plugging in a network cable. After the cables have been safely run through the vehicle, simply plug in the network (RJ45) connector to the appropriate camera port on the Processor (labeled C1-C4).

- Camera 1 Front Left (C1) = Red
- Camera 2 Front Right (C2) = Green
- Camera 3 Rear Left (C3) = Yellow
- Camera 4 Rear Right (C4) = Blue



Connecting the GPS Antenna to the Processor

After the antenna is placed with a line of site to the sky and its cable is securely run back to the Processor, simply plug in the RJ45 connection to the port labeled "GPS" located in the upper left corner of the rear I/O panel.

CAUTION: Plugging the GPS antenna into the wrong port may cause equipment damage and immediately void all warranties. Do **NOT** plug the GPS cable into a NIC or camera port. Do **NOT** plug a camera or network cable into the GPS port.

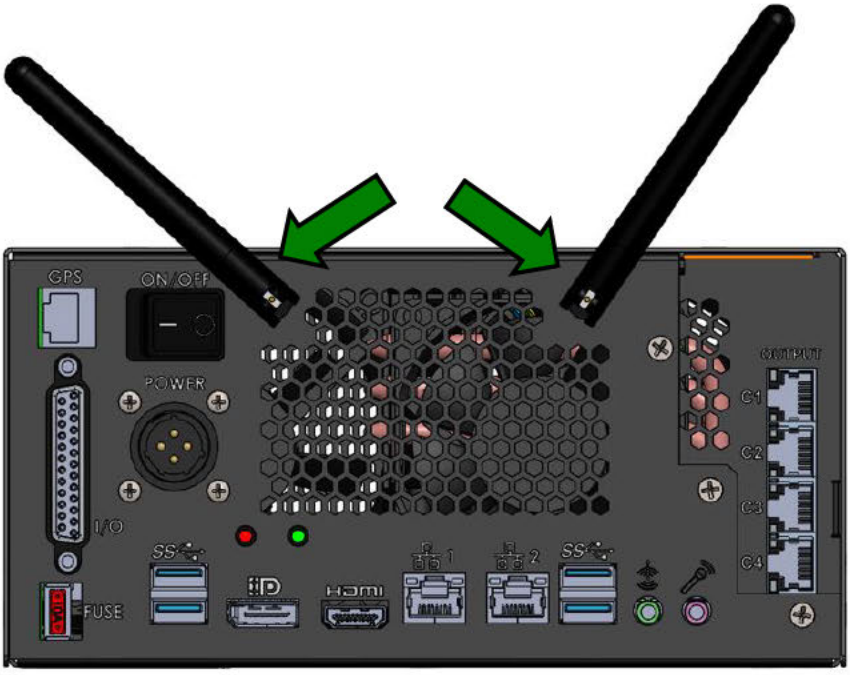


Connecting the Networking Elements to the Processor

The next step is to connect the networking option to the Processor. The most common method is a physical CAT5/6/7 cable from the Processor's NIC port 1 to an MDC/Laptop in the front of the vehicle.

NOTE: The on-board NICs are auto-switching. Meaning the agency can use either a standard network cable or a cross-over cable with no issues.

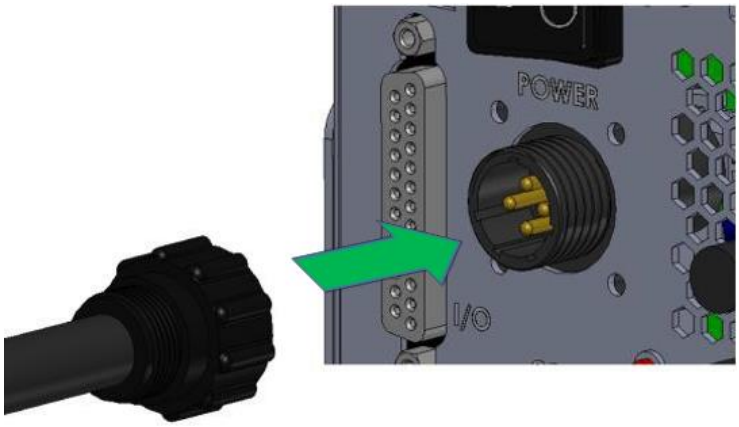
OPTION: In less than 1% of domestic orders, the Mobile Processor is built with Wi-Fi connectivity enabled. If the agency ordered this option, locate the two antennas from the accessories kit shipped with the Processor and install them to the Wi-Fi Networking Posts at the back of the Processor as shown below.

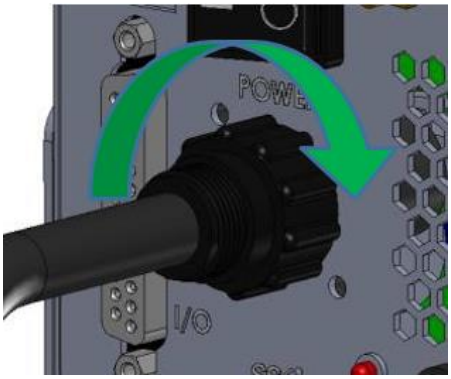


Connecting the Power Cable to the Processor

The last step in connecting all the cables to the Processor is to attach the power cable.

1. Align the notch on the power cable with the connection on the Processor
2. Insert the power cable onto the connection – DO NOT FORCE THE CABLE
3. After seating the cable properly, tighten the screw coupling/locking nut until snug – DON'T OVER TIGHTEN



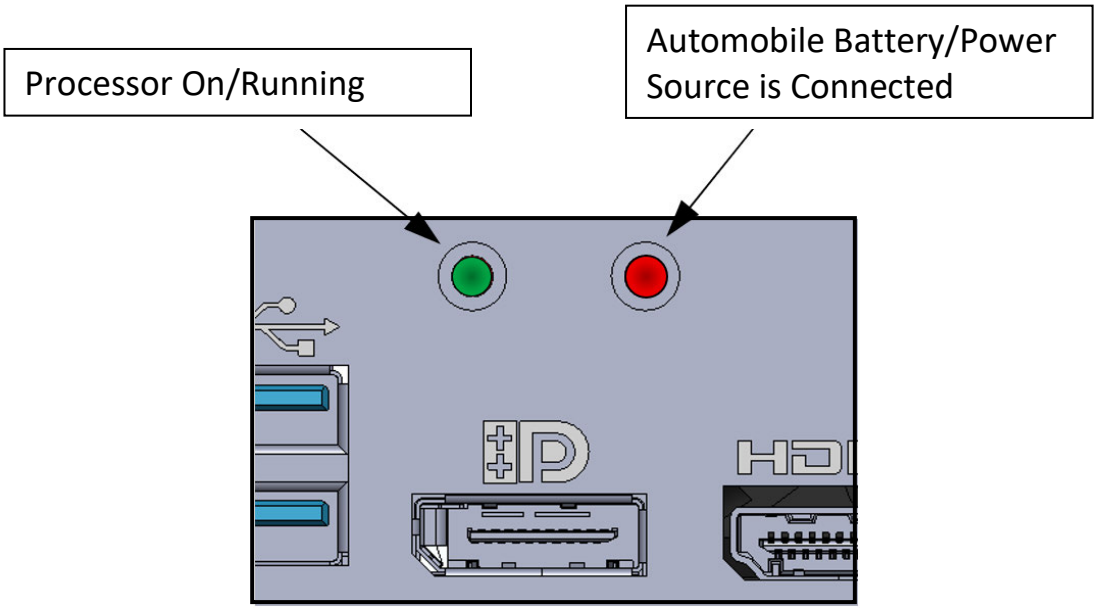


Confirming the Power Status

With all the vehicle wiring complete and the cables connected to the Processor, flip the power switch on the Processor to the On position and start the vehicle. Information on the status lights is below.

- The ignition sensitive fuse (blue wire) will register the start of the vehicle and energize the Processor
- Both the Red and Green LED status lights should illuminate
- The unit will POST and play audible tones (and the fans should spin)
- When ignition power is removed, the Processor will begin its shutdown process, indicated by the green LED flashing
- When the shutdown timer has finished, the unit will completely shut down, indicated by the green LED going out
- Conversely when the ignition is activated, the green light will come on.

NOTE: It is normal for the red LED to stay illuminated. Expected power draw while in standby is roughly 20-40 milliamps.



ALIGNMENT

The purpose of this section is to provide the best practices for the proper alignment of the PIPS Mobile ALPR Dual-Lens Cameras. The more accurate the alignment and illumination, the more effective the ALPR system will be. The values below should be considered as a baseline for general alignment and positioning of the cameras. Based on varying agency vehicles, mounting locations, and use-case scenarios, some fine tuning may be required.

ALIGNMENT PROCEDURE

The steps below assume the ALPR system has been successfully installed, the SX Processor is properly communicating with the cameras, and PAGIS (or Mobile Toolkit) is properly configured and functioning. NOTE: The greater the care taken during this process, the more accurately the ALPR system will perform in the field.

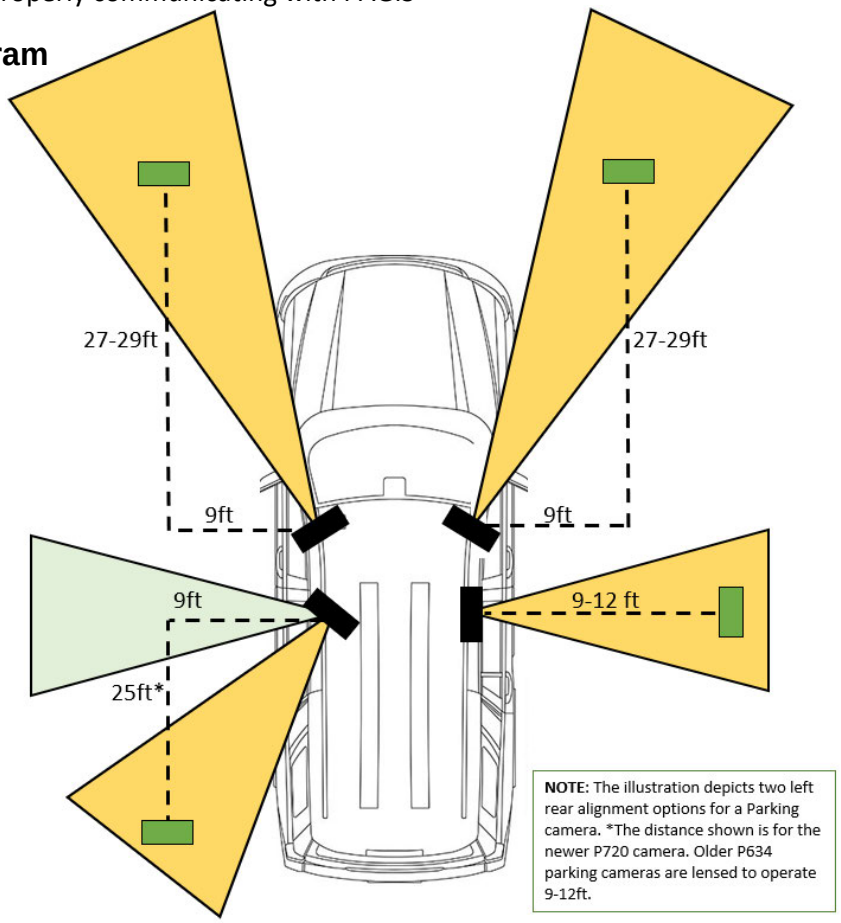
Alignment Requirements

- Large flat area without incline/decline (Ideal dimensions: 30 feet wide by 50 feet deep)
- No atmospheric conditions like fog or rain
- MEASURE ALL DISTANCES FROM THE CAMERA (NOT THE VEHICLE)
- Tripods or stands are stable and place the center of the License Plate at 32 inches above the ground

Tools Required

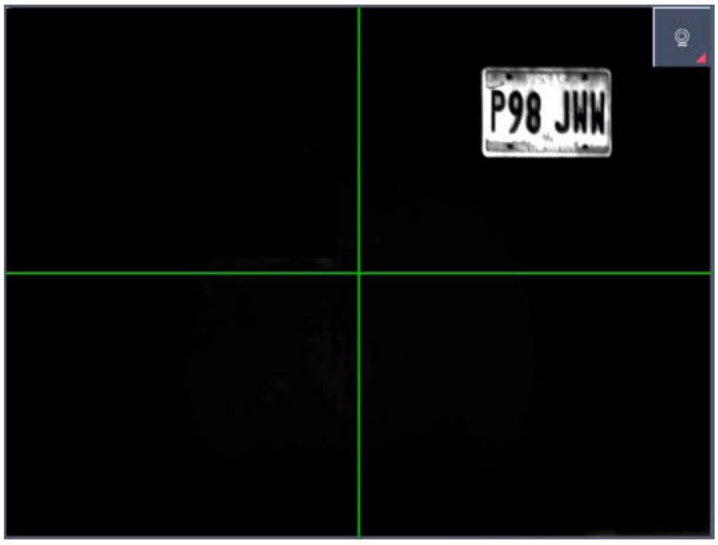
- Step Ladder
- #3, #3.5, and #4 hex/Allen wrench
- Chalk or Tape to mark the ground for template plate distances
- Tripod, tall parking cone, or box to secure test plates at 30-36” above the ground
- Tape measure or distance wheel
- Test license plate
- A configured MDC properly communicating with PAGIS

Distance Marker Diagram



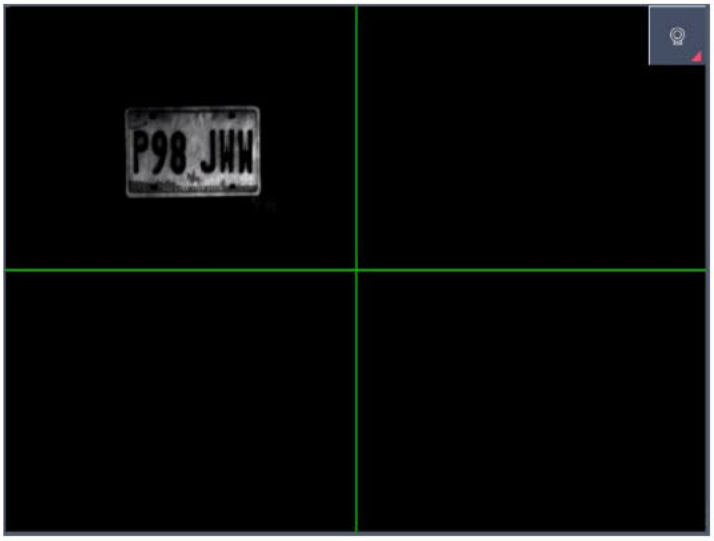
Aligning the Front Left Camera

- Place the completed plate stand on the distance marker
- Launch PAGIS from the MDC
- Login with Admin rights
- Click the Settings button from the top navigation menu (PAGIS 2.12 and above)
- Scroll down on the right-side menu and select “Cam Setup”
- Click the camera name to be aligned
- Use the camera view toggle button to confirm the proper camera is selected then switch the view to Infrared (IR)
- Loosen the mounting screws on the camera bracket just enough to allow for movement
- While monitoring the IR camera feed, position the camera so the plate is viewed as shown below
- Once set, tighten the mounting screws on the bracket to lock the camera in place



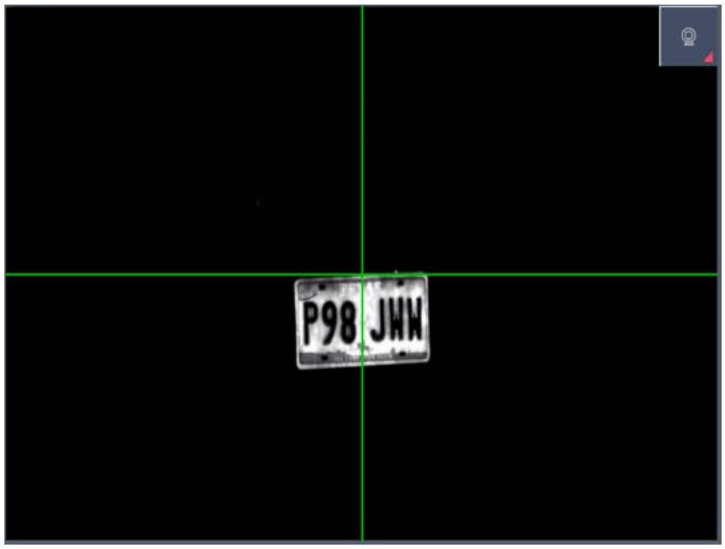
Aligning the Front Right Camera

- Use the preparatory alignment steps from above
- While monitoring the IR camera feed, position the camera so the plate is viewed as shown below
- Once set, tighten the mounting screws to lock the camera in place



Aligning the Right Rear Parking Camera

- Measure 10-12ft to the right side of the vehicle (from the parking camera)
- Place a completed plate stand at the mark
- Launch PAGIS from the MDC
- Login with Admin rights
- Click the Settings button from the top navigation menu (PAGIS 2.12 and above)
- Scroll down on the right-side menu and select "Cam Setup"
- Click the camera name to be aligned
- Use the camera view toggle button to confirm the proper camera is selected then switch the view to Infrared (IR)
- Loosen the mounting screws on the camera bracket just enough to allow for movement
- While monitoring the IR camera feed, position the camera so the plate is viewed as shown below
- Once set, tighten the mounting screws on the bracket to lock the camera in place



Aligning the Left Rear Camera

- Parking Option: Follow the steps for the Right Parking Camera
- Rear Facing Parking Camera Option: Measure 9 feet out and 25 feet down the lane
- Rear Facing (Third) Traffic Camera Option: Follow all steps for front left camera
    - Launch PAGIS from the MDC
    - Login with Admin rights
    - Click the Settings button from the top navigation menu (PAGIS 2.12 and above)
    - Scroll down on the right-side menu and select "Cam Setup"
    - Click the camera name to be aligned
    - Use the camera view toggle button to confirm the proper camera is selected then switch the view IR
    - Loosen the mounting screws on the camera bracket just enough to allow for movement
    - While monitoring the IR camera feed, position the camera so the plate is viewed as shown below
    - Once set, tighten the mounting screws on the bracket to lock the camera in place

CALIBRATING EXPOSURE TABLES

Proper plate illumination is necessary for the mobile ALPR system to function correctly. Administrators should take care not to under or over saturate the plate with Infrared (IR) light. Use the steps below to discover the plate "standard" and then select values just above, and just below that starting point to account for varied environmental conditions over time.

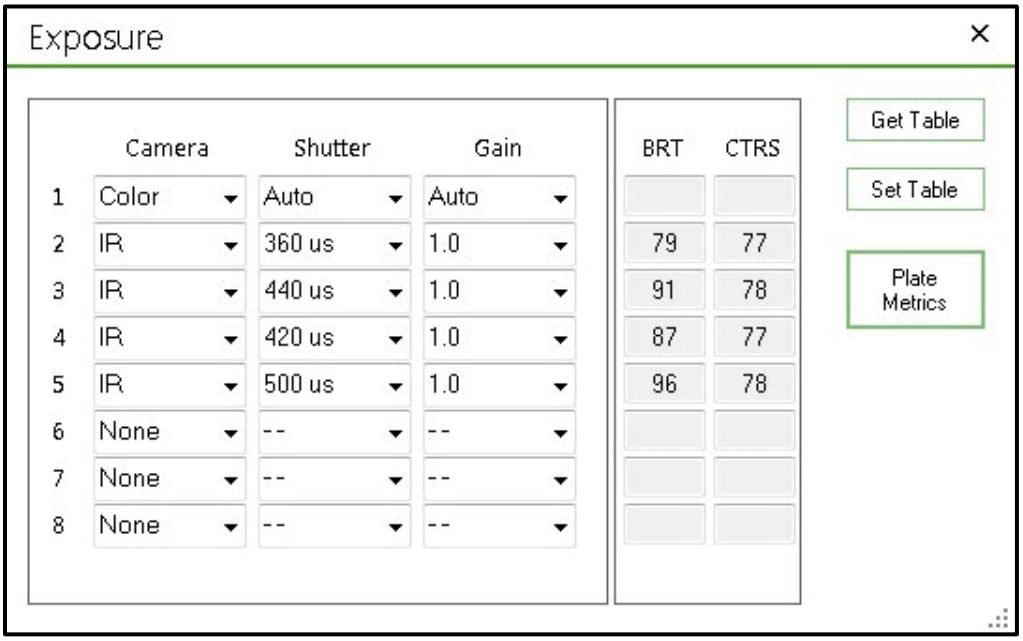
Exposure Table Best Practices

- Only calibrate 1 license plate at a time
- Only use a Gain setting of 1 or 1.5 (values above 1.5 amplify visual "noise" and could lead to misreads)
- Use 1 Color setting and 4 IR settings

Setting the Exposure Table/Plate Illumination

1. Remote Desktop to the SX4e
2. Open Tools from the Desktop
3. Launch Mobile Toolkit
4. The default view is the Infrared (IR) feed of the left front camera (Input 1)
5. Use the Input menu to navigate to the camera to be configured
6. Then from the Settings Menu, select "Exposure"
7. Be sure the plate is clearly viewable for the distance to be calibrated
8. Click the "Get Table" button to import the current exposure settings from the camera
9. Next, use the "Plate Metrics" button to analyze the current illumination
10. Adjust the exposure settings to increase or decrease illumination as necessary
    a. Increasing the Exposure will increase the Brightness (BRT) and Contrast (CTRS)
    b. Ideal BRT is above 60 **NOTE**: BRT over 90 begins to over-saturate the plate and could lead to misreads
    c. Ideal CTRS is roughly 80 (the higher the contrast the better)
11. Be sure to re-run Plate Metrics after each adjustment to the exposure table
12. Once the ideal value is discovered, fill in the other IR fields with values just above, and just below this ideal setting to account for varied atmospheric possibilities
13. Leave the Color setting to "Auto"
14. When all values are selected, click the "Set Table" button to save the changes
15. Then move on to the other cameras

NOTE: In order to read plates two lanes over, the exposure settings will need to be close to the maximum settings. This will over-expose some of the near lane plates and is the tradeoff made by agencies looking to expand ALPR coverage. An example of those settings is below.



MAINTENANCE AND SERVICE

This section discusses the general service and maintenance of the Mobile ALPR System.

Qualifications

To properly install or service the ALPR system, the technician must have a good understanding of automotive electrical systems as well as a proficiency in maintaining computer systems and networks in a mobile environment.

Servicing Mobile ALPR Cameras

Establishing a regular maintenance schedule for the Mobile ALPR cameras extends the life of the system and ensures safety. Periodically check the Mobile ALPR cameras to ensure the camera lenses are clean, all LEDs illuminate when the system is operating, and that all mounted hardware is securely fastened to the vehicle. Also, inspect the camera front cover for cracks, crazing (hairline cracks), discoloration, and other defects.

CAUTION: DO NOT open the camera housing. Each camera is nitrogen purged to remove moisture. If the camera is opened moisture will enter the camera resulting in potential damage to the electronics and accumulation on the lenses. If the camera is opened the warranty is void. For service, support, or replacement please contact Customer Support.

Cleaning Mobile ALPR Cameras

The lens of the camera should be cleaned before each use. Accumulation of insects, road grime, and other debris can obstruct the camera and reduce the plate read capability. To clean the lens, do not use an alcohol or ammonia based cleaner like Windex. Cleaners containing these compounds can damage the polycarbonate cover. PIPS Recommends use of a microfiber cloth and a mild soap and water solution.

Servicing the Mobile ALPR Processor

The housing of each Processor is sealed. If the seals are broken, the warranty of the unit will be void. Software and firmware can be updated at the direction of Customer Support.

Servicing the 10.4 inch Touchscreen Monitor

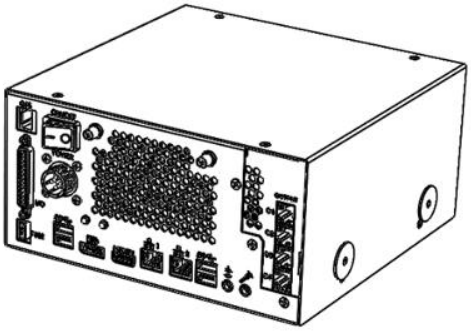
If monitor issues develop, first check the power and video connections. Make sure the cords are connected properly and are not twisted. Then clean the touchscreen. The touchscreen monitor should be cleaned before each use. Oils from fingers accumulate on the screen and can erode performance. To clean the screen DO NOT USE an alcohol or ammonia based cleaner. Cleaners containing these compounds can damage the touch screen. Use of an anti-fog, anti-static cleaner and a microfiber cloth.

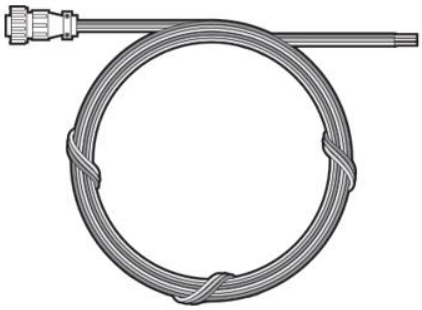
Cleaning the Vehicle

When washing the vehicle, it's best to avoid automatic car washes that use the older rotating nylon bristles. The fibers can become lodged in the camera brackets and misalign the cameras or damage the acrylic cover plate. Automatic car washes that use Soft Cloth or touchless (high pressure spray) can be used as they do not pose a risk to the cameras. For non-lightbar mounting solutions, it is not recommended to use rotating car wash systems for any brackets that use magnets to secure them to the vehicle.

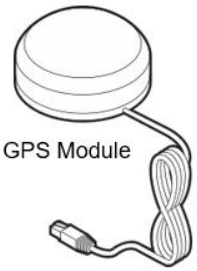
APPENDIX A – ALPR COMPONENTS

Standard Components

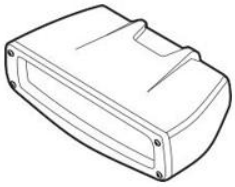




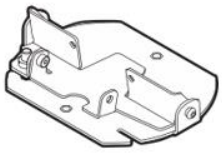
Mobile ALPR Processor
Power Cable



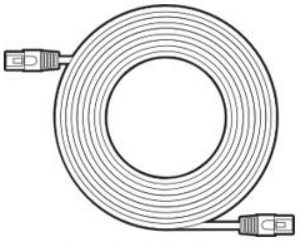
GPS Module



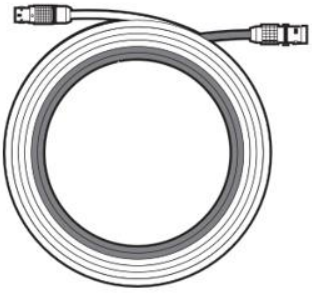
Camera
(1-4 per Processor)



Right-Hand Bracket
(1 per Camera)



Mobile ALPR Processor
Ethernet Crossover Cable



Camera Cable
(1 per Camera)

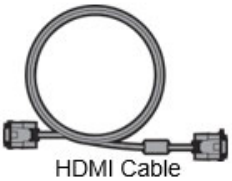
Optional with Stand-Alone Configuration



DC-DC Power Cable

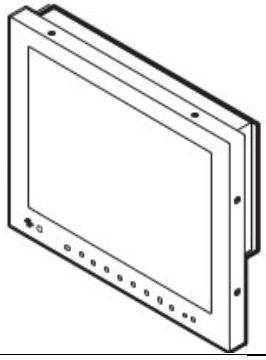


USB Cable
(2 per system)

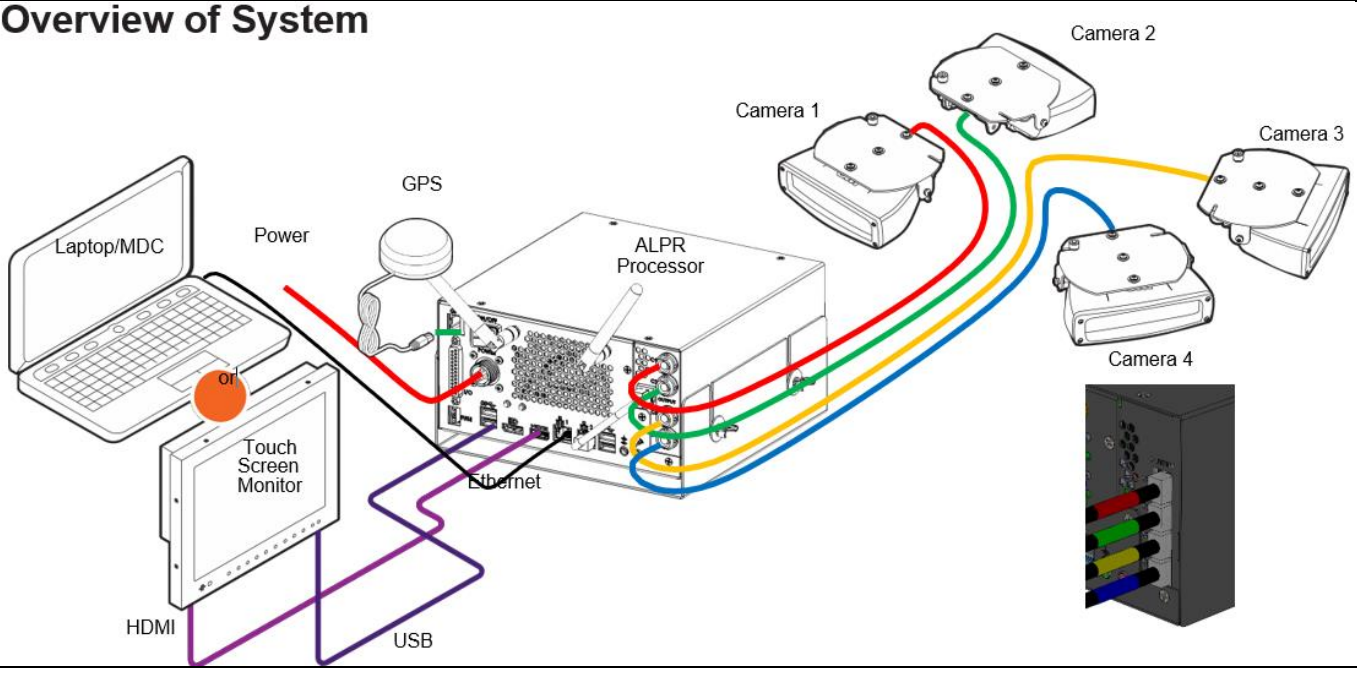


HDMI Cable

Touch Screen Monitor
(Mounting bracket provided by others)

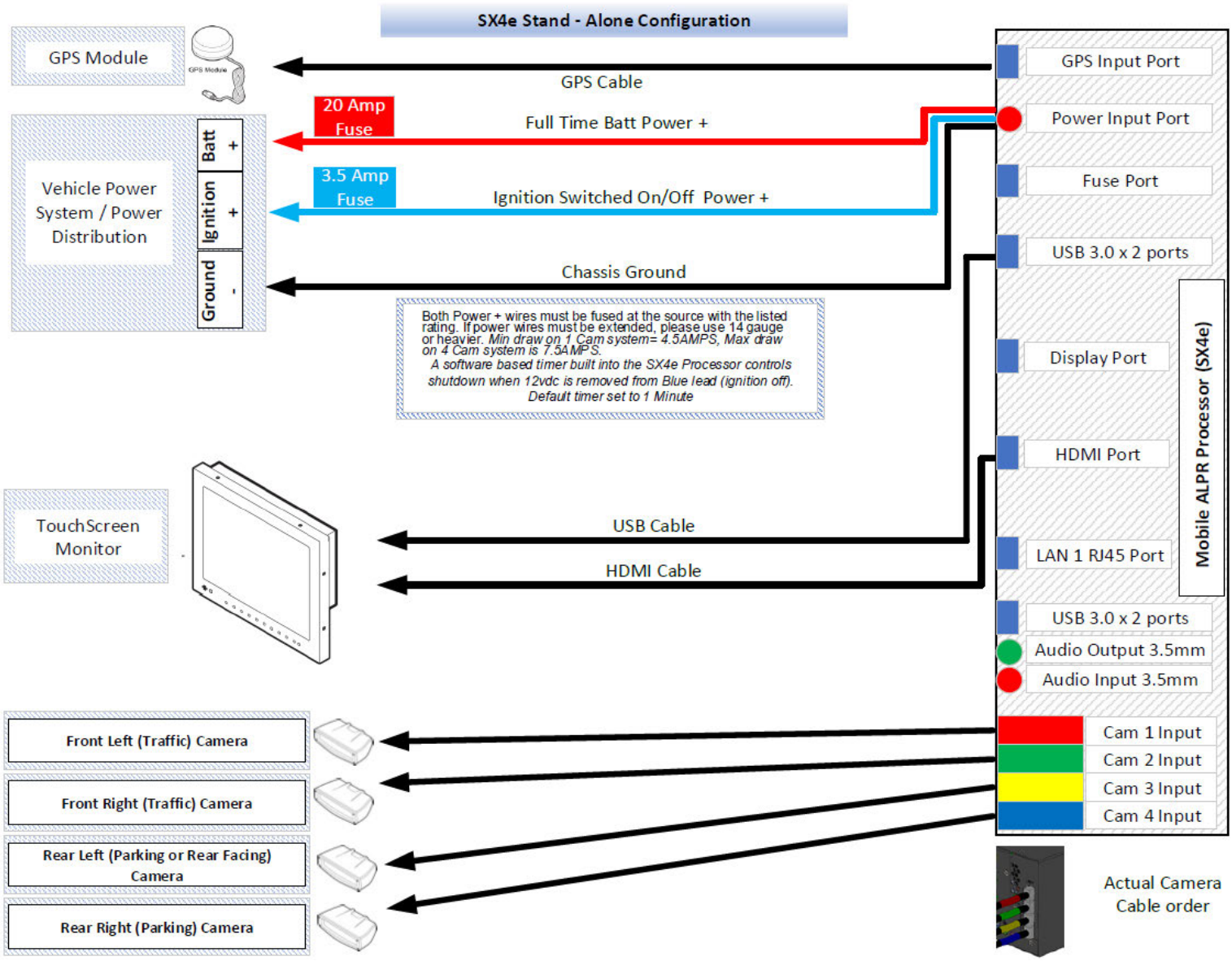


Overview of System



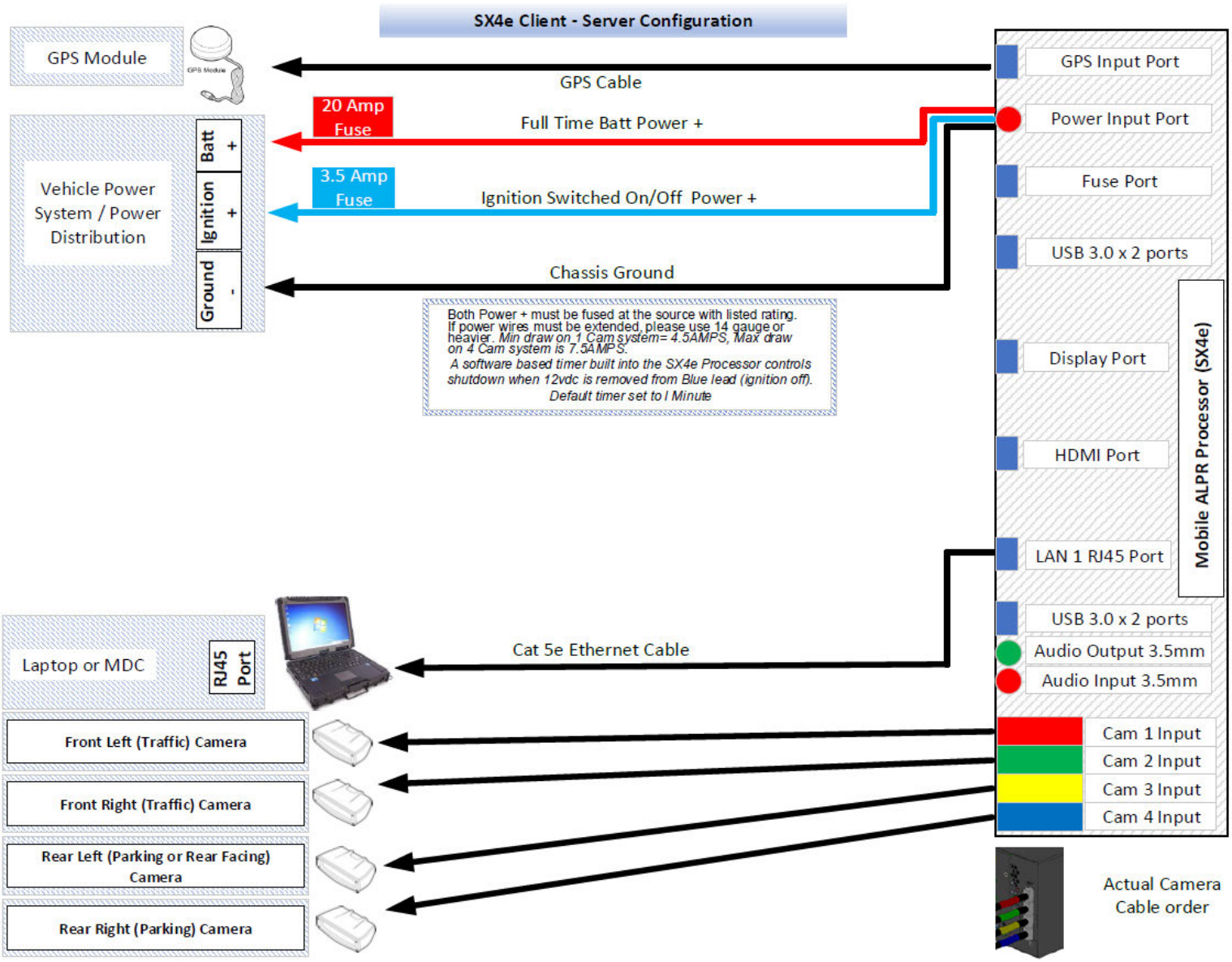
APPENDIX B – WIRING DIAGRAM

Below is the wiring diagram for a Stand-Alone Processor.



APPENDIX C – WIRING DIAGRAM

Below is the wiring diagram for client/server (VPRelay mode) used with a laptop in the front of the vehicle.



UTMC ALPR Protocol

A UTMC Technical Guide
Library reference ***TR007.001c***

Updated July 2020
Cover + 31 pages

Written by UTMC © Copyright UTMC Ltd
Developed in part with PIPS Technology

List of contents

1 Introduction **3**
1.1 About this document 3
1.2 Status of this document 3
1.3 Context 3
1.4 Web service interfaces 4

2 Camera to Instation **5**
2.1 Introduction 5
2.2 PlateRead 5
2.3 ALPR diagnostics 6
2.4 Machine diagnostics 7
2.5 Logs 8
2.6 Images 8
2.7 Camera and Configuration 9
2.8 Configuration request 11
2.9 Heartbeat message 11

3 Instation To Camera **13**
3.1 Introduction 13
3.2 Configuration 13
3.3 Log request 14
3.4 Configuration request 14
3.5 Image request 15
3.6 Acknowledgement 16

4 Tag Hashing algorithm **17**
4.1 About the algorithm 17
4.2 Example 17

Appendix 1 PlateRead Element **19**

Appendix 2 ALPRDiagnostic Element **21**

Appendix 3 MachineDiagnostic Element **23**

Appendix 4 Image Element **25**

Appendix 5 Camera Configuration Elements **26**
A5.1 Camera Element 26
A5.2 Lane Element 27
A5.3 Configuration Element 28

Appendix 6 ImageRequest Elements **31**
A6.1 TimeRangeImageRequest 31
A6.2 PriorVRNImageRequest 31
A6.3 InstanceSetImageRequest 32
A6.4 ContextImageRequest 32

1 Introduction

1.1 About this document

1.1.1 UTMC is a UK-led initiative which provides and maintains a technical framework for traffic management and related systems. It is geared to producing open specifications geared to the needs of real world projects, delivered through an efficient and innovative supply market. UTMC specifications are endorsed by the UK Department for Transport and are published on the UTMC website at: http://www.utmc.uk.com.

1.1.2 To help users get the best out of the UTMC Technical Specification, we provide a set of guidance documents addressing some of the associated issues, ranging from non technical aspects such as procurement policy and operations, to technical aspects such as database design and communications network configuration.

1.1.3 This document is a guidance document primarily for developers, and is concerned with expanding on the technical implementation of UTMC protocols within an ALPR system.

1.2 Status of this document

1.2.1 This document is based on the previous version, TR007 001b, produced by the UTMC ALPR Working Group (2009-2010).

1.2.2 UTMC gratefully acknowledges the work of the members of the Working Group in compiling this guidance and the associated elements of the Technical Specification.

1.3 Context

1.3.1 This protocol is for use by ALPR cameras when connecting to UTMC systems as used by numerous authorities across the UK, with the goal of achieving interoperability between suppliers. Although the primary aim has been to provide standardized ALPR data for journey time systems, the scope of the protocol includes the provision of additional data meeting NAAS requirements (for example images) to satisfy Police requirements in the event that Local Authorities and the Police wish to share cameras.

1.3.2 The UTMC ALPR protocol was developed within the following framework:

- This standard utilises non-proprietary elements and is based on XML. It is recognised that the communications costs associated with the use of XML may be higher at present than those for a less verbose protocol. However, it is hoped that the ease of use and the wide support of XML will lead to the ready exploitation of a forward-looking XML based open standard, particularly in the light of ongoing reductions in communication costs.

- The focus of this protocol is Camera to Instation and Instation to Camera communications. In parallel, a set of attribute extensions have been developed for the Common Database CCTV Data Object, which allow the Instation to add distilled ALPR data to the CDB. This document does not deal with Instation to Instation Journey Time Exchange.

- This protocol should be formed with some consideration of existing protocols and guidance – UTMC, Datex and possibly NTCIP.

- This protocol should be scalable. Elements such as image transfer may not be a requirement of all users. The protocol should be developed in a way to ensure that such additions are optional.

1.4 Web service interfaces

1.4.1 All web interfaces are SOAP (Simple Object Access Protocol) based and are described in WSDL (Web Services Description Language).

1.4.2 To summarise the Instation WSDL, the interface allows the camera to send XML element: <CameraToInstation> and in reply receives an XML element: <InstationToCamera>.

1.4.3 The camera WSDL allows the Instation to send XML element: <InstationToCamera>.

1.4.4 It should be noted that SOAP headers are not included in the UTMC ANPR WSDL files (camera.wsdl and instation.wsdl) or in the xml excerpts shown below. SOAP headers must therefore be generated for any SOAP-compliant implementation.

1.4.5 Both <CameraToInstation> and <InstationToCamera> elements have a mandatory version number attribute:

- SchemaVersion, indicating the version number of the element which contains it (SchemaVersion is a string containing dot-separated numbers (starting with 1.0). The first digit indicates a major revision, the second indicates updates to that revision.)

1.4.6 The xml excerpts shown below relate to V1.2 of the UTMC ALPR Protocol.

2 Camera to Instation

2.1 Introduction

2.1.1 This XML element is intended for transmitting all information from Camera to Instation. It allows for sending: plate data, ALPR and machine diagnostics, proprietary logs, images, current Camera configuration and request for configuration in any combination.

2.1.2 The option must be provided to use Gzip compression of the entire Camera to Instation element. The protocol does not provide for enabling or disabling this feature - it must be enabled or disabled by a commissioning engineer, either on-site or via a remotely connected engineering application.

2.1.3 Mandatory elements are:

- CameraID to identify the Camera
- TimeStamp which is the date and time of message creation

2.1.4 For clarity, each type of information payload is discussed separately; however messages may use any combination of elements.

2.1.5 All array elements include an optional attribute "ManufacturerSpecific" (not shown in the examples) which enables the communication of additional information outside the scope of the pre-defined attributes.

2.2 PlateRead

2.2.1 An optional array of plate read results may be included. For each entry in the array, the following are mandatory:

- InstanceID to identify the plate read event;
- TimeStamp which is the date and time of the sighting;
- LaneID representing the lane in which the plate was travelling;
- VehicleDirection representing the direction the vehicle was travelling in the lane;
- PlateNotRead, a flag to indicate a vehicle has been detected but no plate read.

2.2.2 The following is an example message containing a single plate read.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CameraToInstation xmlns=" http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <CameraID>0</CameraID>
    <TimeStamp>2009-06-29T12:01:59.377+01:00</TimeStamp>
    <PlateReadArray>
        <PlateRead>
            <InstanceID>0</InstanceID>
            <TimeStamp>2009-06-29T12:01:59.379+01:00</TimeStamp>
            <TimeStampError>5</TimeStampError>
            <LaneID>0</LaneID>
            <VehicleDirection>U</VehicleDirection>
            <XYType>OSGB</XYType>
            <XCoord>123456.7</XCoord>
            <YCoord>654321.0</YCoord>
            <PlateNotRead>false</PlateNotRead>
            <VRN>A123BCD</VRN>
            <VRNConfidence>85</VRNConfidence>
```

```
                <Tag>1234</Tag>
                <TagConfidence>90</TagConfidence>
                <Classification>1</Classification>
                <Country>GBR</Country>
                <Make>Ford</Make>
                <Model>Focus</Model>
                <Colour>Red</Colour>
                <Velocity>50</Velocity>
                <VelocityError>5</VelocityError>
            </PlateRead>
        </PlateReadArray>
</CameraToInstation>
```

2.2.3 Where the Camera has been configured to send plate reads immediately, the <PlateReadArray> element will only contain a single <PlateRead> element. Where the Camera is configured to send batches of plate reads, multiple <PlateRead> elements will be present. It is mandatory that each <PlateRead> element contains at least one of <VRN> or <Tag>.

2.2.4 See section 4 for an explanation of the hashing algorithm which is used to convert the <VRN> element to a hashed tag (the <Tag> element) for the purposes of journey time or origin-destination applications.

2.2.5 These elements are described in more detail in Appendix 1.

2.3 ALPR diagnostics

2.3.1 An optional array of ALPR diagnostics may be included (one entry per lane). For each entry in the array, the following are mandatory:

- TimeStamp which is the date and time of end of the diagnostic period;
- DiagnosticType representing whether the entry is a routine diagnostic or an alarm;

2.3.2 The following is an example message containing all defined ALPR Diagnostic objects:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CameraToInstation xmlns=" http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <CameraID>0</CameraID>
    <TimeStamp>2009-06-29T12:01:59.377+01:00</TimeStamp>
    <ANPRDiagnosticArray>
        <ANPRDiagnostic>
            <TimeStamp>2009-06-29T12:01:59.379+01:00</TimeStamp>
            <DiagnosticType>routineDiagnostic</DiagnosticType>
            <LaneID>0</LaneID>
            <MeanVRNConfidence>82</MeanVRNConfidence>
            <MeanTagConfidence>85</MeanTagConfidence>
            <MeanPlateContrast>56</MeanPlateContrast>
            <MeanCharacterHeight>15</MeanCharacterHeight>
            <MeanHorizontalAngle>8</MeanHorizontalAngle>
            <MeanVerticalAngle>2</MeanVerticalAngle>
            <MeanTrajectoryOffset>2</MeanTrajectoryOffset>
            <MeanTrajectoryAngle>11</MeanTrajectoryAngle>
            <MeanVelocity>45</MeanVelocity>
            <MeanVelocityError>4</MeanVelocityError>
```

```
                <PlateToTriggerRatio>90</PlateToTriggerRatio>
                <PlatesNoCountryRatio>3</PlatesNoCountryRatio>
                <PlatesTowardsRatio>43</PlatesTowardsRatio>
                <PlatesAwayRatio>45</PlatesAwayRatio>
                <MeanIRLevel>53</MeanIRLevel>
                <MeanExposure>350</MeanExposure>
                <MeanGain>-10</MeanGain>
            </ANPRDiagnostic>
        </ANPRDiagnosticArray>
</CameraToInstation>
```

2.3.3 These elements are described in more detail in Appendix 2.

2.4 Machine diagnostics

2.4.1 An optional array of machine diagnostics (describing hardware, software and communications performance) may be included. For each entry in the array, the following are mandatory:

- TimeStamp which is the date and time of the end of the diagnostic period;
- DiagnosticType representing whether the entry is a routine diagnostic or an alarm;
- HostName representing the host to which communications diagnostics relate

2.4.2 The following is an example message containing all proposed Machine Diagnostic objects:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CameraToInstation xmlns=" http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <CameraID>0</CameraID>
    <TimeStamp>2009-06-29T12:01:59.377+01:00</TimeStamp>
    <MachineDiagnosticArray>
        <MachineDiagnostic>
            <TimeStamp>2009-06-29T12:01:59.379+01:00</TimeStamp>
            <DiagnosticType>routineDiagnostic</DiagnosticType>
            <MeanCPUTemperature>56</MeanCPUTemperature>
            <MeanTotalCurrent>120</MeanTotalCurrent>
            <MeanIlluminatorTemp>70</MeanIlluminatorTemp>
            <MeanIlluminatorCurrent>90</MeanIlluminatorCurrent>
            <IlluminatorUsage>123</IlluminatorUsage>
            <MeanIlluminatorOutput>90</MeanIlluminatorOutput>
            <LastResetTime>2009-06-29T12:01:59.379+01:00</LastResetTime>
            <NoOfHardwareErrors>0</NoOfHardwareErrors>
            <MeanSignalStrength>-36</MeanSignalStrength>
            <HostName>192.168.1.1</HostName>
            <MeanCommsLag>23</MeanCommsLag>
            <WorstCommsLag>50</WorstCommsLag>
            <NoOfCommsResends>3</NoOfCommsResends>
            <NoOfCommsFailures>1</NoOfCommsFailures>
            <NoOfCommsReconnects>2</NoOfCommsReconnects>
            <MeanSyncDifference>40</MeanSyncDifference>
            <WorstSyncDifference>123</WorstSyncDifference>
            <LastSyncTime>2009-06-29T12:01:59.379+01:00</LastSyncTime>
            <SupplyVoltage>98</SupplyVoltage>
            <TamperAlarm>normal</TamperAlarm>
```

```
            </MachineDiagnostic>
        </MachineDiagnosticArray>
</CameraToInstation>
```

2.4.3 These elements are described in more detail in Appendix 3.

2.5 Logs

2.5.1 An optional array of log messages (representing logged events such as power up, configuration change or communication error) may be included. For each entry in the array, the following is mandatory:

- TimeStamp which is the date and time relating to the log message;

2.5.2 The following is an example message outlining the format of a Log Array:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CameraToInstation xmlns=" http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <CameraID>0</CameraID>
    <TimeStamp>2009-06-29T12:01:59.377+01:00</TimeStamp>
    <LogArray>
        <Log>
            <TimeStamp>2009-06-29T12:01:59.379+01:00</TimeStamp>
            <InstanceID>0</InstanceID>
            <LogMessage>System Restart</LogMessage>
        </Log>
    </LogArray>
</CameraToInstation>
```

2.5.3 The <LogArray> element may contain any number of <Log> elements. LogMessage elements may contain XML or plain text in proprietary format, as long as XML formatting rules are strictly followed.

2.6 Images

2.6.1 An optional array of camera images may be included. For each entry in the array, the following are mandatory:

- TimeStamp which is the date and time at which the image was captured;
- ImageType representing the type of the image e.g. plate patch, ALPR image etc;

2.6.2 The following is an example message containing binary images. Five types of image can be sent: PlatePatch, ALPR Image, Overview Image, Context Image or Context Overview Image:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CameraToInstation xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <CameraID>0</CameraID>
    <TimeStamp>2009-06-29T12:01:59.377+01:00</TimeStamp>
    <ImageArray>
        <Image>
            <InstanceID>0</InstanceID>
            <TimeStamp>2009-06-29T12:01:59.379+01:00</TimeStamp>
```

```
            <VRN>A123BCD</VRN>
            <LaneID>0</LaneID>
            <ImageType>platePatch</ImageType>
            <ImageFormat>jpeg</ImageFormat>
            <BinaryImage>[IMAGE DATA]</BinaryImage>
        </Image>
        <Image>
            <InstanceID>0</InstanceID>
            <TimeStamp>2009-06-29T12:01:59.379+01:00</TimeStamp>
            <VRN>A123BCD</VRN>
            <LaneID>0</LaneID>
            <ImageType>ANPRImage</ImageType>
            <ImageFormat>gif</ImageFormat>
            <BinaryImage>[IMAGE DATA]</BinaryImage>
        </Image>
        <Image>
            <InstanceID>0</InstanceID>
            <TimeStamp>2009-06-29T12:01:59.379+01:00</TimeStamp>
            <VRN>A123BCD</VRN>
            <LaneID>0</LaneID>
            <ImageType>overviewImage</ImageType>
            <ImageFormat>tiff</ImageFormat>
            <BinaryImage>[IMAGE DATA]</BinaryImage>
        </Image>
    </ImageArray>
</CameraToInstation>
```

2.6.3 These elements are described in more detail in Appendix 4.

2.6.4 It should be noted that InstanceID is not required for an ad-hoc context image or any image that may be requested from the Instation where there is no association with a vehicle, and therefore no VRN has been collected with a corresponding Instance ID. However, where an image relates to a plate read, the InstanceID for the plate read is included in the image attributes.

2.7 Camera and Configuration

2.7.1 Optional Camera and Configuration elements may be included in response to a ConfigRequest issued by the Instation via the InstationToCamera element. The following is mandatory in the Camera element:

- HardwareUniqueID which represents a globally unique identifier for the camera

2.7.2 At least one Lane element per camera is mandatory. The following are mandatory in each Lane element:

- LaneID representing the lane relative to the camera to which the lane config applies
- LaneNumber representing the lane position in the carriageway
- LaneDirectionTypeID representing the direction of travel of the carriageway lane
- NormalVehicleDirection - whether vehicles normally travel towards or away from the camera

2.7.3 The following is an example message outlining a Camera and Configuration response to an Instation ConfigRequest, which includes both Camera and Configuration elements:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CameraToInstation xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <CameraID>0</CameraID>
    <TimeStamp>2009-06-29T12:01:59.377+01:00</TimeStamp>
    <Camera>
        < HardwareUniqueID>CA_Traffic:Evo8:7205/0219</ HardwareUniqueID>
        <ShortDescription>My Short description</ShortDescription>
        <LongDescription>My long description</LongDescription>
        <XYType>OSGB</XYType>
        <XCoord>123456.7</XCoord>
        <YCoord>654321.0</YCoord>
        <Height>3.5</Height>
        <TypeID>7</TypeID>
        <MobileCamera>false</MobileCamera>
        <SoftwareVersion>2.1.1</SoftwareVersion>
        <LaneArray>
            <Lane>
                <LaneID>0</LaneID>
                <LaneNumber>1</LaneNumber>
                <LaneDirectionTypeID>5</LaneDirectionTypeID>
                <NormalVehicleDirection>towards</NormalVehicleDirection>
            </Lane>
        </LaneArray>
    </Camera>
    <Configuration>
        <HostName>HOST1</HostName>
        <SendVRNs>true</SendVRNs>
        <SendTags>false</SendTags>
        <SendPlatePatches>false</SendPlatePatches>
        <SendANPRImages>false</SendANPRImages>
        <SendOverviewImages>false</SendOverviewImages>
        <SendPlatesNotRead>false</SendPlatesNotRead>
        <SendANPRDiagnostics>true</SendANPRDiagnostics>
        <SendMachineDiagnostics>true</SendMachineDiagnostics>
        <SendIncrementalLog>true</SendIncrementalLog>
        <SendPeriodicContextImage>true</SendPeriodicContextImage>
        <UseReportingOffset>false</UseReportingOffset>
        <SendHeartbeat>true</SendHeartbeat>
        <StreamPlates>false</StreamPlates>
        <HeartbeatInterval>300</HeartbeatInterval>
        <PlateSendInterval>60</PlateSendInterval>
        <ReportingOffset>15</ReportingOffset>
        <ANPRDiagsSendInterval>1800</ANPRDiagsSendInterval>
        <MachineDiagsSendInterval>3600</MachineDiagsSendInterval>
        <IncrementalLogInterval>600</IncrementalLogInterval>
        <ContextImagePeriod>900</ContextImagePeriod>
        <MaxPlatesToSend>200</MaxPlatesToSend>
        <MinANPRDiagnosticSamples>10</MinANPRDiagnosticSamples>
        <CurrentDateTime>2009-06-29T12:01:59.379+01:00</CurrentDateTime>
    </Configuration>
</CameraToInstation>
```

2.7.4 Elements that are part of the <Camera> element are not configurable by the instation and should be set up on installation of the physical camera by manufacturer specific means (for example pre-configured at the factory or entered by the commissioning engineer).

2.7.5 A number of different lanes may be configured for one camera, however note that the <Configuration> element has no attributes which are lane-specific.

2.7.6 In the <Camera> element, at least one <Lane> element is mandatory. It is anticipated that <Lane> attributes will be entered into the camera by the commissioning engineer – these are not downloadable from the Instation.

2.7.7 Where there are attributes in the <Configuration> element which are not supported by a particular camera, the camera may omit these from the response.

2.7.8 A camera must maintain separate Configuration objects for each host. It will only accept the Configuration for a particular host from that host itself, and will only push a Configuration to the host to which it applies.

2.7.9 The <Camera>, <Lane>, and <Configuration> elements are described in more detail in Appendix 5.

2.8 Configuration request

2.8.1 The following is an example message outlining a request by the Camera for an update of its current Configuration:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CameraToInstation xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <CameraID>0</CameraID>
    <TimeStamp>2009-06-29T12:01:59.377+01:00</TimeStamp>
    <ConfigRequest/>
</CameraToInstation>
```

2.8.2 This is an empty element used by the Camera for requesting the current configuration from the Instation, for example on Camera startup.

2.8.3 The ConfigRequest is directed to a particular host, which will return the Configuration relating only to that host. Where a camera is configured to report to multiple hosts, it is not permitted for one host to have the ability to change the Configuration of another.

2.9 Heartbeat message

2.9.1 The following is an example message outlining a heartbeat, which comprises a CameraToInstation element which is empty apart from the mandatory CameraID and Timestamp attributes:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CameraToInstation xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <CameraID>0</CameraID>
    <TimeStamp>2009-06-29T12:01:59.377+01:00</TimeStamp>
</CameraToInstation>
```

2.9.2 Where a Camera is connected via a network which does provide a fixed IP address (for example some mobile networks), it may not be possible for the Instation to initiate a data transaction with a Camera (it may be impossible to determine the IP address allocated by the network). The Camera should therefore be configured periodically to send a 'Heartbeat' message to allow the Instation to respond with a message to the Camera. This heartbeat message is essentially an empty message which must be sent if no other messages have been sent within a configurable period of time (<HeartbeatInterval>).

3 Instation To Camera

3.1 Introduction

3.1.1 The <InstationToCamera> element is intended primarily for transmitting information from the Instation to the Camera in response to a SOAP call containing the <CameraToInstation> element. It allows for any combination of: a camera configuration, a configuration request, an image request or a log request to be sent. None of these elements is mandatory, hence the <InstationToCamera> element may also be sent empty to provide a receipt acknowledgement.

3.1.2 The option must be provided to use Gzip compression of the entire Instation to Camera element. The protocol does not provide for enabling or disabling this feature - it must be enabled or disabled by a commissioning engineer, either on-site or via a remotely connected engineering application.

3.1.3 Whereas this element is used in response to a <CameraToInstation> element, it mostly contains requests for data from the camera, for the reason that cameras are often connected via mobile networks where the Instation is unable to initiate a TCP/IP connection. Requests for data are therefore 'piggybacked' onto the acknowledgements sent by the Instation to the Camera.

3.1.4 Where the network connection allows the Instation to initiate a TCP/IP connection, the <InstationToCamera> element may also be transmitted on an ad-hoc basis as a SOAP call from the instation to the camera.

3.1.5 All array elements include an optional attribute "ManufacturerSpecific" (not shown in the examples) which enables the communication of additional information outside the scope of the pre-defined attributes.

3.2 Configuration

3.2.1 The Instation may push a new or revised configuration to the camera either at will or in response to a <ConfigRequest> from the camera. It is only possible to push that configuration which is specific to the sending host.

3.2.2 The following is an example message outlining a Configuration response to a camera ConfigRequest (none of the <Configuration> elements is mandatory):

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<InstationToCamera xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <Configuration>
        <HostName>HOST1</HostName>
        <SendVRNs>true</SendVRNs>
        <SendTags>false</SendTags>
        <SendPlatePatches>false</SendPlatePatches>
        <SendANPRImages>false</SendANPRImages>
        <SendOverviewImages>false</SendOverviewImages>
        <SendPlatesNotRead>false</SendPlatesNotRead>
        <SendANPRDiagnostics>true</SendANPRDiagnostics>
        <SendMachineDiagnostics>true</SendMachineDiagnostics>
        <SendIncrementalLog>true</SendIncrementalLog>
        <SendPeriodicContextImage>true</SendPeriodicContextImage>
        <UseReportingOffset>false</UseReportingOffset>
        <SendHeartbeat>true</SendHeartbeat>
        <StreamPlates>false</StreamPlates>
```

```
            <HeartbeatInterval>300</HeartbeatInterval>
            <PlateSendInterval>60</PlateSendInterval>
            <ReportingOffset>15</ReportingOffset>
            <ANPRDiagsSendInterval>1800</ANPRDiagsSendInterval>
            <MachineDiagsSendInterval>3600</MachineDiagsSendInterval>
            <IncrementalLogInterval>600</IncrementalLogInterval>
            <ContextImagePeriod>900</ContextImagePeriod>
            <MaxPlatesToSend>200</MaxPlatesToSend>
            <MinANPRDiagnosticSamples>10</MinANPRDiagnosticSamples>
            <CurrentDateTime>2009-06-29T12:01:59.379+01:00</CurrentDateTime>
        </Configuration>
</InstationToCamera>
```

3.2.3 This is exactly the same <Configuration> element as used for the <CameraToInstation> child element for transmitting the camera's current configuration.

3.2.4 The protocol does not provide for the addition of new hosts to the camera - these must be added or removed by a commissioning engineer, either on-site or via a remotely connected engineering application.

3.2.5 Where there are attributes in the <Configuration> element which are not supported by a particular camera, they will be ignored by the camera.

3.3 Log request

3.3.1 The Instation may request log records from the camera for a specific time period. In the <LogRequest> element, the following (which are the only attributes) are mandatory:

- StartTime which is the date and time at which log records should start;
- EndTime which is the date and time at which log records should end.

3.3.2 The following is an example message containing a response request from the Instation for provision of a Log by the camera:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<InstationToCamera xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <LogRequest>
        <StartTime>2008-11-14T10:50:30.952Z</StartTime>
        <EndTime>2008-11-14T10:50:30.952Z</EndTime>
    </LogRequest>
</InstationToCamera>
```

3.4 Configuration request

3.4.1 The following is an example message outlining a request by the Instation for a camera to upload its current Configuration:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<InstationToCamera xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <ConfigRequest/>
</InstationToCamera>
```

3.4.2 The <ConfigRequest> is an empty element identical to the same child element of the <CameraToInstation> element. (see 2.8).

3.4.3 The <ConfigRequest> is issued by a particular host, and the camera will return only the Configuration relating only to that host.

3.5 Image request

3.5.1 The Instation may request (retrospectively) images related to plate reads which have been stored in a camera. It may also request ad-hoc context images which are not connected with plate reads. There are four different classes of request, depending on the criteria which the Instation wishes to use to identify the required images:

- TimeRangeImageRequest: request images from a specific time period
- PriorVRNImageRequest: request a specific quantity of the most recent images
- InstanceSetImageRequest: request the images for a specific list of plate reads
- ContextImageRequest: request immediate images from one or more camera sensors

3.5.2 Only one of these ImageRequest classes should be used per <InstationToCamera> response, otherwise the instation will not know to which request the images sent by the camera relate.

3.5.3 The following is an example outlining a request from an Instation to a camera requesting the provision of images from a specific time period:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<InstationToCamera xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <TimeRangeImageRequest>
        <StartTime>2008-11-14T10:50:30.952Z</StartTime>
        <EndTime>2008-11-14T10:50:30.952Z</EndTime>
        <ImageTypeArray>
            <ImageType>platePatch</ImageType>
            <ImageType>overviewImage</ImageType>
        </ImageTypeArray>
    </TimeRangeImageRequest>
</InstationToCamera>
```

3.5.4 The following is an example outlining a request from an Instation to a camera requesting a specific quantity of recent images ending at a particular InstanceID:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<InstationToCamera xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <PriorVRNImageRequest>
        <NoOfPriorVRNs>10</NoOfPriorVRNs>
        <EndInstanceID>123456</EndInstanceID>
        <ImageTypeArray>
            <ImageType>platePatch</ImageType>
            <ImageType>overviewImage</ImageType>
        </ImageTypeArray>
    </PriorVRNImageRequest>
</InstationToCamera>
```

3.5.5 The following is an example outlining a request from an Instation to a camera requesting the provision of images for a specific set of plate reads:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<InstationToCamera xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <InstanceSetImageRequest>
        <InstanceIDArray>
            <InstanceID>123456</InstanceID>
            <InstanceID>123454</InstanceID>
            <InstanceID>123452</InstanceID>
        </InstanceIDArray>
        <ImageTypeArray>
            <ImageType>platePatch</ImageType>
            <ImageType>overviewImage</ImageType>
        </ImageTypeArray>
    </InstanceSetImageRequest>
</InstationToCamera>
```

3.5.6 The following is an example outlining a request from an Instation to a camera requesting immediate context images:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<InstationToCamera xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <ContextImageRequest>
        <ImageTypeArray>
            <ImageType>contextImage</ImageType>
            <ImageType>contextOverviewImage</ImageType>
        </ImageTypeArray>
    </ContextImageRequest>
</InstationToCamera>
```

3.5.7 These elements are described in more detail in Appendix 6.

3.6 Acknowledgement

3.6.1 The following is an example message outlining an acknowledgement, which comprises an <InstationToCamera> element that is empty:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<InstationToCamera xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
</InstationToCamera>
```

3.6.2 Where the Instation receives a <CameraToInstation> message and does not require any further information from the camera, the <InstationToCamera> response will be an empty element which provides the camera with an acknowledgment that its transmission has been received.

4 Tag Hashing algorithm

4.1 About the algorithm

4.1.1 Journey time systems based on ALPR require cameras to recognise a plate at two or more locations and to return the recognised plate details to the instation. Although the full plate registration number can be returned to the instation for character by character matching, this may be undesirable in some circumstances. Additionally, to maintain driver and vehicle anonymity, it may be desirable to encrypt or otherwise change the plate string such that the actual registration number cannot be recovered.

4.1.2 ALPR systems are never 100% accurate. Read errors do occur. It is desirable to minimise the effect on the system of these read errors. For example the character D may be read correctly at one location and then the same character may be read as an O at a subsequent location.

4.1.3 The hashing algorithm firstly reduces the possible effect of plate read errors by replacing any characters likely to be confused with one another by a single character. So for example any occurence of O, D, 0 or Q in a plate is replaced with the character O. The following table lists all such substitutions:

ALPR reads character	Reported as
O D 0 Q	O
I 1	I
S 5	S
V Y	V
3 8 B	3
2 Z	2
E F	E
G C	G
H M N W	H

4.1.4 The resultant plate string is then hashed down to a binary number of 24 bits. The hash algorithm chosen is "one_at_a_time_hash". This algorithm has been chosen after reviewing the performance of a large number of algorithms over a database of about 100,000 UK plates and selecting the algorithm which provided the best distribution of hash values.

4.1.5 The "one_at_a_time_hash" hash algorithm was developed by Bob Jenkins. The original reference for the algorithm is: http://www.burtleburtle.net/bob/hash/doobs.html

4.2 Example

4.2.1 Example code (C language) for character substitution and the hash process is shown below.

```
static const char *mixups[] =
{
    "OD0Q", "I1", "S5", "VY", "38B", "2Z", "EF", "GC", "HMNW",
};
#define    NMIXUPS    9

void merge_ambiguous_characters(char *plate)
{
short  i;
char   *cp;

    while(*plate)
    {
        for(i=0; i<NMIXUPS; ++i)
        {
            cp = mixups[i];
            if(ismember(*plate, cp))
            {
                *plate = *cp;
            }
        }
        ++plate;
    }
}


// this function returns the 24 bit hash value directly

unsigned long hash(const char *plate)
{
unsigned   len;
unsigned   hash, i;
const int  hashbits = 24;
char       merge_plate[12];
#define    hashsize(n) ((unsigned)1<<(n))
#define    hashmask(n) (hashsize(n)-1)

    strcpy(merge_plate,plate);
        merge_ambiguous_characters(merge_plate);
    len = strlen(merge_plate);
    for (hash=0, i=0; i<len; ++i)
    {
        hash += merge_plate[i];
        hash += (hash << 10);
        hash ^= (hash >> 6);
    }
    hash += (hash << 3);
    hash ^= (hash >> 11);
    hash += (hash << 15);
    return (hash & hashmask(hashbits));
}
```

Appendix 1 PlateRead Element

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
InstanceID	DYNAMIC	A unique plate reference number for this camera. InstanceID should be incremented for each plate read until the holding variable (typically INT32) wraps, i.e. it is not just unique for a particular timestamp.	uInteger	Y	Combined with CameraID and TimeStamp at Instation to form a unique EventID
TimeStamp	DYNAMIC	ISO 8601 UTC date/timestamp for time of sighting	DateTime	Y	1ms resolution For dateTime format, see section 3.2.7 (dateTime) of W3C document “XML Schema Part 2 - Datatypes Second Edition“
TimeStampError	DYNAMIC	Estimated worst case timestamp error in ms	Integer		
LaneID	DYNAMIC	Camera Lane to which configuration item(s) relate	uInteger	Y	0 is the leftmost lane in the camera field of view. This ID is relative to the camera, not the actual lanes of the carriageway
VehicleDirection	DYNAMIC	Whether vehicle travelling toward or away from camera	Enumerated	Y	e.g. towards, away, unknown. i.e. towards = front plate, away = rear plate
XYType	STATIC	Reference co-ordinate system for XY location	Enumerated		e.g. OSGB or WGS84 (NB OSGB refers to OSGB36 datum)
XCoord	STATIC	X co-ordinate of camera location	Float		e.g. Longitude or Easting (Degrees + decimal degrees for longitude)
YCoord	STATIC	X co-ordinate of camera location	Float		e.g. Latitude or Northing (Degrees + decimal degrees for latitude)
PlateNotRead	DYNAMIC	A vehicle has been detected, but a plate cannot be found or, if found, cannot be recognised	Boolean	Y	Allows an InstanceID to be generated and a PlateRead record to be sent where no plate has been read.
VRN	DYNAMIC	Recognised licence number	Character		No whitespace characters
VRNConfidence	DYNAMIC	Probability that licence number is correct	Percent		0 to 100%
Tag	DYNAMIC	Hashed value formed from VRN	uInteger		In the range 0 to 2^{24} - 1

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
TagConfidence	DYNAMIC	Probability that tag value is correct	Percent		0 to 100%
Classification	DYNAMIC	Class of the recognised vehicle e.g. car, van lorry	uInteger		Numeric values only representing a classification scheme determined by the user.
Country	DYNAMIC	ISO 3166-1 three character country code	Character		e.g. GBR, FRA, DEU
Make	DYNAMIC	Make of Vehicle (Manufacturer)	Character		
Model	DYNAMIC	Model of Vehicle	Character		May be text (e.g. Mondeo) or number (e.g. 520)
Colour	DYNAMIC	Colour of vehicle	Enumerated		See list of standard colours (table below)*
Velocity	DYNAMIC	Estimated vehicle speed in kph	uInteger		
VelocityError	DYNAMIC	Estimated velocity error (magnitude) in kph	uInteger		Mean of the magnitudes of the +ve and -ve error estimates at 95% confidence interval

* A standard set of colours is used as follows:

Red		Green		Dark Purple		Light Brown
Light Red		Light Green		Grey		Dark Brown
Dark Red		Dark Green		Light Grey		Magenta
Orange		Blue		Dark Grey		Turquoise
Light Orange		Light Blue		Gold		
Dark Orange		Dark Blue		Silver		
Yellow		Violet		White		
Light Yellow		Purple		Black		
Dark Yellow		Light Purple		Brown		

Appendix 2 ALPRDiagnostic Element

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
TimeStamp	DYNAMIC	ISO 8601 UTC date/timestamp for end of diagnostic period	DateTime	Y	1ms resolution
DiagnosticType	DYNAMIC	Whether a routine diagnostic or an alarm (warning or fault)	Enumerated	Y	Enumerated type having values "routineDiagnostic", "alarmWarningSet", "alarmWarningClear", "alarmFaultSet","alarmFaultClear"
LaneID	DYNAMIC	Camera Lane to which the Diagnostics relate	uInteger		0 is the leftmost lane in the camera field of view. This ID is relative to the camera, not the actual lanes of the carriageway
MeanVRNConfidence	DYNAMIC	Average Probability that licence number is correct	Percent		0 to 100%
MeanTagConfidence	DYNAMIC	Average Probability that tag value is correct	Percent		0 to 100%
MeanPlateContrast	DYNAMIC	Average plate patch contrast	Percent		0 = all black, 100 = all white
MeanCharacterHeight	DYNAMIC	Average VRN character height in pixels	uInteger		
MeanHorizontalAngle	DYNAMIC	Average character angle to horizontal in degrees	Integer		±90 degrees
MeanVerticalAngle	DYNAMIC	Average character angle to vertical in degrees	Integer		±90 degrees
MeanTrajectoryOffset	DYNAMIC	Average trajectory distance from image centre	Integer		As a percentage of the horizontal image size. -ve for left of centre, +ve for right of centre
MeanTrajectoryAngle	DYNAMIC	Average angle of trajectory to horizontal in degrees	WholeDegrees		Horizontal right to left is zero, increasing anti-clockwise to 360. Values between 180 and 360 for vehicles travelling away from camera.
MeanVelocity	DYNAMIC	Average estimated vehicle speed in kph	uInteger		
MeanVelocityError	DYNAMIC	Average velocity error at 95% confidence interval	uInteger		Value in kph (mean of velocity error magnitude estimates)
PlateToTriggerRatio	DYNAMIC	Ratio of plates recognised to objects detected	Percent		0 to 100%

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
PlatesNoCountryRatio	DYNAMIC	Ratio of plates with unidentified country to all plates	Percent		0 to 100%
PlatesTowardsRatio	DYNAMIC	Ratio of plates towards camera to total plates	Percent		0 to 100%
PlatesAwayRatio	DYNAMIC	Ratio of plates away from camera to total plates	Percent		0 to 100%
MeanIRLevel	DYNAMIC	Average illuminator output level (percentage of max)	Percent		For frames selected for plate recognition
MeanExposure	DYNAMIC	Average exposure time in microseconds	uInteger		For frames selected for plate recognition
MeanGain	DYNAMIC	Average camera gain in dB where max gain is 0dB	Integer		For frames selected for plate recognition

Appendix 3 MachineDiagnostic Element

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
TimeStamp	DYNAMIC	ISO 8601 UTC date/timestamp for end of diagnostic period	DateTime	Y	1ms resolution
DiagnosticType	DYNAMIC	Whether a routine diagnostic or an alarm (warning or fault)	Enumerated	Y	Enumerated type having values "routineDiagnostic", "alarmWarningSet", "alarmWarningClear", "alarmFaultSet","alarmFaultClear"
MeanCPUTemp	DYNAMIC	Average processor board temperature in degrees	Integer		Can be +ve or -ve
MeanTotalCurrent	DYNAMIC	Average current drawn by camera including illuminator in mA	uInteger		Purpose: to identify reduction in illuminator current. Max value is 99,999mA
MeanIlluminatorTemp	DYNAMIC	Average illuminator temperature in degrees	Integer		Can be +ve or -ve
MeanIlluminatorCurrent	DYNAMIC	Average illuminator current in mA (during on-time)	uInteger		Max value is 99,999mA
IlluminatorUsage	DYNAMIC	Total illuminator usage (amps x hours) - cumulative	uInteger		As an indication of illuminator lifetime used
MeanIlluminatorOutput	DYNAMIC	Average illuminator light output as percentage of max when new	Integer		May be > 100%
LastResetTime	DYNAMIC	Date & Time of last CPU reset	DateTime		May be outside this diagnostic interval
NoOfHardwareErrors	DYNAMIC	Number of hardware errors detected	uInteger		
MeanSignalStrength	DYNAMIC	Average signal strength (wireless comms) in dB	Integer		Range is -999dB to 0dB
HostName	DYNAMIC	Name of host to which diagnostics relate	Character	Y	IP address or DNS name
MeanCommsLag	DYNAMIC	Average "round trip" communications delay in ms	uInteger		
WorstCommsLag	DYNAMIC	Worst case "round trip" communications delay in ms	uInteger		
NoOfCommsResends	DYNAMIC	Number of messages re-sent	uInteger		e.g. After failure to open host port
NoOfCommsFailures	DYNAMIC	Number of messages deleted from send buffer after repeated re-send failures	uInteger		
NoOfCommsReconnects	DYNAMIC	Number of reconnections to wireless network	uInteger		

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
MeanSyncDifference	DYNAMIC	Average time correction upon re-synchronisation in ms	Integer		This is a signed value, where a negative difference means the camera clock was fast, and a positive difference means it was slow.
WorstSyncDifference	DYNAMIC	Worst case time correction upon re-synchronisation in ms	Integer		This is a signed value, where a negative difference means the camera clock was fast, and a positive difference means it was slow.
LastSyncTime	DYNAMIC	Date & Time of last successful re-synchronisation	DateTime		May be outside this diagnostic interval
SupplyVoltage	DYNAMIC	Percentage of nominal system SELV supply voltage	Integer		May be >100%
TamperAlarm	DYNAMIC	Indication of unauthorised access to the equipment	Enumerated		Has 3 enumerated values: "normal", "enclosureBreachAlarm", "unauthorisedCommunicationAlarm"

Appendix 4 Image Element

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
InstanceID	DYNAMIC	Unique reference number for this camera to VRN record for a plate in the image	uInteger		
TimeStamp	DYNAMIC	ISO 8601 UTC date/timestamp	DateTime	Y	1ms resolution
VRN	DYNAMIC	Recognised licence plate number	Character		No whitespace characters. Allows images to be transmitted belatedly without the Host needing to refer to a database table referenced by InstanceID in order to associate VRN with images.
LaneID	DYNAMIC	Camera Lane to which image relates	uInteger		0 is the leftmost lane in the camera field of view. This ID is relative to the camera, not the actual lanes of the carriageway
ImageType	DYNAMIC	Whether the image is: a Plate patch (a close-cropped image of the plate as used for recognition) an ALPR image (the full image from which the plate patch has been taken) an Overview image (a visible image of the vehicle to which the plate read relates) a Context image (an uncropped image not related to a plate read) For cameras having separate ALPR and Overview sensors, context images by default relate to the ALPR sensor, but context images from the Overview sensor are also handled.	Enumerated	Y	Format: either "platePatch", "ALPRImage", "overviewImage", “contextImage” (from ALPR sensor) or “contextOverviewImage” (from Overview sensor).
ImageFormat	DYNAMIC	Encoding format of the image e.g. jpeg, tiff	Enumerated		Enumerated type having values "fits", "g3fax", "gif", "ief", "jp2", "jpeg", "jpm", "jpx", "t38", "tiff", "tiff-fx". (These formats are recognised MIME media types maintained in the IANA protocol registry: www.iana.org/assignments/media-types/image/).
BinaryImage	DYNAMIC	Jpeg image base-64 encoded	Binary		

Appendix 5 Camera Configuration Elements

A5.1 Camera Element

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
CameraID	STATIC	Unique identifier for the camera within a system	Character	Y	Local to Instation/Database Cross-reference to definition unique within a system can be compared in use to a "local IP Address"
HardwareUniqueID	STATIC	Globally unique identifier for the camera	Character	Y	Variable length up to 256 characters. Comprises three colon-separated fields i.e. "ManufacturerName:Model:FreeText". Each field any length with no whitespace allowed. ManufacturerName is mandatory, Model is optional - if null is signified by consecutive colons "ManufacturerName::FreeText". Strings must be alphanumeric and may include punctuation marks except colon.
ShortDescription	STATIC	Brief description of camera location	Character		
LongDescription	STATIC	Detailed description of camera location	Character		
XYType	STATIC	Reference co-ordinate system for XY location	Enumerated		e.g. OSGB or WGS84 (NB OSGB refers to OSGB36 datum)
XCoord	STATIC	X co-ordinate of camera location	Float		e.g. Longitude or Easting Degrees + decimal degrees for longitude
YCoord	STATIC	Y co-ordinate of camera location	Float		e.g. Latitude or Northing Degrees + decimal degrees for latitude
Height	STATIC	Height of camera above local ground level	Float		Measured in metres e.g. Height above Lowest road surface in multi-level junction

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
TypeID	STATIC	Type of equipment from generic list	uInteger		Generic ALPR = 5, IR = 6, IR+colour = 7, colour = 8
MobileCamera	STATIC	Whether the camera is mobile or fixed	Boolean		Assume fixed if attribute is absent
SoftwareVersion	STATIC	Software version number of the application generating the machine diagnostics (manufacturer specific)	Character		e.g. 3.5.15.72

A5.2 Lane Element

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
LaneID	STATIC	Camera Lane to which configuration item(s) relate	uInteger	Y	0 is the leftmost lane in the camera field of view This ID is relative to the camera, not the actual lanes of the carriageway
LaneNumber	STATIC	Position of the Lane in relation to the total number of lanes in the carriageway	uInteger	Y	In the range 0 to 99 Lane 0 is the first lane on the left in the direction of travel
LaneDirectionTypeID	STATIC	Direction of the carriageway lane in which vehicles normally travel (Note that this attribute relates to the direction taken by vehicles, not the direction in which the camera is pointing.)	uInteger	Y	e.g. 3 = clockwise, 4 = anticlockwise, 5 = northbound etc Format: see Direction_TypeID in CCTV ALPR Extensions Global Support Object
NormalVehicleDirection	STATIC	Direction relative to the camera in which vehicles normally travel	Enumerated	Y	e.g. towards, away, both "Both" applies for a single track road or tidal lane in a multi-lane road

A5.3 Configuration Element

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
HostName	CONFIG	Name of host to which configuration item(s) relate	Character		The fully qualified host URL or endpoint is set at time of commissioning.
SendVRNs	CONFIG	Whether to send VRN data (true/false)	Boolean		Following config items per host
SendTags	CONFIG	Whether to send Tag data (true/false)	Boolean		
SendPlatePatches	CONFIG	Whether to send plate patch images (true/false)	Boolean		
SendANPRImages	CONFIG	Whether to send full frame ALPR images (true/false)	Boolean		
SendOverviewImages	CONFIG	Whether to send full frame Overview images (true/false)	Boolean		
SendPlatesNotRead	CONFIG	Whether to send PlateRead records where PlateNotRead attribute is true	Boolean		See PlateRead attribute “PlateNotRead”
SendANPRDiagnostics	CONFIG	Whether to send ALPR diagnostics (true/false)	Boolean		
SendMachineDiagnostics	CONFIG	Whether to send machine diagnostics (true/false)	Boolean		
SendIncrementalLog	CONFIG	Whether to send an incremental log file (additions since last send)	Boolean		
SendPeriodicContextImage	CONFIG	Whether to send periodic context images (true/false)	Boolean		Note that in multiple sensor cameras, the sensor from which the context image is to be taken is determined by manufacturer-specific means. For example an image from the overview sensor may be returned during the day and an image from the ALPR sensor at night.

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
UseReportingOffset	CONFIG	Whether the camera should utilise the ReportingOffset (true/false)	Boolean		If false, permits the randomisation of reporting times by another method (for example by starting reporting intervals relative to the last camera power-on or reset) without the need to configure each camera with an individual ReportingOffset. Avoids cameras all reporting at the same time if no ReportingOffset is configured or a default value is assumed.
SendHeartbeat	CONFIG	Whether a generic wrapper should be sent periodically irrespective of whether there is data to send (true/false)	Boolean		Allows the sending of heartbeats to be turned on and off explicitly, rather than relying on whether a HeartbeatInterval has been configured.
StreamPlates	CONFIG	Whether to send a PlateRead record as soon as a plate is recognised (true/false)	Boolean		
HeartbeatInterval	CONFIG	Send at least one generic wrapper during this interval in seconds	uInteger		Maximum value 86400 seconds (=1 day)
PlateSendInterval	CONFIG	Reporting interval for sending VRN and/or tag data in seconds	uInteger		The end of the PlateSendInterval should be aligned with the time of transmission determined by the ReportingOffset, to ensure that the latest plate data is always reported as soon as possible.
ReportingOffset	CONFIG	Reporting time offset as percentage of appropriate send interval	Percent		Relative to a reporting interval commencing at midnight
ANPRDiagsSendInterval	CONFIG	Reporting interval for sending ALPR diagnostics in seconds	uInteger		
MachineDiagsSendInterval	CONFIG	Reporting interval for sending machine diagnostics in seconds	uInteger		
IncrementalLogInterval	CONFIG	Reporting interval for sending incremental log in seconds	uInteger		
ContextImagePeriod	CONFIG	Time interval at which a single context image is returned in seconds	uInteger		Single image only - not a batch

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
MaxPlatesToSend	CONFIG	Maximum number of VRNs/Tags to send per reporting interval	uInteger		Applies when StreamPlates is false - send up to this number of captured plates during a plate reporting interval.
MinANPRDiagnosticSamples	CONFIG	Minimum vehicles to be included in ALPR diagnostic averages	uInteger		Roll samples over from one interval to next
CurrentDateTime	CONFIG	DateTime value to set real time clock. The presence or absence of this attribute in the InstationToCamera response determines whether the Camera clock should be set or not.	DateTime		For dateTime format, see section 3.2.7 (dateTime) of W3C document “XML Schema Part 2 - Datatypes Second Edition“

Appendix 6 ImageRequest Elements

A6.1 TimeRangeImageRequest

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
StartTime	DYNAMIC	ISO 8601 UTC date/timestamp	DateTime	Y	1ms resolution
EndTime	DYNAMIC	ISO 8601 UTC date/timestamp	DateTime	Y	1ms resolution
ImageTypeArray	DYNAMIC	Array element containing 0 to n ImageTypes (list of the types of images required)	Character		See ImageType attribute of Image element (contextImage and contextOverviewImage will be ignored)

A6.2 PriorVRNImageRequest

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
NoOfPriorVRNs	DYNAMIC	Number of most recent VRN instances for which images are required	uInteger	Y	
EndInstanceID	DYNAMIC	The set of images to be sent should end with this InstanceID	uInteger		Used in conjunction with NoOfPriorVRNS to determine the latest InstanceID which should be sent in the set of images defined by these two attributes.
ImageTypeArray	DYNAMIC	Array element containing 0 to n ImageTypes (list of the types of images required)	Character		See ImageType attribute of Image element (contextImage and contextOverviewImage will be ignored)

A6.3 InstanceSetImageRequest

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
InstanceIDArray	DYNAMIC	InstanceArray element containing 0 to n Instance IDs for this camera of VRN records of the plates for which images are required	uInteger	Y	
ImageTypeArray	DYNAMIC	Array element containing 0 to n ImageTypes (list of the types of images required)	Character		See ImageType attribute of Image element (contextImage and contextOverviewImage will be ignored)

A6.4 ContextImageRequest

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
ImageTypeArray	DYNAMIC	Array element containing 0 to n ImageTypes (list of the types of images required)	Character		See ImageType attribute of Image element (anything other than contextImage or contextOverviewImage will be ignored)

THE COMMONWEALTH OF MASSACHUSETTS
EXECUTIVE OFFICE OF PUBLIC SAFETY AND SECURITY
Department of Criminal Justice Information Services
200 Arlington Street, Suite 2200, Chelsea, Massachusetts 02150, MASS.GOV/CJIS
TEL: 617-660-4600 • TTY: 617-660-4606 • FAX: 617-660-4613

Deval L. Patrick, *Governor* | Andrea J. Cabral, *Secretary of Public Safety and Security* | James F. Slater, III, *Acting Commissioner*

EXECUTIVE OFFICE OF PUBLIC SAFETY AND SECURITY DEPARTMENT OF CRIMINAL JUSTICE INFORMATION SERVICES AUTOMATIC LICENSE PLATE RECOGNITION SYSTEMS CENTRAL REPOSITORY COMPANION POLICY

PURPOSE

To establish guidelines and best practices for data use, maintenance, training, and data storage associated with the usage of the Commonwealth Criminal Justice Information Automatic License Plate Recognition Systems Central Repository (Central Repository) by Massachusetts law enforcement agencies.

OVERVIEW

An Automatic License Plate Recognition (ALPR) system is a computerized system that uses high-speed digital cameras combined with sophisticated computer algorithms capable of converting the images of license plates to electronically readable data. The ALPR system captures an infrared image of a license plate and converts it to a text file using Optical Character Recognition (OCR) technology. The technology also compares the digital images of license plates to lists of known plates of interest. Currently, the ALPR is being utilized by many law enforcement and criminal justice agencies in the Commonwealth, which maintain the captured information in a database.

The Central Repository is a centralized data warehouse that stores ALPR information contributed by law enforcement and public safety agencies from the agency's database. By allowing the agencies to share and access the stored information, local, state and federal law enforcement agencies are provided accurate information to be used for official and legitimate law enforcement operations and public safety purposes. Guidelines for submission and retrieval of license plate data for all participating departments are included in the Commonwealth of Massachusetts Global Justice and Public Safety Information Sharing Policy of the Massachusetts Department of Criminal Justice Information Services (DCJIS), which is incorporated by reference, and this ALPR Central Repository Companion Policy. ALPR systems are dependent upon the networking system of Commonwealth's Criminal Justice Information System (CJIS) and all participating agencies and users agree to the terms of these policies.

DCJIS Enhancing Public Safety Through Information Exchange

POLICY

It is the policy of the DCJIS to utilize the technology only in furtherance of official and legitimate law enforcement operations and public safety. Recognizing privacy implications, it is further the policy of DCJIS to ensure the protection of data. Thus, all users of the Central Repository are expected to abide by the guidelines set forth herein when using the Central Repository.

ACRONYMS AND DEFINITIONS

Agency ALPR Administrator: An employee of a Participating Agency designated by that agency to be responsible for the management of its authorized users and the user accounts at the Participating Agency.

Authorized User: An individual designated by a law enforcement agency and properly trained in the use and operational protocols of the ALPR. Only authorized employees who have an approved login and password will be allowed to access or use information in the Central Repository.

Contributing Agency: An agency that contributes ALPR data to the Central Repository.

Non-Contributing Agency: An agency that may access, but does not contribute data to, a data application or system maintained or operated within the DCJIS network or system.

Participating Agency: Either a contributing or non-contributing party that utilizes the Central Repository.

Source Agency: The agency that originally recorded and contributed data to a data application or system maintained or operated within the DCJIS network or system.

PROCEDURES

1. Standard of Use

Central Repository ALPR data shall be accessed and used only for official and legitimate law enforcement operations and public safety and may only be used based on specific and articulable facts of a concern for safety, wrongdoing, criminal investigations, Department-related civil investigations, or pursuant to a court order.

Searches of historical Central Repository ALPR data shall be done in accordance with this policy.

Only users who have been designated by their law enforcement department and properly trained in the use and operational protocols of the ALPR systems shall be permitted to use the Central Repository. DCJIS administrators shall ensure that any changes in hardware, software or law are communicated to all participants. Only authorized employees who have an approved login and password (Central Repository Authorized Users) will be allowed to access or use information in the Central Repository.

When a enforcement action, investigation, or prosecution results from the Repository ALPR data, the information contained in it will be preserved by the agency accessing the information.

Requests for searches of Central Repository ALPR data may be made by authorized members of the Contributing Party or Non-Contributing party subject to the provisions of this policy.

2. Login Application Process

a) Each Contributing and Non-contributing Party shall designate an Agency ALPR administrator to be responsible for management of user accounts at that agency. All authorized users shall be limited to current employees who are legally authorized to review criminal justice information for crime prevention and detection purposes. Each potential user shall submit a request for a login and password to the Agency ALPR Administrator. The Agency ALPR Administrator shall have discretion to deny or revoke individual access.

3. Login Assignment

a) Each Authorized User will be issued a user login and a default password by the Agency ALPR Administrator. Upon logging into the Repository for the first time, each Authorized User shall change the default password to another DCJIS-compliant password.

b) Each Agency ALPR Administrator is responsible for the timely removal of any login accounts as Authorized Users leave their agency.

c) An Authorized User shall not access the Central Repository by using a name and password that was assigned to another user. An Authorized User shall not give his or her password to another person, including another user, to access the system.

4. ALPR Central Repository Data Query Logs

a) An automated log will be maintained for each transaction, which will include the name of the individual accessing the data, along with the date and time of access.

b) Requests to review stored ALPR data and search results will be recorded and maintained in appropriate case files.

c) ALPR Data Query Logs shall be maintained and secured.

d) Audits of the ALPR systems and the central repository shall be conducted by the DCJIS.

5. ALPR Data Sharing and Dissemination

a) Each Contributing Agency authorizes the release of its information as outlined in this Policy to any other criminal justice agency that may participate in the Central Repository in the future.

b) A Contributing Party that does not want certain information from its ALPR system to be shared is responsible for filtering out such information before entering it into the Central Repository.

c) The information contributed to the Central Repository is limited to ALPR data.

d) Central Repository ALPR data can be accessed, retrieved, or shared for official and legitimate law enforcement operations or public safety purposes only.

6. Ownership of Data

a) Each Contributing Party will retain sole responsibility, ownership, management control, and disposition over the information it contributes or allows access to. All system entries will be identifiable to the Contributing Party, and the content of the contributed information remains the sole responsibility of the Contributing Party and is under that Contributing Party's management control.

b) It shall be the responsibility of the party requesting or using the data to confirm the accuracy of the information with the Source Agency before taking any enforcement-related action.

7. Retention of Data

a) Data from field ALPRs will be transferred/uploaded to the Department's server at a time to be determined by the Agency ALPR Administrator.

b) ALPR data shall be stored in the Central Repository for a period of one year except in the following circumstances:

i) Alert data associated with an enforcement action, investigation, or prosecution shall be maintained for one year or until a final disposition has been reached in the particular case, whichever is longer.

ii) Alert data associated with an arrest will be maintained in the criminal case file and retained for the maximum period of time associated with such record.

iii) Alert data associated with criminal investigations will be maintained in the criminal case file and retained for the maximum period associated with such record.

iv) If it is reasonable to believe and the ALPR data will become evidence in a criminal or civil action, the record will be maintained until it is no longer reasonable to believe it will become evidence in a criminal or civil action.

v) Whenever otherwise directed by the ALPR Administrator.

CONFIDENTIALITY OF INFORMATION

Information in the Central Repository is confidential and is not subject to public disclosure, except as required by law. Only Authorized Users are allowed to view and use the information, otherwise, the information shall be kept confidential.

ACKNOWLEDGEMENT OF TERMS AND CONDITIONS OF USE

The Agency ALPR Administrator shall provide a copy of the terms and conditions of the Massachusetts Public Safety Information Sharing Global Policy and this ALPR Central Repository Companion System Policy to all Authorized Users when they are issued a login ID for the system. Each Authorized User shall sign an acknowledgement stating, "I have received a copy of the terms and conditions of usage of the Central Repository. I agree to comply with the terms and conditions and I understand that any violation of the terms and conditions may lead to disciplinary action and/or criminal prosecution." The Agency ALPR Administrator shall maintain the signed acknowledgements at all times.

POLICY REVIEW

The Commissioner of the Department of Criminal Justice Information Services is responsible for the annual review of this policy.



PIPS TECHNOLOGY™

DETECTION INNOVATION



Back Office System Software

User's Manual

Version 3.5 or above

NEOLOGY™ MOBILITY TECHNOLOGIES

Table of Contents

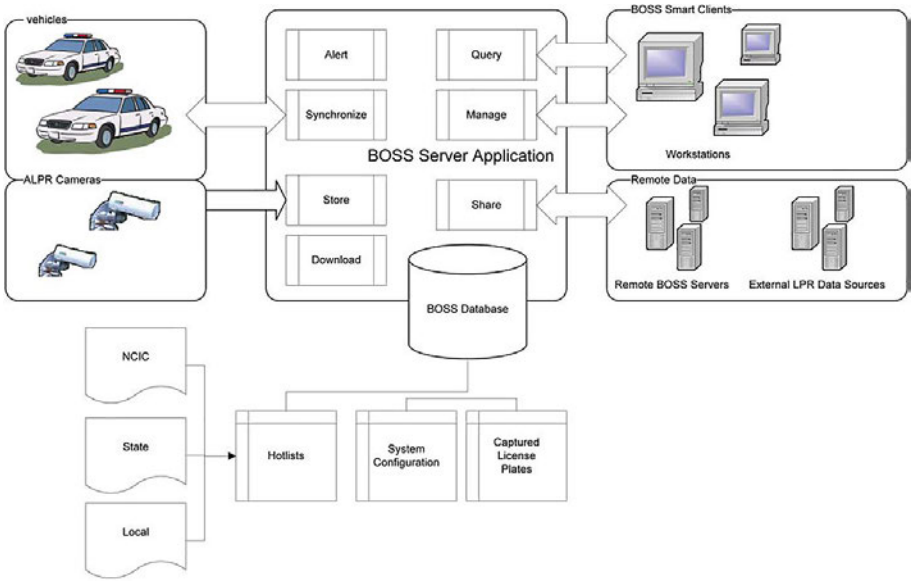
1 Introduction 4
1.1 The Design of PIPS Back Office System Software Version
2 Logging In 5
2.1 PIPS Back Office System Software Administrator Login 5
2.2 User Login 5
2.3 Login Dialog 5
2.3.1 Storing Username and Password 6
2.3.2 BOSS Client Connection Settings 6
3 Application Layout 7
3.1 Components of the BOSS Application Screen 7
3.2 The BOSS Home Screen 8
3.3 Help Documentation 9
3.4 Minimizing the BOSS Application 9
4 BOSS Access Permissions: Users/Groups/Roles 10
4.1 Permission Levels 10
4.2 Permissions 10
4.3 Roles 11
4.4 Groups 12
4.4.1 Creating a New Group 12
4.4.2 Parent Groups 13
4.4.3 Deleting a Group 13
4.5 Users 14
4.5.1 Creating a New User 14
4.5.2 Deleting a User 15
4.5.3 Importing Users from Active Directory 16
4.6 Access Permission Example 17
4.7 Preferences 18
4.7.1 Changing User Preferences 18
5 Devices and Sites 19
5.1 Devices 19
5.1.1 Device Status 20
5.1.2 Defining a Device 20
5.1.3 Editing a Device 21
5.1.4 Enabling and Disabling a Device 21
5.1.5 Deleting a Device 22
5.2 Sites 22
5.2.1 Default Sites 22
5.2.2 Creating a Site 23
5.2.3 Deleting a Site 23
6 BOSS Data Sharing 24
6.1 Configuring BOSS to Allow Remote BOSS Queries 24
6.2 Configuring BOSS to Access a Remote BOSS Server 24
7 Hotlists 25
7.1 Creating a New Hotlist 25
7.1.1 Configuring Basic Hotlist Settings 25
7.1.2 Defining the Hotlist Data Source 27
7.1.3 ZIP Compressed Hotlist Files 29
7.1.4 Defining Hotlist Source Credentials 29
7.1.5 Defining Hotlist Advanced Options 31
7.2 Enabling and Disabling a Hotlist 32
7.3 Modifying Hotlist Entries 32
7.3.1 Querying Hotlist Entries 33
7.3.2 Editing a Hotlist Entry 34
7.3.3 Adding a Hotlist Entry Manually 34
7.3.4 Deleting a Hotlist Entry 35
7.4 Targets 35
7.4.1 Creating a New Target 36
7.4.2 Deleting a Target 36
8 Hotlist Formatters 37
8.1 Creating a New Formatter for Hotlists 37
9 Alerts 38
10 Dispatch 39
10.1 Dispatch Settings 40
10.2 Dispatch Hits 41
10.3 Dispatch Reads 41
10.4 Manual Entries 41
10.4.1 Adding a Manual Read 42
10.4.2 Correcting Reads 42
11 Querying Stored Data 43
11.1 Wildcards 43
11.2 Quick Search Bar 43
11.2.1 Quick Search Fields 43
11.3 Query Result Navigation Icons 43
11.4 Advanced Reads Queries 44
11.4.1 Performing an Advanced Reads Query 44
11.4.2 Entering Advanced Reads Query Criteria 45
11.4.3 Managing Query Results 46
11.5 Multiple Query Tabs 46
11.6 Cross-Referencing External Data 47
11.7 Working with Queried Reads. 48
11.7.1 Viewing Query Results 48
11.7.2 Query Results Actions 49
11.7.3 Viewing Read Details 49
11.8 Favorites 52
11.8.1 Creating a New Favorite 52
11.8.2 Activating a Favorite 52
11.8.3 Deleting a Favorite 53
12 Reports 54
12.1 Running a System Report 54
12.2 Viewing and Printing Reports 54
12.2.1 Viewing the Login Statistics Report 55
13 Client Tools 56
14 Archiving Data 57
15 System Settings 58
15.1 Sessions 58
15.1.1 Viewing and Disconnecting Sessions 58
15.1.2 Workstation Power Management and Sessions 58
15.2 Dispositions 59
15.2.1 Defining a New Disposition 59
15.2.2 Deleting a Disposition 59
15.3 System Parameters 60
15.3.1 Editing System Parameters 60
15.3.2 List of BOSS System Parameters 60
15.3.3 Branding 62
15.4 Roles 63
15.4.1 Adding New Roles 63
15.4.2 Deleting Roles 63

15.5 Report Management ... 64
15.5.1 Assigning Permissions to Access Reports ... 64
15.6 Translations ... 64
15.6.1 Entering a New Translation ... 65
15.7 Justifications ... 66
15.7.1 Entering a New Justification ... 66
15.7.2 Deleting Justifications ... 66
17 Appendix: Installation and Configuration Guide ... 67
17.1 Installing the BOSS Server Application Files ... 68
17.1.1 Running the Installer ... 68
17.1.2 PIPS License Agreement ... 69
17.2 BOSS Version 3.2 and Above License Key Management ... 70
17.2.1 Activating the License Key ... 70
17.2.1.1 Activating the License Key over the Internet ... 71
17.2.1.2 Activating the Software with a License File. ... 72
17.2.1.3 Request a License File to Activate the License ... 72
17.2.2 Updating a License Key ... 73
17.3 Map Display Options with BOSS ... 74
17.3.1 U.S. Census Bureau TIGER Maps ... 74
17.3.2 Advanced Mapping with Microsoft Bing Maps ... 74
17.4 Configuring the BOSS Server Application ... 74
17.4.1 The BOSS Controller Application ... 74
17.4.1.1 Starting the BOSS Controller ... 74
17.4.1.2 Status Colors ... 74
17.4.1.3 Right-Click Menu ... 75
17.4.1.4 Starting the BOSS Service ... 75
17.4.1.5 Stopping the BOSS Service ... 75
17.4.2 BOSS Configuration ... 76
17.4.2.1 Activating the Configuration Wizard ... 76
17.4.2.2 BOSS Configuration Wizard ... 76
17.4.2.3 SQL Server Configuration ... 77
17.4.2.4 Resetting the Administrator Password ... 78
17.4.2.5 Network Port Settings ... 78
17.4.2.6 Regional Hotlist Formatters ... 80
17.4.2.7 NCIC Hotlist Formatters ... 80
17.4.2.8 TIGER Maps Configuration ... 81
17.4.2.9 Finishing Configuration ... 81
17.5 Installing the BOSS Smart Client Application ... 82
17.5.1 Installation over the Web ... 82
17.5.2 Stand-Alone Installation ... 82
17.6 Configuring Client Tools ... 82
18 Troubleshooting ... 84
19 Appendix: Plug-Ins ... 87
19.1 The BOSS Truck Drayage Utility ... 87
19.2 The BOSS LPRD Plug-In ... 87
19.3 The BOSS DEA Plug-In ... 87
20 Appendix: BOSS Mantis ... 88
20.1 How Dose Mantis Work ... 88
20.2 Mantis Security and Encryption ... 89
20.3 Mantis Requirements ... 90
20.4 Mantis Installation ... 90
20.5 Mantis Configurations ... 90
20.6 Mantis Search Features. ... 91
20.6.1 Mantis Search Definitions ... 91
20.7 Additional Mantis Parameters ... 92
20.8 Mantis Configuration Troubleshoot ... 92
20.8.1 Mantis Log Messages Catalog ... 93
Glossary ... 95

1 INTRODUCTION

This document serves as a user's manual for the PIPS Back Office System Software (BOSS) version 3.5 or above and describes the various features and functionality of the application. BOSS is a management and administration tool for the PIPS Automatic License Plate Recognition (ALPR; also known as ANPR, or Automatic License Number Recognition) systems. The BOSS server application provides an interface for user maintenance, data queries, import and export of data, and dispatch functions. BOSS lets an Administrator specify the databases used by both mobile and fixed camera installations. BOSS retrieves these databases on a regular schedule; manages the users of the PIPS PAGIS systems and BOSS Smart Client workstations; provides a central repository for data collected by mobile PAGIS deployments and fixed camera installation; provides reporting and data management tools; provides hit detection and dispatch functions for fixed camera installations; and allows for data mining and data sharing with other agencies.

The following schematic shows how the BOSS server application works together with Smart Client workstations, various data sources, PAGIS, and the full line of ALPR cameras to create a comprehensive solution.



1.1 The Design of PIPS Back Office System Software Version 3.5 and Above

The design of BOSS version 3.5 or above offers ease of accessibility with a user-friendly look and feel. Large, easy-to-identify icons provide intuitive navigation, and the frequently used elements are readily available. The user interface (UI) is very recognizable and comfortable, particularly for users already familiar with Windows-based applications, including Microsoft® Office software, or the Mobile Pagis Software. In addition, users can enter a minimum amount of information to add a data object, with the ability to include more details if needed.

2 LOGGING IN

2.1. PIPS Back Office System Software Administrator Login

During each new installation of the PIPS Back Office System Software, a default user of “admin” is created, with the password of “admin1.” The installer or designated BOSS Administrator can log in with this account to create additional users and otherwise configure the system. It is important that the “admin” password be changed to protect the system’s security. Likewise, it is equally as important to keep this and all passwords confidential to protect the security of the BOSS system. Section 17, Installation and Configuration, offers more information on setting up users and passwords.

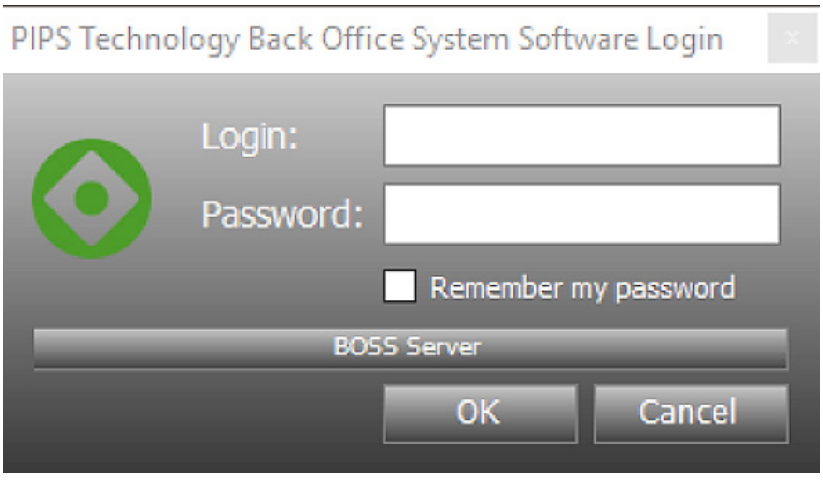
2.2 User Logins

The PIPS Back Office System Software will require a user to log in with a username and password only if there is no BOSS user matching the current Active Directory user login. In other words, if the username currently logged into Windows matches a username in the BOSS system, the user is automatically logged into the application when it is started, and no login screen will appear.

For example, if user “bsmith” is logged in using Windows Domain Authentication through Active Directory (“logged into Windows”), when the BOSS Smart Client is started, and a “bsmith” user exists within the BOSS system, no login screen will appear; the application will authenticate the user and load automatically. If a user logs onto Windows with a name that is not an exact match to a username in the BOSS system, or is not logged into the same Windows Domain, a login screen will appear. The user will then need to enter a correct BOSS user name and password in order to enter the application.

Note: In order for a user to be automatically logged into BOSS, the Active Directory user must be in the same Windows domain as the PIPS™ Back Office System Software server.

2.3 Login Dialog



1. Enter your username in the Login field.

2. Enter the correct password in the Password field.
Note: Passwords are case sensitive.

3. Click OK to complete the login process.

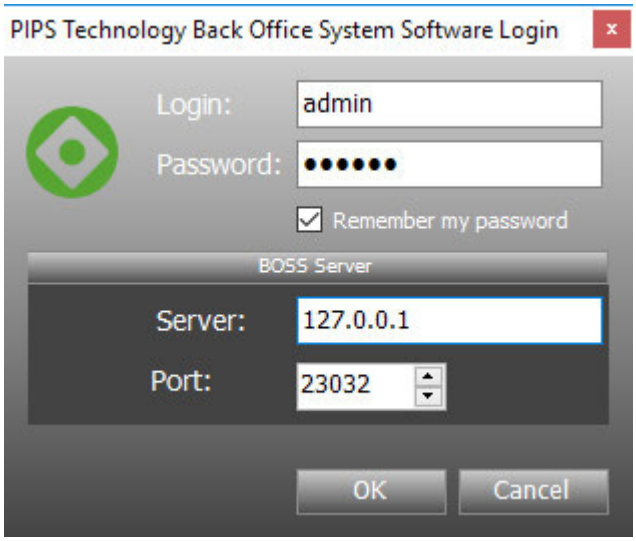
2.3.1 Storing Username and Password

Select the Remember my password option to save the password to the computer's local Windows registry and automatically fill in both Login and Password fields on subsequent logins.
Selecting this option only remembers the login information for the current Windows User on the local computer. It will not apply to a different Windows user logged in the same computer and will not apply to the same user logging in a different computer. This option need not be checked every time. Once checked, the option will stay that way until it is deselected during a login.

Note: The username and the password are stored in the Windows Registry. This can be a security risk. It is recommended that you not use the Remember my password option unless the Windows workstation can be secured against unauthorized access.

2.3.2 BOSS Client Connection Settings

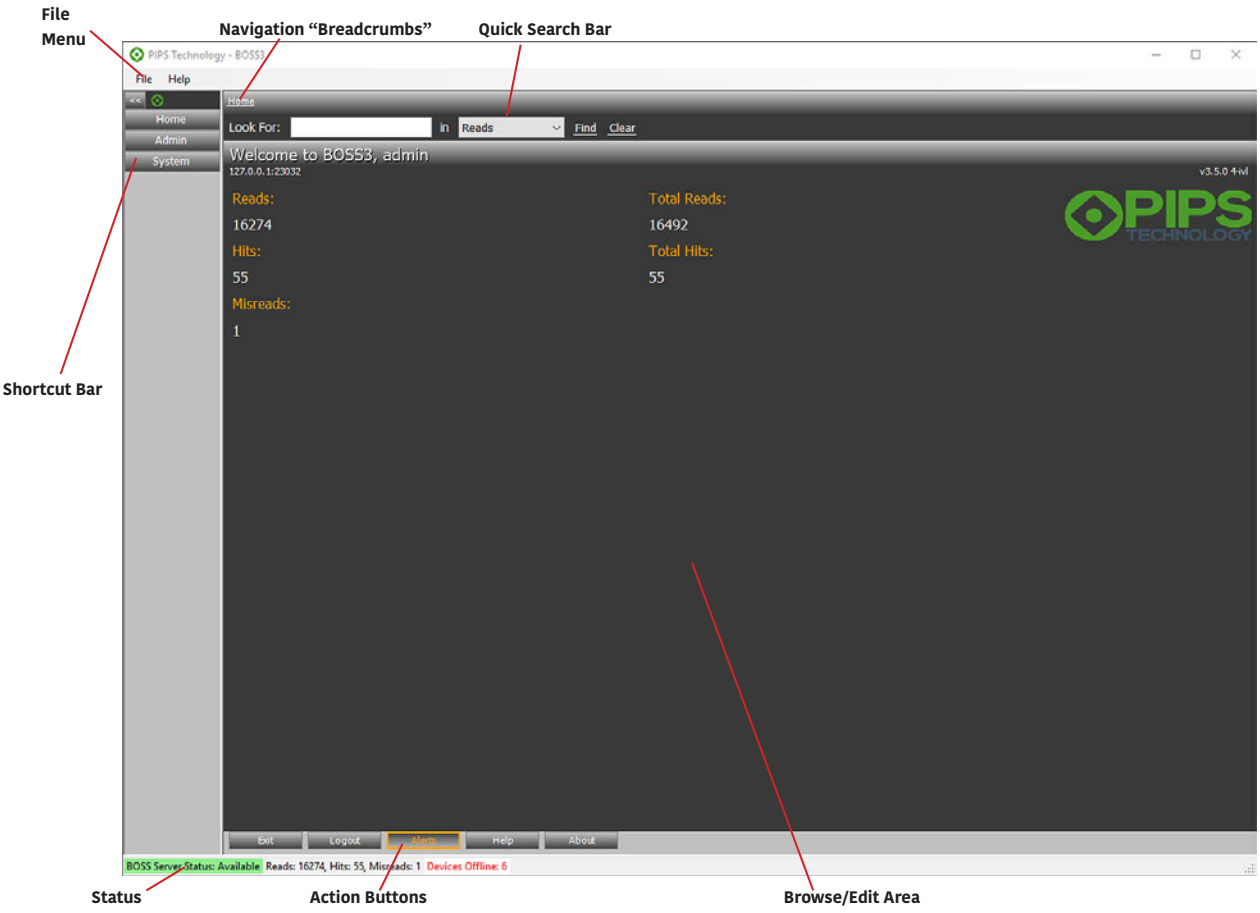
Click the BOSS Server button on the Login screen to view or change the client connection settings.



Server – IP address, computer name, or DNS address can be used in the Server field as long as the client can reach the server using the value entered.
Port – The default port used for connecting to the BOSS server is 23032. This should only be changed here if the BOSS server has been configured to use a non-default port.

3 APPLICATION LAYOUT

3.1 Components of the BOSS Application Screen



File Menu – The File menu of the application resides in the very top left of the application window. The File menu is always visible and available regardless of the screen or shortcut selected. The Exit option is available through this menu.

Navigation – The navigation "breadcrumbs" appear at the top of the BOSS screen as different actions are selected. By clicking on the links it is possible to backtrack to a previous screen.

Shortcut Bar –The Shortcut bar (the panel on the left of the screen) contains icon buttons for the various operations available. The shortcut icons are divided into three categories: Home, Admin, and System. Each time the application is started, all of the categories are closed with no shortcuts displayed. Click on any of the three headings to access the shortcuts within that category. The actual categories and shortcuts that appear depend on the logged-in user's privileges.

The Shortcut bar can be collapsed entirely to provide a larger space for the Browse/Edit area by clicking the << button at the top left of the screen. To expand the Shortcut bar again, click the >> button.

Browse/Edit Area – The widest portion of the application window, the Browse/Edit area is where data is displayed for viewing or editing. The actual data displayed here depends upon the shortcut icon that is selected from the Shortcut bar.

Quick Search Bar – Directly above the Browse/Edit Area, the Quick Search bar allows for simple, immediate queries of BOSS data. Using the Quick Search bar simply involves typing the text to query in the Look For field and selecting the type of data (reads, hits, etc.) to search in the drop-down box.

Action Buttons – These are the buttons directly below the Browse/Edit area. These buttons will differ depending on the shortcut icon selected. The actual buttons that appear will also vary depending upon the user's privileges.

Status Bar – This is the area along the very bottom of the application window that displays the following system information:

- **BOSS System State (Available or Offline):** "Available" status indicates that the client is currently communicating with the BOSS server application and the server is running. This status is highlighted with a green background. "Offline" status indicates that the client is currently not able to communicate with the BOSS server and is highlighted with a red background. In this event, the BOSS UI will continue to check for the BOSS server to become available again. After three attempts to reconnect, the user will be notified that the connection could not be re-established and will be provided further instructions on how to proceed.
- **Reads:** The total number of reads currently contained in the BOSS system.
- **Hits:** The total number of hits currently contained in the BOSS system.
- **Misreads:** The total number of misreads currently contained in the BOSS system.
- **Devices Offline:** The number of fixed camera devices that are currently identified as offline.

3.2 The BOSS Home Screen

The BOSS Home screen is displayed within the Browse/Edit area upon login. The top banner displays the username of the current BOSS user, the BOSS server address, and current system statistics. Statistics may take a few moments to update after login. The action buttons, described below, are displayed along the bottom of the screen. The actual buttons that display will vary depending upon the user's privileges.

Exit – Exit the BOSS application.

Logout – Log out from the current session to the Login screen.

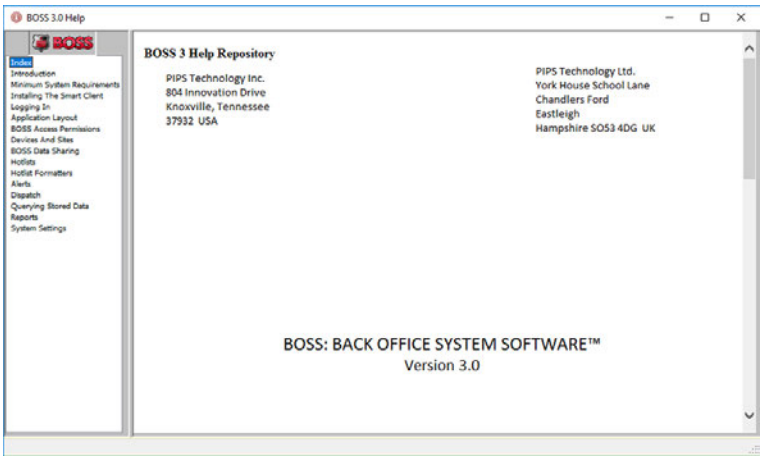
Alerts – Toggle dispatch alerts on (orange highlight) and off. This button will not be displayed if the user is not authorized to access the dispatch screen, or if the user has not chosen to receive dispatch alerts in Preferences (Section 5.3).

Help – Activate the help system.

About – Display application information.

3.3 Help Documentation

BOSS provides a help document accessible in the client application. To access help, select Help in the File menu area or press the F1 button. A help document will be displayed in a browser window and is indexed and searchable for ease of use.



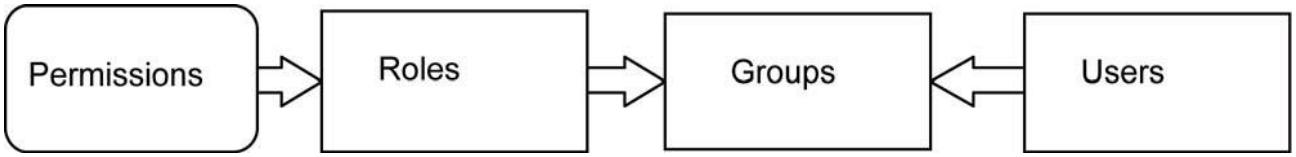
3.4 Minimizing the BOSS Application

The BOSS application can be minimized to the Windows System Tray using the Windows minimize button on the right upper corner of the BOSS application window. To restore the BOSS application, click on the BOSS PIPS icon. When the application is minimized, real-time alerts will still be displayed.



4 BOSS ACCESS PERMISSIONS: USERS/GROUPS/ROLES

Access permissions to various functions (such as reports or dispatches) in BOSS are administered through users, groups, and roles. Each individual who will use the BOSS software must log in via a user account. Each user account is assigned to a group. Every group is assigned a role (such as Administrator or Dispatcher), which determines the set of functionality to which the group's members will have access:



The security parameters defined in a role apply to a user via the group to which the user belongs.

4.1 Permission Levels

The following table lists the levels that apply to permissions:

LEVEL	EXPLANATION
No Access*	No permissions to the function
Read Only	View-only permissions to the function. Add/Change/Delete are not permitted.
Full Access	Complete permissions to the function. View/Add/Change/Delete are permitted.

**When a user's effective permissions to a function are No Access, the function is not visible to the user. For example, if a user has No Access privileges to the System function, the System category is not displayed.*

4.2 Permissions

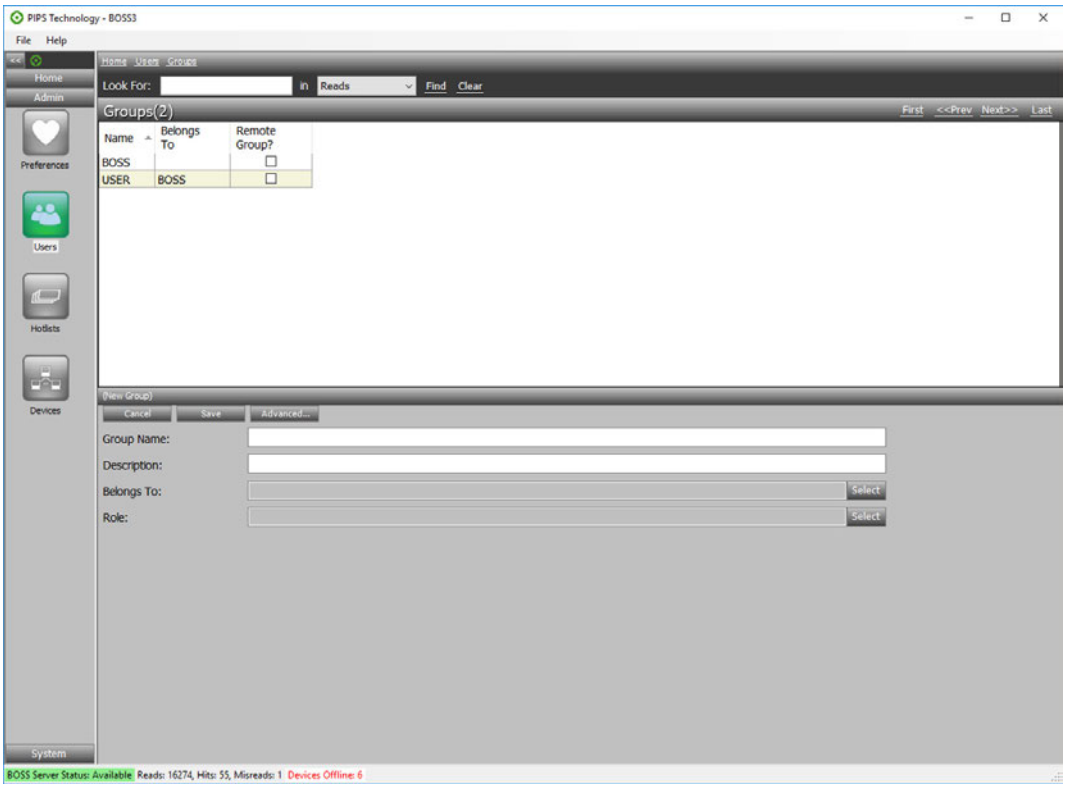
The following table lists the functions that are controlled by permissions levels:

PERMISSION	EXPLANATION
Reads	Plate read information
Dispatch	Real-time monitoring and hit alerts
Users	Groups and user accounts
Hotlists	Hotlists (plates of interest)
Devices	Sites and ALPR camera devices
System	System configuration options

See Section 15.4, Roles, for more information on setting permissions.

4.3 Roles

Roles are access permission profiles. BOSS comes with several predefined roles. A BOSS Administrator is able to add additional roles to the system. A BOSS Administrator is also able to alter and delete any roles. Roles define a permission level for different functions of the system. See Section 15.4, Roles, for additional information.



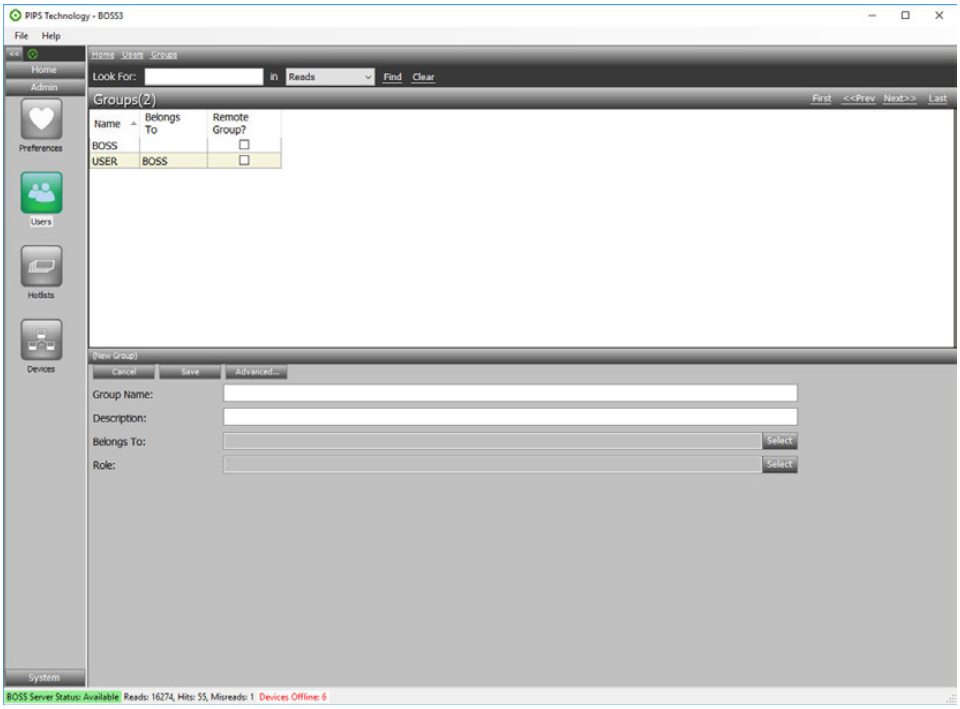
The following roles are installed by default in a BOSS system:

- System Administrators
- User
- Dispatcher
- Group Administrators
- Device Administrators
- Hotlist Administrators

See System Settings section for Role definitions and changes.

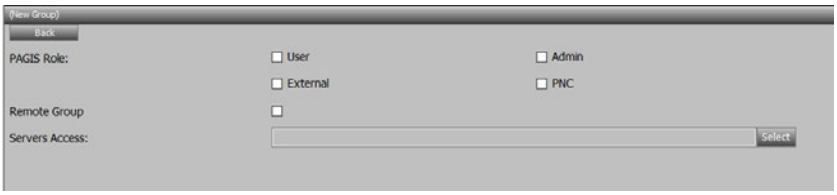
4.4 Groups

Groups are collections of users that have the same permissions. Groups provide an efficient way to organize users, for example by organizational units, and easily assign permissions to those users. Using groups is optional. A default group named “BOSS” automatically exists within a BOSS system, and user accounts will belong to the “BOSS” group by default. The BOSS group cannot be deleted.



4.4.1 Creating a New Group

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Users** shortcut. A list of all current users will display in the Browse/Edit area.
3. Click the **Groups** button at the bottom of the Browse/Edit area. A list of all current groups will display in the Browse/Edit area.
4. Click the **New** button. The New Group Entry screen will display.
5. In the Group Name text box enter a name for the group. (**Note:** The group name must have a minimum of three characters.)
6. In the Group **Description** text box enter a description of the group (optional).
7. Each group, except for the default BOSS group, is required to have a parent group. In the Belongs To field, click the **Select** button to view a list of all existing groups. Click on the desired group and click the **Save** button to select. The name of the selected group will display in the Belongs To field as the parent group.
8. Assign a role to the group. In the Role field, click the **Select** button to select from the existing roles. Click the desired role from the list and click the **Save** button to make the selection. The name of the selected role will appear in the field.
9. Click the **Advanced**... button to access additional, optional settings for the new group.



4.4.1 Creating a New Group (continued)

PAGIS Role (User/Admin/External/PNC) – Check desired PAGIS roles to grant the new group for the associated permissions in Pagis. Please refer to the Pagis User's Manual for more information.

Remote Group – Select this option to designate the group as remote. When a BOSS Administrator wants to give access to another BOSS system for remote queries ("data sharing," see Section 6), a login must be created and assigned to a group that is flagged as a remote group. The remote BOSS Administrator will then create a remote site with credentials for that login.
Servers Access – This option allows for defining which, if any, sites will be accessible by this group. Click the Select button to access a list of sites.

Note: There are two sites defined by default: Manual Entries and Unassigned. If no additional sites have been defined, only the default values are available in this field. Click each desired site and click the **Save** button to complete the selection process. If one site is selected the name of that system will appear in the Server Access field. More than one site can be selected.

Log Queries – This option, when selected, will result in the logging of all queries made by all users of the group. This information is then available via the audits report. **WARNING:** *This can potentially be a very large amount of data. Select this option with care.*

a. Configure these Advanced User settings as desired.

b. Click the **Back** button to return to the main New Group Entry screen

10. Click **Save** to complete creating the new group, or click **Cancel** to clear the new group.

4.4.2 Parent Groups

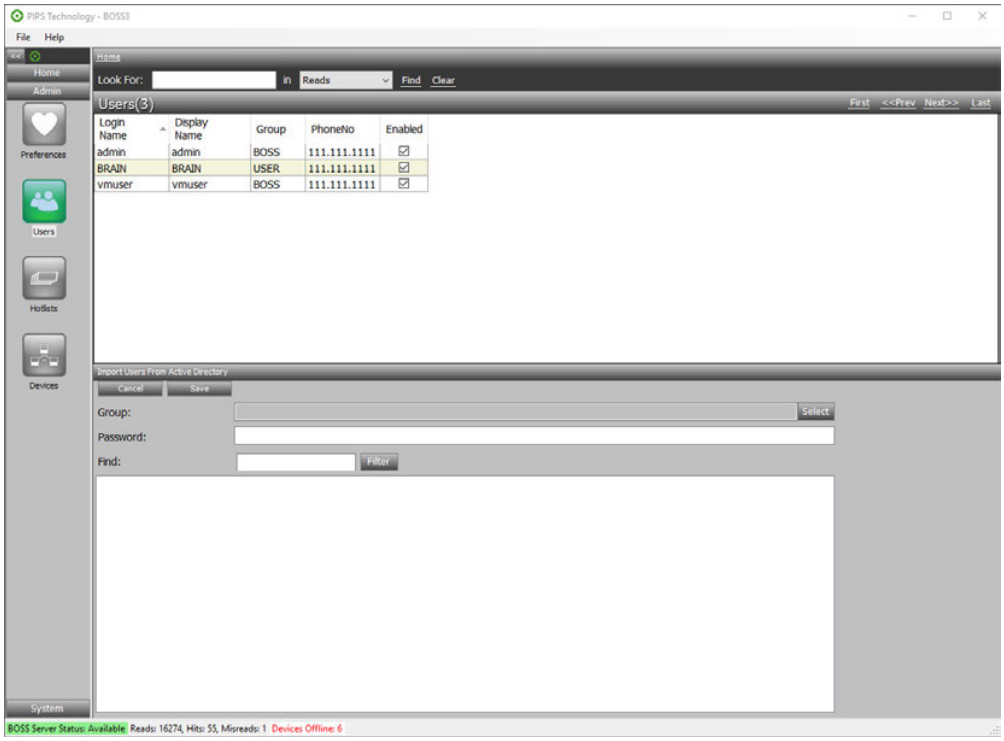
When creating a new group, you must select a parent group (the Belongs To field). BOSS uses a parent-child group structure as an organizational mechanism. This allows the BOSS Administrator to arrange groups into collections based on location, job role, or any other applicable criteria. In BOSS, the parent group can be selected in order to easily reach the entire collection of groups under that parent. This can be especially helpful in large installations with a large number of groups.

4.4.3 Deleting a Group

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Users** shortcut.
3. Click the **Groups** button at the bottom of the Browse/Edit area. A list of all existing groups will display in the Browse/Edit area.
4. Click to select the desired group from the list.
5. Click the **Delete** button.
6. Click **OK** in the confirmation dialog to complete the operation.

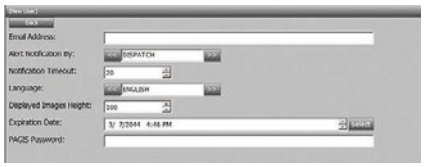
WARNING: Any users currently assigned to the deleted group will be assigned to the default "BOSS" group. You should empty the group by assigning all of its users to different groups prior to deleting it.

4.5 Users



4.5.1 Creating a New User

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Users** shortcut. A list of all existing users will display in the Browse/Edit area.
3. Click the **New** button at the bottom of the Browse/Edit area. The New User Entry screen appears.
4. Enter a **Login Name** for the new user. This is the name the user will enter when logging into the BOSS application. (The login name must be at least three characters.)
5. Enter a **Display Name** for the new user (optional).
6. Enter a **Password** for the new user. (The password must be at least six characters with one Cap, one number and one special symbol.) The strong password requirement cannot be disabled.
7. Select a **Group** for the user. Click the **Select** button to access a list of all groups. Click on the desired group and click the **Save** button to complete the selection.
8. Enter a contact **Phone Number** for the user (optional). This field is for informational purposes only; in case the BOSS Administrator needs to contact the user.
9. Click the **Advanced**... button to access additional, optional settings for the new user. Configure these advanced user settings as desired.



4.4.1 Creating a New Group (continued)

Email Address – Email address or addresses associated with the user. BOSS alerts for the user are sent to the email addresses specified here. Multiple addresses should be separated with a comma.
Alert Notification By – A user can be configured to receive BOSS alerts through the Dispatch application, email, or both. Click the <<
or >> buttons to cycle through the options, stopping at the desired selection.
Notification Timeout – The cutoff time from the time when a hit occurred after which an alert will no longer be sent to the user. For example, if the notification timeout is 20 minutes and a plate of interest is detected at 12:00 pm, notification is not sent to the user after 12:20 pm. This timeout prevents alerts being sent for events that are delayed in arrival to BOSS.
Language – The language preference for the user. The default value is English.
Displayed Images Height – This setting defines the vertical size in pixels of the images (reads and hits) that will display for the user on the Dispatch and Reads screens.
Expiration Date – Date for the user account to automatically be disabled. If no expiration is desired, simply leave this field at its default value (30 years from current date).
PAGIS Password – The user's Pagis password. Strong password requirement not utilized for this field.

Note: The user must be in a group that has been granted PAGIS permissions in order for the user to log in to PAGIS.

---

10. Click the **Back** button to return to the main New User Entry screen.
11. Click the **Save** button to complete creating the new user.

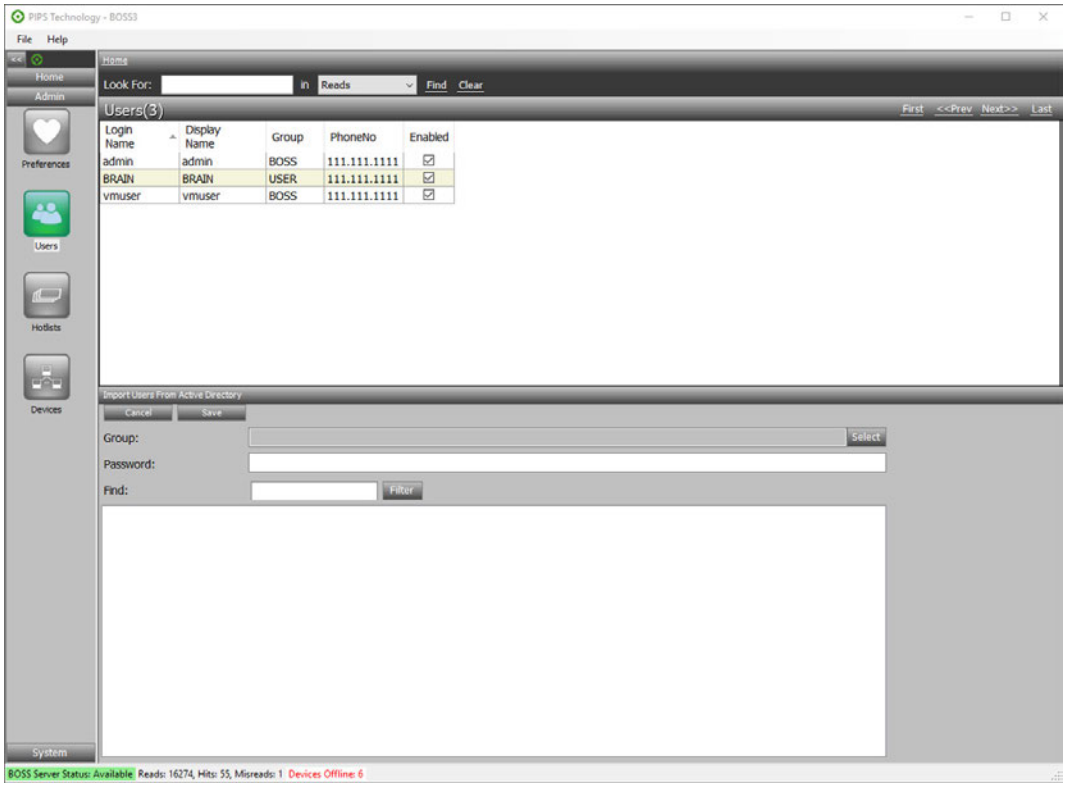
4.5.2 Deleting a User

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Users** shortcut. A list of all existing Users will display in the Browse/Edit area.
3. Click the desired user in the list.
4. Click the **Delete** button at the bottom of the Browse/Edit area.
5. Click **Yes** to confirm the operation.

4.5.3 Importing Users from Active Directory

BOSS allows user logins to be imported from Microsoft Active Directory (AD) service.

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Users** shortcut.
3. Click on the **Import** button.



4. Select the BOSS group that will receive the imported logins. Click the **Select** button to display available groups and **Save** to commit the selection.
5. Enter the default password for the imported logins in the Password field.
6. Browse for the desired users, **or** type in the desired login name (full or partial) in the Find field and press the **Filter** button.
7. Click on the checkbox in front of the desired usernames to select users to be imported to BOSS.
8. Click on **Save** to import the users from Active Directory.

Note: A Windows login cannot have any punctuation included or problems will occur with reads queries being performed.

4.6 Access Permissions Example

The previous sections have described how BOSS user security is designed, using roles, groups, and user accounts. This section presents a working example that integrates the information in this chapter.

A BOSS Administrator creates a role, names the role “Temporary Workers,” and defines the new role to have very limited permissions, as follows:

Reads	Read Only
Dispatch	Read Only
Users	No Access
Hotlists	No Access
Devices	No Access
System	No Access

Then the Administrator creates a group called “Temps.” When creating the group, a role is required. The Administrator selects the new role just created “Temporary Workers,” which assigns the permissions, defined above, to the new group.

Next, the Administrator creates a user account, “Jsmith,” for a temporary worker. While creating the new user, the Administrator is required to select a group for the user, and assigns the user to the “Temps” group just created. The user “Jsmith” has now been created with the permissions shown above because he belongs to the group called “Temps” and that group was assigned the “Temporary Workers” role.

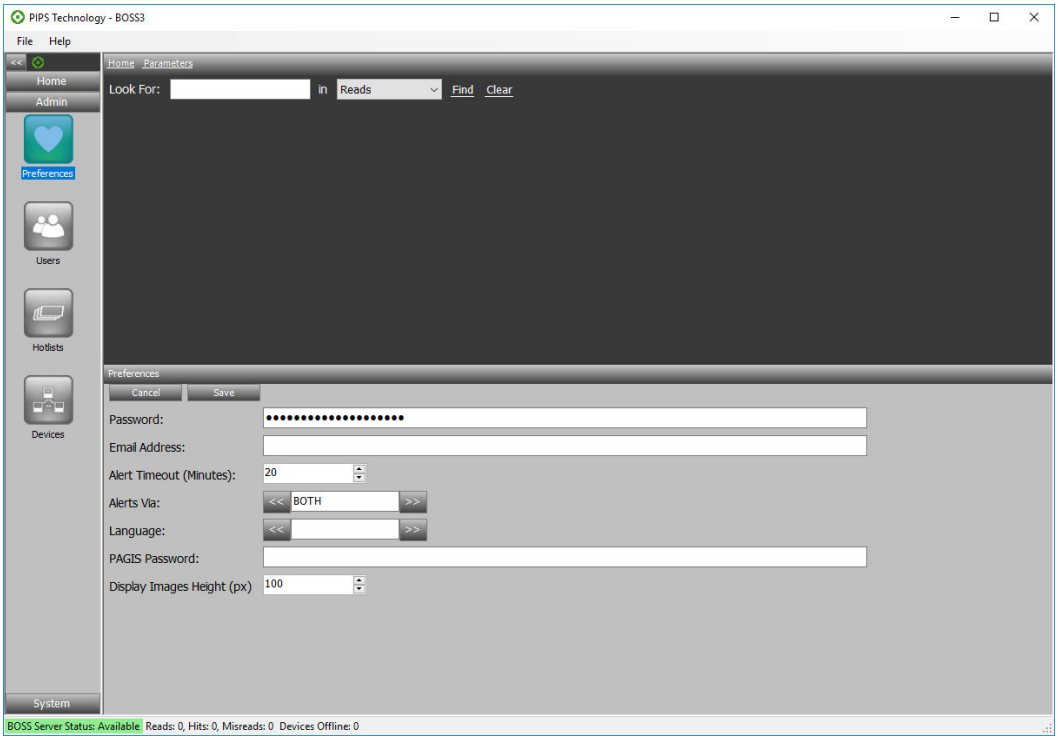
As this example shows, this security design allows reusability of security roles because a BOSS Administrator can define a set of permissions in a role, and that role can be assigned to multiple groups.

4.7 Preferences

The Preferences section allows for changing settings for the currently logged-on BOSS user, such as the password and email addresses.

4.7.1 Changing User Preferences

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Preferences** shortcut. The Preferences Entry screen appears at the bottom of the Browse/Edit area.
3. Modify the preferences settings as desired and click the **Save** button.



Password – Login password for the BOSS user. For security purposes, the existing password does not display on screen.
Email Address – Email address or addresses associated with the user. BOSS alerts for the user are sent to the email addresses specified here. Multiple addresses should be separated with a comma.
Alert Timeout (Minutes) –The cutoff time for older hits to alert the user.
Alerts Via – A user can elect to receive BOSS alerts through the Dispatch screen, emails, or both.
Language – Language preference for the user. The default value is English.
PAGIS Password (PAGIS Password) – The Pagis Software password for the user.

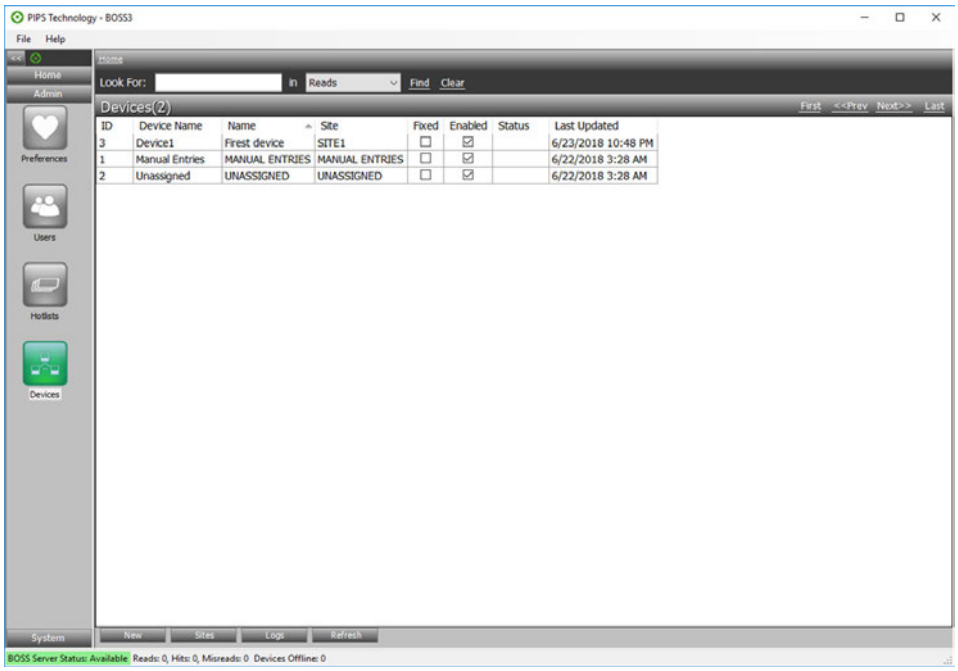
Note: The user must be in a group that has been granted PAGIS permissions in order for the user to log in to PAGIS.

Display Images Height (px) – This setting defines the size in vertical pixels of the images (reads and hits) that will display for the user in the Dispatch and Reads Query sections.

5 DEVICES AND SITES

5.1 Devices

A BOSS device is any source that can input reads into the system. Typically, a device is a camera—either fixed or mobile. Another source for reads is manual entry, in which a BOSS user types the information for a read into the BOSS Dispatch screen .A new BOSS installation automatically contains two default devices, Manual Entries and Unassigned. A BOSS Administrator creates additional devices applicable to his/her organization.



5.1.1 Device Status

To see the current devices in your system with information about their status:

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Devices** shortcut.

The devices will be listed in rows with the following column headings:

Device Name – The name assigned to the device, used in the device selections and is the description of the device. The list will always include Manual Entries and Unassigned.

Name – The name that is given to the device.

Site – The group of devices to which this device belongs. Sites can be grouped by geographical location or other criteria.

See Section 5.2, Sites.

Fixed – This box will be checked if the device is fixed camera, rather than a mobile camera. Enabled – This box will be checked if the device is currently enabled (see Section 5.1.4). Status – The Status field can display the following messages:

Device Added – If the device is newly added to the list, this message will display.

5.1.1 Default Devices (continued)

Offline – This device is a previously connected fixed camera that is not currently connected to BOSS.
Online Heartbeat – BOSS has detected a ping from a fixed camera.
Online Synced – The device's connection with BOSS has been established. This is shown for PAGIS mobile devices only and may not change when the device is offline.
Updated – Information has been sent from BOSS to the device, and the device is up to date.
Received Logins – Updates to the device included logins that were successfully sent to the device.
Received Source – BOSS has found the hotlist source file that it needs in order to send the updated hotlist to the device. Received Source may not be displayed due to timing or events.
Received Hotlist – The hotlist scheduled to be successfully sent has been sent to the device.
Received Hotplates – BOSS is sending "pages" of hotplates for a large hotlist, and the last page was successfully received.
Received Targets – The update to the device included targets that were successfully sent.

5.1.2 Defining a Device

Note: Devices will be defined automatically when a PIPS device, such as an ALPR camera, connects to BOSS the first time. Normally, there is no need to define devices in advance.

---

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Devices** shortcut. A list of existing devices will appear in the Browse/Edit area.
3. Click the **New** button.
4. Enter a name for the new device. (The name must be at least three characters long.) Note that the name **CANNOT BE CHANGED** once the device has been created.
5. Enter a **Description** for the new device. (The description must be at least three characters long.)
6. Select **Mobile** or **Fixed** in the Type field. By default, **Fixed** is selected. To change the current selection, click the **left** or **right** arrow.
7. Select a **Site**. Click the **Select** button next to the Site field to display a list of all available sites. Click on the desired site in the list and click the **Save** button.

Note: In addition to the two default sites, Manual Entries and Unassigned, which are created automatically when a new BOSS system is installed, other sites can be created by an authorized BOSS user. See Section 5.2, Sites, for more information.

---

8. Select **Owners**. Owners are groups that can access this device. For PAGIS units, user logins are sent only to devices where the group is an owner of the device. Click the **Select** button next to the Owners field to display a list of all BOSS groups. Select each desired group by clicking the checkbox. When the desired groups are selected, click the **Save** button. The group name(s) selected will be displayed in the Owners field.

9. Select **Latitude** and **Longitude** values for the geographical location of a device by typing in a value or using the up and down controls on each field to increase or decrease the value. Note that some devices, such as PAGIS units with a GPS attached, will automatically send the latitude and longitude of the device to BOSS.
10. Click the **Advanced** button to display additional options for the device.
    No Reads Alert – Defines how long the device must remain with no reads coming in before the system shows the device as offline.
    Alert Email – The email address or addresses to which alerts associated with this device should be sent.
    Retain Reads – The length of time that reads from this device should be saved in the BOSS database. The Retain Reads setting must be longer or equal to the Retain Images setting.
    Retain Images – The length of time that pictures captured by this device should be saved in the BOSS database.
    Retain Hits – The length of time that hits captured by this device should be saved in the BOSS database.
    SpikeStore – The PIPS High Resolution ANPR/ALPR Camera P382 and the PIPS Compact ANPR/ALPR Camera P372 (formerly the Spike P382 and P372 cameras) allow captured images to be stored in an on-board USB flash drive to be retrieved on demand. Setting a device as a SpikeStore device causes BOSS to attempt to retrieve images from the storage device when the read is requested for viewing.
11. When Advanced Options have been set as desired, click **Back** to return to the New Device screen.
12. Click the **Save** button to complete creation of the new device. The new device will now appear in the devices list above.

5.1.3 Editing a Device

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Devices** shortcut. A listing of all devices appears in the Browse/Edit area.
3. Click the desired device to select it. Details for the selected device appear in the Browse/Edit area.
4. Click the **Edit** button.
5. The Device Edit screen appears in the lower portion of the screen.
6. Modify fields as desired and click the **Save** button.

5.1.4 Enabling and Disabling a Device

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Devices** shortcut. A listing of all devices appears in the Browse/Edit area.
3. Click the desired device to select it. Details for the selected device appear in the Browse/Edit area.
4. Click the **Edit** button.
5. The **Device** Edit screen appears in the lower half of the screen.
6. Click the **Disable/Enable** button. The change will immediately close the edit window and return to the Devices screen. It will also take effect immediately.

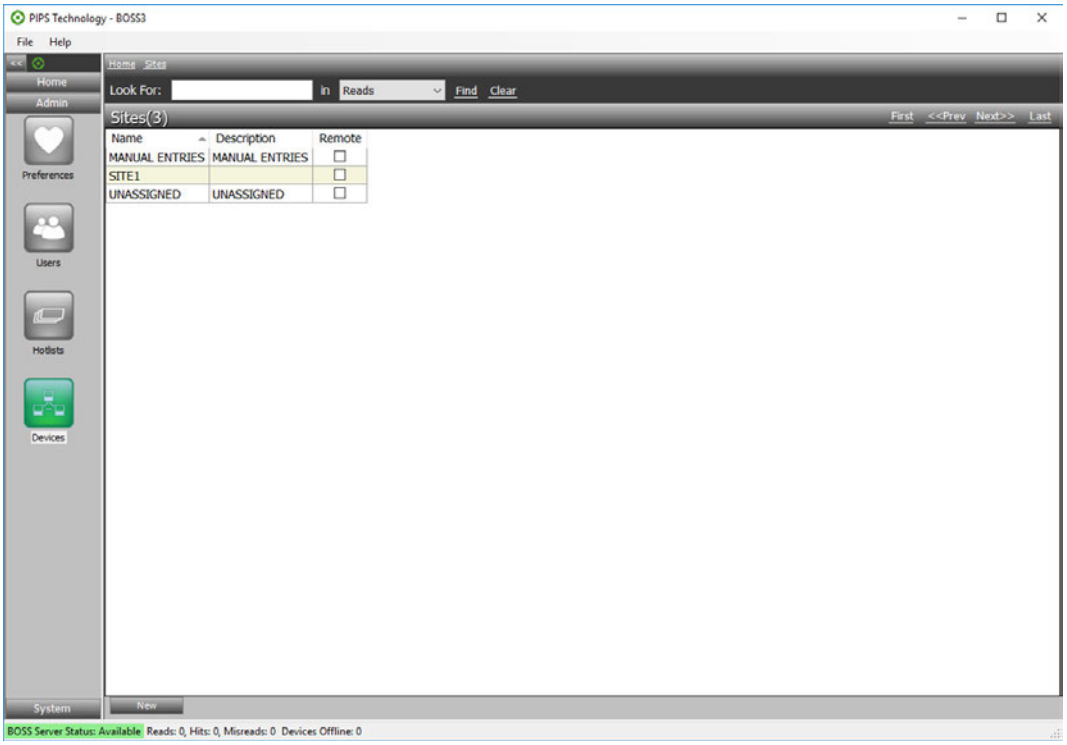
5.1.5 Deleting a Device

Note: It is strongly recommended that **devices are never deleted.** If a device is deleted, queries can no longer be performed using the device as a criterion. Instead of deleting a device, it should be disabled or given a new description.

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Devices** shortcut. (A listing of all existing devices will display in the Browse/Edit area).
3. Click the desired device in the listing.
4. Click the **Edit** button.
5. Click the **Delete** button at the bottom of the Browse/Edit area.
6. Click **Yes** to confirm the operation.

5.2 Sites

A site is a mechanism for organizing devices. This allows a BOSS Administrator to arrange devices into groups according to convenience, such as geographical area or a facility. The ability to group or arrange devices can be quite useful in large installations where there are many devices. Each device created must be assigned to a site.



5.2.1 Default Sites

A new BOSS site automatically contains two default sites, Manual Entries and Unassigned. Normally, a BOSS Administrator will want to create additional sites applicable to an organization.

5.2.2 Creating a Site

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Devices** shortcut.
3. Click the **Sites** button at the bottom of the screen. A list of existing sites will appear in the Browse/Edit area.
4. Click the **New** button at the bottom of the screen.
5. Enter a name for the new site. (The name must be at least three characters long.) Note that the name cannot be changed once the site is created.
6. Enter a description for the site. (The description must be at least three characters long.)
7. Select the parent site for the site. BOSS allows organizing sites into tree-like hierarchies. Click the **Select** button next to the Belongs To field, and select one site from the list. Click the **Save** button to complete the selection. The site name will appear in the Belongs to field.
8. Check the **Remote** option to designate the site as a remote site. (Remote sites are explained in Section 6, BOSS Data Sharing.)

5.2.3 Deleting a Site

Note: It is strongly recommended that sites are never deleted. If a site is deleted, queries can no longer be performed using the site as a criterion. Instead of deleting a site, it is recommended that devices assigned to it should be moved to another site.

---

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Devices** shortcut. A listing of all existing devices will display in the Browse/Edit area.
3. Click the **Sites** button at the bottom of the screen. A listing of existing sites will appear in the Browse/Edit area.
4. Click the desired site in the listing and click the **Edit** button.
5. Click the **Delete** button at the bottom of the Browse/Edit area. Click **Yes** to confirm the operation.

6 BOSS DATA SHARING

BOSS allows "linking" of multiple BOSS systems for data-sharing purposes. When a user issues a query from the Smart Client application that includes a remote site, the query is submitted to the local BOSS server, which in turn makes a query to the remote BOSS server(s). The combined results from all the sites are then returned to the Smart Client. **Data from remote sites is not stored in the local BOSS server.**

The following configuration steps need to be taken to permit BOSS data sharing:

6.1 Configuring BOSS to Allow Remote BOSS Queries

1. Create a BOSS user for remote access. This user account is a "proxy" the local BOSS server will use for all requests from a remote site. This user account will have "Reads" privileges by default; no other privileges need to be given. The user must be assigned to a remote group. (See Section 4.4, Groups, for information about flagging a group as remote.)
2. Give the username and password for this "proxy" user to the BOSS Administrator at the remote BOSS system. The remote BOSS will need to be configured to access this BOSS system, described in the next section.

Note: It is best to create a dedicated user account for remote sites—one that will not be used by an actual user to log in and access the application.

6.2 Configuring BOSS to Access a Remote BOSS Server

1. Obtain username and password from BOSS Administrator at the remote site.
2. Create a site for the remote BOSS server and select the **Remote** option.
3. Enter the remote site IP address and BOSS service port (23032 by default).
4. Add the username and password provided.
5. For each group that is allowed to query the remote BOSS server, assign the remote server to the user via the **Servers Access** option. (See Section 4.4, Groups, for information on selecting Servers Access.)
6. Log out of the application.
7. Log back on using the provided username and password. The Remote BOSS server can then be queried by selecting the desired servers in the Reads Query screen.

Note: BOSS version 3.2 and above only supports data sharing with servers running BOSS 3.0 and above.

---

7 HOTLISTS

A hotlist is a database that contains license plates of interest. When reads from license plate readers arrive at the BOSS server application, they are compared against hotlist records to find matches. Various hotlists can be enabled on a BOSS system and used in this comparison. In addition, hotlists can be assigned individually to specific devices. Only reads from those devices will be compared against these hotlist records. Typical hotlists include stolen vehicles, amber alerts, wants and warrants, etc. When the system reads in a plate that is determined to be a match to a hotlist entry in a hotlist, the BOSS application informs the user either with an alert sound and a pop-up window displaying a picture of the vehicle, or via email, depending on the user's preferences (see "Alerts via" in Section 5.3, Preferences).

A hotlist can be a database imported from an external source, such as another law enforcement agency. It can also be a list created by the local BOSS Administrator. For the BOSS server application to be able to understand how to import the hotlist records into the database, there are three different format types that exist in a BOSS system. In addition, there are several specific formats that are pre-defined and available by default when a new BOSS system is installed (see Section 8, Hotlist Formatters).

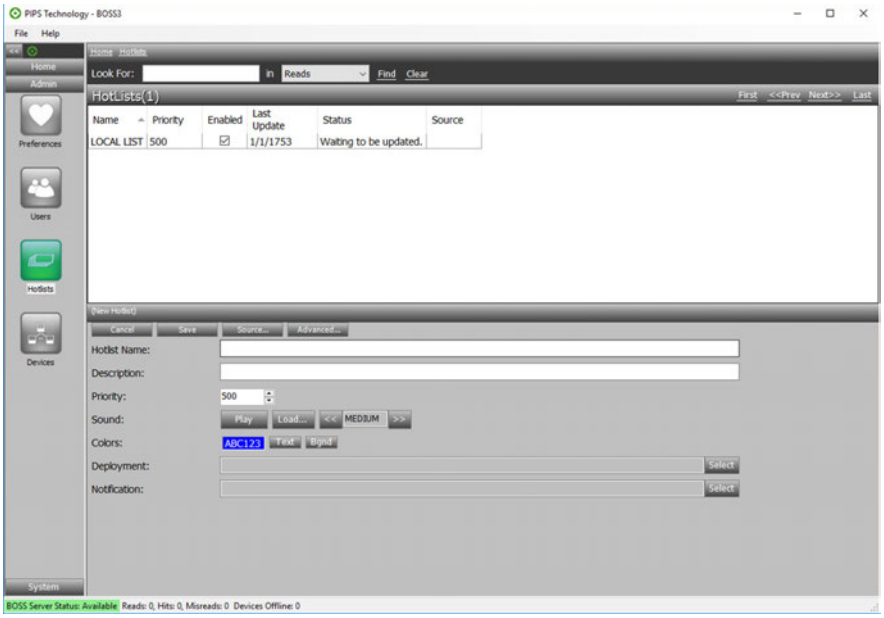
7.1 Creating a New Hotlist

There are three general areas to complete when creating a new hotlist:

- Configure basic settings
- Define a source file location with credentials when necessary.
- Define advanced settings (optional).

7.1.1 Configuring Basic Hotlist Settings

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Hotlists** button. Currently existing Hotlists appear in the Browse/Edit area.
3. Click the **New** button at the bottom of the Browse/Edit area. The New Hotlist Entry form appears.



4. Enter a **Hotlist Name** for the hotlist. It must be at least three alphanumeric characters, and it cannot be an existing hotlist name.
5. Enter a **Description** for the hotlist (optional).

6. Select a **Priority** for the hotlist. When there are multiple hits/alerts, the priority determines which alert will occur first. (The lower the number, the higher the priority.)
7. Select a **Sound** for alerts resulting from this hotlist (optional). Click the **Load** button to select a wave sound file (*.wav). To test the selected sound, click the Play button. Optionally, one of the three default sounds may be selected, **Low, Medium**, or **High** alert.
8. Select **Colors** for the alert if desired (optional). The default is white text on a royal blue background. Custom color settings affect the entries in dispatch. The background color also applies to alerts given in PAGIS.
9. Click the **Text** button to select a color for the text.
10. Click the **Bgnd** (Background) button to select a color for the background.

Note: Currently selected text and background colors are displayed in the sample box (showing "ABC123").

---

11. Select devices for **Deployment**. Click the **Select** button to select devices from the list of those currently available. Click the checkbox next to a device in order to select it. When desired devices are checked, click the **Save** button to make the selection. One or more devices can be selected, and they will be displayed in the Deployment field.

Note: Deployment means distributing the hotlist to a device or devices. Only the devices where a hotlist is deployed will produce hits from the hotlist.

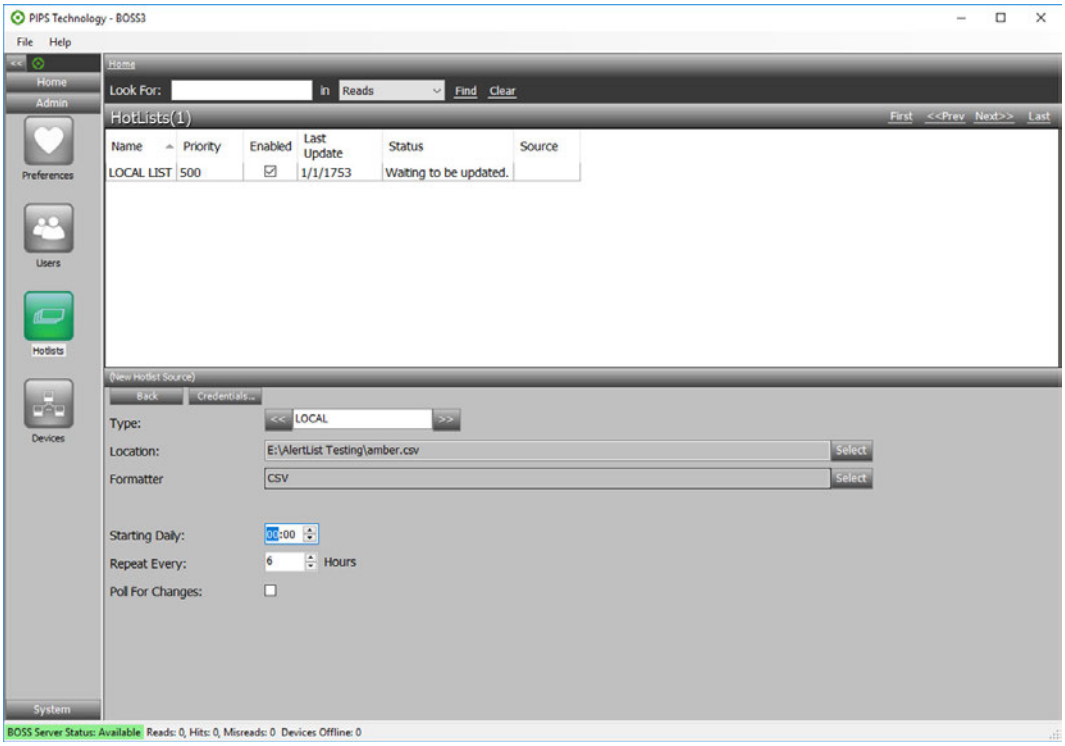
---

12. Select groups for Notification. Click the **Select** button to see a list of all BOSS groups. Click the checkbox next to a group to select the group. When you select a parent group, child groups are automatically selected. When desired groups are checked, click the **Save** button to make the selection.

Note: In order to receive alerts for hits on the hotlist, the user must be in the notification list of the hotlist. For more information see Section 7.1.5, Defining Hotlist Advanced Options.

7.1.2 Defining the Hotlist Data Source

1. On the New Hotlist Entry screen, click the **Source**... button to open the screen shown in the lower half of the following image:

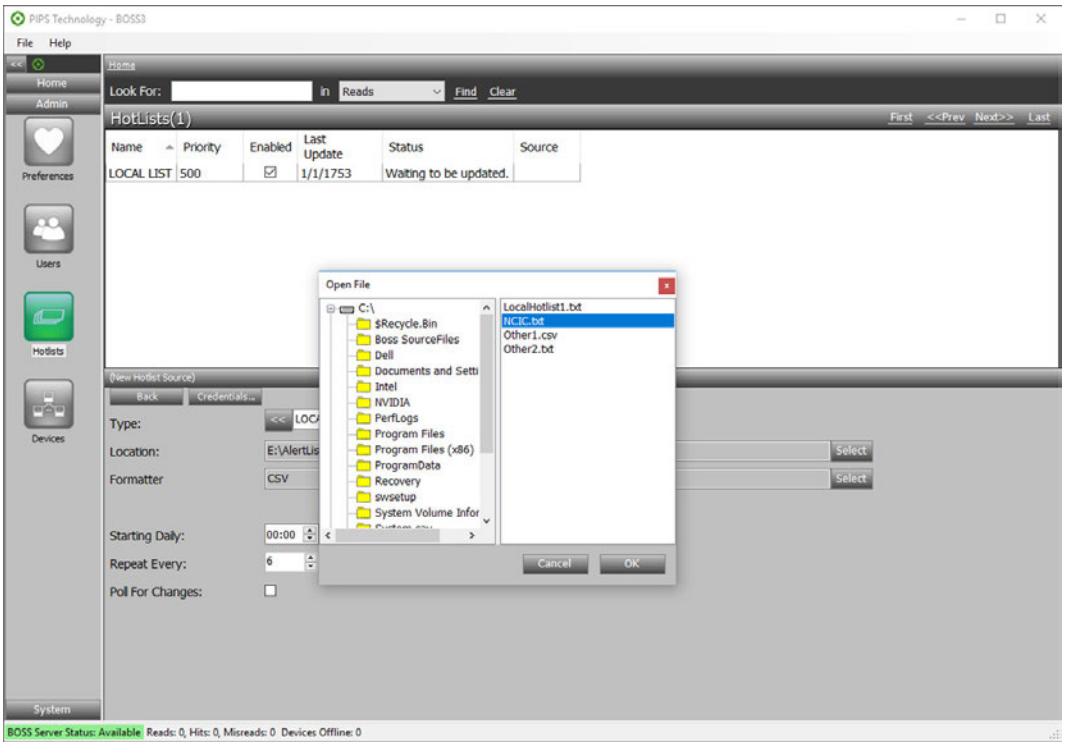


2. Choose the appropriate entries for each of the fields that describe the new hotlist:
   Type (**Network** or **Local**) – A local source means that the file is stored on the BOSS server's Windows file system. A network source means that the hotlist source resides outside the BOSS server.

Note: If a Local source is selected, the source file location (folder) must be accessible to the Windows process running the BOSS server application ("PIPS BOSS3" Windows service).

Location – Enter the location of the hotlist file. Click the **Select** button to the right of the location field.

For a local source, a file dialog will display, allowing you to navigate to a path and select a file.



For a network source, select one of the default locations displayed (if applicable), **or** type in the location of the source:

HTTP – The location format must be in Hypertext Transfer Protocol (HTTP) format: “http://server:port/path.” There are a few predefined HTTP locations (such as CA DOJ) included in BOSS. These locations can be accessed with the **Select** button. Boss also supports FTP & SFTP, examples : “ftp://server:21/path” , : ftp://server:22/path.

Remote BOSS System – The location format must be “boss://server:port/hotlist,” where “hotlist” is the hotlist name on the remote system.

Note: The remote system hotlist name **MUST** be alphanumeric and **CANNOT** contain any spaces.

Formatter – Formatter defines the way a hotlist database file is parsed into discrete fields. Click the **Select** button next to the Formatter field. A list of available formatters appears. Click on the desired formatter and click the **Save** button to make the selection. The name of the selected formatter will appear in the field.

Note: Normally one of the several default formatters included with BOSS is sufficient. A new custom formatter can be created if necessary. See Section 8.1, Creating a New Formatter for Hotlists, for more information.

7.1.2 Defining the Hotlist Data Source (continued)

Starting Daily – Specify the time of day the hotlist should begin updating each day. The time is formatted as hours:minutes in the 24-hour clock, i.e., between 00:00 and 24:00 can be selected.
Repeat Every – Specify the time interval, in hours (1 – 24), between updates.

OR

Poll for Changes – If you choose this setting, BOSS will check for updates to the hotlist approximately every 30 seconds. When this option is selected, the **Starting Daily** and **Repeat Every** options are disabled.

Note: If **Poll for Changes** is selected, and the hotlist source resides on the network, BOSS will attempt to make a network connection every 30 seconds. This frequency may add significantly to network traffic. Use with caution.

7.1.3 ZIP Compressed Hotlist Files

BOSS will automatically recognize and extract a hotlist data file contained in a ZIP archive file, such as Windows Explorer compressed (zipped) folder.

Note: There can be only one file in the ZIP archive.

7.1.4 Defining Hotlist Source Credentials

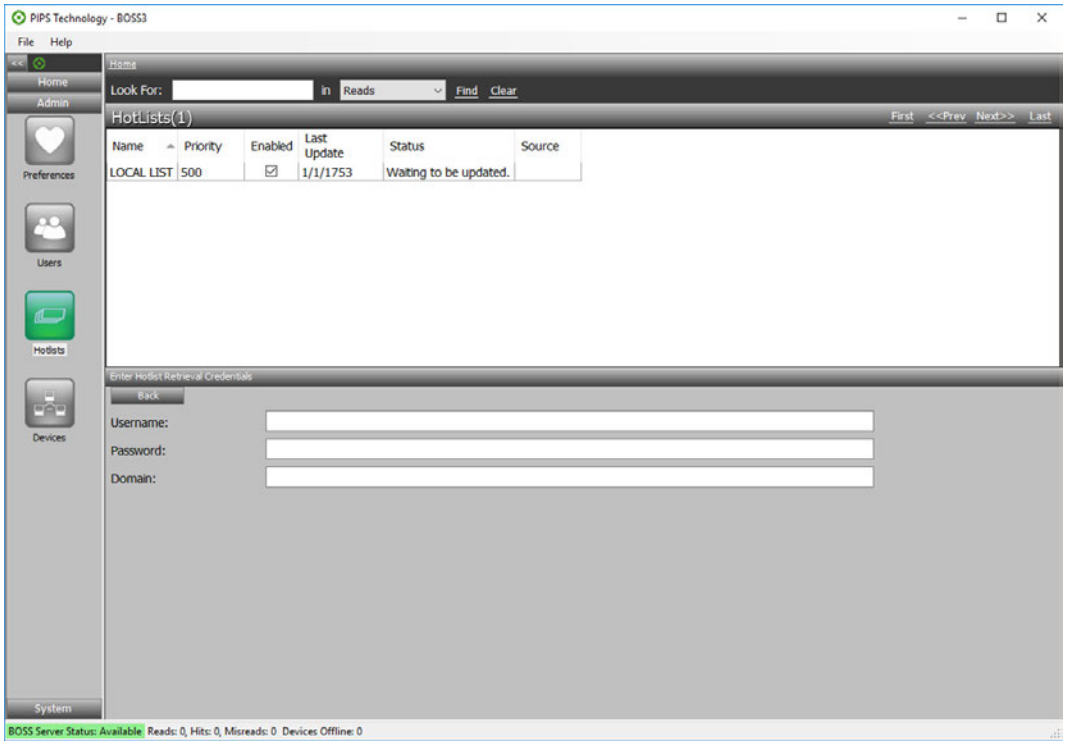
Some sources will require credential settings (e.g., login information) in order to allow BOSS to access that data. To enter the **Credentials** Settings screen from the Hotlist Source screen, click the Credentials button.
The credentials depend on the source type as follows:

Network-HTTP – If the HTTP (website) source defined requires login information, it should be entered in the Credentials Setting screen. This information will include username and password. The domain field may be necessary as well. Consult the Administrator of the HTTP source for required login information.

Network-Remote BOSS system – A username and password valid on the remote BOSS system must be entered (as in remote sites configuration, described in Section 6.0, BOSS Data Sharing). Consult the Administrator of the remote BOSS system for a username and password.

To set credentials for a source:

1. Click the **Credentials** button. The Credential Input screen appears.
2. Enter the username, password, and domain information applicable to the source you are specifying.
3. Click the **Back** button to return to the Source Entry form.
4. Click the **Back** button again to return to the New Hotlist Entry screen.



Advanced Options are values that allow you to further define details of the new Hotlist. To access the Advanced Options, click the **Advanced**... button.

Covert – A covert hotlist is one that contains sensitive information that should only be available to certain user groups. The effects of defining a hotlist as covert are as follows:

- A Hit on covert hotlist will not be alerted to users in mobile vehicle “Pagis”, unless the logged-in user is a Pagis administrator.
- A hit on the covert hotlist will not be alerted in the Boss application, regardless of the user’s alert preference. Hit alerts for covert hotlist can be send via email.
- When reads are queried, git information on covert hotlist will be displayed only to users in the Notification list for the hotlist. Other users will see that the read is a hit, but no information will be shown.
- Hit information for hits from covert hotlist will not be sent to remote Boss servers.

Whitelist – This option, when selected, defines the hotlist to be a whitelist, which works in reverse to a normal hotlist. A whitelist defines a list of plates that are **authorized** and not of concern. When a whitelist is active, license plates read that do **not** match an entry on the list will trigger a hit/alert.

7.1.5 Defining Hotlist Advanced Options (continued)

An example of whitelist use might be a secure parking lot where fixed camera devices are monitoring vehicles entering. Authorized plates will match entries in a whitelist hotlist. If a plate is read that does not match an entry in the whitelist, an alert occurs.

Whitelists and hotlists can be active simultaneously for a device.

Note: Whitelist support in PAGIS requires a separate license. If you do not have the license and wish to use whitelists, please contact your PIPS sales representative for further information.

Ext Trigger – This option, when selected, sets the External Trigger flag on a hotlist when it is passed to PAGIS. It is only supported in PAGIS version 2.6.6 or above and will have no effect on earlier versions of the software.
One Time – This option, when selected, specifies that the hotlist data should only be accessed from its defined source one time; no subsequent updating will occur after the initial import.
Alert Timeout – This setting allows you to define how current a hit (from this hotlist) must be in order to cause an alert. This primarily pertains to information coming in from mobile units, where there may be a large delay. Alert Timeout can be specified in minutes, hours, days, or months.
Delete Inactive – BOSS updates hotlists in an incremental manner, and instead of deleting hotlist entries that no longer exist, non-existent entries are marked as "inactive." If the entry subsequently becomes valid, the entry is marked as active again. The Delete Inactive value determines how long inactive entries are kept in the BOSS hotlist database.
Notify Email – One or multiple email addresses may be defined to receive an alert when there is a hit. Multiple

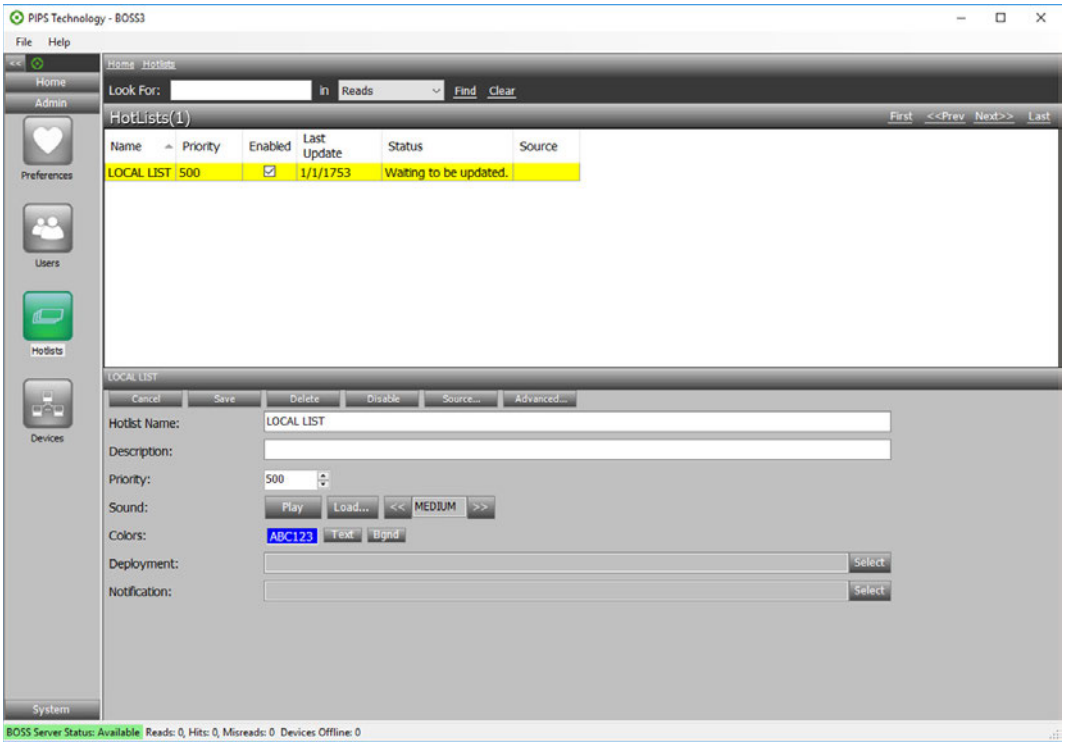
Note: If PAGIS mobile units are used, this value should be set to the longest time between begin shift downloads to PAGIS.

email addresses can be entered in the field, separated by a comma.
Remote Alerts To – Select the remote sites in which to send alerts. When a BOSS system sends an alert to a remote system, it is sent as a read; the remote BOSS system then determines whether to treat the read as a hit.

Note: This setting is only applicable if remote sites are defined.

Expires – Determines the date that the hotlist will stop importing data from its source. For a hotlist that is intended to be permanent, leave the expiration at the default value, 30 years from current date.

7.2 Enabling and Disabling a Hotlist



1. Select the **Admin** category on the Shortcut bar.
2. Click the **Hotlists** shortcut. A list of all hotlists appears in the Browse/Edit area.
3. Click the desired hotlist. Details for the selected hotlist appear in the Browse/Edit area.
4. Click the **Edit** button.
5. The Hotlist Edit screen appears in the lower half of the screen.
6. Click the **Disable** or **Enable** button.

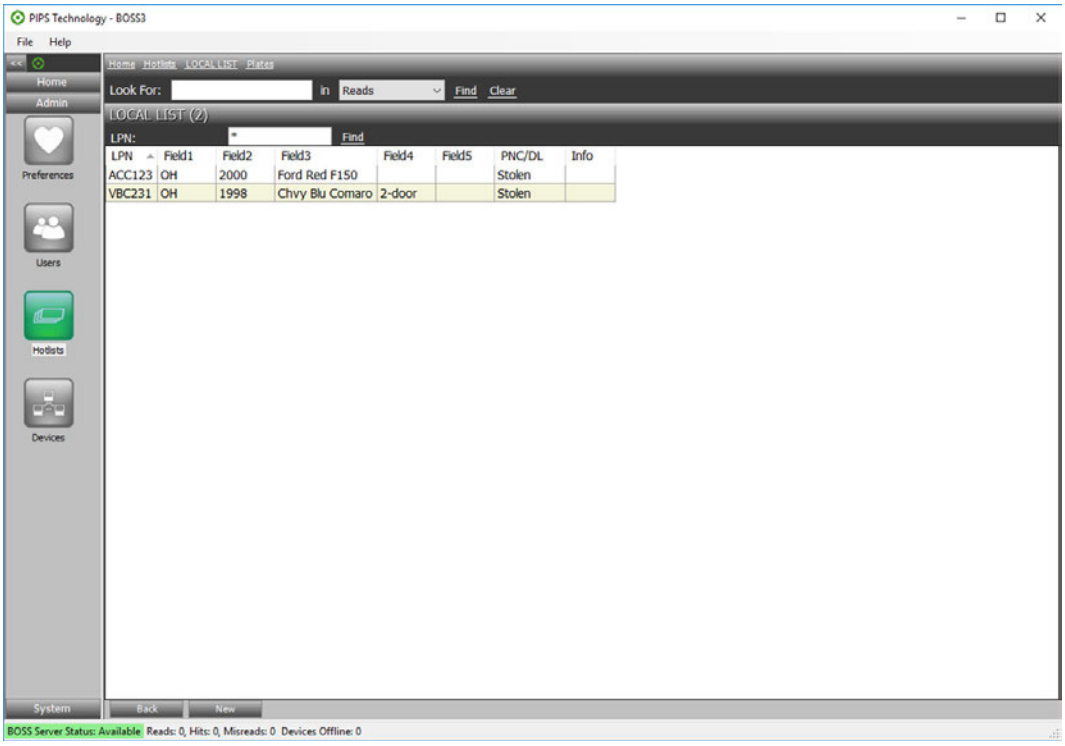
7.3 Modifying Hotlist Entries

BOSS allows viewing, adding, editing, and deleting hotlist entries.

Note: If the hotlist is set to update automatically, any changes to that hotlist made from within the BOSS User Interface application will be lost at the next automatic update.

7.3.1 Querying Hotlist Entries

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Hotlists** shortcut. A listing of all hotlists appears in the Browse/Edit area.
3. Click the desired hotlist. Details for the selected hotlist appear in the Browse/Edit area.
4. Click the **Plates** button.
5. The Hotlist Plates screen will be displayed.

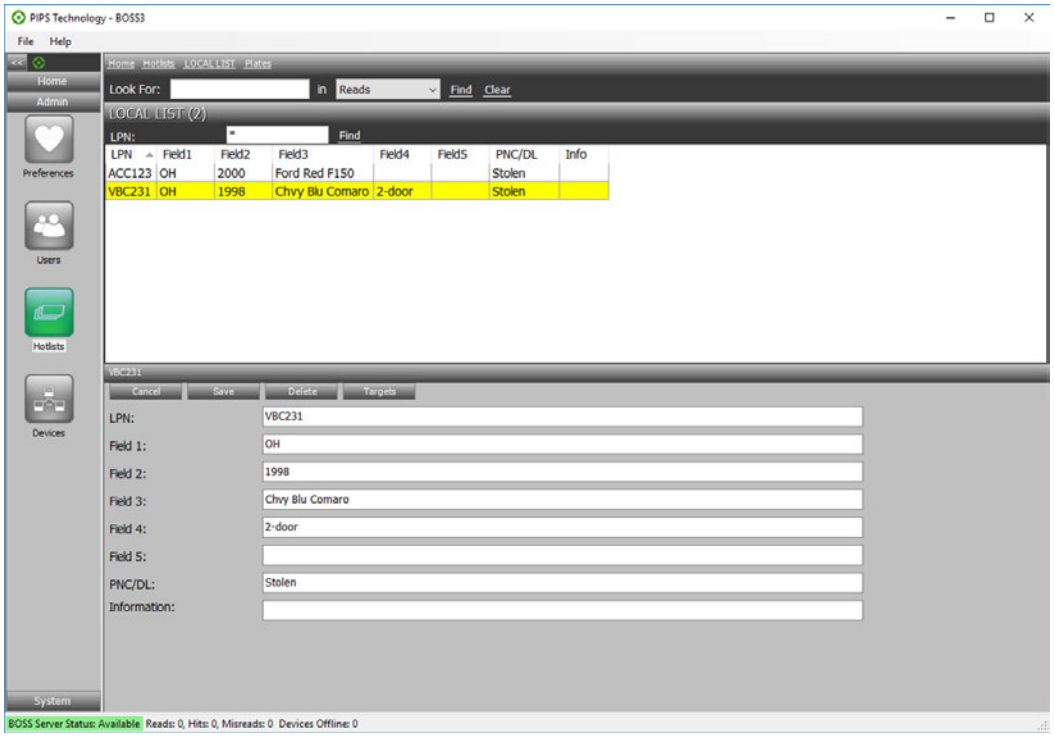


6. Type in the full or partial plate text to search for in the LPN field. (Wildcard searches are supported. See Section 11.1, Wildcards, for more information.)
7. Click on **Find**. License plates that match the criteria will be displayed. Note that only the first 1,000 matching license plates will be shown.

7.3.2 Editing a Hotlist Entry

1. Retrieve hotlist plates as instructed in the previous section.
2. Click on the row showing the desired plate.
3. The Plate Edit form will be displayed at the bottom of the screen.
4. Edit the field values as desired.
5. Click **Save** to save changes.

Note: Manually edited hotlist entries will be lost the next time the hotlist is updated.



7.3.3 Adding a Hotlist Entry Manually

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Hotlists** shortcut. A listing of all hotlists appears in the Browse/Edit area.
3. Click the desired hotlist to select. Details for the selected hotlist appear in the Browse/Edit area.
4. Click the **Plates** button.
5. Click the **New** button. The Plate Edit form will be displayed at the bottom of the screen.
6. Enter the **LPN** (mandatory) and other fields (optional).
7. Click **Save** to save changes.

Note: Manually edited hotlist entries will be lost the next time the hotlist is updated.

7.3.4 Deleting a Hotlist Entry

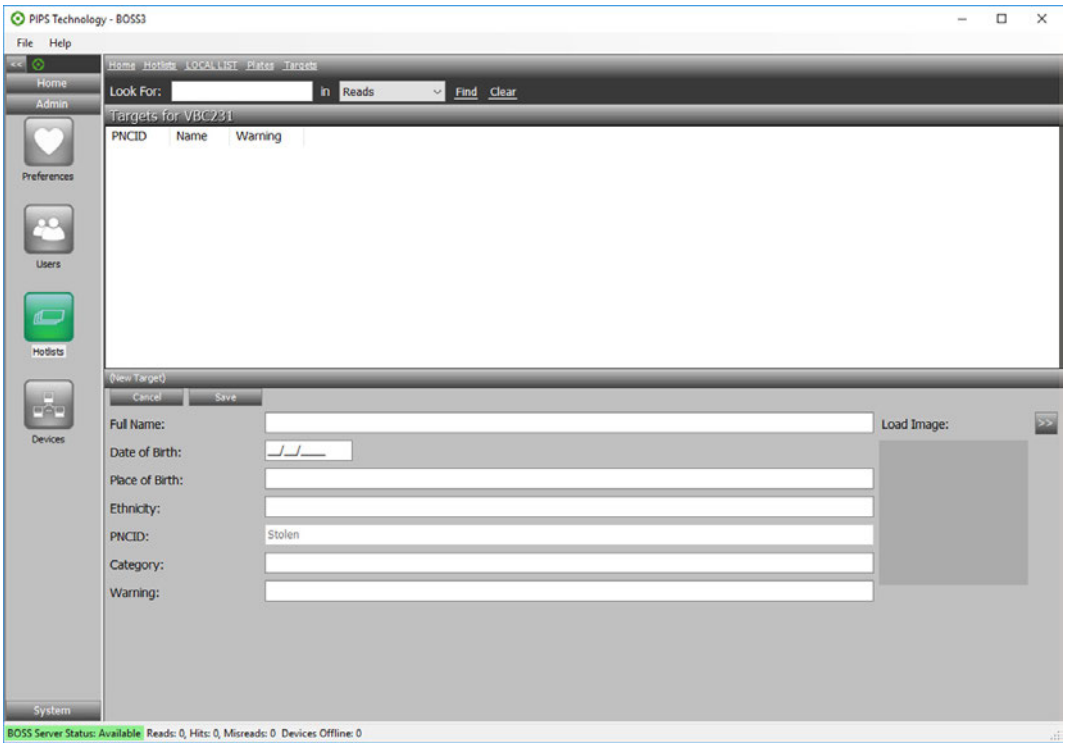
1. Retrieve hotlist plates as instructed in the Querying Hotlists Entries section.
2. Click on the row showing the desired plate. The Plate Edit form will be displayed at the bottom of the screen.
3. Click the **Delete** button.
4. Click **Yes** to confirm the deletion.

Note: Manually deleted hotlist entries may be re-added the next time the hotlist is updated.

7.4 Targets

Targets are individuals of interest associated with a license plate. Target information is downloaded to the PAGIS mobile application from BOSS.

1. Retrieve hotlist plates as instructed in Section 7.3.1, Querying Hotlists Entries.
2. Click on the row showing the desired plate.
3. The Plate Edit form will be displayed at the bottom of the screen.
4. Click the **Targets** button. Information about the target will display.



7.4.1 Creating a New Target

1. Click the **New** button.
2. The Target Edit form will be displayed.
3. Fill in the fields, listed below, with appropriate values.

   Full Name – The first and last name of the target. Date of Birth – The date of birth of the target.

   Place of Birth – The location where the target was born.

   Ethnicity – The ethnicity (race or national origin) of the target.

   PNCID – This field can be used to enter any type of identification number that is available. In the UK this is the Police National Computer identification number of the target. This field is linked to the PNCID field in the hotlist information in the PAGIS application. *See the sample INI configuration file in Section 5 of the Pagis Software User's Manual.*

   Category – The category of the target, such as Felon, Suspect, etc.

   Warning – The warning information to display to the officer.

   Load Image – An image of the target, such as a DMV photo or "mugshot," can also be associated with the Target record. Upload an image by clicking on the Select button and browsing to the image file. Supported formats include JPG, GIF, or BMP.
4. Click the **Save** button.

7.4.2 Deleting a Target

1. Access the Targets screen as described above.
2. Click the row containing the target to be deleted.
3. The Target Edit form will be displayed.
4. Click the **Delete** button.
5. Click **Yes** to confirm deletion.

8 HOTLIST FORMATTERS

Hotlist Formatters define the structure of source data that is imported into BOSS Hotlists. BOSS includes several default formatters when the software is installed. There are three types of formatters:

CSV (comma-separated values) – A flat text file containing one line for every record. Each field in the record is separated by a comma.

Fixed Length – A flat text file containing records that are all the same length. No separator characters are used to determine where each field ends and another begins, but rather, field and record lengths are known up front. In a fixed length file, padding spaces are used where necessary, to accomplish the correct field length.

NCIC (United States National Crime Information Center) – The NCIC database is a computerized index of criminal justice information (i.e., criminal record history information, fugitives, stolen properties, missing persons, etc.), that is available to law enforcement agencies 24 hours a day, 365 days a year. Several NCIC import sources/formats exist within BOSS.

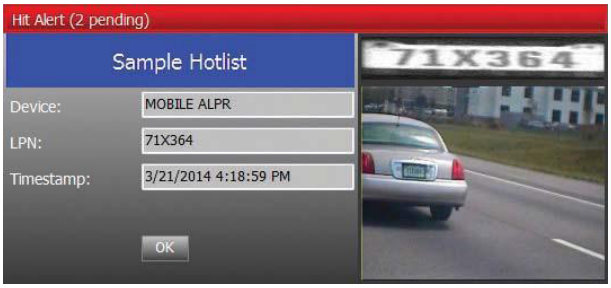
8.1 Creating a New Formatter for Hotlists

Normally, when creating a new hotlist, you will find that one of the default formatters can be used. However, BOSS does give you the flexibility to create new hotlist formatters. Creating a new formatter or modifying an existing formatter should be approached with caution and is beyond the scope of this manual. For more information, please contact PIPS™ Technical Support.

9 ALERTS

BOSS can provide real-time alerts on-screen, via the BOSS User Interface application, or through email. In order to receive alerts through the BOSS application, **the logged-on user must be in a group that is assigned the Dispatch permission**. Email alerts can be sent to any BOSS user or email recipient.

A real-time alert for a hit can pop up on the screen at any time when the BOSS application is running, regardless of which screen the user has active. A sound associated with the hit will be played. Alerts will be queued until the user acknowledges them by clicking **OK**. Real-time alerting in the BOSS application can be turned off by clicking on the **Alerts** toggle button on the BOSS Home screen. The settings for real-time alerts can be modified through the Dispatch screen, (see Section 10, Dispatch).

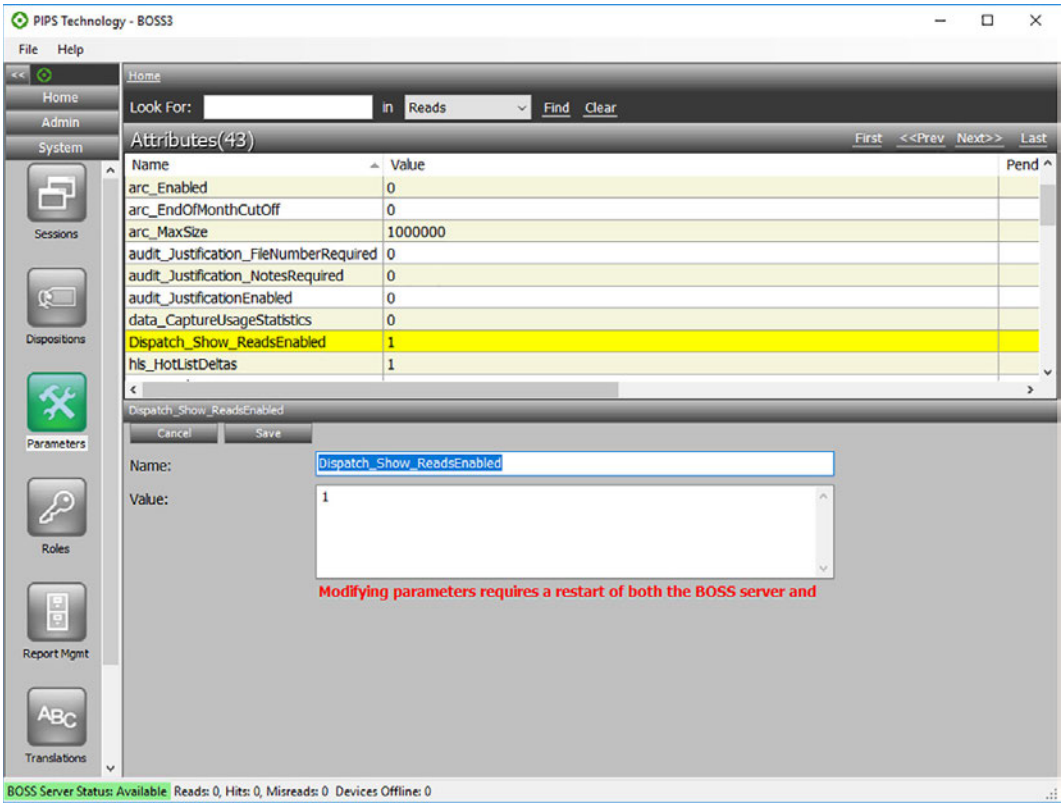


10 DISPATCH

The Dispatch screen is a tool often used by first responder dispatchers. It enables them to easily view hits, monitor reads, and correct license plates as they enter the BOSS system. The information displayed is as near to real time as possible. For ease of viewing, there are three configurations that can be set:

- If only the hits are set to display, they will appear on the whole screen.
- Similarly, if only the reads are set to display, they appear on the whole screen.
- Of the dispatcher is monitoring both hits and reads, then the hits will be displayed on the top half of the screen and the reads will be displayed on bottom half.

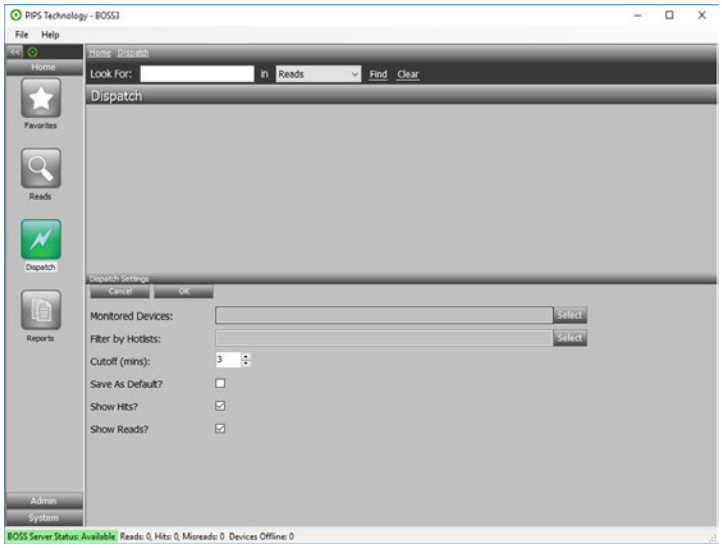
Note: By default, the ability to monitor reads via dispatch is disabled for new Boss installations, this feature can be turned back on by editing the Boss parameter “Dispatch_Show_ReadsEnabled” and setting the value to 1 for on. The Boss service must be restated for this to take effect.



10.1 Dispatch Settings

Dispatch Settings allow you to choose the information shown on the Dispatch screen.

1. Select the **Home** category in the Shortcut bar.
2. Click the **Dispatch** shortcut.
3. Click the **Settings** button in the bottom of the Browse/Edit area.



4. The following settings are available on the Dispatch screen. Change these settings as desired:

   Monitored Devices – Camera sources can be selected or deselected from a pick list to control which ones will supply reads (and resulting hits) to the Dispatch screen. Individual dispatchers can focus on particular camera inputs by selecting/deselecting any combination of sources (one, multiple, or all) for monitoring.

   In large BOSS systems, it may not be practical for a single dispatcher to monitor all sources simultaneously. An organization may choose to assign individual dispatcher personnel to different sources or may select to focus on particular sources during certain time periods or events.

   Filter by Hotlists – Hotlists may be selected to only show hits from designated hotlists. If there are no hotlists selected, hits from the monitored devices will be displayed.

   Cutoff (mins) – The cutoff setting determines how current from the present time a hit or read must be in order to display on the dispatch screen This setting determines the number of minutes before data is discarded from the on-screen display. The maximum time is 10 minutes.

   Save As Default – If checked, the current settings are saved and restored the next time the user logs in. Note that selected devices will always default to the devices where the user is configured to receive notifications in the Hotlist settings. See additional information on notifications in Section 7.1.1, Configuring Basic Hotlist Settings.

   Show Hits? – If checked, hits will display in rows in the top section of the Dispatch screen as they occur. If this option is deselected, rows of hits are not displayed in this section of the Dispatch screen. However, pop-up alerts will still display for hits, regardless of this setting.

Note: If the Alert Toggle button is set to the Off position, hits and reads will not display in the Dispatch screen. See Section 9, Alerts, for additional information.

   Show Reads? – If checked, all reads included in the devices selected in the Monitored Devices field display in the dispatch screen. By default, this option is not selected.

Note: Monitoring reads may slow down the BOSS server. It is recommended that reads are only monitored for diagnostics purposes.

5. Click the **Save** button for the changes to take effect.

10.2 Dispatch Hits

For each row, the columns displayed are:

Device – The device where the read originated.
LPN – The license plate characters read in by a camera or manually entered by a user.
Timestamp – Date and time when the read occurred.
Syntax – The state or region of the plate, if available.
Misread – If checked, indicates that the hit resulted from a read that was marked as a misread. Manual – If checked, indicates that the hit resulted from a manual entry (put in by a BOSS user). Patch – A thumbnail image of the license plate.
Overview – Color overview picture of the vehicle.
Hotlist – The name of the hotlist from which the hit occurred.
Field1 ... Field5 – Fields originating from the hotlist. The content and meaning of these fields vary depending on the composition of the hotlist.
PNC/DL – This field can be used for a driver's license (DL) number in US installations, but primarily used in United Kingdom installations for storing the UK Police National Computer identification number.
Info – Commonly contains additional text associated with the hit record. When the hotlist source contains additional fields, the information from those fields is all stored in this one field.
Priority – Priority assigned to the hotlist, with a lower number being given a higher priority.
Annotation – Notes associated with the read. Annotations are entered by BOSS users.

10.3 Dispatch Reads

For each row, the columns displayed are:

Device – The device where the read originated.
LPN – The license plate characters read in by a camera or manually entered by a user.
Syntax – The state or region of the plate, if available. Timestamp – The date and time when the read occurred. Patch – A thumbnail image of the license plate.
Overview – Color overview image of the vehicle.
Misread – If checked, indicates that this record was marked as a misread.
Hit – If checked, indicates this read resulted in a hit.
Manual – If checked, indicates this read was input manually by a BOSS user, rather than originating from a device.
Annotation – Notes associated with the read. Annotations are entered by BOSS users.

10.4 Manual Entries

There may be times when a read must be manually entered or when a camera does not correctly read a plate. For example, if there was an obstruction between the camera and the plate, then characters may be missed in the read. For this reason, manual entries can be completed by an authorized user via the Dispatch screen.

10.4.1 Adding a Manual Read

1. From the Dispatch screen, click the **Add** button. The Manual Entry screen appears in the lower half of the Browse/Edit area.

Note: The **Add** button will only be present if the logged in user has the Edit Access permission to reads.

2. Enter the plate characters in the LPN field.
3. Click the **Select** button to the right of the disposition field.
4. Select the desired disposition(s) and click the **Save** button to complete the selection.
5. Click the **Save** button to finish saving the manual entry. If the "Manual Entries" device is not being monitored, the manual entry will not appear in the Dispatch screen.

10.4.2 Correcting Reads

1. From the Dispatch screen, click the Add button. The Manual Entry screen appears in the lower half of the Browse/Edit area.
2. Enter the plate characters in the LPN field.
3. Click the **Select** button to the right of the disposition field.
4. Select the desired disposition(s) and click the **Save** button to complete the selection.
5. Click the **Save** button to finish saving the manual entry. If the "Manual Entries" device is not being monitored, the manual entry will not appear in the Dispatch screen.

11 QUERYING STORED DATA

The Reads screen allows for searching and viewing past read records on a local server or on a remote server that has granted access. Reads can be quickly searched by entering a license plate number. This screen also allows for more advanced queries where data can be filtered based on additional fields such as date ranges, location, and radius. Additionally, the Reads screen allows you to perform multiple queries with the use of tabs.

For the queried results returned, there are no limits to the number returned from a local server. To limit the impact on outside systems, there is a limit of 1,000 records returned from a remote server. A maximum of 1000 records will be displayed per page.

Note: Depending on factors such as the size of the BOSS database, the speed of the server, the bandwidth of the connection between client and server, and the parameters of the query, there may be a delay before the results are displayed. A status bar will display that shows that the query progress.

11.1 Wildcards

Wildcards are special characters that represent any alphanumeric character and can be used in searches and queries. Wildcards can make finding a match easier because they can define a portion of the criteria to be ambiguous. Wildcards supported in BOSS are described in the following table.

WILDCARD USED	REPRESENTS
a%	Any values that start with the letter “a”
a	Any values containing “a”
% or *	Any/all values
a_	Any values that are exactly two characters long and start with “a”
_a*b	Any values that have “a” as the second letter and end with “b”
[abc]*	Any values that start with “a”, “b” or “c”

11.2 Quick Search Bar

The Quick Search bar is always visible and available on the top of the BOSS screen regardless of the category or shortcut currently selected. This feature allows for quick, simple searches of various BOSS data.

1. Type the value to search for in the Look For field. This value can include wildcard characters. Multiple values can be entered separated by a comma (e.g., ABC123, XYZ234). However, wildcard values cannot be used when searching for multiple values.
2. In the “In” drop-down box select an area to search. The available options are **Reads**, **Hotlists**, **Users**, **Group Users**, **Groups**, **Devices**, and **Sites**. These areas are described below.
3. Click the Find link to initiate the search. The results will be displayed in the Browse/Edit area of the screen.

11.2.1 Quick Search Fields

When performing a query using the quick search feature, keep in mind that the search is performed in one significant area that can be selected. The search is then run against the significant field in that area, not all fields in that area. For example, when performing a quick search in Users, the text entered is compared against the Username field of all user records.

However, it is not compared to the display names for users. The following is a list of the fields used in the Quick Search:

SEARCH IN AREA	FIELD USED FOR SEARCH
Reads	LPN
Users	Username
Groups	Group Name
Site	Site Name
Hotlists	Hotlist Name
Group Users	Group Name
Devices	Device Name

11.3 Query Result Navigation Icons

Just above the query results are navigation icons that facilitate moving through the data results. These icons can be very useful for larger result sets, providing an easy way to move through records.



Move to the very beginning of the data results, i.e., the first record.



Move forward through the data results.



Move backward through the data results.



Move the very end of the data results, i.e., the last record.

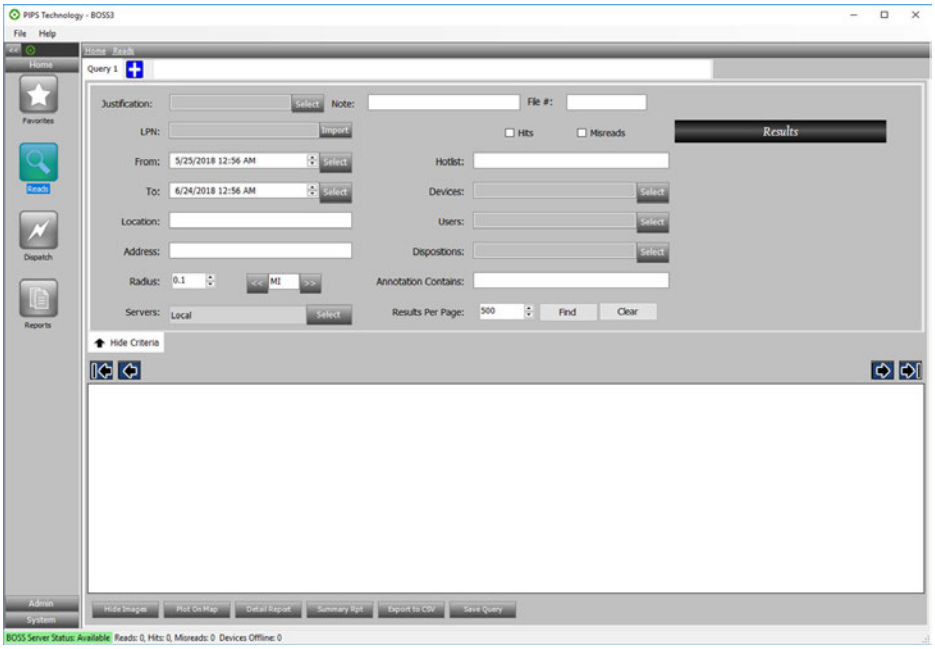
11.4 Advanced Reads Queries

The Reads screen allows for searching and viewing past read records. Reads can be quickly searched by entering a license plate number. The Reads screen also allows for more advanced read queries where data can be filtered based on additional fields such as date ranges, location, or radius. As indicated earlier, a maximum of 1000 records will be displayed.

11.4.1 Performing an Advanced Reads Query

1. Select the **Home** category on the Shortcut bar.
2. Click the **Reads** shortcut.
3. Enter desired query criteria (see the following section, 11.4.2, Entering Advanced Reads Query Criteria). All fields do not have to be filled in. Leaving a query field blank simply means there will be no filtering on that field.
4. Click the **Find** button to run the query.

11.4.2 Entering Advanced Reads Query Criteria



The query criteria fields are:

LPN – Full or partial (using wildcards) license plate number.
From – The start date and time for reads to be retrieved. Either click the **Select** button to display a calendar for quick selection, or type in the date.
To – The end date and time for reads to be retrieved. Either click the **Select** button to display a calendar for quick selection, or type in the date.
Location – The location as entered in the PAGIS application (see the Pagis Software User's Manual for more information).
Near Address – An address to use as the center of a radius search. The address format depends on the mapping system used but typically street name, house number, city and state, or zip code can be entered.
Radius – When a Near Address filter is entered, the search radius from the center point must be entered here.
Servers – Information can be queried from one or more remote BOSS servers. Click the Select button to display a list of authorized BOSS servers.
Justifications – Select the justification that best describes the purpose for the query being performed. This field will only be displayed if Justifications have been enabled in the System Parameters. See Sections 15.3.2, List of BOSS System Parameters, and 15.7, Justifications, for more information.
Justification Note – Enter any additional information necessary to more accurately document the query being performed. This field will only be displayed if Justifications have been enabled in the System Parameters. See Sections 15.3.2, List of BOSS System Parameters, and 15.7, Justifications, for more information.
Hits Only – If checked, only hits are queried.
Misreads Only – If checked, only reads that are marked as misreads are queried.
Hotlist – A search on hits can be limited to a specific hotlist, which can be entered here.
Devices – A query can be narrowed to reads originating from a particular device. Click the Select button to display a list of devices, select one or more.
Users – A query can be narrowed to reads originating by a particular user. Click the Select button to display a list of users and select one or more.

Note: The username can also be typed in.

Dispositions – A query can be narrowed to reads with a particular disposition. Click the **Select** button to display a list of dispositions. Then select one or more dispositions.

Annotation Contains – If text is entered in this field, only reads that contain the text in the annotation field are queried.

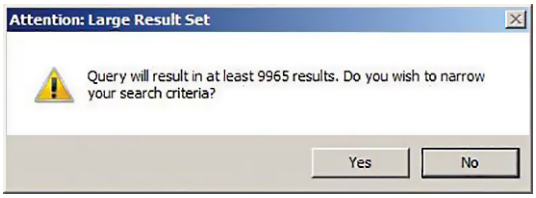
Results Per Page – The maximum number of reads that will be displayed. The default is 500, the maximum is 1,000.

Clear – If clicked, the fields on the current tab will be returned to their default values.

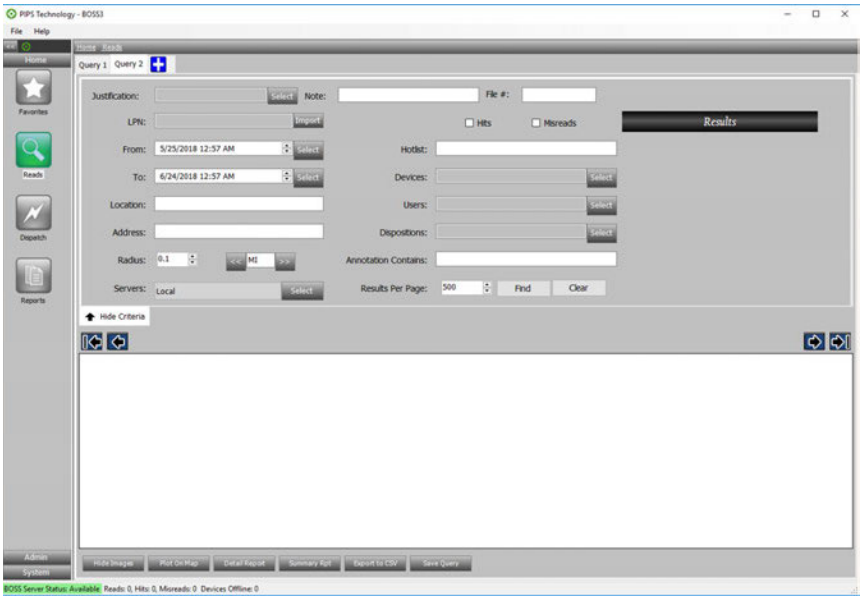
11.4.3 Managing Query Results

With the ability to obtain any number of results from a local server comes the option to narrow the potential results to be returned. If a large number of results will be returned based on the criteria entered, a message is displayed asking if the search criteria should be narrowed. If you select **Yes**, the search criteria is redisplayed offering the chance to make any necessary changes to reduce the results. If you select **No**, the query is performed based on the current criteria selections.

Note: A large number of results can take several minutes to be displayed.



11.5 Multiple Query Tabs



With Query tabs, users can perform multiple queries at a time. By clicking on the last tab, which contains the plus icon, you can access additional Reads Query screens. Enter the desired search criteria on each new screen to obtain additional information through the varying results. Each query can be given a descriptive name by right-clicking on the tab, and obsolete queries can be removed the same way.

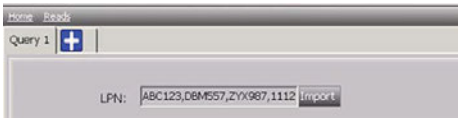
11.6 Cross-Referencing External Data

BOSS allows cross-referencing external data, such as DMV information. To query BOSS based on external information, take the following steps:

1. Create a CSV text file containing the license plate numbers to be cross-referenced. **The license plate number must be in the first field.**
2. Open the Reads Query screen.
3. Click the **Import** button next to the LPN field.



4. Click **Open** to import the plate numbers. A maximum of 50 plate numbers can be referenced at a time. Imported plate numbers will show up in the LPN field:

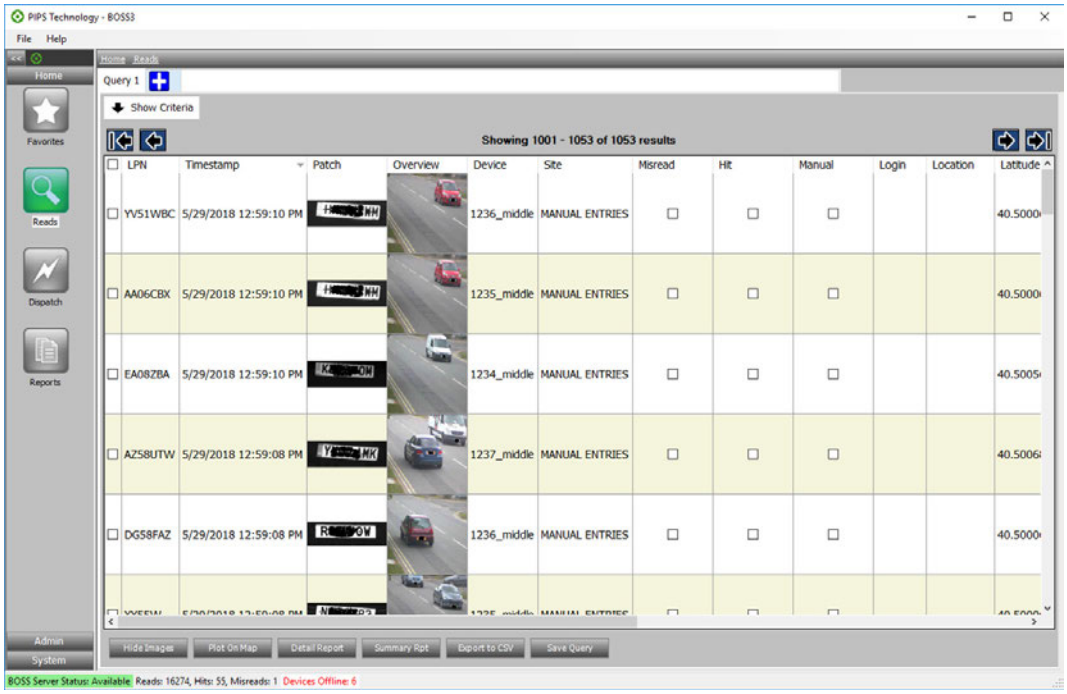


5. Enter other query criteria, as needed, and click **Find** to run the query.

11.7 Working with Queried Reads

11.7.1 Viewing Query Results

The results of both Quick Searches and Advanced Reads Queries are presented in the same manner.



The columns displayed are:

LPN – The plate text (characters) read in by a camera or manually entered by a user.
Timestamp – The date and time when the read occurred.
Patch – A thumbnail image of the license plate. Overview – The color overview picture of the vehicle. Device – The device where the read originated.
Site – The site where the read originated.
Misread – Indicates whether the read was marked as a misread by a user.
Hit – Indicates whether the read is a hit.
Manual – Indicates whether the read was entered manually.
Login – The username logged into the device at the time the read originated.
Location – The location entered in the PAGIS system. See the Pagis Software User's Manual for more information.
Latitude – The latitude coordinates of the device at the time the read originated. Longitude – The longitude coordinates of the device at the time the read was originated. Hotlist – The name of
the hotlist that produced the hit.
Field1 ... Field5, PCNID, Information – Information from the hotlist that produced the hit.
Annotation – Annotations entered for the read.
Server – The name of the server that has provided this information. This can be a local or remote server.

11.7.2 Query Results Actions

There are several button options available at the bottom of the Reads Query Results screen that offers additional uses of the data results.



Hide Images/Show Images – Used to remove the image columns, patch and overview, from the view. This can be done to provide more room for text fields to be displayed. When clicked, the Hide Images button's caption changes to Show Images. When the button is clicked again, images will again be displayed.

Plot On Map – When clicked, any selected records will be plotted on a map. One or multiple records can be selected by clicking the checkbox in the first column of the record. To select all of the records, click the checkbox in the headings column.

Detail Report – Click to generate a detailed report of selected reads. To select one or more records, click the checkbox in the first column of the record. To select all of the records on the current page, click the checkbox in the headings column. Use the navigation buttons to move to additional pages to select additional records.

Summary Rpt – Click to get a summary report of selected reads. To select one or more records, click the checkbox in the first column of the record. To select all of the records on the current page, click the checkbox in the headings column. Use the navigation buttons to move to additional pages to select additional records. To include all results choose the All Results option in the Reads Summary Detail Report option box.

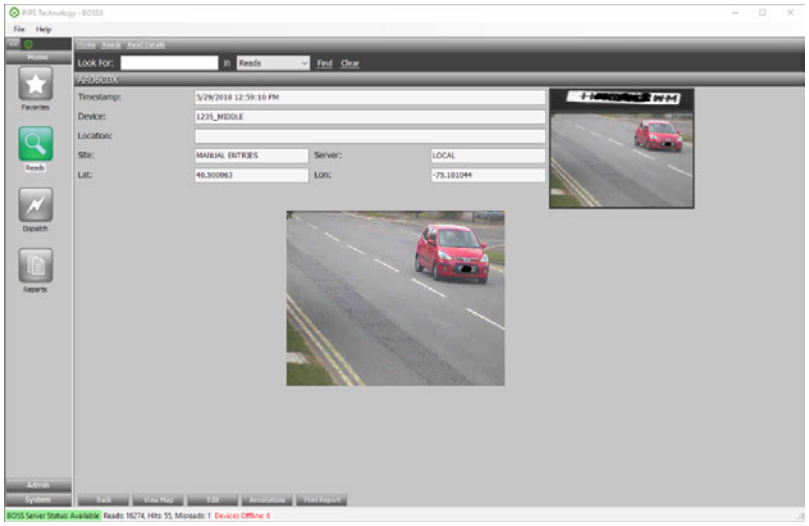
Export to CSV – Click to save the results to a file in a CSV format. Select to save the current page or all results provided. Use the navigation buttons to move to additional pages to select additional records.

Save Query – Click to save the query criteria as a favorite for future use. See Section 11.8, Favorites, for more information.

11.7.3 Viewing Read Details

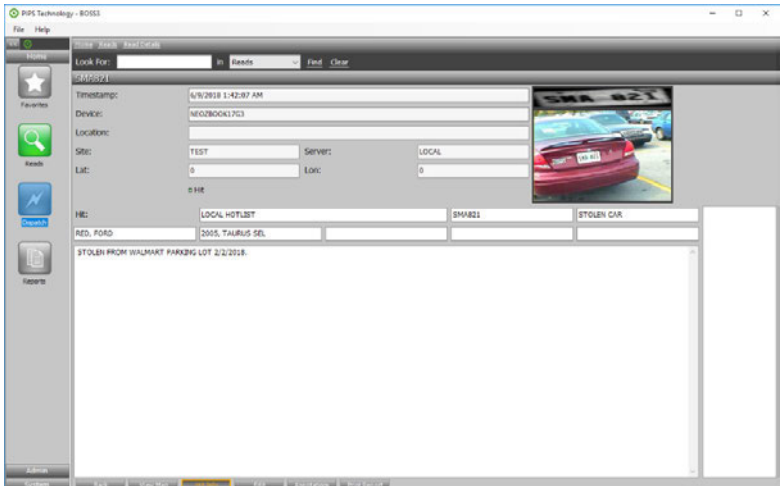
Click a row in the query results to view the details of the record.

The Read Details screen displays the license plate text in the title. The timestamp, originating device, site, and geographical coordinates are displayed below. The plate patch and vehicle color overview images are on the right.

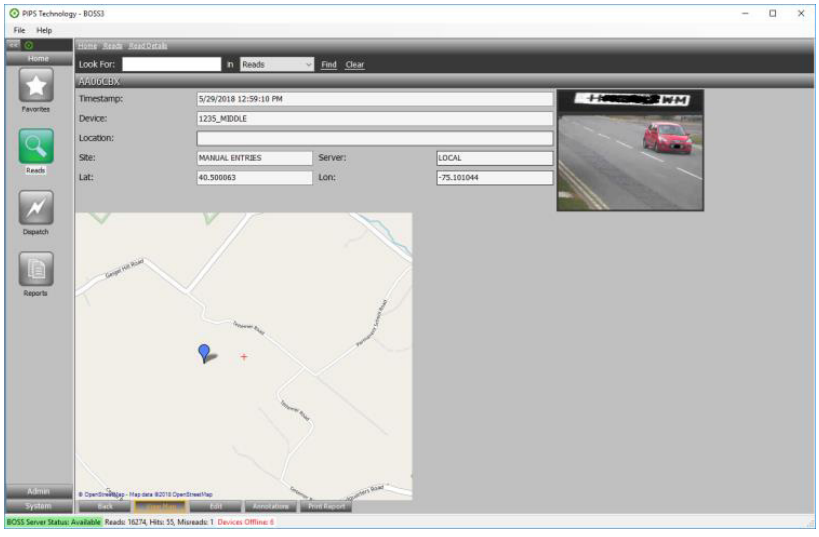


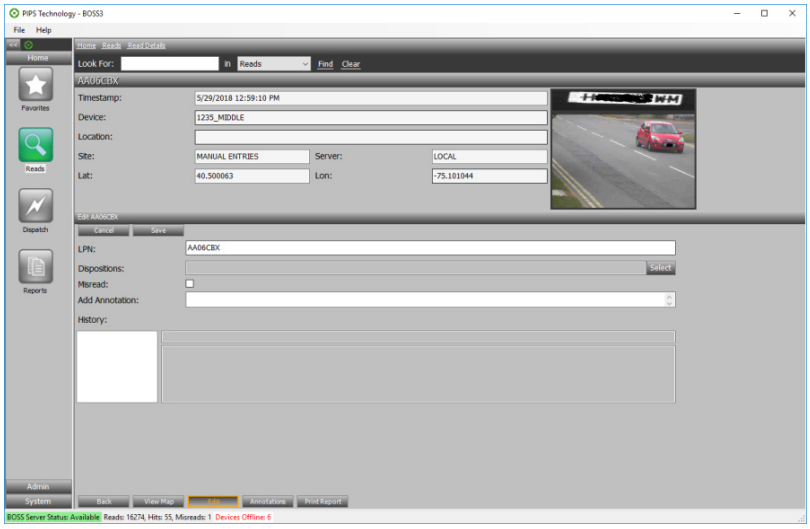
The vehicle color overview picture can be enlarged by clicking on the picture. Use a mouse scroll wheel or the cursor up and down keys to resize the image. Left-click on the enlarged image to close. Right-click on the image to copy the image to the Windows Clipboard.

If the read is a hit, details of the hit can be displayed by clicking on the Hit Info button at the bottom of the screen.

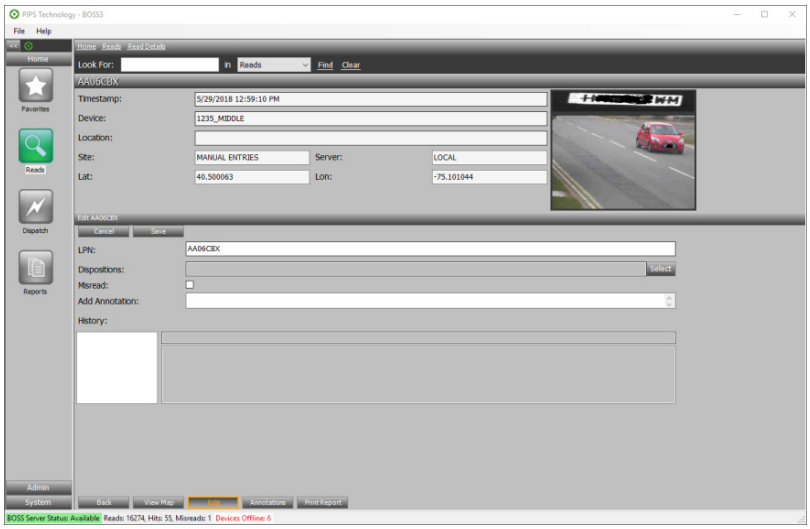


A map plotting the location where the read occurred can be displayed by clicking on the View Map button.

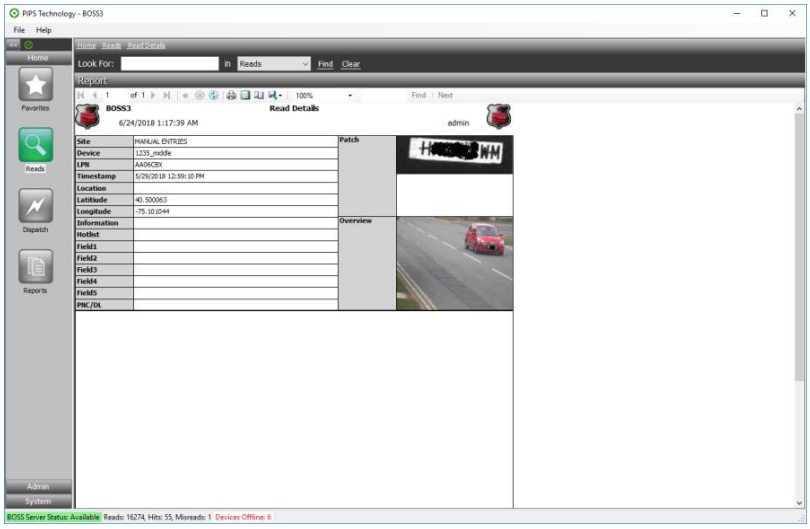




Use the Edit button to correct the plate text and/or assign a disposition and annotation to the read. Click on Save to save the changes. The plate text can also be marked as misread if the read information is found to be incorrect.



Annotations associated with the read can be viewed by clicking on the Annotations button.



A report containing the read's details can be printed by clicking on the Print Report button.

11.8 Favorites

Favorites are read queries that use specified criteria, which have been saved. Favorites can be reused, which allows the user to quickly perform frequently needed queries without having to define the parameters each time. Favorites are specific to each user.

11.8.1 Creating a New Favorite

1. Select **Home** on the Shortcut bar to access its icons.
2. Click on the **Read** shortcut.
3. Enter the desired query parameters in the Browse/Edit area (e.g., data range, location, radius, servers).
4. Click the **Go** button to run the query.
5. When the query results window appears, click the **Save Query** button.
6. A dialog box will appear, prompting for a name. Enter a descriptive name for the new favorite.
7. Select the Use Relative Date Range option if desired.

   Use Relative Date Range Option – If this option is selected when saving a query, and when the resulting favorite query is run in the future, it will use a From and To date and time range relative to the From and To date and time entered for the original query. It will not use the actual range entered in the original query. Also, it is important to remember that the time span between the From and To date and the time range used is relative to the date and time when the original query was run.

   Consider a query that is saved as a favorite and originally defined on 8/9/20xx to search reads between 8/02/20xx and 8/8/20xx (the prior week). If the Relative Date Range option is selected, the query is saved to always run against the prior week rather than those actual dates. If the Favorite option is invoked on 12/3/20xx, it will return results from 11/26/20xx through 12/2/20xx. It is important to note that the results will be relative to the actual time of the original query and when it is rerun. Suppose you run a query at 5 pm today to search for reads occurring between 9 am and 5 pm and save it as a favorite. When you run the query again tomorrow, it will search for reads that occurred eight hours **before** the current time, which may not necessarily fall between 9 am and 5 pm.
8. Click **OK** to complete. The query definition is now saved as a favorite and can be accessed at any time.

11.8.2 Activating a Favorite

1. Select the **Home** category in the Shortcut bar (if not already selected).
2. Click the **Favorites** shortcut.
3. A listing of all favorites is displayed in the Browse/Edit area.
4. Click the desired favorite. (The selected favorite will be highlighted in yellow.)
5. Click the **Go** button in the bottom area of the Browse/Edit area.
6. The query results will appear in the Browse/Edit area.

11.8.3 Deleting a Favorite

1. Select the **Home** category in the Shortcut bar (if not already selected).
2. Click the **Favorites** shortcut.
3. A listing of all favorites is displayed in the Browse/Edit area.
4. Click the desired favorite. The selected favorite will be highlighted in yellow.
5. Click the **Delete** button in the bottom area of the Browse/Edit area.
6. Press **Yes** to confirm deletion.

12 REPORTS

Several reports are included, automatically, with a new BOSS installation. These reports are available for use as soon as a BOSS Administrator assigns role permissions to the reports.

12.1 Running a System Report

1. Select the **Home** category on the Shortcut bar.
2. Click the **Reports** shortcut.
3. The Browse/Edit area will display a list of available reports. (Reports to which the user does not have permissions are not displayed.)
4. Click the desired report. The selected report is highlighted in yellow. Parameters for the report appear in the bottom of the Browse/Edit area.
5. Select **Date Range**. All reports call for From and To dates to define the time range for the report data. By default, the values in these fields define a report for the most recent two weeks. You can change these dates by typing different information into these fields, using the **Up/ Down** arrow keys to the right of the field or by clicking the **Select** button to the right of the field and selecting a date on the calendar and then clicking the **Save** button.
6. Some reports also permit you to filter report results by user(s). For example, the pictures report, which reports pictures taken in PAGIS, allows you to define one or more users to report on.
7. Once desired parameters are selected for the report, click the Go button. The report screen immediately displays, indicating that the server is generating the report until results are displayed.

12.2 Viewing and Printing Reports

The Report screen displays the date and time the report was generated and the title of the report in the heading area. When you place your mouse above a shortcut on the Report Shortcut bar, a label appears indicating what the shortcut button does. Note that some of the buttons on the Shortcut bar are not relevant to BOSS reports and are therefore disabled.
The Report Results Shortcut bar icons are as follows:



First Page – Return to the first page of the report.
Previous Page – Go to the previous page of the report.
Page Input – In this text box, type in a particular page number to bring up on screen.
Next Page – Go to the next page of the report.
Last Page – Go to the last page of the report.
Stop Rendering – This button can be used to cancel the report processing. This can be helpful if a large report was initiated, but is no longer desired.
Refresh – Refresh the report using the most current BOSS data.
Print – Print the report.
Print Layout – Toggle between available print layouts.
Page Setup – Choose among the options for standard page setup, such as page orientation, and paper size.
Save As – Excel/PDF/Word – Save the current results to a Microsoft Excel (.xls), an Adobe Portable Document Format (.pdf) or a Microsoft Word (.doc) document.
Width Zoom Setting – This drop-down list allows you to select a zoom view for the report results on the screen.

12.2.1 Viewing the Login Statistics Report

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Devices** shortcut.
3. Click the **Logs** button at the bottom of the screen.



4. Click **Go** to view the Login Statistics Report.
   Begin Date – Select the start date for the report.
   End Date – Select the end date for the report.
   Selected Users – Select the users to include in the report. Click the **Select** button. Click the checkbox of the desired user. Click on the **Save** button.

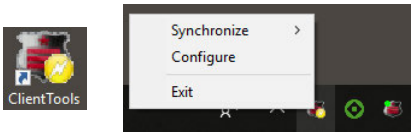
13 CLIENT TOOLS

The Client Tools utility is used to transfer any necessary files needed for a shift from BOSS to an PAGIS system that is being run in the Disk Sync mode. After the completion of a shift, Client Tools can then be used to transfer read data files captured during a shift into BOSS. The utility is configurable and processes files stored on a local, network, or USB flash drive. Like Smart Client, the Client Tools utility does not have to be run on the BOSS server; it can be configured to access the server via an IP Address.

Client Tools does not have a customary interface. Once the utility is started, the Client Tools icon will appear in the Windows System Tray.

Before use, Client Tools must be configured, which is described in Appendix 17. Once the Client Tools has been configured, it can now be used to synchronize information between BOSS and PAGIS:

1. To start, right-click on the **Client Tools** icon.

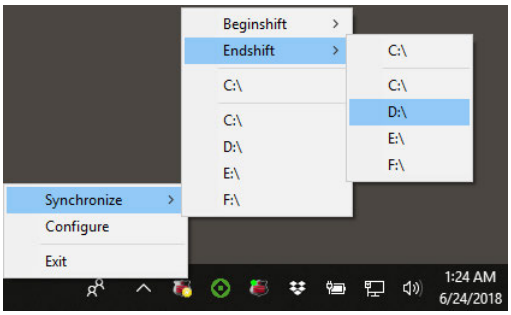


2. Select **Synchronize**. The next menu displayed is divided into three sections.

   a. The first section allows the user to select either **Create Begin Shift Files or Synchronize End Shift Files**. When either option is selected, the next menu is displayed. It is divided into two sections; it is the bottom two sections of the previous menu and functions the same way.

   b. The second section displays the path defined during configuration. This is a shortcut to perform Begin Shift and End Shift at the same time, storing the Begin Shift files in the defined location and processing the End Shift files at the defined location. If there are no End Shift files to process, this feature will be complete after the Begin Shift file is created. No error message will be displayed if the End Shift files are not found.

   c. The last section lists the drive letters currently on the workstation. If one is selected, Client Tools will perform a Begin Shift first and store the files at the root of the drive selected. Then Client Tools will check to see if there are End Shift files at that location. If found, the files will be processed. If not found, the synchronization process is complete. No error message will be displayed. This is an additional option if the configured drive is not currently available.



Note that once End Shift files have been processed, they are deleted.

14 ARCHIVING DATA

It is possible to archive reads that have accumulated in the BOSS database. Based on settings that are configurable in System Parameters, reads that meet the specified criteria are transferred from the main BOSS database to an archived BOSS database. *(See Section 15.3.2, List of BOSS System Parameters, for additional information on configuring this feature.)*

Once enabled, this process is handled by the BOSS server. There should be no noticeable difference to a user logged into a BOSS Smart Client when reviewing or reporting on stored reads. The only indication in the BOSS Smart Client that reads have been archived will be on the BOSS Home screen. The user will be able to see a calculable difference between the reads and hits counts compared to the total reads and total hits counts. The difference between the values will be the number of reads and hits stored in the archived database.

15 SYSTEM SETTINGS

15.1 Sessions

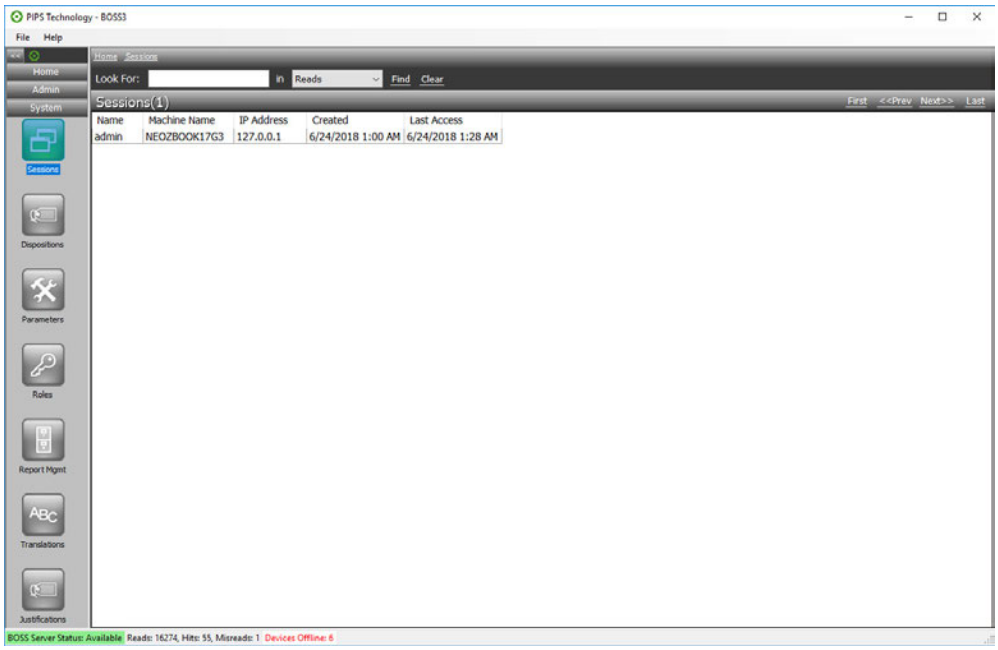
The Sessions screen allows for viewing the current list of logged-on BOSS users. Each login on each computer utilizes a concurrent license of the software. Since BOSS is licensed per concurrent active session, a BOSS Administrator may need to have a session disconnected in order to release a session license. A BOSS Administrator can force a session disconnect in the Sessions screen.

Note: BOSS allows a single "admin" login to access BOSS even if the number of concurrent sessions has been exhausted. Please see Section 2.1, BOSS Administrator Login, for more information about the "admin" username.

15.1.1 Viewing and Disconnecting Sessions

1. Select the **System** category on the Shortcut bar.
2. Click the **Sessions** shortcut. A list of current user sessions appears in the Browse/Edit area.
3. The heading in the Browse/Edit area indicates the total number of current sessions.
4. Click on a session to see details in the bottom half in the Browse/Edit area.
5. To disconnect, click the **Disconnect** button that appears in the detail area, and click **OK**.

Note: You cannot disconnect your own session in this manner. To disconnect your own session, simply log off the BOSS application.



15.1.2 Workstation Power Management and Sessions

Using Windows Power Management to hibernate or suspend a workstation running the BOSS Smart Client will cause the session in BOSS to be terminated after five minutes. When the workstation is resumed from hibernation or a suspended state, the user will have to log in to BOSS again.

15.2 Dispositions

Dispositions are pre-defined classifications that can be assigned to hits. “Arrest Made,” “Vehicle Recovered,” “Surveillance Established” are examples of dispositions. A BOSS Administrator is able to define any number of dispositions for her system. Users can then use those dispositions to specify the action taken or the status of the hit. A new BOSS system will have a Default Disposition category that includes one disposition of “No Action.” Additional categories can be defined as needed.

15.2.1 Defining a New Disposition

1. Select the **System** category on the Shortcut bar.
2. Click the **Dispositions** shortcut. A list of all current dispositions appears in the top of the Browse/Edit area.
3. Click the **New** button in the bottom of the Browse/Edit area.
4. Enter a name for the disposition. If adding it to the default category, simply enter the name of the disposition. If adding it to a new category, the format of the name should be [Category : Disposition Name], i.e., **Auto :Vehicle Recovered**.
5. Enter a **Description** for the new disposition.
6. Specify a **Priorit**y for the disposition. (A lower number means a higher priority.)
7. Select the **Back Office Only** option if the disposition should not be available only in the Correct Reads screen in BOSS, and not exposed in PAGIS.



15.2.2 Deleting a Disposition

1. Select the **System** category in the Shortcut bar (if not already selected).
2. Click the **Dispositions** shortcut.
3. A list of all dispositions is displayed in the Browse/Edit area.
4. Click the desired Disposition. The selected disposition will be highlighted in yellow.
5. Click the **Delete** button in the bottom area of the Browse/Edit area.
6. Press **Yes** to confirm deletion.

15.3 System Parameters

System Parameters allow for configuration parameters for a BOSS system. System parameters only need to be configured during initial system configuration and normally do not need to be modified again after that.

15.3.1 Editing System Parameters

1. Select **System** from the left Shortcut bar.
2. Click on the **Parameters** button in the Shortcut bar.
3. Click on the desired parameter in the right Browse/Edit window. The bottom pane of the Browse/Edit window will display the entry field for the selected parameter.
4. Modify the parameter value as desired and click the **Save** button.

15.3.2 List of BOSS System Parameters

arc_ActiveRetentionDays – This setting dictates how long reads will be maintained in the BOSS database. After reads have been stored for this time, they will be moved to the archived database, creating space for additional reads in the main database. The default setting is 730 days but can be varied based on the size and needs of the system.
arc_ArchiveDBRetentionDays – This setting dictates how many days to retain an archived database. After an archived database has been stored for this time it will be removed, creating space for additional archived databases. The default setting is 0 days, which indicates that the archived databases will never be removed, but the number of days can be modified based on the size and needs of the system.
arc_DatabaseLocation – This setting allows the user to specify where the archived databases should be saved. A blank entry will save them in the SQL default location.
arc_Enabled – To allow the BOSS server to archive aged reads and free up space, enable archiving by setting this to 1. When archiving is not desired, this setting should be 0.
arc_EndOfMonthCutOff – This setting forces a restriction on the size of the archived databases, so that nothing will be added after the end of each month. The default setting is disabled (0). To enable the setting, change the value to 1.
arc_MaxSize – This setting allows the Administrator to determine the number of reads that can be stored in the archived database. The default value is 1 million and can be varied based on the size and needs of the system. Once an archived database has reached this maximum number of records, a new archived reads database will be created.
audit_Justification_FileNumberRequired – When this setting is enabled (1), users performing read queries are required to enter a file number.This information will also be listed in the audit report. The default setting is disabled (0).
audit_Justification_NotesRequired – When this setting is enabled (1), users performing read queries are required to enter a justification note. This information will also be listed in the audit report. The default setting is disabled (0).
audit_JustificationEnabled – When this setting is enabled (1), users performing read queries are required to select a pre-defined justification. This information will also be listed in the audit report. The default setting is disabled (0).
data_CaptureUsageStatistics – When this setting is enabled (1), information sent from a PAGIS device that has been modified due to Privacy settings will still be utilized to generate usage statistic reports. The default setting is disabled (0).
hls_HotListDeltas – When this setting is enabled (1), updated hotlists will be deployed in full. Changing the setting to disabled (0) will cause only the changes made in the updated hotlists to be deployed.
Password_Expiration_Days-Number of days a password is allowed to remain unchanged. Value “1”=enabled, “0”=disabled.

15.3.2 List of BOSS System Parameters (continued)

Proxy_uri/proxy_username /proxy_password/proxy_domain – These settings are only necessary if there is a proxy server involved that requires authentication for connection. Enter a valid Uniform Resource Identifier (URI), username, password, and domain in the associated fields to allow communication through the proxy server. Consult the network Administrator for proxy authentication information

purge_Minutes – This setting is the time, in minutes, between each session of purging or archiving. The default value is 15 minutes and is configurable to any value of 1 minute or greater.

purge_ReadCount – This setting is the number of records to be processed by the purging or archiving process per session. It can be any value, but setting it according to system limitations is recommended because the process can be resource intensive if set too high.

readQuery_fromDate – This setting allows the user to adjust the default From date on the Reads Query screen. Any value can be entered and it is used to decrement from today. Example – a value of 7 would result in a from date seven days earlier than today.

readQuery_toDate – This setting allows the user to adjust the default to date on the Reads Query screen. Any value can be entered and it is used to incremented from today. Example – a value of 7 would result in a to date seven days later than today.

Recent_Read_Time- Time in min. of how long to hold reads in the "Recent reads" table for hit evaluation.

Recent_Reads_Amt- Number of records to delete from "Recent reads" if older then Recent read time.

ResendEmailNotice- Resend Offline notification on Fixed Camera after this amount of time has expired.

rq_ReaperHours – This setting manages how long to retain a temporary database table created when running certain read queries. This allows the user to continue to review the results of those queries for a longer time. The default is a minimum of 48 hours, and there is no maximum value.

smtp_AlertTemplate- Default email template, definitions listed in table below.

smtp_SenderName – In order for the BOSS server to send alerts to email addresses, the SMTP settings must be configured correctly. The SMTP sender field should contain the username that will appear in the from field on an email generated by the BOSS system.

smtp_Server – The name or IP address of the SMTP server should be entered here. The name or address used here must be one by which the SMTP server can be reached from the BOSS server. This field must be populated correctly in order for the BOSS system to send any alerts to email addresses.

smtp_SSL – If Secure Sockets Layer (SSL) is used on your SMTP server, the value of this field should be set to 1. If you do not use SSL, this field should be set to 0.

smtp_SubjectTemplate – This field sets the subject line of alert emails generated by BOSS. The following entry in the field incorporates both static text and a BOSS field variable as well: BOSS alert FROM [SRC].

TOKEN	DESCRIPTION	TOKEN	DESCRIPTION
[LPN]	license plate	[FD1]	field1
[STE]	site	[FD2]	field2
[SRC]	device	[FD3]	field3
[LOC]	location	[FD4]	field4
[LAT]	latitude	[FD5]	field5
[LON]	longitude	[PNC]	PNCID/DL
[HOT]	hotlist name	[INF]	information

smtp_UserName/smtp_password – The SMTP username and password fields should contain a valid SMTP username and associated password for sending alerts through the SMTP (email) server. Normally, a BOSS Administrator coordinates with his SMTP Administrator to create a special SMTP user that will be used exclusively for BOSS alerts.

Soap variables- All are now legacy features not currently used.

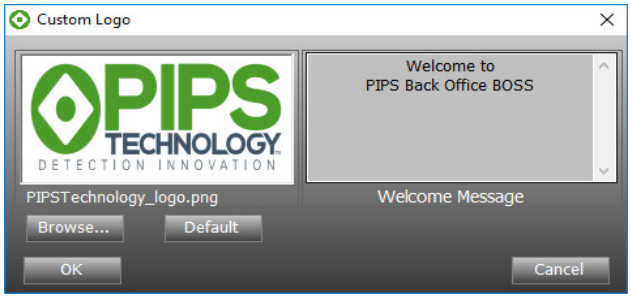
verint_HotlistsMonitored- Enter hotlist by name separated by commas.

verint_NotificationConfigured- Indicates whether the Verint notifier should be used.

15.3.2 Branding

BOSS allows the BOSS Administrator to upload a logo image and a welcome message that is displayed to BOSS users on the Home screen. To define the image and message:

1. Select **System** from the left Shortcut bar.
2. Click on the **Parameters** button in the Shortcut bar.
3. Click on **Branding**.
4. If needed, click **Default** to remove current custom settings.
5. Pick the desired logo image using the **Browse**... button.
6. Type in a message in the Welcome Message box.



Browse – Select an image file (JPEG, GIF, BMP) to be displayed on the home screen. The largest recommended image size is 120 by 380 pixels.

Default – Remove the custom logos and texts.

Welcome Message – A custom welcome message can be typed in here.

7. Click **OK** to save changes, or **Cancel** to discard changes.

15.4 Roles

In addition to the default roles that are automatically created by BOSS, the Administrator can create and configure custom roles as needed. *See Section 4.2, Permissions, for more information.*



15.4.1 Adding New Roles

1. Select the **System** category on the Shortcut bar.
2. 2. Click the **Roles** shortcut. The Browse/Edit area will display a list of existing roles.
3. 3. Click on the **New** button. The New Role entry window will be displayed in the bottom of the window.
4. 4. Enter the name of the new role and assign the desired permissions.
5. 5. Click the **Save** button.

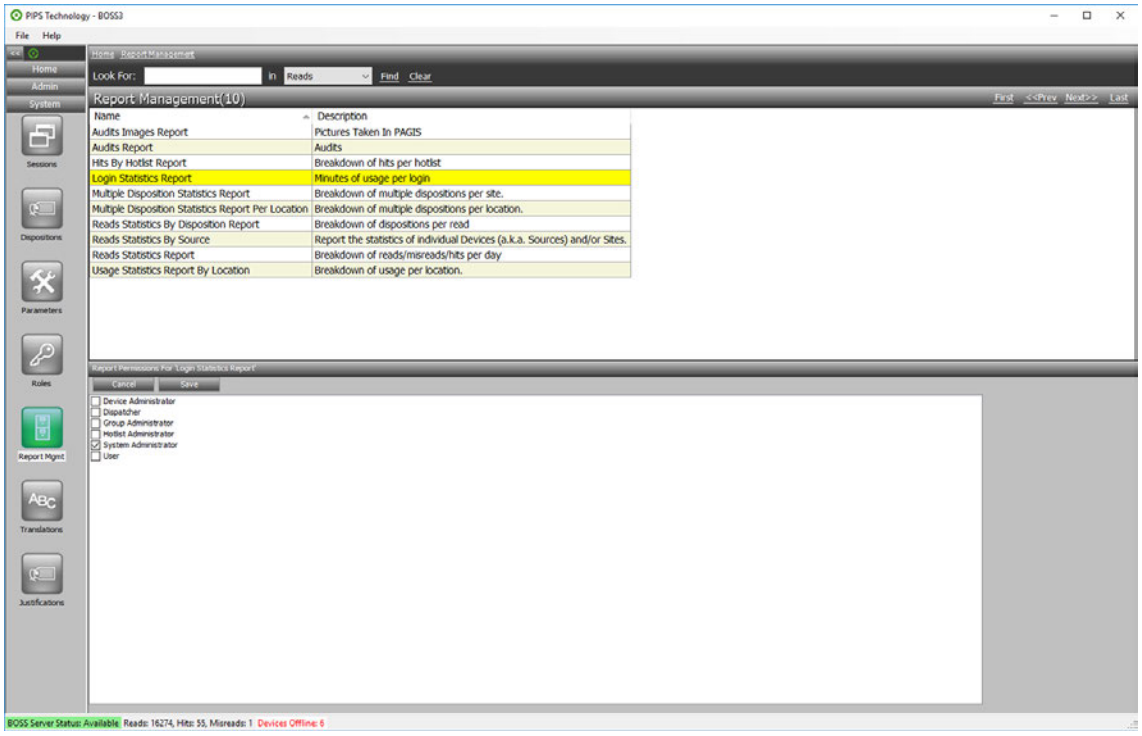
15.4.2 Deleting Roles

1. Select the **System** category on the Shortcut bar.
2. 2. Click the **Roles** shortcut. The Browse/Edit area will display a list of existing roles.
3. 3. Click on an existing role and the edit window will be displayed in the bottom of the window.
4. 4. Click the **Delete** button. Click **Yes** when prompted to complete the operation.

15.5 Report Management

15.5.1 Assigning Permissions to Access Reports

1. Select the **System** category on the shortcut bar.
2. Click the **Reports Mgmt** shortcut. The Browse/Edit area will display a list of available reports.
3. Select a report by clicking the name in the list. The selected report will be highlighted in yellow.
4. Current report permissions for the type of report chosen display in the bottom of the Browse/Edit area. Each BOSS role is listed along with a checkbox. Click a role in the list to select. Click a second time to change an unchecked box to a checked box.
5. After selecting the desired permissions for the report, click the **Save** button.



15.6 Translations

Across various organizations and agencies, terminology related to BOSS can differ significantly. For this reason, a new function added in the BOSS version 3 series gives customers flexibility in naming conventions used in the application. The Translations function provides for changing wording on BOSS screens, which allows a customer to tailor screen labeling to correspond to their own vernacular. Text items in the translations editor correspond to labels on BOSS screens. Authorized users can change these text items as necessary.

Note: This feature is not intended as a replacement for language-specific versions of BOSS. For international versions of BOSS, please contact PIPS™ Technical Support.

15.6.1 Entering a New Translation



1. Select the **System** category on the Shortcut bar.
2. Click the **Translations** shortcut. A list of all current translations appears in the top of the Browse/Edit area.
3. Click the **New** button and the new Translations Entry screen appears in the bottom area.
4. Enter an existing label from the BOSS application in the Caption field, using the exact case and spelling that normally appears on the screen.
5. Enter the desired replacement text in the Translation field.
6. Click the **Save** button to complete the operation.

Note: The user must log off and on again for translation to take effect in the current session.

For Example: A customer preferring to see a label of “Plate” where the software normally uses the term “LPN” would use the translations feature to create the replacement for their installation. The translation Entry Caption field would contain “LPN,” while the Translation field would contain the replacement term “Plate.”

15.7 Justifications

To ensure that sensitive information is being kept secure, systems can be configured to require that users who are performing queries on reads have a valid reason for doing so. Enabling the audit Justification Enabled parameter requires users to justify their reason for querying reads. There are five justifications created by default: Audit, BOLO Post Scan Query, Crime Scene Query, Test and Trend Analysis. These queries will also be documented in audit reports.



15.7.1 Entering a New Justification

1. Select the **System** category on the Shortcut bar.
2. 2. Click the **Justifications** shortcut. A list of all existing justifications appears in the top of the Browse/Edit area.
3. 3. Click on the **New** button. The Justifications Entry screen appears in the bottom area.
4. 4. Enter a justification. There is no validation on the entry for this field.
5. 5. Click the **Save** button to complete the operation.

15.7.2 Deleting Justifications

1. Select the **System** category on the Shortcut bar.
2. 2. Click the **Justifications** shortcut. A list of all existing justifications appears in the top of the Browse/Edit area.
3. 3. Click on the justification to be deleted. The Justifications Edit screen appears in the bottom area.
4. 4. Click the **Delete** button. Click on **Yes** when prompted to complete the operation.

17 APPENDIX: INSTALLATION AND CONFIGURATION

This section is intended for authorized personnel in installation and configuration of a BOSS system. The information in this guide is organized sequentially, in the order that steps would be performed when initially setting up a new BOSS system, with the first section describing the software installation process, and the subsequent sections describing configuration options for a BOSS system.

Upon initial installation of a new BOSS system, the BOSS server application must be configured using the BOSS Controller application. BOSS Administrators may also find the need to modify configuration settings after the system has already been in use. Therefore, the configuration section can be used as an ongoing reference for authorized personnel responsible for maintaining the system.

Note: It is critical that only an IT Administrator or other knowledgeable personnel attempt configuration modifications to a BOSS system. Incorrect configuration settings can cause serious issues with operation and/or adversely affect data integrity. When in doubt, you should consult PIPS Technical Support before making system configuration changes.

OS feature requirements

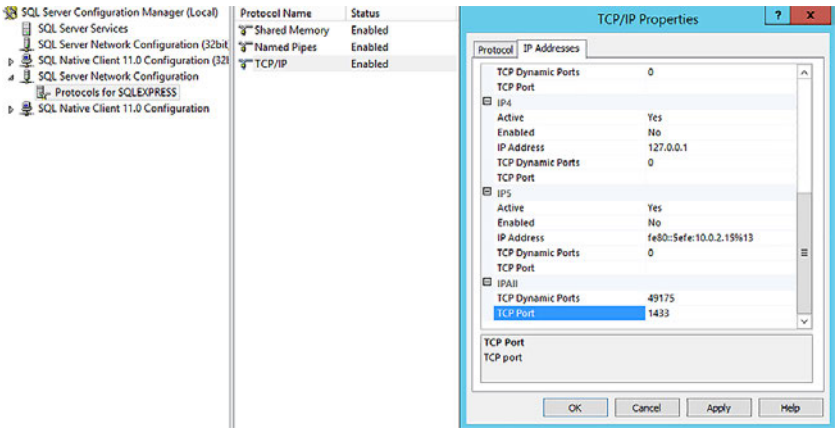
- Windows server 2008 or newer.
- Net. TCP Port Sharing Service must be enabled and running.
- Framework .Net 4.0.

SQL Server Requirements

1. SQL version 2012 or newer required.
2. 2. SQL login account “NT AUTHORITY\SYSTEM” is required to be mapped to Boss3 database as db_owner. For system with existing “Boss3” databases this should be applied prior to Boss software installation. For new installation this can be applied after the Boss service has ran for the first time and created the Boss3 database. See- “Common issues”

Settings under SQL Server Configuration Manger:

3. “SQL Server Network Configurations” Name Pips must be enabled.
4. “SQL Server Network Configurations” TCP/IP must be enabled, with “IP All” set to port 1433.
5. SQL restart required after changes.



17.1 Installing the BOSS Server Application Files

17.1.1 Running the Installer

This guide assumes that the Microsoft SQL Server 2012 or newer instance has already been installed and is available. If the SQL Server is not available, stop now and continue installation after the SQL Server has been installed. To install the Microsoft SQL Server, please follow the instructions provided by Microsoft.

Note: 1. It is recommended that antivirus utilities be disabled during the install.

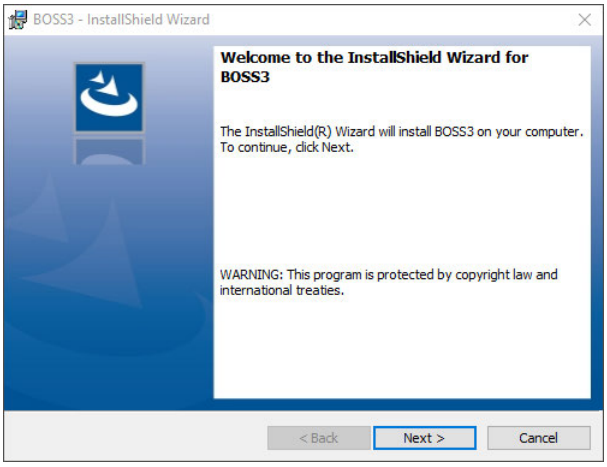
To commence the installation:

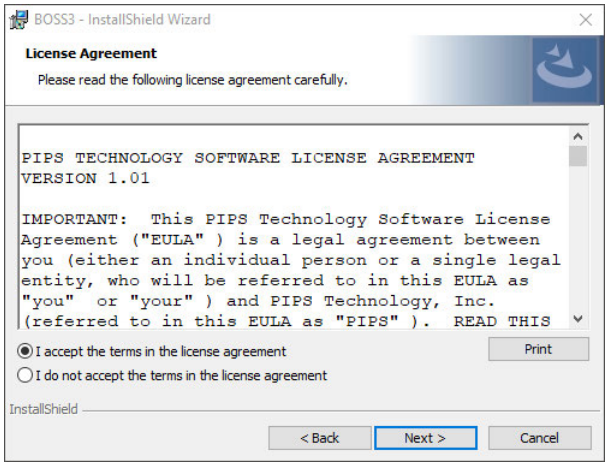
1. Select the link supplied by PIPS to the BOSS installation application.
2. Run the BOSS Setup executable.

Note: Right-click on the installer icon and select Run As Administrator.

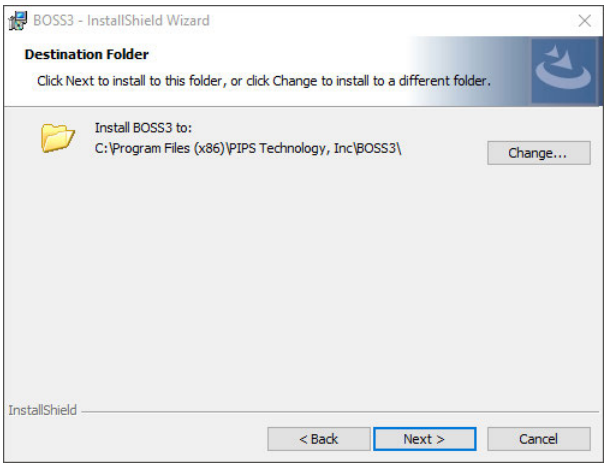
17.1.2 License Agreement

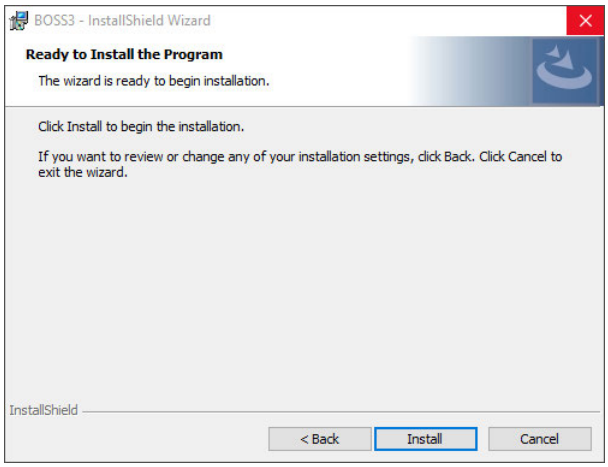
1. Click **Next** then check the license agreement checkbox to acknowledge agreement with the license terms.
2. Click **Next** to continue.



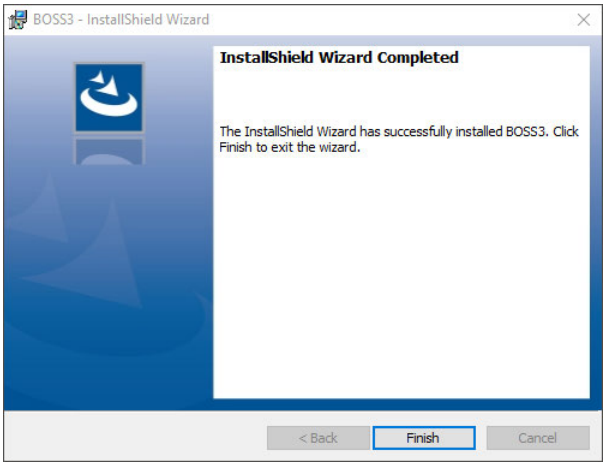


3. Accept the default installation file path or change.
4. Click “Next” to proceed to “Install”





5. When the Installation Complete message is displayed, click **Finish** to proceed to the Licensing.

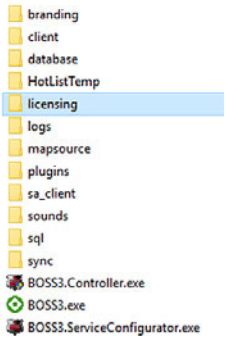


17.2 License Key Management

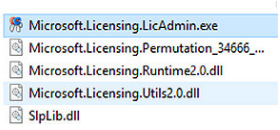
17.2.1 Activating the License Key

Following a new installation, a valid BOSS license key must be entered. There are three options available discussed in the sections below that can be used to activate the license. For upgrades or reinstallation on same server this step is not required as the licensing tool will automagical re-acquire the licensing code.

1. Navigate to the licensing folder in the BOSS3 installation folder.



2. Start Microsoft License Manager (Microsoft.Licensing.LicAdmin.exe). This must be run as an Administrator.



3. In the License Manager User interface, select **File → Activation Wizard** to install the new license
4. When the Activation Wizard dialog opens select one of the following:
   a. I want to activate the software over the Internet. *See Section 17.2.1.1.*

   or

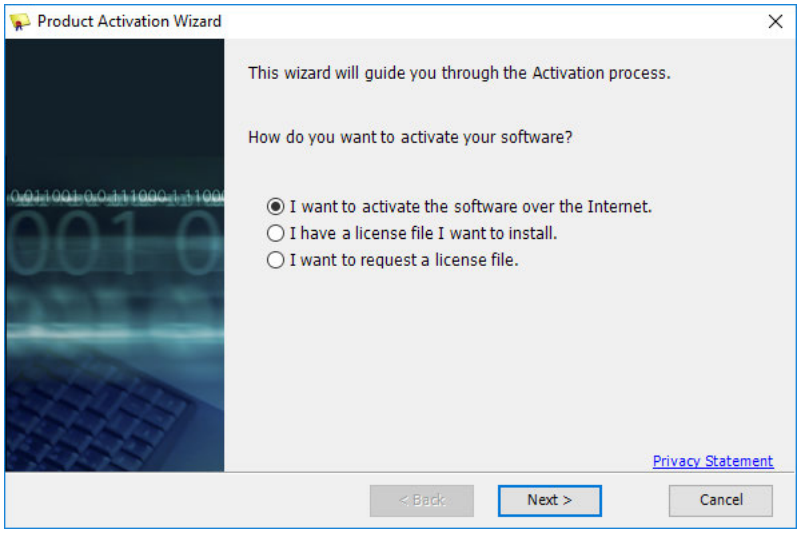
   b. I have a license file I want to install. *See Section 17.2.1.2.*

   or

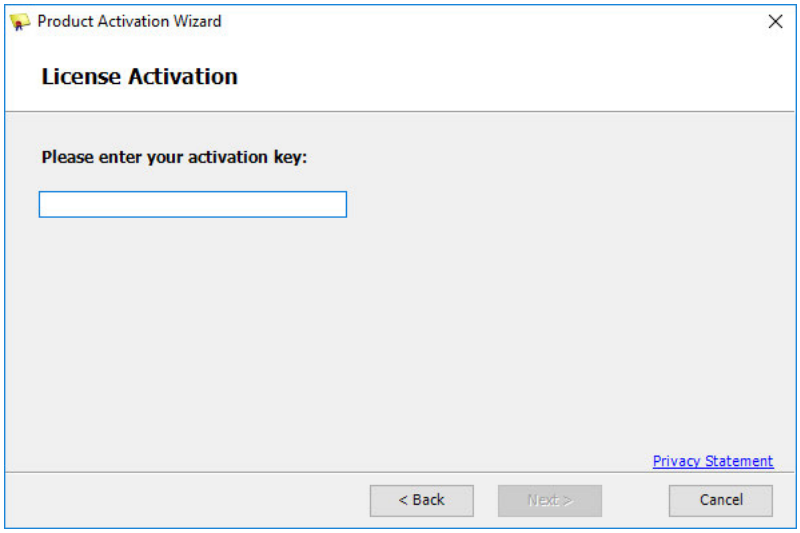
   c. I want to request a license file. *See Section 17.2.1.3.*

17.2.1.1 Activating the License Key over the Internet

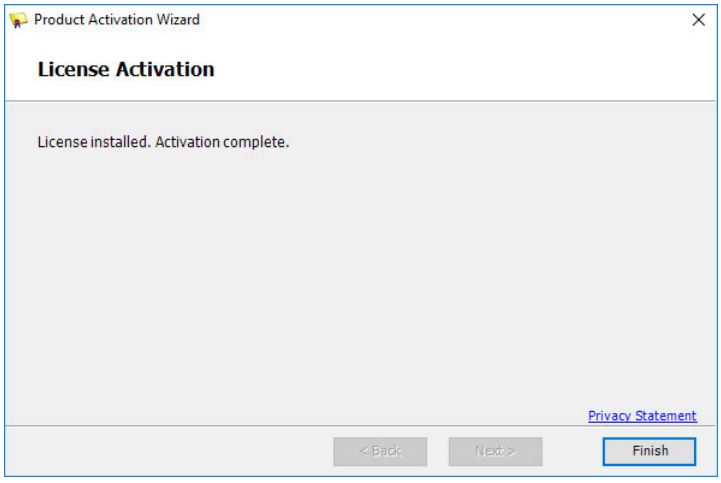
1. Check **I want to activate the software** over the Internet.
2. Click **Next** to continue.



3. Enter the activation key provided by PIPS and click **Next**.



4. The license key will be activated over the Internet. The following screen will display. Click **Finish** to continue.



17.2.1.2 Activating the Software with a License File

1. Check I have a license file I want to install.
2. Click **Next** to continue.
3. Navigate to the location of the license file and select it.
4. Click **Next** to continue.
5. When the activation is completed click **Finish**.

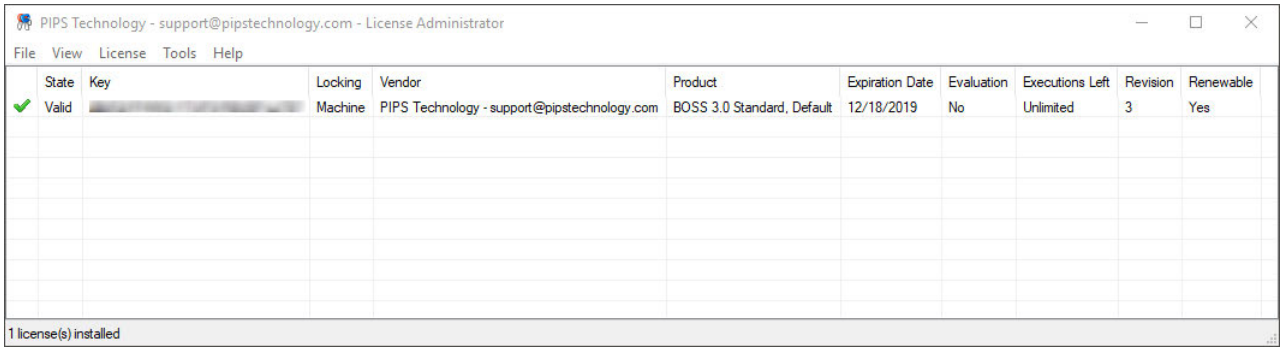
17.2.1.3 Request a License File to Activate the License

1. Click **I want to request a license file**. Press Next.
2. Enter the license key you received previously. Press **Next**.
3. In the screen that displays, copy the text block highlighted (starts with "—BEGIN Request") to the clipboard and paste it into an email. Send the email to PIPS Technical Support (support@pipstechnology.com).
4. Close the Activation Wizard by clicking the **Finish** button.
5. You will be sent an activation file via email. Extract the license file (*.bin) and copy it to a folder on the computer where BOSS is installed. Return to Section 17.2.2 and follow the steps to activate the license.

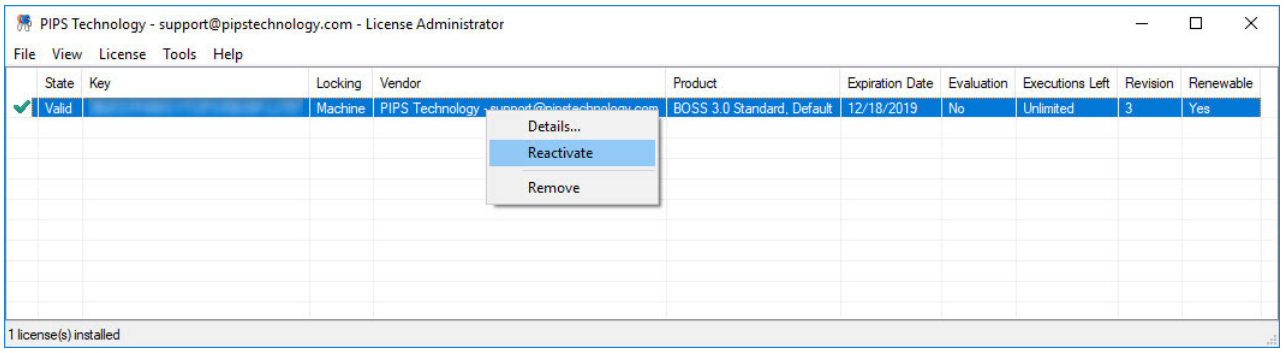
17.2.2 Updating a License Key

If the BOSS license key becomes invalid, or if the license is upgraded, follow these steps to reactivate a BOSS license key:

1. Start Windows Explorer on the BOSS server.
2. Navigate to the folder where the BOSS server application is installed (by default C:\Program Files\PIPS Technology, Inc\BOSS3).
3. Locate the licensing folder as described in Section 17.2.1.
4. Open the folder and right click on the application Microsoft.Licensing.LicAdmin.exe. Select to run as the Administrator. You will see the following screen:



5. Select the license key. Right-click, and from the context menu, select Reactivate.



6. Click Next.
7. When the Installation Complete message is displayed, click Finish.

17.3 Map Display Options with BOSS

BOSS can display collected plate read information plotted on a map. There are two different mechanisms for displaying maps within the BOSS Smart Client application.

17.3.1 U.S. Census Bureau TIGER Maps

U.S Census Bureau TIGER Maps now discontinued.

17.3.2 Advanced Mapping with Internet Maps

PIPS provides an option to purchase an "Advanced Mapping" feature with BOSS. This option enables integration of Maps, an Internet-based service that BOSS can use to display maps in the Smart Client application.

Note: In order to use Advanced Mapping, the BOSS Smart Client will need an unimpeded Internet connection.

17.4 Configuring the BOSS Server Application

After the BOSS installation is completed, the application must be configured using the BOSS Controller program. The following sections explain how to use this program as well as the configuration settings that are available.

17.4.1 The BOSS Controller Application

17.4.1.1 Starting the Boss Controller

BOSS Controller (BOSS3.Controller.exe) is the application used to configure and control the BOSS service. The BOSS Controller is installed on the server computer along with the server application. After the installation is complete the Controller program will start automatically. If this is a new installation the license will need to be activated first. Choose to configure BOSS at a later time by clicking on Cancel.

The shortcut to the BOSS Controller program can be found on the desktop or in the All Programs → PIPS Technology → BOSS3 menu. Right-click on the Controller icon and select Run As Administrator. When the BOSS Controller program is started an icon for the application will appear in the Windows System Tray at the lower right corner of the desktop.

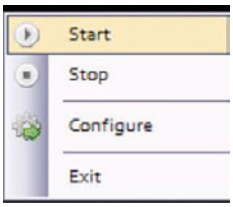


17.4.1.2 Status Colors

The icon for the Controller program includes a "traffic light" that uses a color indicator to show the status of the BOSS service application. When the BOSS service application is running, the indicator is green. When the BOSS service application is not running, the indicator is red. Yellow color indicates that the application is changing state (starting or stopping).

17.4.1.3 Right-Click Menu

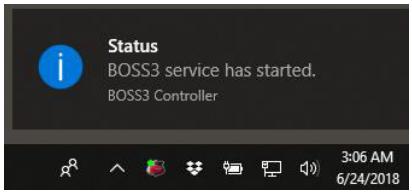
When you right-click the BOSS Controller System Tray icon, a pop-up menu will appear:



Start	Start the BOSS service.
Stop	Stop the BOSS service.
Configure	Present the BOSS Configuration Wizard.
Exit	Close the BOSS Controller application. (Note: This closes the BOSS Controller program, but does not stop the BOSS Service.)

17.4.1.4 Starting the BOSS Service

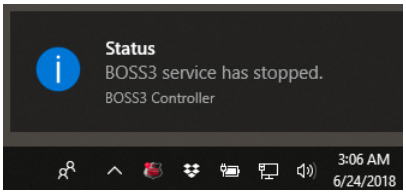
When the **Start** action is selected, and the service starts successfully, a Success message will be displayed:



The traffic light in the BOSS Controller icon will turn green to indicate the status.

17.4.1.5 Stopping the BOSS Service

When the **Stop** action is selected, and the service stops successfully, another Success message will be displayed, and the traffic light changes to red:

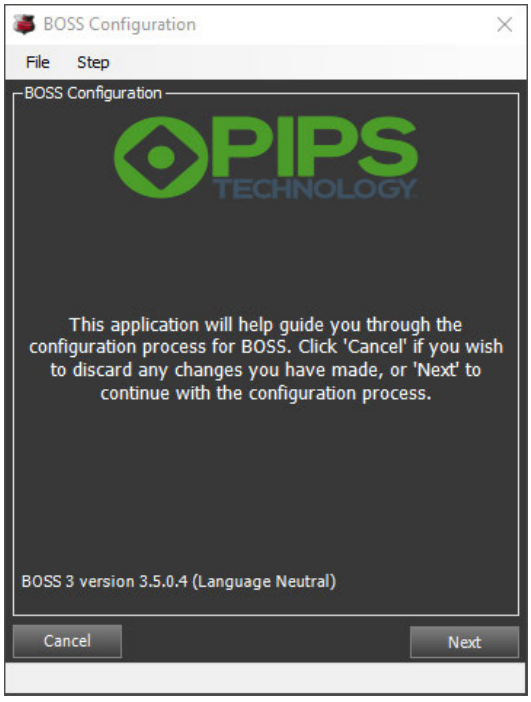


17.4.2 BOSS Configuration

17.4.2.1 Activating the Configuration Wizard

1. Right-click the **Controller System Tray** icon.
2. Select the **Configure** option. The Configuration Wizard options are explained in the following sections.

17.4.2.2 BOSS Configuration Wizard



Step through all configuration screens in the BOSS Configuration Wizard by simply clicking the **Next** button on this first screen. Click **Next** on each subsequent screen after entering in the desired settings. Note: This step-by-step process is recommended when you are configuring the system for the first time.

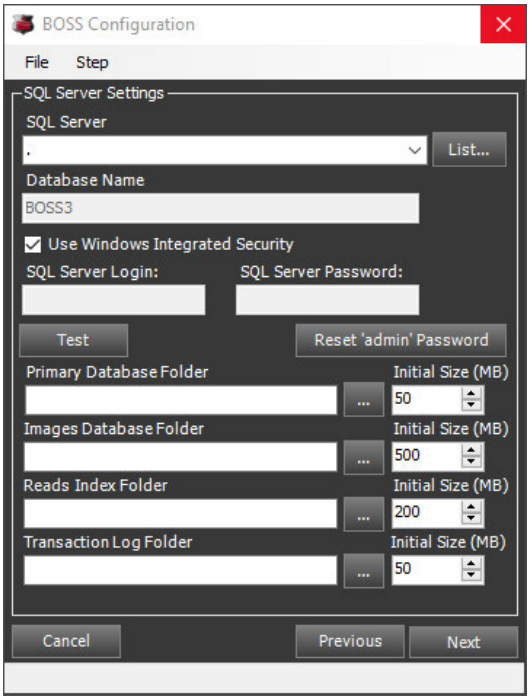
OR

Click the **Step** menu option to access the configuration menu and proceed to the step choice.

For each configuration step (described in Sections 17.4.2.3 – 17.4.2.9), clicking **Next** will take you to the next configuration screen, clicking **Previous** will take you to the previous one, and clicking Cancel will clear any changes you have made on the current screen.

17.4.2.3 SQL Server Configuration

SQL Server configuration is required for a new BOSS system, in order to specify the location and necessary authentication information for the SQL database.

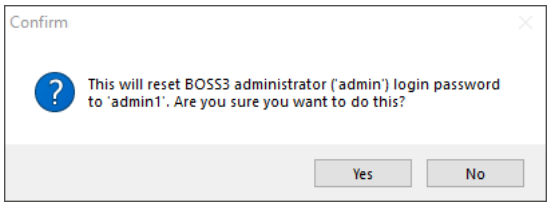


SQL Server – Select the SQL Server instance for BOSS. Press **List** to choose from a list of available SQL Servers. The SQL Server Browser service must be running at this point. You may also type in the server IP address or host name. Enter a dot "." to use a local SQL Server that is running on the same machine as the BOSS service.
Use Windows Integrated Security – If checked, BOSS will use Windows Integrated Security to access the SQL Server database.
SQL Server Login and SQL Server Password – If Windows Integrated Security is not selected, enter the SQL Server username and password provided for BOSS to use to access the database.
Test – The **Test** button can be used to test the SQL Server settings currently in place. The Test button initiates a connection. A message box will appear to indicate whether the test connection fails or succeeds.
Database file locations: BOSS database can be divided among multiple locations as follows if necessary. When selecting a folder path for the database files keep in-mind that the folder path is referenced from the standpoint of the SQL server location.
Primary Database Folder – The drive and folder where the BOSS primary database will reside.
Images Database Folder – The drive and folder where the BOSS will store images.
Reads Index Folder – The drive and folder where BOSS will store database indices for stored plate reads.
Transaction Log Folder – The drive and folder where BOSS will store the database transaction log file.
Initial Database Sizes - By Default Boss will predefines the sizes as indicated in the controller.



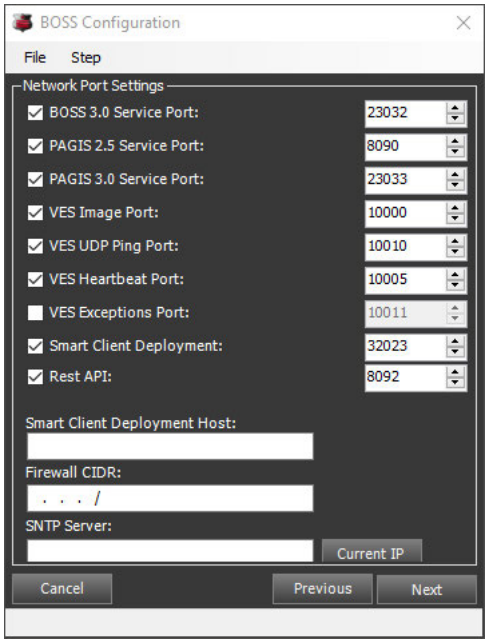
17.4.2.4 Resetting the Administrator Password

If you have forgotten the BOSS administrator (admin) password, you can press the **Reset 'admin' password** button to reset the password to "admin1."



Pressing **Yes** will immediately reset the password.

17.4.2.5 Network Port Settings



BOSS uses a number of TCP/IP and UDP network ports for communication between server and client applications and server and license plate reading devices.

17.4.2.5 Network Port Settings (continued)

FIELD	DESCRIPTION	DEFAULT PORT
BOSS 3.0 Service Port	TCP/IP port used to provide access for BOSS Smart Clients	**23032**
PAGIS 2.5 Service Port	TCP/IP port used to provide access for older mobile client versions older than Pagis 2.6.8	**8090**
PAGIS 3.0 Service Port	TCP/IP port used to provide access to various mobile client versions	**23033**
VES Image Port	TCP/IP port used to receive reads from fixed cameras	**10000**
VES UDP Ping Port	UDP port used to receive keep alive ping messages from fixed cameras	**10010**
VES Heartbeat Port	TCP/IP port used to receive heartbeat status messages from fixed cameras	**10005**
VES Exceptions Port	TCP/IP port used to receive exceptions messages from fixed cameras	**10011**
Smart Client Deployment	TCP/IP port used for BOSS client installations via BOSS server	**32023**
REST API Port	HTML port used for the communication between the BOSS service and newer versions of PAGIS	**8092**

If the checkbox in front of the port name is left unchecked, the corresponding connection will be disabled.

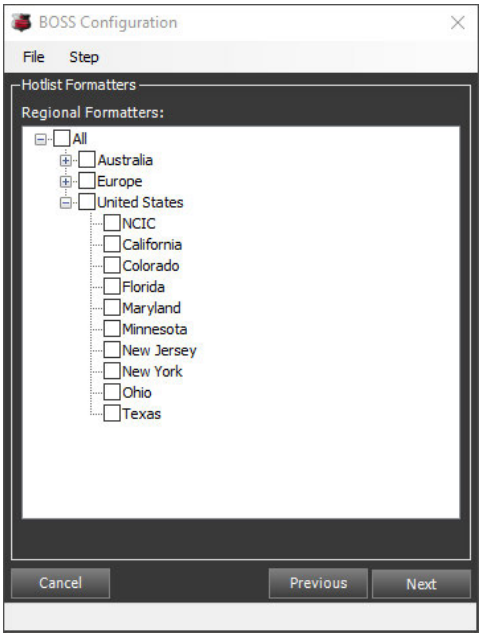
Smart Client Deployment Host – If this information is entered, BOSS Smart Clients will use the given hostname to distribute the smart client application. This can be left blank to use the local host name.

Firewall CIDR – BOSS provides a built-in firewall for incoming fixed camera connections. If a value is entered, only cameras with an IP address matching the CIDR will be allowed to connect. CIDR (Classless Inter-Domain Routing) is a standard industry method for specifying a range of included IP addresses. The format of the CIDR entry is A.B.C.D/N, in which the dotted decimal portion before the "/" is interpreted, like an IPv4 address, as a 32-bit binary number that has been broken into four octets. The value of N indicates the number of shared initial bits, counting from the left-hand side of the address.

For Example: For an entry of 10.200.200.255/24, the CIDR value 24 leaves 8 bits that can be changed. Therefore, addresses 10.200.200.x are permitted addresses.

SNTP Server – BOSS has a built-in time service. The fixed ANPR/ALPR cameras do not support automatic daylight savings time (DST) adjustment. The BOSS time service provides a customized SNTP service for these cameras in order to support DST. To use the built-in time service, Windows Time Service has to be disabled in the Services Control panel, and the BOSS time server IP address entered in this field.

17.4.2.6 Regional Hotlist Formatters

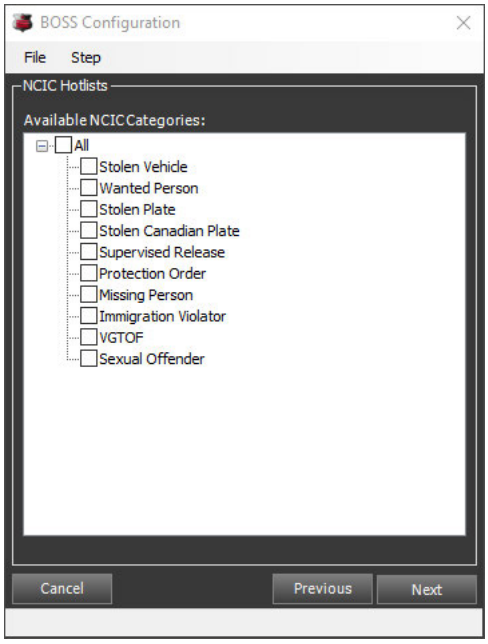


The BOSS allows the selection of predefined hotlist formatters. These formatters define the input format (structure) of hotlist data files. Custom formatters can be defined via the BOSS Smart Client application *(see Section 13 of this manual for more information)*. Also, when installing BOSS in the United States, National Crime Information Center (NCIC) data formatters can be selected for specific states (see section following).

To select or unselect formatters, click on the formatter title to add or remove a check mark. Additional formatters can be added to a system as needed. These will be provided by PIPS Technical Support upon request.

17.4.2.7 NCIC Hotlist Formatters

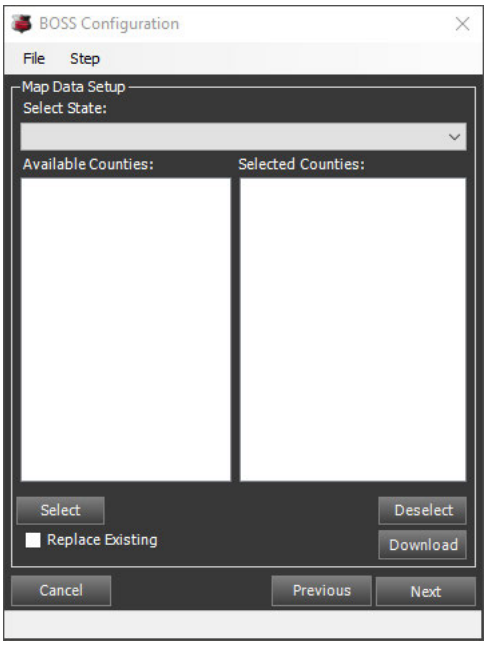
BOSS supports hotlist import in the United States National Crime Information Center data format. This option is available only in the United States.



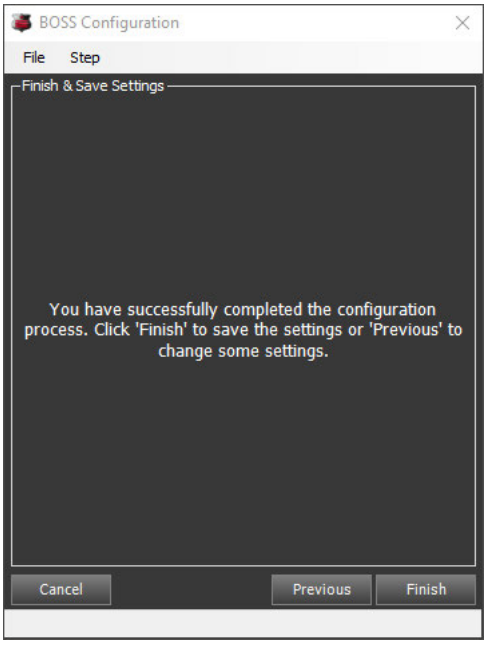
To configure formatters for the desired categories, check those categories. Once the desired categories have been selected, press **Next** to proceed.

17.4.2.8 Map Data Setup

U.S Census Bureau TIGER Maps now discontinued. Do not utilize this section, click “Next”



17.4.2.9 Finishing Configuration



Click **Finish** to complete configuration. BOSS will save the chosen configuration.

17.5 Installing the BOSSUI Smart Client Application

17.5.1 Installation over the Web

To initiate a web installation on a workstation, start up Microsoft Internet Explorer and navigate to this web address: **http://{boss_server_ IP_address}:32023/publish.htm**, where {boss_server_IP_address} is the address of the server running the BOSS server application.

For Example: To install the Smart Client on the BOSS server itself, navigate to http://127.0.0.1:32023/publish.htm. The installation webpage will be presented. The advantage of installing the Smart Client over a web browser is that the application will automatically check for updated versions every time it is started.

17.5.2 Stand-Alone Installation

The BOSS Smart Client is a zero-administration desktop application meant for administration of the BOSS server application and querying data collected in the BOSS database as described in this manual. The BOSS Smart Client is installed as a single executable program. This program can be copied to any Windows workstation, or to a shared network drive.

To install the stand-alone application:

1. Start Windows Explorer on the BOSS server.
2. Navigate to the folder where the BOSS server application is installed (**by default C:\Program Files\PIPS Technology, Inc\BOSS3**)
3. Locate folder **sa_client.**
4. Copy the **sa_client** folder to the workstation or shared network folder of choice.

17.6 Configuring Client Tools

Client Tools is used to transfer any files needed during an Pagis shift from BOSS to an Pagis system that is being run in the Disk Sync mode. *See Section 13, Client Tools, and the Pagis Software User's Manual.*

Client Tools does not have a customary interface. Once the utility is started, the Client Tools icon will appear in the Windows System Tray. Before use, Client Tools must be configured and can be quickly completed with the simple configuration wizard provided:

1. To start the wizard, right-click the icon and select **Configure**. The initial screen provides information about the tool.
2. Click **Next** to continue the configuration, or **Cancel** to exit the wizard.
3. Enter a path so that Client Tools knows where to store the files it creates and where to look for files to process. This path can be a local, network, or external drive. Enter the path or click on the … button and browse to the location.
4. If the Begin Shift files that Client Tools creates need to be encrypted, click **Encrypt Output**. Click **Previous** to return to the previous screen, or click **Next** to continue.
5. The data used to create the Begin Shift files is created and managed in BOSS. Client Tools needs to know where the BOSS Server is located. Enter the server IP and the port to use to connect to it. Click **Previous** to return to the previous screen, or click **Next** to continue.
6. The final screen provides additional information on how to use the wizard. Click **Previous** to return to the previous screen, or click **Finish** to save the changes and exit.

Common Issues

Missing Permissions on the database user

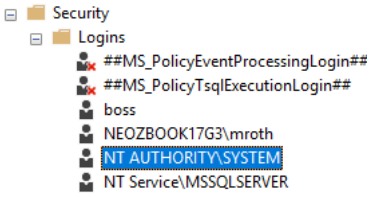
PIPS Boss service does not start: If the service does not start after two tries, go to the logs file located in "C:\Program files(x86)\PIPS Technology, Inc\BOSS3\logs", there look for the following message:

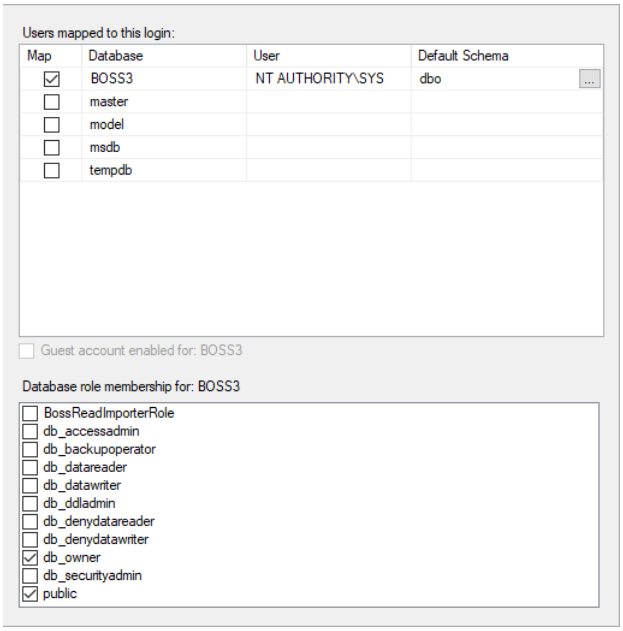
a. The server principal "user" is not able to access the database "BOSS3" under the current security context:
This problem is caused by missing permissions in the database user you are using.
To fix this problem you need to go to the Microsoft SQL Server Management Studio application and connect with a user with sysadmin privileges, inside the object explorer expand the folder Security, within the logins folder identify your user, right click on the user and select Properties. Inside "Server Roles" mark the sysadmin box.
After this restart the BOSS service.

The Underlying Provider failed

When a read query is made, the application shows the message **The Underlying Provider failed**

a. Inside the logs file, look for the line with the message "Login failed for user" identify the user, example- "Login failed for user 'NT AUTHORITY\SYSTEM". If this occurs log into SQL Studio Manager and map the BOSS3 Db to that account, also add the membership role of "db_owner" to the account.





Failed login

Check that the service is running, and the credentials are valid, also, check the server configurations, if you have localhost instead of 127.0.0.1 replace it for 127.0.0.1. If the problem persists go to the logs file and identify the error and contact PIPS customer support support@pipstechnology.com.

Relocating BOSS3 database

- When an upgrade requires you to move your existing BOSS3 database to a new location follow the recommend step in our "PIPS Relocate Boss Data Files" document for step by step instructions.

18 Appendix: Troubleshooting

When troubleshooting an issue, always start by looking for error messages in the Server log file, usually found at ...\PIPS Technology, Inc\ BOSS3\logs\BOSSServerLog.txt. Proceed based on the following information, recognizing that escalation may be necessary. If so, obtain a copy of the complete error message and include it with all escalated documentation.

ISSUE REPORTED	EXPLANATION	STEPS TO CORRECT
Just after an installation/upgrade, the UI won't start.	It takes several moments for the BOSS Server to be completely started and ready for information to be accessed.	After starting the BOSS server, wait for several moments before attempting to start the UI. If this is an upgrade this could be several minutes while the database is being updated.
I start the BOSS Controller, but it stops a moment later. The following error message may display "Error: Error in BOSS3 Controller. Please check the log files." (New installation scenario)	The license was not activated. When checking the BOSS Server Log, there will be two error messages : – 'Licensed for 0 concurrent clients' and – 'Failed to set registry parameter [_tmpbaliked a63] to value System.Byte[].'	Return to the licensing activation and updating checklist. (*See Section 17.2, BOSS Version 3.2 and Above License Key Management.*)
I start the BOSS Controller, but it stops a moment later. The following error message may display "Error: Error in BOSS3 Controller. Please check the log files." (Upgrade scenario)	The Upgrade Tool must be run before starting the Controller.	Run the Upgrade Tool. (*See Section 17.7 The BOSS Upgrade Tool.*)
I start the BOSS Controller, but it stops a moment later. The following error message may display "Error: Error in BOSS3 Controller. Please check the log files." (Other scenario)	If the Upgrade Tool has been run, there may be a problem with the database.	Look for error messages in the BOSS Server Log. Provide this information to Technical Support.
A fixed camera won't connect.	The firewall could be blocking the communications.	Ensure that the firewall is allowing communications through the VES ports, found in the BOSS Configuration Controller on the Ports screen.
PAGIS won't connect.	The firewall could be blocking the communications.	– Ensure that the firewall is allowing communications through the REST API (for PAGIS 2.7.x) and PAGIS 3.0 Service (for versions of PAGIS) ports, found in the BOSS Configuration Controller on the Ports screen. – Ensure that the device has been enabled in the BOSS UI Devices screen.
Hotlist will not update.	There is typically a problem with the source file.	– If it is a network hotlist, ensure that the site can be reached by entering the address in a browser. – If a local hotlist, ensure that the file is on the system and can be opened.
The NCIC Hotlist formatter that I need is not available. (New installation scenario)	The NCIC formatters were not added during the initial installation.	Stop the BOSS Service. Go to the Configure option on the BOSS Controller. Step to the NCIC screen. Select the desired NCIC formatters. Click **Save** and exit. Restart the BOSS Service. The formatters will now be available.

ISSUE REPORTED	EXPLANATION	STEPS TO CORRECT
I am unable to see reads/hits in the Dispatch screen.	The time on the read/hit coming in must be relatively close, within a couple of minutes, to the BOSS server time.	For a mobile ALPR system, correct the time on the laptop or ALPR processor. A fixed camera can be configured to use a time server. If issue persists, the server that BOSS is running on could also be configured to sync with a time server.
An error message, "Compressed method not supported," was found in the BOSS Server Log.	There are various reasons that this message can occur.	Obtain a copy of the complete error message. Provide this information to Technical Support.
An error message, "Transaction has aborted," was found in the BOSS Server Log.	There are various reasons that this message can occur.	Obtain a copy of the complete error message. Provide this information to Technical Support.
An error message. "Error #nn appeared in the db for Stored Procedure xxxx on line nn." was found in the BOSS Server Log.	An error occurred when running the stored procedure listed in the message.	Obtain a copy of the complete error message. Provide this information to Technical Support.
An error message, "Timeout expired. The timeout period elapsed prior to completion of the operation or the server is not responding," was found in the BOSS Server Log.	A SQL timeout error has occurred.	Obtain a copy of the complete error message. Provide this information to Technical Support.
An error message, "SNTP server not started, could not bind to InterNetwork 0.0.0.0:123," was found in the BOSS Server Log.	This is an expected error message that occurs when BOSS has not been configured to access a time server.	If no time server has been configured, this message can be ignored. If one has been configured, this needs to be escalated for further assistance.
After a new installation, the BOSS server stops running with an error message, "Failed in working with the database. Ensure connectivity is properly defined. Try running the BOSS Controller again and checking settings," was found in the BOSS Server Log.	When BOSS was started, there was a connection issue between it and the SQL Server.	Start by checking the information in the Controller. If that is all correct, then check to ensure that the SQL Server is running. If no issues are found there contact Technical Support Obtain a copy of the complete error message.
After a new installation, the BOSS Server stops with no error message in the BOSS Server Log.	The server needs to be run with Administrator privileges.	The server should be restarted in the Console as an Administrator. If running BOSS as a service then the BOSS Controller must be run as Administrator.
Error message in BOSS Server Log says that the file "httpconfig.exe" cannot be found.	This is an error that can occur when the system has not been updated in some time. It has been seen for other uncertain reasons as well.	Obtain a copy of the complete error message. Provide this information to Technical Support.
After a new installation, the BOSS Server starts but stops moments later. The BOSS Server Log contains the error message. "The system cannot find the file specified Additional Exception Message: Unhandled exception from 'Name:BOSS3.exe. There are no context policies." However, no file is listed in the message.	This typically occurs on older systems, especially Windows Server 2003, or systems that have not been updated for a while.	The file httpcfg.exe needs to be copied into the c\Windows\System32 directory.
The BOSS Server won't start, and there is an error message, "Transport Manager failed to listen on the supplied UIR using the NetTcpPortSharing service: failed to start the service because it is disabled," in the BOSS Server Log.	The NetTcpPortSharing Service is not running.	Obtain a copy of the complete error message. Provide this information to Technical Support.
The BOSS server stops running, and there is an error message, "Cannot open database "<Database Name>," in the BOSS Server Log.	There is an issue with the connection between the BOSS server and the SQL Server.	Start by checking the information in the Controller. If correct, then check to ensure that the SQL Server is running. If no issues are found contact Technical Support. Obtain a copy of the complete error message.

ISSUE REPORTED	EXPLANATION	STEPS TO CORRECT
The BOSS Server won't start and there is an error message "A file activation error occurred. The physical file name '<filename>' may be incorrect." in the BOSS Server Log.	There could be multiple reasons, but it is probably due to a database connection issue.	Obtain a copy of the complete error message. Provide this information to Technical Support.
When running the upgrade tool, an error message is displayed. A message is included in the BOSS Server Log: "Current upgrade state: One of the upgrade scripts failed to run as expected. Please contact support for direction."	This most likely occurred due to upgrading from an old version of BOSS.	Obtain a copy of the complete error message. Provide this information to Technical Support.
An unexpected response or behavior occurs in BOSS, and there is an error message, "Object reference not set to an instance of an object," in the BOSS Server Log.	This is a generic error message that can occur for various reasons.	Unless the issue has an obvious cause contact Technical Support. Obtain a copy of the complete error message.
The following error message, "Discarding tmp buffer because it's corrupted," has been found in the BOSS Server Log.	This message is associated with a database issue.	Obtain a copy of the complete error message. Provide the information to Technical Support.
The following error message, "SMTP server is not defined, email alerts disabled," has been found in the BOSS Server Log.	This message is informational indicating, as it states, that an email server has not been configured.	If attempts have been made to configure an email server and this error message occurs, recheck the settings and the server. If the error remains contact Technical Support.
The BOSS Service stops running, and the BOSS UI indicates that the server is not available. The following error message, "Cannot access a disposed object," is found in the BOSS UI Log.	This is an informational message provided by the UI confirming that it is no longer able to communicate with the BOSS server.	Restart the BOSS server and the BOSS UI will reconnect. If this does not correct the issue contact Technical Support.
The following error message, "The socket connection was aborted," is found in the BOSS UI Log.	This is an informational message provided by the UI confirming that it is no longer able to communicate with the BOSS server.	Restart the BOSS server, and the BOSS UI will reconnect. If this does not correct the issue contact Technical Support.
A problem occurs while adding a hotlist and the following error message "Invalid object name '<hotlist name here>'," has been found in the BOSS Server Log.	This indicates that there is an issue with the hotlist formatter being used.	Confirm that the correct formatter is being used. If so, confirm the source file is formatted correctly. If so, contact Technical Support. Provide a copy of the full error message.
While installing BOSS, an error message displays: "Error opening file for writing: <File Name>."	This indicates that the application listed in the error message is still running.	Check the Windows System Tray for any BOSS applications still running on the system. Close the application(s) and continue the installation.
The BOSS applications are installed under one user, but are not found when another user logs in.	The application was not installed using administrative privileges.	The application will need to be uninstalled and reinstalled using administrative privileges.
While using Client Tools to create Begin Shift files, an error message displays: "Client has not been activated on the server."	Mobile devices must be enabled on BOSS to synchronize data to it. This message is displayed the first time that Client Tools is used to create Begin Shift files because it has not been enabled yet.	Configure Client Tools on BOSS (see Section 17.6) so that BOSS adds Client Tools as a device.
When using Client Tools to synchronize End Shift files to BOSS, the following error message displays: "Error: Could not find <file and path name>."	Client Tools was unable to find the End Shift files to be processed at the defined path.	Check that the location assigned for the End Shift file matches the location chosen when Client Tools was configured. If it does not, move the file to the configured location.

19 Appendix: Plug-Ins

BOSS allows the use of third-party code via a plug-in that serves the needs of BOSS customers with specific data requirements. Once a plug- in is created and compiled, a copy of the DLL and any other necessary files can be copied to the plug-ins directory under BOSS. BOSS will automatically detect the existence of the plug-in at that point and permit reads to be passed to the ReceiveData method of your plug-in.

The functions of the currently available BOSS plug-ins are described in Sections 19.1 and 19.2. For more information and guidance on installing a plug-in, contact PIPS Technical Support for guidance.

19.1 The BOSS Truck Drayage Utility

Regulation of diesel-fueled heavy-duty trucks and a Drayage Truck Registry (DTR) were implemented by the California Air Resources Board (ARB) to help reduce both emissions from these vehicles and public exposure to contaminants in those emissions. Drayage trucks subject to regulation (Class 7 and Class 8) are registered and information about them is maintained on an ARB web service.

The Truck Drayage Utility is BOSS plug-in that provides access to the ARB web service. The utility is designed to contact the web service, retrieve data, and add it to a comma-separated values file. In BOSS, the Hotlist Administrator will then create a whitelist that uses this CSV file as the source file.

The connection to the ARB web service (managed by the Windows Task Scheduler) can be made once daily for a full download of the data, with subsequent connections allowed no more frequently then every 30 minutes for updates. This whitelist can then be deployed to a mobile or fixed camera in the monitored area. If a plate is read that is not included on the whitelist, a notification will be displayed in BOSS. Appropriate action can be taken at that time.

If the ARB web service is unavailable and downloads cannot be completed, the BOSS whitelist will not be updated. There will also be warning messages in the BOSS log such as “Could not connect to <web service address>. TCP error code nnnnn: <Error description>.” If this occurs, the utility will try again in 30 minutes. If the errors persist, it may be necessary to seek assistance.

19.2 The BOSS LPRD Plug-in

The BOSS LPRD plug-in relays the reads the BOSS server receives on to the national database at the Automated Regional Justice Information System (ARJIS), a joint powers agency that facilitates information-sharing among more than 70 law enforcement agencies—local, state, and federal—in the two California counties (San Diego and Imperial) that border Mexico. ARJIS operates a secure intranet (ARJISnet) with more than 11,000 users in San Diego County alone.

19.3 The BOSS DEA Plug-in

The BOSS DEA plug-in writes LPR messages to the file system as reads are received by the BOSS server. Those files will then be available for the Drug Enforcement Agency, DEA, File Transporter to act upon.

20 Appendix: BOSS Mantis

The Mantis service adds analytical analyses to new and existing read images within BOSS providing the user the ability to search based on vehicle Type, Brand, Color & Unique markings. BOSS Mantis is an additional PAID service that can be enabled on BOSS versions 3.6.x.x and above, older version of BOSS can support this feature by upgrading, providing they meet the system

20.1 How Dose Mantis Work

The service is hosted in the Amazon Web Services (AWS) Elastic Compute Cloud (EC2) platform, running in instances comprised mainly by Graphics Processing Units (GPUs). The only information sent to the Mantis endpoint is the vehicle image, known as the Overview image by the BOSS. Communication between BOSS and Mantis is performed as a client-server architecture, meaning the Mantis server uses the 443 (https) port to allow clients to reach the Mantis endpoint.

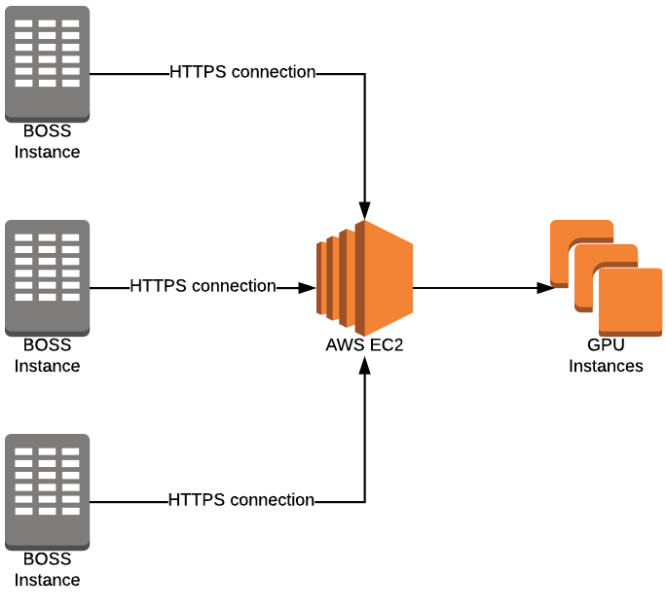


Figure 1 Multiple BOSS instances connected to the Mantis API.:

The information between BOSS and Mantis flows only in one way, this means that only BOSS clients can send data to Mantis, where it will be processed, and a response will be received by the BOSS server. Mantis cannot reach the BOSS Server or perform any kind of operations on the user's behalf over the data stored inside BOSS.

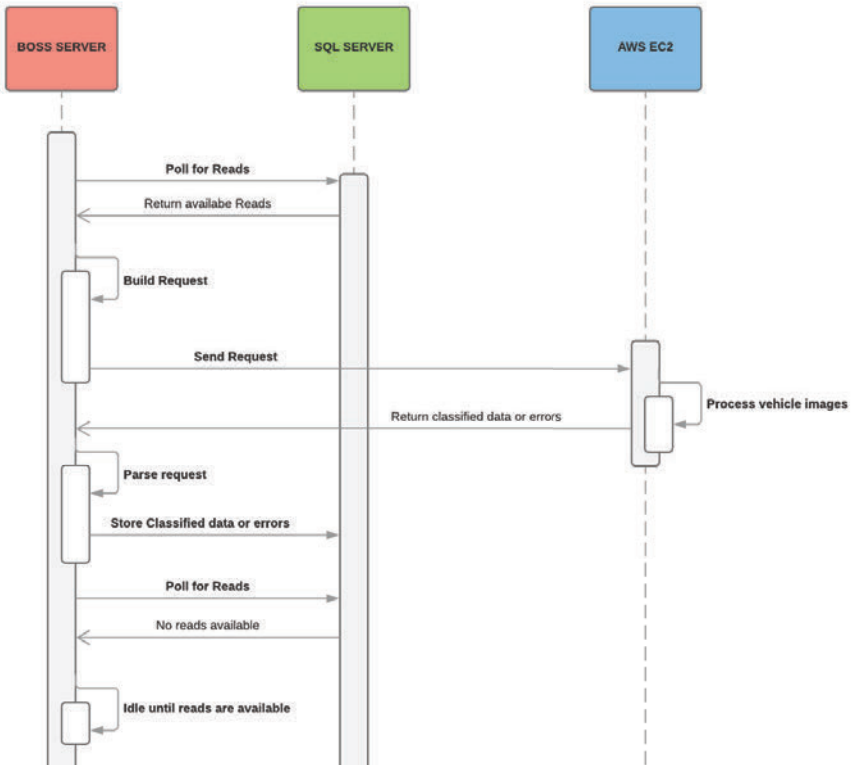


Figure 2 Sequence diagram for the current BOSS-Mantis Integration

20.2 Mantis Security and Encryption

As a summary description for the HTTPS protocol, its security is that of the underlying TLS (Transfer Layer Security) cryptographic protocol, where a certificate is used to authenticate the server, thus, the data flow between the client and the server is encrypted.

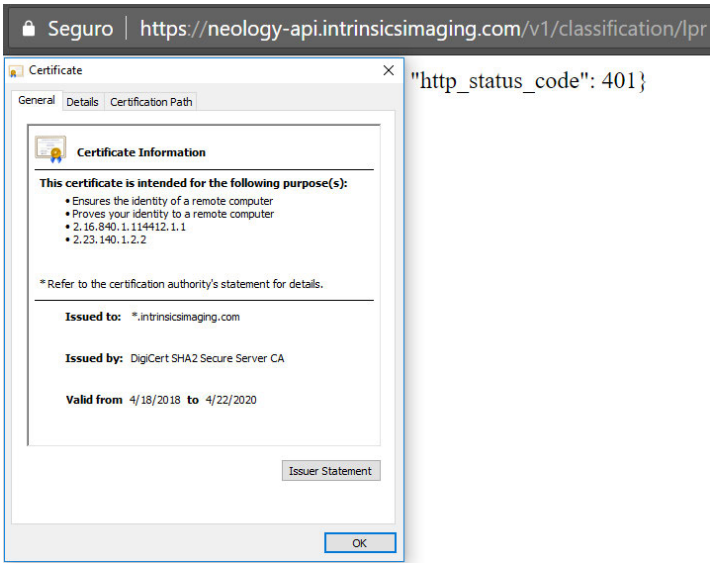


Figure 3 Available details for the certificate on the Mantis-Neology endpoint

20.3 Mantis Requirements

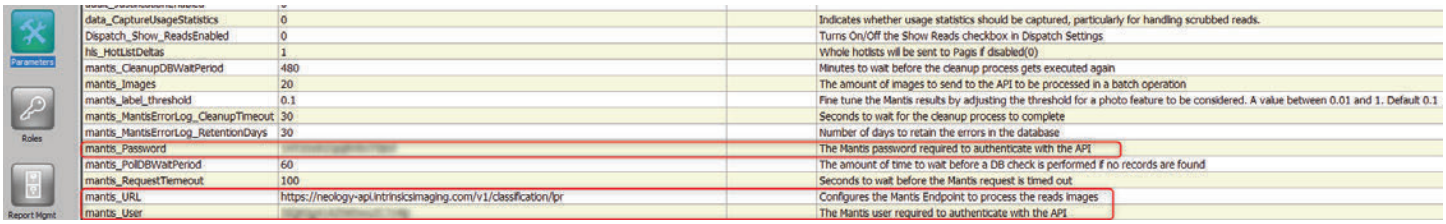
1. BOSS version 3.6 or newer.
2. Open communication to Mantis API URL (https://neology-api.intrinsicsimaging.com/v1/classification/lpr) via port 443.
3. Mantis Licensing feature required.
4. A valid Mantis User name and password. User name and password provided at time of licensing purchase.

20.4 Mantis Installation

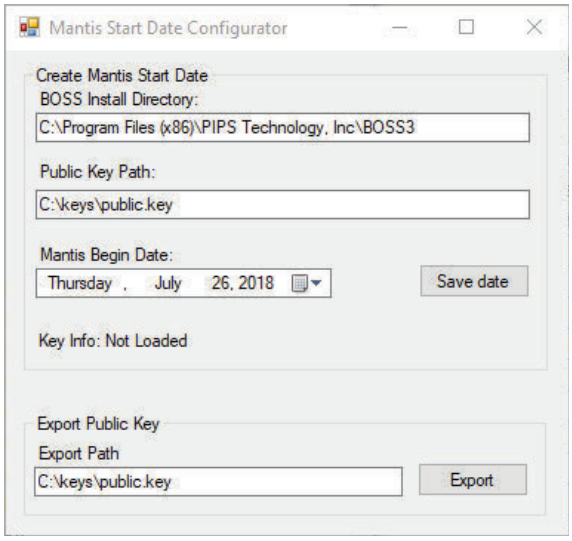
1. To upgrade or install Mantis version of BOSS follow the installation steps provide under Appendix 17. If upgrading from previous BOSS version you will also need to reactive your existing license to reflect the addition of the Mantis feature, see section 17.2.2.
2. Once BOSS is installed or upgraded, start the BOSS service to perform additional Mantis configurations.

20.5 Mantis Configurations

1. Start and login to the BOSS UI, navigate to System > Parameters.
2. In the Attributes table, look for the entries with the following names:
    - **a. mantis_User:** Assign the provided Mantis user name here.
    - **b. mantis_password:** Assign the provided Mantis user password here.
    - **c. mantis_URL:** Set the Mantis URL here. https://neology-api.intrinsicsimaging.com/v1/classification/lpr

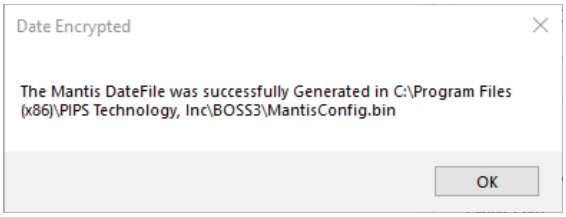


3. Additional parameters can be configured, see Mantis Parameters for details.
4. Once all the entries were assigned their corresponding values, close the BOSS UI and stop the BOSS service.
5. Download and place the “MantisStartDateGenerator.exe” file in the root BOSS3 folder, this executable is sperate from the BOSS installer and will need to be downloaded and placed manually.
6. Start the “MantisStartDateGenerator.exe” utility with administrator permissions.



7. Set the BOSS Install Directory to the Path of the folder where BOSS was installed.:

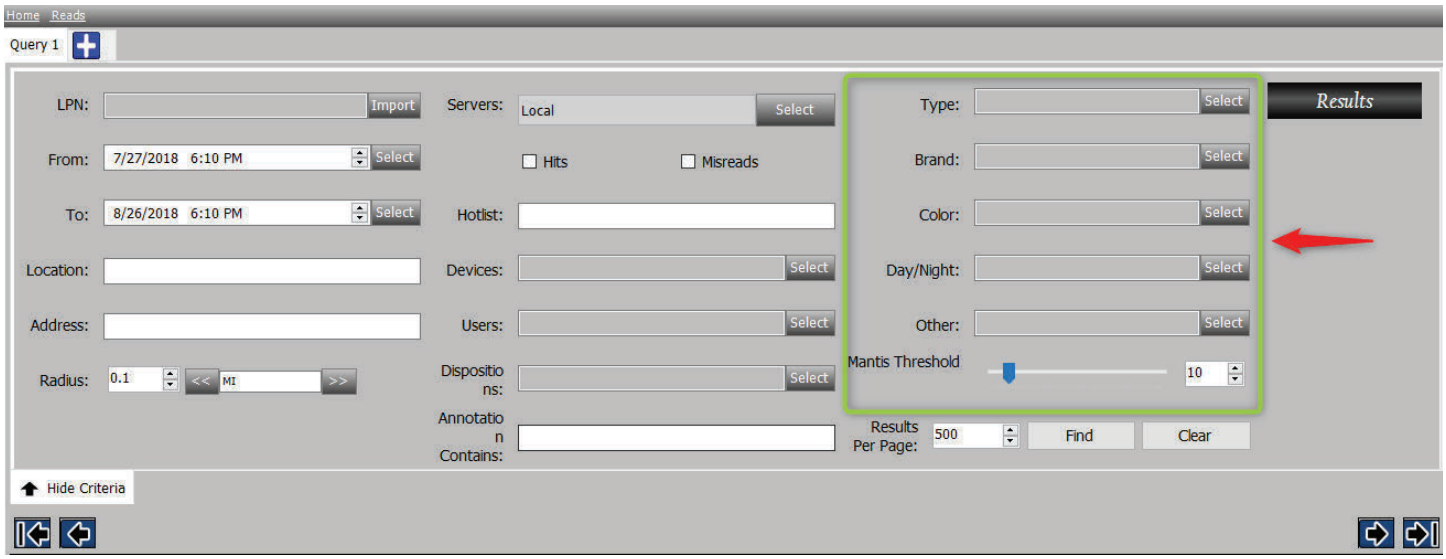
8. Set the Export Public Key path to a folder where you can access the generated public key, then click the Export button, and verify that the key was exported to the path.
9. Select a date that you want Mantis to take as the begin date for reads to be retrieved “Mantis Begin Date”. Reads that entered the system before this date, won’t be processed.
10. Click the Save date button to create the “MantisConfig.bin” file in the installation directory. A message confirming the file creation will appear.



11. Start the BOSS service.
12. When BOSS is started, the existing reads in the BOSS database will be sent to and processed by the Mantis API. The results will be stored on the local database.
13. Start and login to the BOSS UI.

20.6 Mantis Search Features

The Mantis fields should be visible in the right side of the reads panel in the BOSS UI. In case the fields are not available, diagnose the possible problems in the Mantis Configuration Troubleshoot section 20.8.



20.6.1 Mantis Search Definitions

- **Type=** Vehicle configuration style, i.e. Car, Box-Truck, Full-Size-Van, Hatchback, Minivan, Other-Truck, Pickup, Sedan, Suv.
- **Brand=** Vehicle manufacture.
- **Color=** Vehicle primary color.
- **Day/Night=** Vehicle capture in day or night.
- **Other=** Includes additional vehicle identifiers such a roof racks, spare-time, spoiler, ect...
- **Threshold=** Adjust the threshold slide bar to increase or decrease the confidences level of the Mantis search criteria based on selected filters, 1 being the lowest and 100 the highest confidence level available. When threshold is utilized in searches a new “Confidence” column will appear in the results, a user may now use this column to further sort the results by descending or ascending order.

20.7 Additional Mantis Parameters

As a summary description for the HTTPS protocol, its security is that of the underlying TLS (Transfer Layer Security) cryptographic protocol, where a certificate is used to authenticate the server, thus, the data flow between the client and the server is encrypted.

Parameter Name	Description	Default value
mantis_URL	The URL for the Mantis endpoint. The latest value should be available in this document. See Ports configuration for the corresponding value or ask a PIPS Technology representative.	None
mantis_User	Part of the credentials provided, it may be referenced also as the Mantis API key.	None
mantis_Password	Part of the credentials provided, it may be referenced also as the Mantis API password.	None
mantis_Images	The number of images to send to the API to be processed in a batch operation	20 images
mantis_PollDBWaitPeriod	The amount of time to wait before a DB check is performed if no records are found	60 seconds
mantis_RequestTiemeout	Seconds to wait before the Mantis request is timed out	100 seconds
mantis_MantisErrorLog_RetentionDays	Number of days to retain the errors in the database	30 days
mantis_MantisErrorLog_CleanupTimeout	Seconds to wait for the cleanup process to complete	30 seconds
mantis_CleanupDBWaitPeriod	Minutes to wait before the cleanup process gets executed again	480 minutes
mantis_label_threshold	Fine tune the Mantis results by adjusting the threshold for a photo feature to be considered. A value between 0.01 and 1.	10% (0.1)

20.8 Mantis Configuration Troubleshoot

To trouble shoot any Mantis issue, access to the BOSS Server logs is required. The logs are available inside the logs directory, inside the installation folder, e.g. "C:\Program Files (x86)\PIPS Technology, Inc\BOSS3\logs".

Inside this folder, there are two types of outputs:

- **BOSSMantisLog.txt.*:** This files contain Mantis Service specific information.
- **BOSSServerLog.txt.*:** This files contain overall BOSS Server information.

Known errors

L	Level	Error	Description
	INFO	**Mantis Service: Not available**	The Mantis feature was not enabled in the license key with which BOSS was activated
		Solution	Contact a Neology PIPS Technology agent for information on how to request the activation of the feature in your current license key
	INFO	**Mantis configuration not loaded, the service will not be started**	This error signals missing configuration Look for the additional messages described in the following rows.
	ERROR	**Mantis endpoint not configured, shutting down service**	The mantis URL parameter was not set properly, it cannot be a null or empty value.
		Solution	Review the ports configuration and set the mantis URL parameter to the given mantis URL. If you have an outdated version of this document, contact the Neology PIPS Technology support team to get the latest information.

	ERROR	**Mantis credentials are not configured, shutting down service**	Either the mantis_User or the mantis_password parameter was not set.
		Solution	Check that these values do not have a null or empty value. If you were not provided with these credentials, contact the Neology PIPS Technology support team.
	INFO	**Due to a request error, the next Mantis request will be performed in seconds**	There are three known errors related to mantis functionality: • **Mantis Failure**: Mantis failed to process the uploaded information. This error will not be retried because with the same image, Mantis will produce the same output. • **Connection error**: There was a problem establishing a connection with the server. This batch will be retried. • **Mantis Server Error**: An exception was received from the server. This error will be retried.
		Solution	For the above three errors, the possible solutions or actions to take are described below: • **Mantis Failure:** If too many instances of this error appear, contact the support team to diagnose the error. • **Connection error:** Verify that the appropriate rules for the firewall and whitelisting for URL and ports was set. See Mantis requirements for more details. • **Mantis Server Error:** If too many instances of this error appear, contact the support team to diagnose the error.

For a full list of all the messages produced by Mantis and a more detailed explanation about them, see the Mantis Log messages catalog.

20.8.1 Mantis Log Messages Catalog

Below is a description for the messages produced by the Mantis Service. Only applicable messages will have a solution appended to them.

Glossary

Term	Definition
ALPR	Automatic license plate recognition (also called automatic number plate recognition, or ANPR)
Annotation	A note or comment that can be made about and added to a read.
Deployment	The distribution or making available of a hotlist to a device
Device	A source of ALPR data; an PAGIS unit or a fixed or mobile camera
Disposition	The classification of a hit; e.g., a recovered stolen vehicle
Fixed Camera	An ALPR camera permanently mounted above a roadway
Group	A group of BOSS users that belong together administratively
Hit	A match on a plate read against a hotlist
Hotlist	A list or database of license plates of interest, e.g., the NCIC database
Justification	A purpose for running a query on the captured data. There are several justifications included in the system by default. The BOSS Administrator can also create custom justifications to be used.
LPN	License plate number; also known as the Vehicle Plate Number
PAGIS	PIPS™ Mobile Software, the ALPR Mobile application
Local Server	A server running on a local system, in relation to the SQL server or the BOSS UI Misread A read that was marked as a misread by a user
Mobile Unit	An ALPR system with cameras, a mobile processor, and software, such as Pagis Software, installed in a vehicle
Notification	Propagation or delivery of an alert resulting from a hit
Overview	A color image of the vehicle to which the license plate is attached
Patch	A small image of the license plate
Permission	Authorization to access specified functionality in BOSS
Read	A license plate detection event that results in the plate text optical recognition and pictures being taken
Remote Server	A BOSS server that is running in another location
Role	A position, such as Administrator, with the authorization to access specified functionality in BOSS
Site	A group of related devices
Translation	The interpretation from a word in English to a word in a selected language
User	An authorized BOSS user (with a username and password)
Whitelist	In BOSS a whitelist hit is the opposite of a hotlist hit. When a license plate read does not exist in an enabled whitelist database, the same Hits (Alert) screen will be displayed.

For additional information, assistance or maintenance questions please contact Neology ALPR/ANPR Support at:
PHONE: 833-PIPS-LPR (833-747-7577)
• Option 1 for Sales
• Option 2 for Support

For the U.S/Can and all other areas:
Sales Enquiry Email: sales@pipstechnology.com
Support Request Email: support@pipstechnology.com

For Europe, Middle East and Africa:
Sales Enquiry Email: sales@pipstechnology.co.uk
Support Request Email: support@pipstechnology.co.uk

IS A TRADEMARK OF NEOLOGY INC., AND EITHER REGISTERED OR PENDING REGISTRATION IN SEVERAL JURISDICTIONS.

Neology Headquarters San Diego
Address: 12760 Danielson Ct.,
Suite A Poway, CA 92064

Neology UK Ltd
Address:Form 1 Bartley Wood Business Park
Hook, Hampshire
RG27 9UP

Neology México
Plaza Carso II, Lago Zurich No. 219-Piso 10
C.P. 11529 Ciudad de México

	BOSS 4 Annual License Subscription	MANTIS 4-D Vehicle Detection Annual Subscription	Hosted Subscription
BOSS 4 Standard Software Application For either on-premise or Neology Hosted option	x		
Free Periodic SW Enhancements and Maintenance release in line with Neology standard SW release cycle	x		
Unlimited Helpdesk Access for BOSS 4 SW Available from 08:00 to 17:00 Central Standard Time	x		
Vehicle Classification Add-in for all vehicle detections including: - Vehicle Type - Vehicle Brand - Vehicle Feature (Spoiler, roof rails etc) - Vehicle Color -		x	
Enhanced ALPR "Deep Learning" capability enabled on Neology's latest generation Mobile (Golden Eagle) and Fixed (IRIS) Camera		x	
Access to the latest OCR and Vehicle Classification algorithms for all Neology / PIPS legacy devices in line with Neology standard release cycle		x	
Application and Database Server(s) with corresponding network provided on CJIS compliant Infrastructure			x
Elastic Database retention and storage in line with subscription level			x

High Availability and Resilience to ensure 99.999% infrastructure availability with 4 layers of Severity Monitoring (Urgent, High, Medium, Low)			x
Infrastructure Security Monitoring, including annual penetration testing and patching where required			x
Proactive System Health Monitoring (database, application and infrastructure) to pre-empt incidents			x
Service Management reporting on quarterly basis			x
Out of Hours Support for Critical Severity Infrastructure Issues			x

Clear Form

BOSS4 Questionnaire

After completion and submission of this document, the delivery team will review and submit to you the recommended Systems Specifications. Further logistical planning shall proceed after delivery of the initial Systems Specifications.

BOSS4 Server Type		Software Upgrade	
On-Prem: ☐	Hosted (Cloud): ☐	BOSS Upgrade. Yes: ☐ No: ☐	Current BOSS Version:

Customer Information			
Agency Name:		Date:	
Point of Contact Name:			
Email Address:			
Phone Number:			

Items to Migrate When Upgrading					Not Applicable: ☐
Migrate Reads	Yes: ☐	No: ☐	Migrate Hits	Yes: ☐	No: ☐
Migrate Users	Yes: ☐	No: ☐	Migrate Groups	Yes: ☐	No: ☐
Migrate Roles	Yes: ☐	No: ☐	Migrate Devices	Yes: ☐	No: ☐
Migrate Sites	Yes: ☐	No: ☐	Migrate Hotlists	Yes: ☐	No: ☐

Current ALPR Data Statistics			Not Applicable: ☐
Average **Monthly Read** intake.		Average **Yearly Read** intake.	
Current number of **Devices.**		Current number of **Users.**	
Current number of **Hotlists.**		Current Data **Retention Policy.**	

5 Year Projected Growth - ALPR Statistics

Projected read estimates help us ensure the ALPR system specifications are properly configured over time. Example, if the agency currently reads 500,000 plates per month, and growth is expected to double that count in five years, the projected number would be 1,000,000 below.

Projected number of **Reads** per/month.		Projected number of **Devices.**	
Projected number of **Users.**		Projected Data **Retention Policy.**	

Data Integration

Are you planning or are you currently using any kind of third-party application to ingest data from the BOSS database? If so, please provide a detailed explanation of this process.

BOSS4 Cloud
Specifications for Requirements

Cloud Application Servers

Below, there are the minimal recommended configurations for different capacity configurations for BOSS4 hosted on Amazon Web Services infrastructure.

Application Servers Specifications				
Configuration	**Demo**	**Medium**	**Large**	**High Capacity**
ALPR Devices	1 to 3	3 to 50	50 to 150	Beyond 150
Average Daily Intake	Around 30,000 events	Around 500,000 events	Around 1,500,000 events	Beyond 1,500,000 events
Average of users querying data	3 users	15 users	25 users	Beyond 25 users
Alert list averaging	Around 1M records	Around 2M records	Around 2M records	Around 2M records
EC2 AWS Instances for Microservices	t3.small 2.5GHz Intel 2 cores 2 GB RAM Amazon Linux	t3.large 2.5GHz Intel 2 cores 8 GB RAM Amazon Linux	t3.xlarge 2.5GHz Intel 4 cores 16 GB RAM Amazon Linux	t3.2xlarge 2.5GHz Intel 5 cores 32 GB RAM Amazon Linux
EC2 AWS Instance for Controller	t2.small 3.3GHz Intel 1 core 2GB RAM Amazon Linux	t2.large 3.0GHz Intel 2 cores 8GB RAM Amazon Linux	t2.xlarge 3.0GHz Intel 4 cores 16GB RAM Amazon Linux	t2.2xlarge 3.0GHz Intel 8 cores 32GB RAM Amazon Linux
Fargate AWS Instance for Microservices	3.3GHz Intel 5 cores 8GB RAM	3.0GHz Intel 16 cores 32GB RAM	3.0GHz Intel 32 cores 32GB RAM	3.0GHz Intel 48 cores 128 GB RAM
Storage and Application Space	Amazon EBS gp2 SSD 128GB	Amazon EBS io1 SSD 256GB	Amazon EBS io1 SSD 320GB	Amazon EBS io1 SSD 512GB

This document and its contents are intended for the recipient only. Copying, redistributing, or discussing with any other party outside of the intended recipient and Neology is prohibited.

Cloud Database Service

BOSS4 uses the MongoDB engine.

Database Service Specifications				
Configuration	**Demo**	**Medium**	**Large**	**High Capacity**
ALPR Devices	1 to 3	3 to 50	50 to 150	Beyond 150
Average Daily Intake	Around 30,000 events	Around 500,000 events	Around 1,500,000 events	Beyond 1,500,000 events
Average of users querying data	3 users	15 users	25 users	Beyond 25 users
Alert list averaging	Around 1M records	Around 2M records	Around 2M records	Around 2M records
Database Server Engine	MongoDB Atlas	MongoDB Atlas MongoDB Enterprise		
Dedicated Cluster	M20 2 vCPU 4 GB RAM Network Performance 100MB	M50 8 vCPU 16 GB RAM, Network Performance 10Gbps	db.r5.4xlarge 16 vCPU 64 GB RAM Network Performance 10Gbps	db.r5.8xlarge 32 vCPU 131 GB RAM Network Performance 10Gbps
Storage	General	General	General / Local NVMe SSD	General / Local NVMe SSD
Multimedia Storage	AWS EBS General Purpose SSD (gp2)		AWS EBS Provisioned IOPS SSD (io1)	

This document and its contents are intended for the recipient only. Copying, redistributing, or discussing with any other party outside of the intended recipient and Neology is prohibited.

BOSS4 On-Premise Specifications for Requirements

On-Premise Applications Server

Below, there are the minimal recommended configurations for different capacity configurations for BOSS4 On-Premise infrastructure.

Application Servers Specifications				
Configuration	**Demo**	**Medium**	**Large**	**High Capacity**
ALPR Devices	1 to 3	3 to 50	50 to 150	Beyond 150
Average Daily Intake	Around 30,000 events	Around 500,000 events	Around 1,500,000 events	Beyond 1,500,000 events
Average of users querying data	3 users	15 users	25 users	Beyond 25 users
Alert list averaging	Around 1M records	Around 2M records	Around 2M records	Around 2M records
Operating System	Amazon Linux / Amazon Linux 2 x64 Linux x64 (RHEL/CentOS, Ubuntu, Debian, SUSE) macOS x64 Windows 10 Professional x64 Windows Server 2016 x64			
Memory	16GB	32GB	64GB	192GB
Processor	x64 2.0 GHz 8 cores o better	Server Processor x64 (Intel Xeon Gold) 2 GHz 4 cores, 8 threads, 4MB cache	Server Processor x64 (Intel Xeon Platinum) 2.4 GHz 16 cores, 32 threads, 8MB cache	Server Processor x64 (Intel Xeon Platinum) 2.4 GHz 24 cores, 48 threads, 24MB cache
Hard Drive	7200 RPM SATA3	SSD SATA3	SSD SATA3 or NVMe PCI Express	SSD SATA3 or NVMe PCI Express
Application Space	128 GB of available space	256GB of available space	320GB of available space	512GB of available space

This document and its contents are intended for the recipient only. Copying, redistributing, or discussing with any other party outside of the intended recipient and Neology is prohibited.

On-Premise Database Server

BOSS4 uses the MongoDB Database Engine.

Specifications of the Database Server				
Configuration	**Demo**	**Medium**	**Large**	**High Capacity**
ALPR Devices	1 to 3	3 to 50	50 to 150	Beyond 150
Average Daily Intake	Around 30,000 events	Around 500,000 events	Around 1,500,000 events	Beyond 1,500,000 events
Average of users querying data	3 users	15 users	25 users	Beyond 25 users
Alert list averaging	Around 1M records	Around 2M records	Around 2M records	Around 2M records
Database Engine	Mongo DB Community	MongoDB Enterprise		
Operating System	Amazon Linux / Amazon Linux 2 x64 Linux x64 (RHEL/CentOS, Ubuntu, Debian, SUSE) macOS x64 Windows 10 Professional x64 Windows Server 2016 x64			
Processor	x64 2.0 GHz 8 cores o better	Server Processor x64 (Intel Xeon Gold) 2.5 GHz 4 cores, 8 threads, 4MB cache	Server Processor x64 (Intel Xeon Platinum) 2.4 GHz 16 cores, 32 threads, 16MB cache	Server Processor x64 (Intel Xeon Platinum) 2.4 GHz 24 cores, 48 threads, 24MB cache
Memory	N/A	32 GB	128GB	256GB
Hard Drive	7200 RPM SATA3 Not suitable for camera implantation with any kind of data retention expected	SSD SATA3 RAID level redundancy and scheduled DB backups recommended *See sizing chart for storage.*	SSD SATA3 or NVMe PCI Express RAID level redundancy and scheduled DB backups recommended *See sizing chart for storage.*	SSD SATA3 or NVMe PCI Express RAID level redundancy and scheduled DB backups recommended *See sizing chart for storage.*

This document and its contents are intended for the recipient only. Copying, redistributing, or discussing with any other party outside of the intended recipient and Neology is prohibited.

BOSS4 On-Premise & Cloud Storage

The calculation of storage applies to Cloud and On-Premise configurations.

Assumptions for the calculation:

Storage of metadata per read event: 32KB
Storage of imagery per read event: 160KB

Events from Golden Eagle or P500 cameras			
# of records	Database size Metadata and indexes	Repository Size Imagery	Total
1 Million	32GB	153GB	**185GB**
5 Million	64GB	763GB	**827GB**
10 Million	320GB	1.5TB	**1.82TB**
50 Million	1.6TB	7.5TB	**6.1TB**
100 Million	3.2TB	15TB	**18.2TB**

The calculation for the storage is approximated and it can vary depending on the conditions for the processing of the indexes, Mantis Metadata, compression of the images, among others.

It is not considered the storage for the backup of the databases nor the imagery repository.

This document and its contents are intended for the recipient only. Copying, redistributing, or discussing with any other party outside of the intended recipient and Neology is prohibited.

MASSACHUSETTS STATE POLICE

EXECUTIVE OFFICE OF PUBLIC SAFETY AND SECURITY
HIGHWAY SAFETY DIVISION
FFY 2016 FUNDING PROPOSAL

ALPR TRAILER

PROBLEM STATEMENT

Law enforcement agencies throughout the nation and around the world are increasingly adopting Automated License Plate Recognition (ALPR) systems. In Massachusetts, ALPR is utilized by over 41 different public safety agencies including the MSP. ALPR systems function to automatically capture an image of the vehicle's license plate, transform that image into alphanumeric characters using optical character recognition or similar software, compare the plate number acquired to one or more databases of vehicles of interest to law enforcement and other agencies, and to alert the officer when a vehicle of interest has been observed. Currently the MSP utilize ALPR to enhance their enforcement and investigative capabilities, expand their collection of relevant data, and expedite the tedious and time consuming process of comparing vehicle license plates with lists of stolen, wanted, and other vehicles of interest.

GOALS & OBJECTIVES

ALPR is used every day in Massachusetts to generate investigative leads that assist law enforcement in solving murders, rapes, and serial property crimes, recover abducted children, detect drug and human trafficking rings, find stolen vehicles, apprehend violent criminal alien fugitives, and support terrorism investigations. With an aging population, an increasing amount of "Silver Alerts" are generated to located missing elderly individuals. Quite often these individuals are operating a motor vehicle when they become disoriented.

COUNTERMEASURE TO ADDRESS PROBLEM

To provide investigative support focusing on site specific locations and to augment security at large scale events the department proposes to deploy a trailer mounted covert ALPR system. This system would be enclosed within a speed or variable message board and deployed to such large scale events as the Boston Marathon or the July 4th Esplanade celebration. The message/speed board will provide a highway safety function while capturing the ALPR data and storing it in a central repository.

LINE ITEM BUDGET

One Kustom 850 VSM/Speed board prepped for ALPR
Two 3M model 492 ALPR Cameras

Total $50,000.00

MEASURING SUCCESS/EVALUATION METHOD

The qualitative assessment of ALPR utilization will focus on feedback from the involved stakeholders, to include local law enforcement, media, government agencies and the people we serve.

SELF-SUFFICIENCY PLAN

The Massachusetts Department of State Police supports the utilization of ALPR technology to assist in intelligence gathering in effort to prevent terrorist activity and solve criminal investigation. Without federal funding the Department cannot sustain and enhance its ALPR capabilities.

SUPPLANTING

Absent federal or grant funding, the Massachusetts State Police does not purchase ALPR equipment.

INSTITUTIONALIZED PLAN

ALPR Utilization is a fully institutionalized program of the Massachusetts State Police. It is incorporated into our daily patrol function and is enshrined in our policy and procedures.

Submitted by

Colonel Timothy P. Alben
Superintendent, Massachusetts State Police

MMARS DOCUMENT ID: ISAEPSFY16ALPRPOL16A.

4680

COMMONWEALTH OF MASSACHUSETTS
INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM

This Form is issued and published by the Office of the Comptroller (CTR) pursuant to 815 CMR 6.00 for use by all Commonwealth Departments. Departments may add non-conflicting additional terms, but changes to the official printed language of this Form shall be void.

BUDGET FISCAL YEAR: 2016	RFR REFERENCE NUMBER ENTER RFR NUMBER: OR _X_ N/A.
MMARS ALPHA *BUYER/PARENT* DEPARTMENT CODE: EPS	MMARS ALPHA *SELLER/CHILD* DEPARTMENT CODE: POL
BUSINESS MAILING ADDRESS: 10 PARK PLAZA, SUITE 3720 BOSTON, MA 02116	BUSINESS MAILING ADDRESS: 470 WORCESTER ROAD FRAMINGHAM, MA 01702
ISA MANAGER: DIANE PERRIER	ISA MANAGER: DEB BRODERICK
PHONE: **617-725-3301** FAX: 617-725-0260	PHONE: **508-820-2146** FAX: 508-820-2146
E-MAIL ADDRESS: DIANE.PERRIER@STATE.MA.US	E-MAIL ADDRESS: DEBORAH.BRODERICK@STATE.MA.US

Purpose of ISA: (Check one option only and complete applicable information) (Attachment A required for New ISAs and all ISA Amendments.)

_X_ New ISA. Current Maximum Obligation for total duration of ISA **$ 50,000.00** (Use "N/A" for Non-Financial ISA.) (Complete Attachment B)

___ Amendment to Existing ISA. What is being amended? (Attachment C required for all Federal and Bond Account Amendments)

____ Amend Budget/Accounts. Change Maximum Obligation from: $_____ to New Maximum Obligation $ _____ (Attachment B)

____ Amend Budget/Accounts. No Change in Maximum Obligation (Attachment B)

____ Amend Dates of Performance. New Dates of Service: Start Date:_____ End Date:_____ (Subject to execution dates below.)

____ Amend Scope of Services/Performance

BRIEF DESCRIPTION OF PERFORMANCE GOALS TO BE ACCOMPLISHED BY ISA, OR IF AMENDMENT, IDENTIFY WHAT IS BEING AMENDED:

FFY2016 Automated License Plate Recognition (ALPR) system, includes related equipment.
PT-16-07-01

WILL SELLER/CHILD DEPARTMENT STATE EMPLOYEES (AA OBJECT CLASS) BE FULLY OR PARTIALLY FUNDED UNDER THIS ISA? **_X_ No ___ Yes.** If Yes, Seller/Child certifies that the ISA is not being used as an alternative funding mechanism for state employees, that the identified personnel in Attachment A are necessary for completion of the ISA due to particular expertise or other factors that can not be obtained through the use of contractors, and that if federal funds are being used, funds shall not be used to supplement the regular salary or compensation of any officer or employee of the Commonwealth for services performed during their regular working hours. M.G.L. c. 29, § 6B.

ACCOUNT INFORMATION. Complete for all new ISAs and Amendments (even if account information is not changing) Check one option, indicate "add", "delete" or "no change" and enter account, fund, major program code and program code.

_X_ BGCN – non-subsidiarized (federal, capital, trust). Attachment C required for any new ISA or ISA Amendment involving federal funds.

____ BGCS – subsidiarized (budgetary)

____ Other (CT, RPO as authorized by CTR): _____.

____ Non-Financial ISA (no funds are transferred from Buyer/Parent to Seller/Child), however, resources are committed to ISA.

____ Amendment with no Accounting Changes to Budget/Accounts or to Attachments B or C. (Indicate no change below and complete account information.)

_X_ ADD __ DELETE __ NO CHANGE	Account: 80004804	Fund: 0100	Major Program Code: HSPGTS	Program Code: F16ALPR
__ ADD __ DELETE __ NO CHANGE	Account:	Fund:	Major Program Code:	Program Code:
__ ADD __ DELETE __ NO CHANGE	Account:	Fund:	Major Program Code:	Program Code:
__ ADD __ DELETE __ NO CHANGE	Account:	Fund:	Major Program Code:	Program Code:

ISA ANTICIPATED START DATE: **01/15/2015**, provided that the Seller/Child certifies that it will not incur any obligations related to this ISA prior to the date that this ISA is executed, NOR prior to the date that sufficient funding for the obligations for this ISA is available in the Seller/Child account for expenditure.

TERMINATION DATE OF THIS ISA: This ISA shall terminate on **06/30/2016** unless terminated or properly amended in writing by the parties prior to this date.

BUYER/PARENT AND SELLER/CHILD DEPARTMENT CERTIFICATIONS. IN WITNESS WHEREOF, by executing this ISA below, the Buyer/Parent and Seller/Child certify, under the pains and penalties of perjury, that Buyer/Parent and Seller/Child understand and agree that any Buyer/Parent or Seller/Child officer or employee who knowingly violates, authorizes or directs another officer or employee to violate any provision of state finance law relating to the incurring of liability or expenditure of public funds, includng this ISA, may be considered to be in violation of M.G.L. c. 29, § 66, and therefore the Buyer/Parent and the Seller/Child agree to ensure that this ISA complies with, and that all staff or contractors involved with ISA performance are provided with sufficient training and oversight to ensure compliance with 815 CMR 6.00, CTR applicable policies and the ISA Terms and Conditions which are incorporated by reference into this ISA, in addition to the performance requirements identified in Attachment A of this ISA, and that all terms governing performance of this ISA are attached to this ISA or incorporated by reference herein, and the Buyer/Parent and Seller/Child agree to maintain the necessary level of communication (including immediate notification of any amendments to accounting information, program codes or performance needs), coordination, access to reports and other ISA information, and cooperation to ensure the timely execution and successful completion of the ISA, amendments, and state finance law compliance; and that the Buyer/Parent certifies it will ensure that sufficient funds are timely made available in the Seller/Child account(s), with the proper accounting codes, prior to the Seller/Child's need to begin initial or amended performance; and that the Seller/Child will not allow initial or amended performance to begin until the ISA is executed AND the ISA Seller/Child account is sufficiently funded to support encumbrances and payments for performance (including payroll), and the Seller/Child will make encumbrances and payments (including payroll) only from the authorized ISA Seller/Child account(s) and shall not be entitled to transfer charges made from any other account not approved in writing by CTR in advance of expenditures by the Seller/Child.

BUYER/PARENT DEPARTMENT'S AUTHORIZED SIGNATURE: **DATE:** (Date must be handwritten by signatory at time of signature)	**SELLER/CHILD DEPARTMENT'S AUTHORIZED SIGNATURE:** **DATE:** (Date must be handwritten by signatory at time of signature)
PRINT NAME: ART KINSMAN	PRINT NAME:
PRINT TITLE: EXECUTIVE DIRECTOR, OFFICE OF GRANTS & RESEARCH	PRINT TITLE:

INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM
TERMS AND CONDITIONS

The following terms and conditions are incorporated by reference into any ISA.

Role of the Office of the Comptroller. All ISA fiscal transactions shall be made through the state accounting system as prescribed by the Office of the Comptroller (CTR). CTR will interpret 815 CMR 6.00 and applicable policies and take any fiscal or other actions necessary to ensure ISA compliance with state finance law, including but not limited to correcting accounting transactions, resolving ISA disputes and identifying corrective action by the Buyer/Parent or Seller/Child Departments.

Seller/Child Department Certifications. By executing an ISA the Seller/Child certifies that it is statutorily authorized to provide the type of performance sought by the Buyer/Parent, and shall at all times remain qualified to perform the ISA, that performance shall be timely and meet or exceed ISA standards, that the Seller/Child will not allow initial or amended performance to begin, may not authorize personnel or contractors to work, nor incur any obligation to be funded under an ISA prior to the execution of an ISA AND the availability of ISA funding in the Seller/Child account to support encumbrances and payments for performance. The Seller/Child will make encumbrances and payments (incuding payroll) only from the authorized ISA Seller/Child account(s) and shall not be entitled to transfer charges made from any other account not approved in writing in advance by CTR.** The Seller/Child must immediately notify CTR whenever a delay in funding is anticipated for which performance is expected. The Seller/Child is authorized to use ISA funding only for the actual costs of ISA performance and may not use ISA funds to supplement non-ISA related personnel or expenditures.

Buyer/Parent Department Certifications. Signature by the Buyer/Parent certifies that it is statutorily authorized or required to procure the type of performance required under this ISA, that the Buyer/Parent certifies it will ensure that sufficient funds are timely made available in the Seller/Child Seller/Child account(s), with the proper accounting codes, prior to the Seller/Child's need to begin intial or amended performance; that the Buyer/Parent will monitor and reconcile ISA performance in compliance with state appropriation language or federal grant requirements, communicate all fiscal information necessary for the set up of the Seller/Child account(s) including budget information, and if the ISA is funded with federal funds provide accurate accounting information in Attachment C, and immediately notify the Seller/Child of any changes in Attachment C (such as program codes) to ensure the ISA and Seller/Child account can be timely updated to avoid lapses in funding or the inability of the Seller/Child to make timely payroll and other expenditures from the Seller/Child account.

Chief Fiscal Officer. The Chief Fiscal Officer (CFO) for the Buyer/Parent and Seller/Child will be responsible for the fiscal management of ISAs within their Departments in accordance with these ISA Terms and Conditions, 815 CMR 6.00 and policies and procedures published by CTR.

ISA Manager. Both the Buyer/Parent and Seller/Childs are responsible for ensuring that the ISA Manager listed on the ISA, or ISA Amendment, is current and that the ISA Manager is an authorized signatory for the Department supported by the appropriate Security Profile. If the listed ISA Manager changes, the CFO shall be the ISA Manager until a replacement is identified in the same manner as other Written Notice.

Record-keeping and Retention, Inspection of Records. The Buyer/Parent and Seller/Child shall maintain all ISA records in such detail as necessary to support claims for payment, including reimbursement or federal financial participation (FFP), for at least seven (7) years from the last payment under an ISA Seller/Child account, or such longer period as is necessary for the resolution of any litigation, claim, negotiation, audit or other inquiry involving an ISA. In addition to any specific progress, programmatic or expenditure reports specified in Attachment A, the Seller/Child is required to provide the Buyer/Parent (and to CTR, the State Auditor and the House and Senate Ways and Means Committees upon request) with full cooperation and access to all ISA information.

Payments and Compensation. The Seller/Child may accept compensation only for performance delivered and accepted by the Buyer/Parent in accordance with the specific terms and conditions of the ISA. All ISA payments are subject to appropriation pursuant to M.G.L. C. 29, or the availability of sufficient non-appropriated funds for the purposes of an ISA. Overpayments or disallowed expenditures shall be reimbursed by the Seller/Child or may be offset from future ISA payments in accordance with state finance law and instructions from CTR.

ISA Termination or Suspension. An ISA shall terminate on the date specified, unless this date is properly amended prior to this date, or unless terminated or suspended under this Section upon prior written notice to the Seller/Child. The Buyer/Parent may terminate an ISA without cause and without penalty with at least thirty days prior written notice, or may terminate or suspend an ISA with reasonable notice if the Seller/Child breaches any material term or condition or fails to perform or fulfill any material obligation required by an ISA, or in the event of an elimination of an appropriation or availability of sufficient funds for the purposes of an ISA, or in the event of an unforeseen public emergency mandating immediate Buyer/Parent action. Upon immediate notification to the other party, neither the Buyer/Parent nor the Seller/Child shall be deemed to be in breach for failure or delay in performance due to Acts of God or other causes factually beyond their control and without their fault or negligence. Contractor failure to perform or price increases due to market fluctuations or product availability will not be deemed factually beyond the Seller/Child's control.

Written Notice. Any notice shall be deemed delivered and received when submitted in writing in person or when delivered by any other appropriate method evidencing actual receipt by the Buyer/Parent or the Seller/Child. Unless otherwise specified in the ISA, legal notice sent or received by the Buyer/Parent's ISA Manager or the CFO (with confirmation of actual receipt) through the listed fax number(s) or E-Mail address for the ISA Manager will satisfy written notice under the ISA. Any written notice of termination or suspension delivered to the Seller/Child shall state the effective date and period of the notice, the reasons for the termination or suspension, if applicable, any alleged breach or failure to perform, a reasonable period to cure any alleged breach or failure to perform, if applicable, and any instructions or restrictions concerning allowable activities, costs or expenditures by the Seller/Child during the notice period.

Confidentiality. The Seller/Child shall comply with M.G.L. C. 66A if the Seller/Child becomes a "holder" of "personal data". The Seller/Child shall also protect the physical security and restrict any access to personal or other Buyer/Parent data in the Seller/Child's possession, or used by the Seller/Child in the performance of an ISA, which shall include, but is not limited to the Buyer/Parent's public records, documents, files, software, equipment or systems. If the Seller/Child is provided access with any other data or information that triggers confidentiality requirements under FIPA, HIPPA or other federal or state laws, the Seller/Child shall be responsible for protection of this data as instructed by the Buyer/Parent.

Assignment. The Seller/Child may not assign, delegate or transfer in whole or in part any ISA, or any liability, responsibility, obligation, duty or interest under an ISA, to another Department or an outside contractor. Assumption of an ISA by a successor Department due to a legislative change in the Seller/Child or Buyer/Parent's department status shall be accomplished through the execution of a new ISA.

Subcontracting By Seller/Child. Since it is presumed that contracting through the Seller/Child is more cost effective and a better value than the Buyer/Parent directly contracting with an outside contractor(s), any subcontract entered into by the Seller/Child for the purposes of fulfilling the obligations under an ISA must be approved by the Buyer/Parent in advance of the ISA and justified as part of the ISA Attachment A. The Seller/Child is responsible for full state finance law and procurement compliance for all subcontracts, and shall supply a copy of any subcontract to the Buyer/Parent upon request.

Affirmative Action, Non-Discrimination in Hiring and Employment. In performing this ISA, the Seller/Child shall comply with all federal and state laws, rules, regulations and applicable internal state policies and agreements promoting fair employment practices or prohibiting employment discrimination and unfair labor practices and shall not discriminate in the hiring of any applicant for employment nor shall any qualified employee be demoted, discharged or otherwise subject to discrimination in the tenure, position, promotional opportunities, wages, benefits or terms and conditions of their employment because of race, color, national origin, ancestry, age, sex, religion, disability, handicap, sexual orientation or for exercising any rights afforded by law. The Seller/Child commits to, when possible, to purchasing supplies and services from certified minority or women-owned businesses, small businesses or businesses owned by socially or economically disadvantaged persons or persons with disabilities in accordance with the Commonwealth's Affirmative Market Program.

Waivers. Forbearance, indulgence or acceptance by the Seller/Child or Buyer/Parent of any breach or default in any form shall not be construed as a waiver and shall not limit enforcement remedies or allow a waiver of any subsequent default or breach.

Risk of Loss. The Seller/Child shall bear the risk of loss for any materials, deliverables, personal or other data that is in the possession of the Seller/Child or used by the Seller/Child in the performance of an ISA until is accepted by the Buyer/Parent.

Disputes. The Buyer/Parent and Seller/Child agree to take all necessary actions to resolve any dispute arising under the ISA within 30 calendar days including department head and secretariat involvement, but in no event shall a dispute remain unresolved beyond May 30th in any fiscal year, nor may the Buyer/Parent or Seller/Child allow a dispute to create a state finance law or other violation of ISA terms (such as a delay in funding, failure to timely communicate funding or program code changes, or failure to timely process ISA paperwork). Seller/Child and Buyer/Parent must immediately notify CTR to assist in resolution of the dispute and shall implement any actions required by CTR to resolve the dispute, which shall be considered final.

Interpretation, Severability, Conflicts with Law, Integration. Any amendment or attachment to any ISA that contains conflicting language or has the affect of deleting, replacing or modifying any printed language of the ISA shall be interpreted as superseded by the ISA Form as published. If any ISA provision is superseded by state or federal law or regulation, in whole or in part, then both parties shall be relieved of all obligations under that provision to the extent necessary to comply with the superseding law, provided however, that the remaining provisions of the ISA, or portions thereof, shall be enforced to the fullest extent permitted by law. The terms of this ISA shall survive its termination for the purpose of resolving any claim, dispute or other action, or for effectuating any negotiated representations and warranties.

4682

INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM
TERMS AND CONDITIONS

ATTACHMENT A – TERMS OF PERFORMANCE AND JUSTIFICATIONS:

This Attachment Form must be used. Insert (type or copy and paste) all relevant information using as many pages as necessary. Attach any additional supporting documentation as appropriate. If Amending the ISA, completion of Sections 1, 2 and 3 identifying what is being amended and the reasons for the amendments is required. For sections 4-9 enter only the amended language in the sections being amended.

1. [REQUIRED] Purpose and other performance goals of ISA, or as amended:

   - To decrease motor-vehicle fatalities 10% from the 2009-2013 calendar base year average of 354 to 319 by December 31, 2016.
   - To decrease the number of serious traffic injuries 10% from 4,134 in 2013 to 3,721 by December 31, 2016.
   - To decrease unrestrained vehicle occupant fatalities in all seating positions 10% from the 2009-2013 base calendar year average of 108 to 97 by December 31, 2016.

2. [REQUIRED] Identify in detail, the responsibilities of the parties, the scope of services and terms of performance under the ISA, or as amended:
   The MSP seeks to enhance their enforcement and investigative capabilities through the purchase of a portable trailer equipped with an Automated License Plate Recognition (ALPR) system.

   MSP will maintain an equipment database for the life of the property as required by EOPSS.

   The Division of Field Services will ensure that all MSP personnel assigned to EOPSS/HSD grant funded enforcement initiatives are familiar with the related goals and expectations.

   With EOPSS/HSD assistance, the MSP will acknowledge EOPSS as the funding source on all news releases.

3. [REQUIRED] Identify schedule of performance or completion dates or other benchmarks for performance, or as amended:

   See Section 1 & 2.

4. [REQUIRED] Justification that use of ISA is best value vs. contract with outside vendor:
   N/A

5. Will Seller/Child department state employees (AA Object Class) be fully or partially funded under this ISA? X No ___ Yes.
   If yes, justify necessity to use state employees for the ISA vs. use of contractors (contract employees or outside vendors).

6. Subcontractors. Since it is presumed that contracting through the Seller/Child is more cost effective and a better value than the Buyer/Parent directly contracting with an outside contractor(s), any subcontract entered into by the Seller/Child for the purposes of fulfilling the obligations under an ISA must be approved by the Buyer/Parent in advance of the ISA and justified as part of the ISA Attachment A, as follows: (enter "N/A" if subcontractors will not be funded with ISA funds)
   N/A

7. Identify any equipment that will be leased or purchased by the Seller/Child using ISA funds: (The Buyer/Parent shall determine ownership of equipment purchased by the Seller/Child with ISA funds. Enter "N/A" if equipment not included in ISA.)
   ALPR system with related trailer equipment.

8. [REQUIRED] Identify the format and timing of ISA reports to the Buyer/Parent Department. Include the type of reports (e.g., progress or status, data, etc.), timing of reports (e.g., weekly, monthly, final) and the medium for submission of reports (e.g., e-mail, Excel spreadsheet, paper, telephone):

The equipment will be purchased when funds become available in MMARS. All equipment must be purchased and received prior to the close of the federal fiscal year on September 30, 2016. Invoice(s) must be submitted to EOPSS' Highway Safety Division within 30 days of the purchase(s).

The MSP will submit an Annual Report outlining the deployment and utilization associated with the ALPR system.

9. Additional ISA Terms: [Insert Terms here. Do not refer to separate attachment(s)]

General Federal Grant Conditions

The basic federal grant conditions that follow apply to all federal grants, regardless of the federal department making the funds available.

- Audit Requirement of Federal Funds
  - 2 CFR 200 (formerly OMB Circular A-133) requirements apply to each non-profit organization, each institution of higher education, and local governments as a whole when they or one of their departments receives federal funds. Any non-profit organization, institution of higher education, or local government spending more than $750,000 in federal funds *from all sources* within a 12-month period must have an audit performed on the use of the funds. OGR defines the 12-month period as July 1 to June 30. The following webpage provides the full text of this basic federal grant requirement:

    http://www.gpo.gov/fdsys/pkg/FR-2013-12-26/pdf/2013-30465.pdf

- Data Universal Number System (DUNS) and Central Contractor Registration (CCR)
  - All subrecipients of federal funds must have a nine-digit DUNS number in order. For more information: 1-866-705-5711 or http://fedgov.dnb.com/webform.
  - All subrecipients of federal funds must maintain annual registration in the System for Award Management (SAM) database: www.sam.gov.

- Transparency Act Reporting for Federal Funds
  - The Federal Funding Accountability and Transparency Act (FFATA) requires EOPSS to report on a federal website specific award and subrecipient identifying information for each award greater than $25,000 OGR makes with federal funds it received after October 1, 2010. Prior to receiving funds, each affected subrecipient must report certain information to OGR so that EOPSS can fulfill its FFATA reporting requirements. Data reported by EOPSS may be viewed at www.USASpending.gov.

- Cost Principles for Federal Grants to *State and Local Governments*
  - 2 CFR Part 225 (formerly known as OMB Circular A-87) requirements apply only to state and local government subrecipients. These regulations list and define general categories of costs that are both allowable and unallowable. Examples are included below.
    - Supplanting, including: (a) replacing routine and/or existing State or local expenditures with Federal grant funds and/or (b) using Federal grant funds for costs of activities that constitute general expenses required to carry out the overall responsibilities of State, local, or Federally recognized Indian tribal governments is unallowable.
    - The cost of alcoholic beverages is unallowable.
    - Costs incurred by advisory councils are allowable.
    - Audit costs are allowable.
    - Compensation costs are allowable so long as they are consistent with that paid for similar work in other activities of the local government.
    - Entertainment costs are unallowable.

- Equipment costs are allowable with the prior approval of OGR. Equipment having a useful life of more than one year or a current per-unit fair market value of $5,000 or more must be tracked. When replacing equipment purchased with federal funds, the equipment to be replaced may be used as a trade-in or can be sold with the proceeds used to offset the cost of the replacement equipment. In addition, during the period of the contract with OGR, insurance on the equipment is allowable.
- Travel costs are allowable if pre-approved by OGR and if they are consistent with costs normally allowed in like circumstances for non-federally funded activities. The following webpage provides the full text of this basic federal grant requirement: http://www.whitehouse.gov/omb/fedreg/2005/083105_a87.pdf.
- If a subrecipient uses grant funds to pay its employees, the subrecipient must maintain timesheets for work performed with the grant funds. Timesheets must show the hours worked and must be signed by the employee paid with the grant funds.

- Cost Principles for Federal Grants to *Non-Profit Organizations and Institutions of Higher Education* requirements apply only to the non-profit and higher education subrecipients. The CFRs referenced below list and define general categories of costs that are allowable and unallowable. The links below provide the full text of these two basic federal grant requirements.
  - 2 CFR Part 220 pertains to Educational Institutions (formerly known as OMB Circular A-21): http://www.whitehouse.gov/omb/fedreg/2005/083105_a21.pdf.
  - 2 CFR Part 230 pertains to Non-profit Organizations (formerly known as OMB Circular A-122): http://www.whitehouse.gov/omb/fedreg/2005/083105_a122.pdf.

U.S. Department of Transportation Funds

The National Highway Traffic Safety Administration (NHTSA) of the U.S. Department of Transportation offers two documents that present requirements for the use of the funds and outline the purpose of each category of grants provided.

- Urls for the two programmatic and financial guide documents from NHTSA are below.
  - Highway Safety Grant Funding Policy: http://www.nhtsa.gov/nhtsa/whatsup/TEA21/GrantMan/HTML/GrantFundPolicy_mkm_revJuly07.pdf

    Pay particular attention to the sections on: (1) allowable costs for equipment, travel, training, and consultant services; and (2) unallowable costs for equipment, facilities and construction, training and program administration.

    A more complete document on administrative requirements is found in 49 CFR Part 18 - the Uniform Administrative Requirement for Grants as promulgated by the U.S. Department of Transportation.
  - Highway Safety Grant Management Manual: http://www.nhtsa.gov/nhtsa/whatsup/TEA21/GrantMan/HTML/00_Manl_Contents1_01.html. This document provides information on each of the grant programs including Sections 154, 164, 402, 405a, 405b, 405c, 405d, 405e, 405f and 405g grant programs.

Additional current NHTSA grants management resources may be found at:
http://www.nhtsa.gov/About+NHTSA/Programs+&+Grants/Resources+Guide

In Addition to the links above, recipients of NHTSA funding must also adhere to the following conditions:

INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM
TERMS AND CONDITIONS

- **NONDISCRIMINATION (APPLIES TO SUBRECIPIENTS AS WELL AS STATES):** The State highway safety agency will comply with all Federal statutes and implementing regulations relating to nondiscrimination. These include but are not limited to: (a) Title VI of the Civil Rights Act of 1964 (Pub. L. 88-352), which prohibits discrimination on the basis of race, color or national origin (and 49 CFR Part 21); (b) Title IX of the Education Amendments of 1972, as amended (20 U.S.C. 1681-1683 and 1685-1686), which prohibits discrimination on the basis of sex; (c) Section 504 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794), and the Americans with Disabilities Act of 1990 (Pub. L. 101-336), as amended (42 U.S.C. 12101, *et seq.*), which prohibits discrimination on the basis of disabilities (and 49 CFR Part 27); (d) the Age Discrimination Act of 1975, as amended (42 U.S.C. 6101-6107), which prohibits discrimination on the basis of age; (e) the Civil Rights Restoration Act of 1987 (Pub. L. 100-259), which requires Federal-aid recipients and all subrecipients to prevent discrimination and ensure nondiscrimination in all of their programs and activities; (f) the Drug Abuse Office and Treatment Act of 1972 (Pub. L. 92-255), as amended, relating to nondiscrimination on the basis of drug abuse; (g) the comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970 (Pub. L. 91-616), as amended, relating to nondiscrimination on the basis of alcohol abuse or alcoholism; (h) Sections 523 and 527 of the Public Health Service Act of 1912, as amended (42 U.S.C. 290dd-3 and 290ee-3), relating to confidentiality of alcohol and drug abuse patient records; (i) Title VIII of the Civil Rights Act of 1968, as amended (42 U.S.C. 3601, *et seq.*), relating to nondiscrimination in the sale, rental or financing of housing; (j) any other nondiscrimination provisions in the specific statute(s) under which application for Federal assistance is being made; and (k) the requirements of any other nondiscrimination statute(s) which may apply to the application.

- **BUY AMERICA ACT 49 U.S.C 5323 (J) (APPLIES TO SUBRECIPIENTS AS WELL AS STATES):** Only steel, iron and manufactured products produced in the United States may be purchased with Federal funds unless the Secretary of Transportation determines that such domestic purchases would be inconsistent with the public interest, that such materials are not reasonably available and of a satisfactory quality, or that inclusion of domestic materials will increase the cost of the overall project contract by more than 25 percent. Clear justification for the purchase of non-domestic items must be in the form of a waiver request submitted to and approved by the Secretary of Transportation. **The Buy America Act does not apply to purchases under $5,000.**

- **Political Activity Act (Applies to Subrecipients as well as States):** The State will comply with provisions of the Hatch Act (5 U.S.C. 1501-1508) which limits the political activities of employees whose principal employment activities are funded in whole or in part with Federal funds.

- **Certification Regarding Federal Lobbying (Applies to Sunrecipients as well as States):** The authorized signatory certifies, to the best of his or her knowledge and belief, that:

  1. No Federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.

  2. If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, “Disclosure Form to Report Lobbying,” in accordance with its instructions.

  3. The undersigned shall require that the language of this certification be included in the award documents for all sub-award at all tiers (including subcontracts, subgrants, and contracts under grant, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.

  This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by section 1352, title 31, U.S. Code. Any person who fails to file the

required certification shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure.

- **Restrictions on State Lobbying (This Applies to Subrecipients as well as Sates):** None of the funds under this program will be used for any activity specifically designed to urge or influence a State or local legislator to favor or oppose the adoption of any specific legislative proposal pending before any State or local legislative body. Such activities include both direct and indirect (e.g., “grassroots”) lobbying activities, with one exception. This does not preclude a State official whose salary is supported with NHTSA funds from engaging in direct communications with State or local legislative officials, in accordance with customary State practice, even if such communications urge legislative officials to favor or oppose the adoption of a specific pending legislative proposal.

- **Certification Regarding Debarment and Suspension (This Applies to Subrecipients as well as States):**

  Instructions for Primary Certification

  1. By signing and submitting this proposal, the prospective primary participant is providing the certification set out below.

  2. The inability of a person to provide the certification required below will not necessarily result in denial of participation in this covered transaction. The prospective participant shall submit an explanation of why it cannot provide the certification set out below. The certification or explanation will be considered in connection with the department or agency's determination whether to enter into this transaction. However, failure of the prospective primary participant to furnish a certification or an explanation shall disqualify such person from participation in this transaction.

  3. The certification in this clause is a material representation of fact upon which reliance was placed when the department or agency determined to enter into this transaction. If it is later determined that the prospective primary participant knowingly rendered an erroneous certification, in addition to other remedies available to the Federal Government, the department or agency may terminate this transaction for cause or default.

  4. The prospective primary participant shall provide immediate written notice to the department or agency to which this proposal is submitted if at any time the prospective primary participant learns its certification was erroneous when submitted or has become erroneous by reason of changed circumstances.

  5. The terms *covered transaction, debarred, suspended, ineligible, lower tier covered transaction, participant, person, primary covered transaction, principal, proposal, and voluntarily excluded,* as used in this clause, have the meaning set out in the Definitions and coverage sections of 49 CFR Part 29. You may contact the department or agency to which this proposal is being submitted for assistance in obtaining a copy of those regulations.

  6. The prospective primary participant agrees by submitting this proposal that, should the proposed covered transaction be entered into, it shall not knowingly enter into any lower tier covered transaction with a person who is proposed for debarment under 48 CFR Part 9, subpart 9.4, debarred, suspended, declared ineligible, or voluntarily excluded from participation in this covered transaction, unless authorized by the department or agency entering into this transaction.

  7. The prospective primary participant further agrees by submitting this proposal that it will include the clause titled “Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion-Lower Tier Covered Transaction,” provided by the department or agency entering into this covered transaction, without modification, in all lower tier covered transactions and in all solicitations for lower tier covered transactions.

INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM
TERMS AND CONDITIONS

8. A participant in a covered transaction may rely upon a certification of a prospective participant in a lower tier covered transaction that it is not proposed for debarment under 48 CFR Part 9, subpart 9.4, debarred, suspended, ineligible, or voluntarily excluded from the covered transaction, unless it knows that the certification is erroneous. A participant may decide the method and frequency by which it determines the eligibility of its principals. Each participant may, but is not required to, check the list of Parties Excluded from Federal Procurement and Non-procurement Programs.

9. Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render in good faith the certification required by this clause. The knowledge and information of a participant is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.

10. Except for transactions authorized under paragraph 6 of these instructions, if a participant in a covered transaction knowingly enters into a lower tier covered transaction with a person who is proposed for debarment under 48 CFR Part 9, subpart 9.4, suspended, debarred, ineligible, or voluntarily excluded from participation in this transaction, in addition to other remedies available to the Federal Government, the department or agency may terminate this transaction for cause or default.

Certification Regarding Debarment, Suspension, and Other Responsibility Matters-Primary Covered Transactions

(1) The prospective primary participant certifies to the best of its knowledge and belief, that its principals:

(a) Are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded by any Federal department or agency;

(b) Have not within a three-year period preceding this proposal been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, State or local) transaction or contract under a public transaction; violation of Federal or State antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of record, making false statements, or receiving stolen property;

(c) Are not presently indicted for or otherwise criminally or civilly charged by a governmental entity (Federal, State or Local) with commission of any of the offenses enumerated in paragraph (1)(b) of this certification; and

(d) Have not within a three-year period preceding this application/proposal had one or more public transactions (Federal, State, or local) terminated for cause or default.

(2) Where the prospective primary participant is unable to certify to any of the Statements in this certification, such prospective participant shall attach an explanation to this proposal.

INSTRUCTIONS FOR LOWER TIER CERTIFICATION

1. By signing and submitting this proposal, the prospective lower tier participant is providing the certification set out below.

2. The certification in this clause is a material representation of fact upon which reliance was placed when this transaction was entered into. If it is later determined that the prospective lower tier participant knowingly rendered an erroneous certification, in addition to other remedies available to the Federal government, the department or agency with which this transaction originated may pursue available remedies, including suspension and/or debarment.

3. The prospective lower tier participant shall provide immediate written notice to the person to which this proposal is submitted if at any time the prospective lower tier participant learns that its certification was erroneous when submitted or has become erroneous by reason of changed circumstances.

4. The terms *covered transaction, debarred, suspended, ineligible, lower tier covered transaction, participant, person, primary covered transaction, principal, proposal, and voluntarily excluded,* as used in this clause, have the meanings set out in the Definition and Coverage sections of 49 CFR Part 29. You

may contact the person to whom this proposal is submitted for assistance in obtaining a copy of those regulations.

5. The prospective lower tier participant agrees by submitting this proposal that, should the proposed covered transaction be entered into, it shall not knowingly enter into any lower tier covered transaction with a person who is proposed for debarment under 48 CFR Part 9, subpart 9.4, debarred, suspended, declared ineligible, or voluntarily excluded from participation in this covered transaction, unless authorized by the department or agency with which this transaction originated.

6. The prospective lower tier participant further agrees by submitting this proposal that it will include the clause titled "Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion—Lower Tier Covered Transaction," without modification, in all lower tier covered transactions and in all solicitations for lower tier covered transactions. (See below)

7. A participant in a covered transaction may rely upon a certification of a prospective participant in a lower tier covered transaction that it is not proposed for debarment under 48 CFR Part 9, subpart 9.4, debarred, suspended, ineligible, or voluntarily excluded from the covered transaction, unless it knows that the certification is erroneous. A participant may decide the method and frequency by which it determines the eligibility of its principals. Each participant may, but is not required to, check the List of Parties Excluded from Federal Procurement and Non-procurement Programs.

8. Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render in good faith the certification required by this clause. The knowledge and information of a participant is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.

9. Except for transactions authorized under paragraph 5 of these instructions, if a participant in a covered transaction knowingly enters into a lower tier covered transaction with a person who is proposed for debarment under 48 CFR Part 9, subpart 9.4, suspended, debarred, ineligible, or voluntarily excluded from participation in this transaction, in addition to other remedies available to the Federal government, the department or agency with which this transaction originated may pursue available remedies, including suspension and/or debarment.

Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion—Lower Tier Covered Transactions:

1. The prospective lower tier participant certifies, by submission of this proposal, that neither it nor its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any Federal department or agency.

2. Where the prospective lower tier participant is unable to certify to any of the statements in this certification, such prospective participant shall attach an explanation to this proposal.

OGR Grant Conditions

INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM
TERMS AND CONDITIONS

In addition to the federal and state general grant conditions outlined above, the Office of Grants and Research (OGR) in the Executive Office of Public Safety and Security (EOPSS) has certain grant conditions that are essential to the administration of grant awards. Whether subrecipients are receiving funds from a federal or state grant, they must adhere to these conditions.

- **Federal *and* State Conditions** must be adhered to by subrecipients of federal grant funds.
- **Drug-Free Workplace Certification** for Departments Receiving Federal Grants for federal fiscal year 2014 available at http://www.mass.gov/osc/guidance-for-agencies/fiscal-year-updates/fy2014/fy2014-12.html
- **Time extensions**, while uncommon, may be granted at the option of OGR. They are not encouraged or guaranteed.
    - If a subrecipient needs additional time to complete the scope of work for the grant award, OGR may grant a time-only extension as long as the revised ISA containing the extension request is executed by both the subrecipient and OGR before the current end date of the ISA. No time extension can be granted if the revised ISA form is executed after the current ISA end date.
    - Requests for time extensions must to be made at least 30 days before the end date of the ISA.
- **Interdepartmental Service Agreement (ISA) spending** must adhere to the dates specified in the ISA. Spending occurring after the specified ISA end date may result in denial of those costs. The "child" department will be responsible for covering those costs with an account other than that funding the ISA. Subrecipients may not ask the Office of the Comptroller to extend an end date of the program code associated with the ISA without prior agreement by OGR. Should this occur, OGR will deny costs against the ISA. If the costs have already been accepted in MMARS, OGR will ask the "child" department to execute an expenditure correction transaction in MMARS to move those costs to another account belonging to the department.
- **Award amounts remaining at the end of the ISA** will be reverted back to OGR.
- **All goods must be received and all services rendered by the end date of the ISA.**
- **Each ISA has a defined accounts payable period.** All payments must be completed and disbursed by the end date of the specified accounts payable period.
- **An ISA that crosses a state fiscal year (June 30) into the next fiscal year, must observe the Commonwealth's policies on payment corrections or overpayments.** That is, any mistakes in coding must be corrected with an EX transaction before August 31. All payroll corrections must be made by the date in July specified in the Fiscal Year Open/Close guidance issued each year by the Office of the State Comptroller. Any overpayments must be corrected with an ER transaction before August 31. **If these actions are not taken by the times specified, the child department must move the charges to a non-OGR funded appropriation so that the funds can be returned to the federal government.**
- **Programmatic and financial reports** must be received in accordance with the requirements of the specific award. **OGR requires all Financial reports to be submitted along with a Warehouse Query detailing the expenditures made for that period.**
- **Procurement practices** specified by OSD must be followed. The subrecipient should ensure that its procurement practices conform to any specific federal guidelines found in the references in the federal conditions section above. Where there is a difference between the practices of the subrecipient agency/organization and a federal guideline, the more restrictive procedure applies.
- **Site visits and other monitoring** of subrecipients will be made by OGR periodically. All records, papers, and other documents of any kind related to the funded activity must be made promptly available upon request for inspection and copying to any person authorized by OGR.
- **Grant-related documents** must be retained for a period of six years from the close of the contract.
- **Evaluations** of a subrecipient's funded program by an outside evaluator during or at the conclusion of the project period, should be reported to OGR in writing and a copy of the evaluation should be provided.

INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM
TERMS AND CONDITIONS

- **Reporting alleged fraud, waste or abuse** to the Office of the State Auditor or Inspector General and/or to an applicable federal agency is the responsibility of the subrecipient. This includes any alleged violations, serious irregularities, sensitive issues or overt or covert acts involving the use of public funds in a manner not consistent with federal statutes, related laws and regulations, appropriate guidelines, or purposes of the grant.
- **Use of funds should begin** within 60 days of the start of the ISA, and if they are not, the subrecipient must report to OGR the steps taken to initiate the grant activities, the reasons for the delay, and the expected start of the use of the funds. If meaningful implementation steps have not begun after 60 days of the grant start date, OGR reserves the right to cancel the ISA.
- **Subcontractors** implementing activities with grant funds must adhere to the grant provisions in this document and should be approved by OGR prior to subrecipients executing subcontracts.
- **Instructional materials** created or produced with grant funds will be “work made for hire,” as defined in United States copyright law, and EOPSS shall be considered the author. EOPSS shall be the sole owner of all rights pertaining to these materials, including copyrights and all rights to use, reproduce, or publish the materials, and subrecipients may not use, reproduce, or distribute such materials without prior written approval of OGR. If a project results in the production of **other original books, manuals, or copyrightable material**, unless otherwise provided in the contract documents, EOPSS reserves a royalty-free, non-exclusive and irrevocable license to reproduce, publish, translate or otherwise use, and authorize others to publish and use, such material. If paid with federal funds, the grant number must appear on the materials.
- **Audio visual or written materials** developed as part of the grant may be required to incorporate specific language or disclaimers (e.g., regarding the federal source of funding) and in some instances pre-approval from the federal funding agency as instructed by the OGR grants manager.

INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM

ATTACHMENT B - BUDGET

Check one: _X_ Initial ISA Budget

___ ISA Budget/Account Amendment. Maximum Obligation of ISA before this Amendment: $_____.

PRIOR MMARS DOCUMENT ID: _____ (for reference - if applicable)

CURRENT DOC ID: _____.

[See Instructions for Additional Guidance on completion. Insert as many additional lines as necessary.]

A Budget Fiscal Year	B Seller/Child Account	C Object Class	D Description	E Initial ISA Amount / or Amount Prior to Amendment	F Indicate Add or Reduce +/-	G Amendment Amount	H Enter "YES" if Amount is a prior FY budget reduction or a current FY "Carry-in" authorization for Federal ISA Funds	I New Amount After Amendment
2016	8000-4804	KK	**ALPR System**	$50,000.00				

FISCAL YEAR SUBTOTALS AND TOTAL MAXIMUM OBLIGATION FOR DURATION OF ISA	
FISCAL YEAR: _2016_____ SUBTOTAL (*or New Subtotal if Fiscal Year Subtotal being amended*	$ 50,000.00
FISCAL YEAR: ___ ____ SUBTOTAL (*or New Subtotal if Fiscal Year Subtotal being amended*	$
FISCAL YEAR: _____ SUBTOTAL (*or New Subtotal if Fiscal Year Subtotal being amended*	$
FISCAL YEAR: _____ SUBTOTAL (*or New Subtotal if Fiscal Year Subtotal being amended*	$
TOTAL MAXIMUM OBLIGATON FOR DURATION OF ISA (*or New Total Maximum Obligation if amended*)	$ 50,000.00

Additional Budget Specifications:

INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM

ATTACHMENT C – FEDERAL GRANT SELLER/CHILD ACCOUNT

[Complete ONLY if Buyer/Parent Account is a Federal Grant Account. Seller/Child Department must signoff in order to process document.]

__X__ NEW ISA ___ ISA AMENDMENT	BUDGET FISCAL YEAR: 2016
BUYER/PARENT DEPARTMENT: EPS	SELLER/CHILD DEPARTMENT: POL
CTR ONLY - REVENUE BUREAU WILL ASSIGN	
Revenue Budget	Revenue Source
BUYER/PARENT DEPARTMENT MUST COMPLETE ALL ITEMS BELOW	
CENTRAL BUDGET STRUCTURE (BGCN - BQ89)	
Appropriation Number: 80004804	Payroll Indicator : ___Yes __X__No
Budgetary Estimated Receipts $	BGCN Document Identification No.: ISAEPSFY16ALPRPOL16A
COST ACCOUNTING STRUCTURE (BGRG- BQ88)	
Total Maximum Obligation of ISA: $ 50,000.00	BGRG Document Identification No.: ISAEPSFY16ALPRPOL16A
MAJOR PROGRAM TABLE SET-UP	
Major Program (6 chars. or less) HSPGTS	Major Program Short Name (same as appropriation number): 80004804
Major Program Name: Highway Safety Program on GTS	
PROGRAM PERIOD TABLE SET-UP OR EXTENDED PROGRAM PERIOD	
Effective From Date:	Effective To Date:
Program Period:	
Program Period Name: Extended Program period	Program Period Short Name:
PROGRAM TABLE SET-UP	
Effective From Date: 02/01/2016	Effective To Date: 07/30/2016
Program Name: Automated License Plate Recognition	Program Short Name ALPR
Program Code: **(MUST START WITH "F" followed by up to 9 characters) F16ALPR**	Sub Account:

FUNDING PROFILE - FUNDING LINE		
Draw Name:	Customer ID	Payment System Code – **Check one option only**
EDCAPS:	VC7000000001	___**D**
ECHO:	VC7000000002	___**E**
LOCES:	VC7000000003	___**L**
SMARTLINK:	VC7000000004	___**S**
ASAP- OTHER:	VC7000000005	___**Y**
ASAP:	VC7000000006	___**Z**
GRANT- NON DRAW:	VC7000000007	__**X**__ **No Code**

FUNDING IDENTIFICATION	
Federal Catalog Agency: (2 digit code) 20	Federal Catalog Suffix: (3 digit code) **600**
Letter of Credit No.:	

Authorized Signatory Seller/Child Department: _____ Date: _____ Name: _____

4693

INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM INSTRUCTIONS

The Interdepartmental Service Agreement (ISA) Form is issued by the Office of the Comptroller (CTR) pursuant to 815 CMR 6.00 for use by all Commonwealth Departments. The ISA Instructions are provided to assist both Buyer/Parent and Seller/Child Commonwealth Departments with the interpretation and completion of the ISA Form and are incorporated by reference into the ISA. The ISA Form is the "Contract" that documents the business agreement (joint venture) between two Commonwealth departments within the Executive, Judicial and Legislative Branches of government. A Department must be recognized as a Department in the State Accounting System (hereinafter referred to as "MMARS") in order to transfer or receive funding under an ISA. The ISA must comply with funding language in any appropriation act funding the ISA, as well as all applicable general and special state or federal laws, regulations. The Buyer/Parent and Seller/Child are responsible for reviewing and complying with the applicable CTR policies (including but not limited to the ISA, electronic signature and state finance law policies) located at the CTR Knowledge Center under Procurement and Contracts and also at the CTR Website at: Comptroller Policies. While reasonable efforts have been made to assure the accuracy of the legal requirements for ISAs, Departments should consult with their legal counsel to ensure compliance with all legal requirements related to their performance under an ISA. PLEASE NOTE THAT NOT ALL APPLICABLE LAWS HAVE BEEN CITED IN THIS DOCUMENT. INSTRUCTIONS AND HYPERLINKS MAY BE ADDED OR CHANGED WITHOUT NOTICE, SO CHECK THIS DOCUMENT PERIODICALLY FOR UPDATES.

➔ MMARS DOCUMENT ID: Enter the state accounting system (MMARS) BGCN or BGCS or other authorized MMARS document number associated with this ISA. ISA related DOC ID Numbering must be done as described below. The Doc ID must be the Doc ID entered into MMARS and reflected on the supporting ISA paperwork. All ISA Doc IDs MUST START WITH "ISA", as follows:

EXAMPLE DOC ID Number: **ISA**EPS12345678SDF06A

First 3 Characters	Second 3 Characters	Next 8 Characters	Next 3 Characters	Next 2 Characters*	Last Character
ISA	Buyer/Parent Department Alpha	Buyer/Parent defined. May be numeric, alpha or combination	Seller/Child Department Alpha	Fiscal Year	A (initial document) B (1st Amendment) C (2nd Amendment)
ISA	EPS	12345678	SDF	06	A

➔ BUDGET FISCAL YEAR. Enter the Budget Fiscal Year of the ISA or ISA Amendment, as appropriate.

➔ REQUEST FOR RESPONSE REFERENCE NUMBER. If the Seller/Child responded to an RFR that was posted on Comm-PASS, enter the RFR Reference Number as posted. If an RFR was not used, indicate "N/A". Seller/Child Departments may respond to a Request for Response (RFR) or other solicitation of a Buyer/Parent Department. If the Seller/Child Department is selected as a contractor, the ISA Form must be used as the "contract" (instead of the applicable Commonwealth Terms and Conditions and Standard Contract Form and Instructions).

➔ BUYER/PARENT/SELLER/CHILD DEPARTMENT NAME: Enter the 3 Alpha MMARS Department Code. For Example "CTR" for the Office of the Comptroller.

➔ BUSINESS MAILING ADDRESS: Enter the address where all correspondence to the ISA Manager must be sent. Unless otherwise specified in the ISA, legal notice sent or received by the Department's ISA Manager (with confirmation of actual receipt) through the listed fax number(s) or electronic mail address for the ISA Manager will meet any requirements for written notice under the ISA.

➔ ISA MANAGER: Identify the authorized ISA Manager who will be responsible for managing the ISA. ISA Managers must be Department Head Authorized Signatories in order to execute the ISA and otherwise obligate the Department with the appropriate MMARS Security to support Department Head Signature Authorization.

➔ PHONE/FAX/E-MAIL ADDRESS: Identify the phone, fax number(s) and electronic mail (e-mail) address of the ISA Manager.

➔ PURPOSE OF ISA. Check off whether this is a new ISA or an ISA Amendment. For New ISAs, enter the total Maximum obligation for the duration of the ISA. If an ISA Amendment, check off any of the Amendments that are being made and complete any information in the blanks provided and the Attachments that are identified.

➔ BRIEF DESCRIPTION OF PERFORMANCE GOALS TO BE ACCOMPLISHED BY THIS ISA, OR IF AMENDMENT, IDENTIFY WHAT IS BEING AMENDED: Identify a brief description of the ISA, ISA name and performance to be accomplished under the ISA. If an ISA Amendment, identify what is being amended. Merely stating "see attached" or referencing attachments without a narrative description of performance is insufficient *and will result in ISA or Amendment being returned to MMARS Liaison of Buyer/Parent Department*. The description is used to specifically identify the ISA performance, match the ISA with attachments and determine if the appropriate process has been selected.

➔ INDICATE WHETHER SELLER/CHILD DEPARTMENT STATE EMPLOYEES (AA OBJECT CLASS) WILL BE FULLY OR PARTIALLY FUNDED UNDER THIS ISA. Justification for use of state employees and details of who will be working and work that will be performed must be included as part of ATTACHMENT A.

➔ ACCOUNT INFORMATION.

- Check the correct option for either a BGCN – non-subsidiarized (federal, capital, trust); BGCS – subsidiarized (budgetary); Other (CT, RPO or other document authorized by CTR); Non-Financial ISA (no funds are transferred from Buyer/Parent to Seller/Child with resources committed to ISA; or Amendment without Budget changes to ISA (used only for an Amendment if there are no changes to the budget and no changes to Attachments B and C (if applicable).
- Identify for each account under the ISA whether the account is "added", "deleted or "no change". **THIS SECTION MUST BE COMPLETED FOR AMENDMENTS EVEN IF THE ACCOUNT INFORMATION HAS NOT CHANGED.** Enter each ISA account, fund, major program code and program code for all funding under the ISA. Attachment B must be completed for all financial ISAs and ISA Amendments (with Budgetary or Account amendments). Attachment C must be completed for any financial ISAs or ISA Amendments with Budgetary or Account amendments involving federal or capital funds).

➔ ISA ANTICIPATED START DATE**.** Enter the anticipated start date, provided that the Seller/Child certifies that it will not incur any obligations related to this ISA prior to the date that this ISA is executed, NOR prior to the date that sufficient funding for the obligations under this ISA available in the Seller/Child account for expenditure.

Note - ISA Duration. ISAs can be executed for the duration that makes sense from a business perspective. Multi-Year ISAs are encouraged if it best supports the Buyer/Parent and Seller/Child business processes. Similar to other types of contracts, all ISAs are subject to appropriation or other available funding. Therefore, Departments can enter into a Multi-year ISA even if funding transactions have to be processed annually to support each fiscal year of the ISA. Buyer/Parent and Seller/Child Departments are responsible for ensuring that the funding is in place in the authorized Seller/Child account(s) to ensure that the Seller/Child Department can timely encumber funds and pay employees, contractors, grantees, etc. from the authorized ISA Seller/Child account(s)in accordance with the ISA Terms and Conditions.

➔ TERMINATION DATE OF THIS ISA: The Buyer/Parent Department must enter the date the ISA will terminate. An ISA must be signed for the full duration and amount in accordance with what is negotiated between the Buyer/Parent and Seller/Child Department. Amendments to extend the

INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM INSTRUCTIONS

termination date, such as renewals, must be made using the ISA Form and must be signed by authorized Department Head signatories (with appropriate MMARS Authorized Signatory Security roles) of both the Buyer/Parent and the Seller/Child Department contemporaneously with the need for the amendment but no later than the termination date (or as previously amended) in accordance with 815 CMR 6.00.

➔ AUTHORIZING SIGNATURE FOR BUYER/PARENT DEPARTMENT/DATE: The Authorized Buyer/Parent Department Signatory must, in their own handwriting, and in ink, sign AND enter the date the ISA is signed. **THE DATE IS AN INEXTRICABLE PART OF THE SIGNATURE AND MUST BE COMPLETED BY THE SIGNATORY AND MAY NOT BE PRE-FILLED OR ENTERED AFTER THE SIGNATURE BY ANOTHER PERSON.** Rubber stamps, typed or other images are not acceptable. See CTR policies on Electronic Signature and Department Head Signature Authorization for Department Head and Authorized Signatory certifications and responsibilities.

➔ NAME /TITLE: The Buyer/Parent and Seller/Child Department Authorized Signatory's name and title must appear legibly.
NOTE: Secretariat signoff is not required in order for CTR to process an ISA. However, Seller/Child and Buyer/Parent Departments are required to follow any internal secretariat procedures when obtaining authorization for an ISA (or for certain ISA transactions such as an inter-subsidiary transfer "TS") prior to submission to CTR. All ISAs are periodically reviewed by CTR to verify that the signatories are authorized by their Department Head to execute contracts. Departments are responsible for timely processing through secretariats to ensure timely funding as required under the Department Head certifications.

➔ **ATTACHMENT A – TERMS OF PERFORMANCE AND JUSTIFICATIONS.** ***Attachment A is required for all new ISAs and for all ISA Amendments.*** Departments must use this attachment and insert (type, or copy and paste) the required information in addition to other terms of performance negotiated by the parties under Section 9. Sections 1-8 are mandatory and must be answered in detail or the ISA will be returned to the Buyer/Parent Department MMARS Liaison. All information must be inserted into Attachment A using as many pages as necessary. If Amending the ISA, completion of Sections 1, 2 and 3 identifying what is being amended and the reasons for the amendments is required. For sections 4-9 enter only the amended language in the sections being amended.

➔ **ATTACHMENT B - ANTICIPATED BUDGET.** ***Attachment B is required for all New ISAs and for all ISA Amendments with budget and accounting transactions.*** Departments must use this form. Insert all required information and use as many additional lines and pages as necessary. This attachment must breakdown the specifics of the ISA funding, by fiscal year, Seller/Child account, object class, description and amount. For multi-year ISAs the Attachment must provide a subtotal each fiscal year of the ISA (which equals each fiscal year's anticipated maximum obligation). All ISAs must provide a total maximum obligation for the total duration of the ISA (which must equal the total of all fiscal year subtotals) and must match the "Total Maximum Obligation for Duration of ISA" on the executed ISA.

- Check "Initial ISA Budget" , or "ISA Amendment"
- Identify the MMARS Doc ID if the ISA is being amended.
- **Complete Columns A-E For New ISAs. Complete Columns A-I for Amendments.**
  - **Column "A" (Budget Fiscal Year).** Enter the fiscal year of the funding, or amendment. For Multi year ISAs Column A must list planned expenditures by each fiscal year of the ISA.
  - **Column "B" (Seller/Child Account).** Enter the number of each Seller/Child account listed on the ISA Form. For ISAs using multiple Seller/Child Accounts, Column B must list planned expenditures for each Seller/Child account.
  - **Column "C" (Object Class).** Enter the Object Class (subsidiary) as outlined in the CTR Expenditure Classification Handbook (for example, "AA" for Employee compensation, "EE" for Administrative Expenses, "HH" for Consultant Contracts, etc.). IF the line item is authorized for multiple fiscal years, enter a separate line-item for each fiscal year of the ISA in which the line-item is authorized, specifying the estimated amount of the authorized expenditure. Line-items break downs of estimated expenditures by Object Class are required even if the Buyer/Parent account is non-subsidiarized, since the Budget acts as the authorization for the ISA expenditures. For subsequent fiscal years, entering "Balance Forward Amount" for federal, bond and trust accounts is insufficient, since good project management practices presume that departments will be managing estimated expenditures over the life of a project with planned fiscal year obligations, rather than managing projects solely based upon remaining uncommitted estimated receipts or uncommitted balances.
  - **Column "D" (Description).** Enter a brief description of the type of authorized budget expenditure or category, (e.g., "Conference Materials", "Program Manager", "Health Evaluations" etc.)
  - **Column "E" (Initial ISA Amount/or Amount Prior to Amendment).** Enter the amount for the budget item authorized under the ISA for each fiscal year. If the ISA is being amended, enter the current amount for this line-item, prior to the amendment. The Amendment amount will be entered in Column G and the new total will be entered in Column I.
  - **Column "F" (+/-)** is only used if the ISA is being amended to add or reduce a budget line item. Enter "+" for budget addition or "-" for a budget reduction.
  - **Column "G" Amendment Amount** is only used if the ISA is being amended to add or reduce a budget line item. Enter the amount of the budget line being increased or decreased.
  - **Column "H" (Carry-In)** is only used if the ISA is being amended to reduce a prior year federal grants fund line item with uncommitted estimated receipts that are being re-authorized in the current or a future fiscal year. Enter "YES" in this column for each line item being amended (by object class and description) to reflect a reduction in the budget in a prior fiscal year line item, and for each line item being added (by object class and description) to reflect a reauthorization of the funds in the current or a future fiscal year.
  - **Column "I" New Amount After Amendment** is only used if the ISA is being amended to add or reduce a budget line item. Enter new ISA Amount after the adding or reduction of the line-item amount referenced in Column G.
- FISCAL YEAR SUBTOTALS AND TOTAL MAXIMUM OBLIGATION.
  - Fiscal Year Subtotals. For single fiscal year ISAs enter the fiscal year (e.g., "Fiscal Year 2007") and enter the subtotal of all "Current Amounts" (Column E) for that fiscal year. For Multi-year ISAs, enter each fiscal year of the ISA as a separate subtotal and enter the subtotal of all "Current Amounts" for each fiscal year.
  - Total Maximum Obligation for Duration of ISA. Enter the Total Maximum Obligation for the Duration ISA for all fiscal years (as identified on the executed ISA Form). For single fiscal year ISAs, this amount should be the same as the Fiscal Year Subtotal. For Multi-fiscal year ISAs, this amount should equal the total of all the listed fiscal year subtotals.

➔ **ATTACHMENT C – FEDERAL GRANT SELLER/CHILD ACCOUNT** (complete only if Buyer/Parent Account is a Federal Account). Please enter the following information on this form.

- Enter whether this is a "New" ISA or an ISA Amendment and enter the Budget fiscal year.
- Enter the Buyer/Parent and Seller/Child Departments, which must match the ISA.
- *Skip the Revenue Budget and Revenue Source which will be completed by CTR.*
- CENTRAL BUDGET STRUCTURE:
  - Appropriation Number. Enter the Appropriation Number assigned by ANF.

INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM INSTRUCTIONS

- Payroll Indicator. Enter a Payroll indicator of Yes or No.
- Estimated Budgetary Receipts. Enter the amount of the Estimated Budgetary Receipts (the amount estimated in the ISA or Amendment for the current state fiscal year).
- BGCN Document Identification No. Enter the MMARS Document Identification Number for the Central Expense Document (BGCN). The BGCN must be entered and submitted to PEND in MMARS. Providing a screen print of the BGCN aids CTR in the processing of the ISA and set up of the accounts or account changes.

✸ COST ACCOUNTING STRUCTURE.

- Total Maximum Obligation of ISA or ISA Amendment Amount. For New ISAs, enter the Total Maximum Obligation of the ISA for the full duration of the ISA. For ISA Amendments, enter the amount of the modification.
- BGRG Document Identification No. Enter the MMARS Document Identification Number for the Reimbursable Grant Budget Document (BGRG). The BGRG must be entered and submitted to PEND in MMARS. Providing a screen print of the BGRG aids CTR in the processing of the ISA and set up of the accounts or account changes.

✸ MAJOR PROGRAM TABLE SET-UP. This sets up the cost accounting hierarchy with groups of activities (programs) all part of one structure. For example – a major program could be wastewater management – WASTE. All documents (contracts, encumbrances, payments will reference this code.) All documents (contracts, encumbrances, payments will reference this code.)

- Major Program. Enter the 6 (or fewer) character Major Program Code assigned by the department.
- Major Program Name. Enter the full Major Program Name.
- Major Program Short Name. Enter the Major Program Short Name.

✸ PROGRAM PERIOD TABLE SET-UP OR EXTENDED PROGRAM PERIOD (EPP). Enter the Program Period or Extended Program Period (EPP) information. This establishes the effective period of the grant. Please note that end dates are "hard edited" by the system, thus please take into account the accounts payable period for grants when establishing this date. Multiple periods allow for easy periodic reporting aligned to federal reporting dates. However, a Buyer/Parent department may choose to use 1 reporting period – EPP – that encompasses all dates. The downside of this method is that specific periodic federal reporting by the system is not achieved.

- Enter the Program Effective From Date and Effective to Date.
- Enter the Program Period or Extended Program Period (EPP) information.
- Enter the Program Period Name, and Program Period Short Name.

✸ PROGRAM TABLE SET-UP.

- Enter Program Name. For example a program could be for "storm water discharge".
- Enter Program Short Name:
- Program Code. Enter the 10 (or fewer) characters. All Federal Program codes must begin with the letter "**F**". This is the second level of the cost accounting hierarchy. Programs are individual activities within a Major Program. Using the major program example, a program could be for storm water discharge – the program code would be "Fstormdis". All documents (Recurring Payment Order (RPO), payments will reference this code.)
- The sub account must be the sub account in the award letter or the draw on the federal grant will fail. If a sub-account changes, this code must change.

✸ FUNDING PROFILE - Funding Line. This must be filled out properly – indicating the federal payment system to be used. If the wrong payment system is indicated, the draws on the federal grant will fail. Enter a check next to appropriate Payment System Code.

✸ FUNDING IDENTIFICATION.

- Federal Catalog Agency Code. Enter the 2 digit Federal Catalog Agency code.
- Federal Catalog Suffix. Enter the 3 digit Federal Catalog Suffix code from your award letter or contact the appropriate agency. This must align to the grant award. The proper grant identification information is a federal reporting requirement.
- Letter of Credit No. Enter the Letter of Credit No. for this grant award.

COMPLETED ISAS SHOULD BE SUBMITTED FOR PROCESSING TO:

Office of the Comptroller, One Ashburton Place – 9th Floor, Attention: Accounts Payable Bureau, Contracts, Boston, MA 02108
CTR Helpline: **617-973-2468**

Access Control Systems

PO Box 7521
Milford, NH 03055

Invoice

Date	Invoice #
1/8/2016	ACS16-4281

Bill To

MA State Police Fusion Ctr
Trpr. Brian Egnitz
470 Worcester Road
Framingham, MA 01701

FEID 35-2353461
DUNS 05-3355991

P.O. No.	Terms	Project	Rep
2016ACSYSU07POL21...	Net 30	MA State Police Fusion Ctr	CRP

Description	Qty	Qlfy	Rate	Amount
Wanco Systems- Mini Remote Video Monitoring System: WVT3(A) 3 Lines x 8 characters, 14" default font size, Upgrade solar panel 255W, 3 x 12V batteries, 600 Ah total capacity, 45 amp charger, Telescoping tower with 360 degree rotation, Full size computer console, Orange powder-coat finish, 2" ball hitch, Hydraulic Tower Lift, 400W inverter. Includes 1 Axis P5624E Camera or current model, Mounted 3M LPR single camera system, cellular remote modem: Sierra Wireless GX450, 3 RJ45, 1 serial, GPS, antennas mounted to sign and shipping. Estimated run time: All equipment: 9 days winter, 30 days summer. LPR 30 days Fall/Winter, Autonomous Spring Summer	1		34,125.00	34,125.00

Please remit to above address.

Total	
Payments/Credits	
Balance Due	

Access Control Systems

PO Box 7521
Milford, NH 03055

Invoice

Date	Invoice #
1/8/2016	ACS16-4281

Bill To

MA State Police Fusion Ctr
Trpr. Brian Egnitz
470 Worcester Road
Framingham, MA 01701

FEID 35-2353461
DUNS 05-3355991

P.O. No.	Terms	Project	Rep
2016ACSYSU07POL21...	Net 30	MA State Police Fusion Ctr	CRP

Description	Qty	Qlfy	Rate	Amount
Wanco Systems- Speed Trailer: Full matrix display - 26" LED characters - 24"x 30" regulatory speed limit sign with changeable speed limit numbers - Approach- only K band radar, FCC approved - Two 85 watt solar panels - Three 12VDC AGM batteries, 600 Ah total capacity - Telescoping tower with 90-degree rotation - Locking control box - White powder-coat finish - 2" ball hitch - 45A Battery charger, Axle Bar Lock, 400W inverter. Includes: Customer specified Sierra Wireless GX450 Modem with 3-RJ45 and 1 Serial Connection and Antenna mounted to sign and mounting of (1) 3M Camera (provided by other) and shipping. Estimated run time: 6-10 days between battery and charge, seasonal performance	1		21,060.00	21,060.00

Please remit to above address.

Total	
Payments/Credits	
Balance Due	

Access Control Systems

PO Box 7521
Milford, NH 03055

Invoice

Date	Invoice #
1/8/2016	ACS16-4281

Bill To

MA State Police Fusion Ctr
Trpr. Brian Egnitz
470 Worcester Road
Framingham, MA 01701

FEID 35-2353461
DUNS 05-3355991

P.O. No.	Terms	Project	Rep
2016ACSYSU07POL21...	Net 30	MA State Police Fusion Ctr	CRP

Description	Qty	Qlfy	Rate	Amount
Wanco Systems- Custom Mast Trailer: As per picture w/ previous mount for 3M LPR, 500 W Solar/ 3 x 200Ah, AGM Batteries (600 total Ah), 400W Inverter, 45A Battery Charger, Sierra Wireless GX450. Includes mounting of 3M camera (provided by other) and shipping. Estimated run time: Autonomous all year round	2		18,557.50	37,115.00
Training Services- One Day at customer site with a Wanco Factory Technician to go over commissioning , system operations and basic maintenance. ** Training DOES NOT cover the 3M LPR system **. Training requires a minimum of 2 weeks advanced scheduling.	1		2,925.00	2,925.00
PURCHASED VIA PO# 2016ACSYSU07POL21948				

Please remit to above address.

Total	$95,225.00
Payments/Credits	$0.00
Balance Due	$95,225.00

Overdue payments will result in late fees of 1.5% monthly. For billing questions call (603) 249-9820. If your check is returned for non-sufficient funds, you expressly authorize your account to be electronically debited or bank drafted for the amount of the check plus any applicable fees. Payment by check is your acknowledgement and acceptance of this policy and its terms and conditions.

LAW ENFORCEMENT EQUIPMENT, SUPPLIES, & SERVICES



SAFEWARE®

SAFEOPS



ACCESSORIES
- B-Square
- Blackinton
- Break-Free
- Hoppe's
- KleenBore
- M-PRO 7
- Smith & Warren
- Speedfeed

AERIAL DRONES
- Aeryon
- DJI
- FLIR

APPAREL
- 5.11 Tactical
- Arc'teryx
- Bulwark
- Elbeco
- Horace Small
- LION
- PROPPER
- Spiewak
- TRU-SPEC

BAGS, CASES & PACKS
- 5.11 Tactical
- BLACKHAWK!
- Crye Precision
- Hatch
- OK-1
- Pelican
- Plano
- R&B Fabrications
- Wolfpack Gear

BALLISTIC SHIELDS
- Hatch
- Paulson Mfg.
- PROTECH Tactical
- United Shield

BATONS
- ASP
- Monadnock

BODY ARMOR & HELMETS
- 3M
- ABA
- Angel Armor
- Armor Express
- Crye Precision
- Custom Armor Group
- FirstSpear
- HESCO
- PROPPER
- PROTECH Tactical
- Second Chance
- Team Wendy
- United Shield

BODY CAMERAS
- Kustom Signals
- HauteSpot Networks

BUNKERS & BARRICADES
- Mitigation Technologies
- Special Ops Bunker

COMMUNICATIONS
- Atlantic Signal
- Con-Space
- LRAD
- NowForce
- Peltor
- Tactical Electronics

CRIME SCENE INVESTIGATION
- DetectaChem
- EVI-PAQ
- Forensics Source
- FoxFury
- Identicator
- Lightning Powder
- Mistral Security
- NIK Public Safety
- ODV
- TacticID by B&W Tek

DECONTAMINATION
- Decon7
- DuPont
- Force1Decon
- Kappler
- Lakeland
- TrueTech

DUTY GEAR
- Bianchi
- BLACKHAWK!
- Boston Leather
- Gould & Goodrich
- Safariland
- Uncle Mike's

EOD
- ADS
- BAHIA 21
- Inert Products
- Lindon Defense
- Med-Eng
- Mistral Security
- Tactical Electronics
- TacticID by B&W Tek
- United Shield

EYEWEAR
- 3M
- Crossfire Safety
- Edge Eyewear
- ESS
- MSA
- Paulson Mfg.
- Pyramex Safety
- Radians
- Revision Military
- Smith Optics
- Wiley X

FIELD TESTING, DRUG & ALCOHOL
- DetectaChem
- Field Forensics
- Intoximeters
- Mistral Security
- TacticID by B&W Tek
- Thermo Fisher
- TrueTech

FIRE SUPPRESSION
- Cold Fire Tactical

FIRST AID & TRAUMA
- Combat Medical Systems
- H&H Medical
- North American Rescue
- Tactical Medical Solutions
- Z-Medica

FLASHLIGHTS & ILLUMINATION
- BLACKHAWK!
- Brite-Strike
- Cyalume
- Eflare
- FoxFury
- Nightstick by Bayco
- Pelican
- Streamlight
- SureFire

FOOTWEAR
- 5.11 Tactical
- Black Diamond
- BLACKHAWK!
- Danner
- HAIX
- Onguard Industries
- Timberland PRO
- Tingley Rubber

GLOVES & ACCESSORIES
- 5.11 Tactical
- Ansell
- Best Glove
- Hatch
- HexArmor
- Honeywell

HANDCUFFS & RESTRAINTS
- CTS Thompson
- Hiatt
- Monadnock

HAZARDOUS ENVIRONMENT APPAREL
- Blauer
- DuPont
- Kappler
- Kimberly-Clark
- Lakeland
- LION
- Radiation Shield Technologies

HAZARDOUS ENVIRONMENT MONITORING
- ADVNT Biotechnologies
- Biosystems
- Bruker Detection Corp.
- BW Technologies
- Chemring
- Draeger
- GFG Instrumentation
- Honeywell
- MSA
- Proengin
- RAE Systems
- Response Biomedical/ RAMP
- Scott Safety

HEAD PROTECTION
- CMC Rescue
- Custom Armor Group
- Hatch
- Revision Military
- Team Wendy
- United Shield

HEARING PROTECTION
- Howard Leight
- MSA
- Peltor

HYDRATION & COOLING
- CamelBak
- TechNiche

K-9
- Castle's K-9
- Vohne Liche Kennels

KNIVES
- Benchmade

LESS LETHAL
- Combined Systems
- Defense Technology
- FNH
- Royal Arms
- Sage Control Ordnance

LICENSE PLATE RECOGNITION
- 3M
- Cintel
- Vigilant Solutions

OPTICS, THERMAL & NIGHT VISION
- Aimpoint
- Argus
- ATN
- Bushnell
- Dueck Defense
- FLIR/Armasight
- Fraser Optics
- Holosun
- ITT Night Vision
- L3-EOTech
- Morovision
- Night Optics USA
- Vortex Optics
- Wilcox

RESPIRATORY
- 3M
- Avon Protection
- Draeger
- Honeywell
- MSA
- North
- Scott Safety

RIOT CONTROL
- Argus
- Armadillo Merino
- Cold Fire Tactical
- Damascus
- DMS
- FirstSpear
- Hatch
- Mehler Law Enforcement
- Original S.W.A.T.
- Yaffy

ROBOTS
- ICOR Technology
- Mistral Security
- Northrop Grumman
- RoboteX
- QinetiQ

SECURITY
- ADANI Systems
- CEIA
- Garrett
- Rapiscan Systems

TOOLS & TACTICAL ENTRY EQUIPMENT
- Armadillo Tactical Gear
- BLACKHAWK!
- Broco
- HURST Jaws Of Life
- J&N Tactical
- Mistral Security
- Osen-Hunter
- Wilcox

TRAFFIC SAFETY & SPEED DETECTION
- Bone Safety Signs
- Eflare
- Harris Industries
- JBC Safety
- Kustom Signals
- ML Kishigo
- MPH Industries
- Stalker Radar
- Wanco

TRAINING EQUIPMENT
- Monadnock
- UTM

TRAINING SERVICES
- Blackthorne Services Group
- Safariland
- Survival Edge Tactical Systems

VEHICLES
- ICS
- LDV
- Lenco
- Nomad
- Polaris

VIDEO & SURVEILLANCE
- AgileMesh
- Camero
- Kustom Signals
- Tactical Electronics

WEAPON ACCESSORIES
- Badger Ordnance
- FirstSpear
- SureFire
- TAB Gear

WEAPON SECURITY
- Auto Vault











TABLE OF CONTENTS

4702

HEAD PROTECTION 6
COMMUNICATIONS 7
RESPIRATORY 8
BODY ARMOR 10
BALLISTICS 10
ACTIVE SHOOTER 11
PUBLIC ORDER 12
- FR BASE LAYER 12
- FR OUTER GARMENT 13
- SCORPION BODY ARMOR 14
- SCORPION BODY ARMOR/VESTS 15
- HEAD PROTECTION 16
- HAND & FOOT PROTECTION 17
- RESPIRATORY PROTECTION 18
- SHIELDS/BATON 19
- FIRE SUPPRESSION 20
- LESS THAN LETHAL 20
- IDENTIFICATION 21
- ACCESSORIES 21

FIRST AID & TRAUMA 22
EXPLOSIVE MITIGATION 24
ROBOTS 26
DRUG DETECTION 27
NIGHT VISION 28
THERMAL IMAGING 28
FLASHLIGHTS & ILLUMINATION 29
VIDEO & SURVEILLANCE 30
TACTICAL ENTRY 31
TRAINING SERVICES 32
K9 32
BODY CAMERA 33
SPEED DETECTION 33
VEHICLES 34
GAS DETECTION 34
RADIATION DETECTION 35
PPE 35
DECONTAMINATION 37
HEARING 38
APPAREL 38
FOOT PROTECTION 39
DUTY GEAR 40

FOR MORE INFORMATION OR TO PLACE AN ORDER:

800.331.6707 | info@safewareinc.com | www.safewareinc.com

UNITED SHIELD ACH/MICH MIL BALLISTIC HELMET

The new US Military design featuring a low profile compact helmet with minimum target area and weight.



- Weight: 2.6-2.8 lbs.
- Features an advanced 7 comfort pad system
- Offers improved head stability with a 4-point adjustable harness, suede covered chip cup and nape strap
- Ballistic performance to NIJ 0106.01 and HP White 0401.01
- Shock absorption - US Army ACH Spec for impact
- Hemi-Anvil, 10ft/sec with less than 150 G's force transmitted to head
- Fragmentation performance to US ACH Mil-Spec

UNITED SHIELD SPEC OPS DELTA GEN II

Made from advanced Aramid composites and provides lightweight robust protection from ballistic and fragmentation projectiles as well as other low energy threats.



- Weight: 2.7 lbs.
- NEW carbon fiber Universal NVG mount with guaranteed no-rattle fit
- NEW USI Rapid Adjustment Dial BOA® retention system with 2-way adjustments
- NEW 4D Combat Pad ultra comfort system with phase change technology
- Industry leading ballistic proprietary thermoplastic aramid composite shell
- Removable suede split chin strap to allow for laundry, replacement or use of gas mask extender
- 4-point adjustment harness, picatinny rails, helmet VELCRO® brand fastener kit and bungees
- NIJ 0106.01 Level IIIA, HP White 0401.01B Level IIIA and exceeds US MIL-SPEC for ACH helmet for 2, 4, 16, 64, 17 grain fragments

REVISION MILITARY BATLSKIN VIPER™ P4 HELMET

The Viper P4 head protection system is the most advanced combat helmet, weighing up to 24% lighter than the legacy U.S. Army ACH system - pushing the boundaries of obtainable weight reduction while maintaining superior ballistic and fragmentation protection.



- Stops NIJ IIIA level threats
- Available with Revision's MSS Liner System for enhanced comfort and stability
- Every helmet meets U.S. Army's strict performance, protection and quality standards
- Foundation for all Batlskin modular protection system components and accessories
- Available in 3 cuts (full, mid and high) and 4 sizes (S-XL)

UNITED SHIELD PASGT BALLISTIC HELMET

The PASGT helmet is manufactured with state of the art advanced high strength multi-layered Aramid composites laminated under heat and pressure.

- Excellent bullet resistance
- Minimal deformation at a weight of approximately 3 lbs.
- Offers improved head stability with a 4-point adjustable harness, suede covered chip cup and nape strap
- Ballistic performance to NIJ 0106.01 and HP White 0401.01B
- Wider cut around ears and collar cut to reduce interference from other equipment



TEAM WENDY EXFIL® BALLISTIC HELMET

With a ballistic rating of NIJ Level III-A, it exceeds current ACH Blunt Impact Protection requirements and offers optimal comfort, fit and stability.

- Hybrid composite shell for increased strength and a unique geometry for ideal fit
- Boltless CAM FIT™ retention utilizes a Boa® Fit System with Cam Lock sliders for one-handed adjustment. Left Eye Dominant (LED) option also available.
- Zorbium® foam liner provides customizable comfort while protecting against blunt impact, and allows for an overhead communications headband
- Lanyard compatible Wilcox® shroud secures any standard NVG mount
- Complete system weight of 2.6 lbs. (size 1) and 2.75 lbs. (size 2) includes the helmet shell, accessory rails, impact liner and retention system





LRAD® 100X

Self-contained, hand-held portable voice broadcast system for on-scene and tactical communications.

- Powerful, intelligible communication up to 600 meters
- 20-30 decibels louder than bullhorns and vehicle P.A. systems
- Focused, directional sound pattern for target-ed communication
- Create instant acoustic standoff perimeter
- 8-hour rechargeable battery
- Simple operator interface
- Water resistant



LRAD® 100X MAG-HS KIT

Rapidly deployable, self-contained voice broadcast system with high-strength magnet mount and wireless operation capability.

- Wireless control up to 300 meters and a high strength, easy on/off magnetic mount system
- Up to 6X louder than systems of comparable size and weight
- Focused, directional sound pattern for targeted communication with unparalleled clarity
- Create instant acoustic standoff perimeter
- High-strength neodymium mount system
- Wireless system batteries operates up to 8 hours
- 8-hour rechargeable battery
- Simple operator interface
- Water resistant



LRAD® 450XL

Low profile, lighter weight and designed for temporary or fixed mounting on tripods, vehicles, and small boats. Generates the audio output of systems almost twice its size and weight.

- Powerful, intelligible communication up to 1,700 meters
- Voice boost for extended coverage
- Safely communicate beyond standoff distances to determine intent
- Clear, long-range directional communication
- All-weather use
- Creates isntant acoustic standoff perimeter



LRAD® 500X-RE

Compact long range communication system designed for mounting on tripods, larger vehicles and boats.

- Fixed or portable mounting
- Powerful, intelligible communication up to 2,000 meters
- Voice boost for extended coverage
- Creates instant acoustic standoff perimeter
- Rugged, military tested construction
- All-weather use
- Low power requirements: 60W w/voice, 260W w/ tone
- Simple operator interface



LRAD® 360XT SOLAR W/ SATELLITE CONTROL

Mobile, self-contained mass notification system on wheels. Broadcasts highly intelligible voice messages and warning sirens with uniform 360° area coverage.

- Integrated with a fully self-contained, ruggedized trailer and features lockable electronics and equipment enclosures containing the amplifier modules and battery pneumatic systems
- Battery bank can be charged using the built-in AC powered battery charger or optional solar panel
- Standard configuration of a 3 stack 360X emitter provides a 1,000 meters radius of clear communication coverage



LRAD® 500X-MMT

Fully self-contained helicopter mounted, air-to-ground communication system featuring rugged mount with fu pan-and-tilt range of motion.

- Powerful, intelligible communication up to 2,000 meters
- Quickly installed and removed from helicopter
- Self-powered for 6+ hours of continuous operation when fully charged
- Supplemental type certificates not required
- Simple operator interface



LRAD® 360XL-MID MOBILE KIT

Rapidly deployable, fully self-contained mass notification and incident management communication system.

- 360° uniform sound coverage
- Powerful, highly intelligible voice communications over 2.0 km2
- Complete mass notification kit (emitter head, power amplifier, control module, push-to-talk microphone)
- Lightweight and compact form factor
- Low power consumption for hours of continuous operation
- Industry-leading voice clarity and intelligibility

LRAD

AVON FM54™ AIR PURIFYING RESPIRATOR

Provides maximum level of protection to the face, eyes, and respiratory tract from CBRN, riot agents, TICs, and toxic industrial materials while maintaining extreme user flexiblity as mission profiles change.

- Functions in both negative and positive pressure modes (APR, SCBA, CCBA, and PAPR)
- Panoramic single lens visor
- Electronic communication port for integrated voice projection and radio communication
- 4 sizes to accommodate all operators
- Low profile brow for superior helmet compatibility
- Interchangeable silicone nosecups for custom fit
- Multiple modes
- Optional VPU provides ability to easily communicate while wearing mask



AVON C50™ MASK ASSEMBLY

Based on the U.S. M50/JSGPM (Joint Services General Purpose Mask) and sharing key technologies, provides maximum operational flexibility to counter multiple threat scenarios, including CBRN agents, TICs and TIMs.

- Offers high protection, outstanding field of vision and superior comfort
- The innovative design features optimize the user's time in the operational area

FOR A NON-CBRN OPTION, ASK ABOUT AVON'S PC50



AVON ST53™ SCBA

Combines Avon's FM53 mask technology with an advanced modular breathing apparatus to provide positive pressure SCBA and/or PAPR capability for specialist operations.

- Utilizes black anodised lightweight components
- Enables a fast response to changing operational conditions in one complete modular system
- A switch between negative (filter) and positive (SCBA) pressure is achieved at the flick of an easy to locate lever on the front of the mask
- Can attach a short or long duration compressed air cylinder and enter a location on filter mode, assess the situation and change to SCBA mode if the need arises



MSA G1 SCBA

Designed solely with your safety and comfort in mind. The G1 SCBA offers integrated and enhanced solutions to exceed your needs today as well as years into the future.

- Facepiece is lightweight and compact (no electronics needed)
- Control module provides dual color LCD and analog displays
- Improved visibility through buddy lights and reflective material
- Heads up display (HUD) shows remaining cylinder pressure in 4 increments via colored LEDs
- Electronic communications are integrated into every unit
- G1 SCBA ergonomics
- Central power system for all electronics
- Available in easily-upgradeable threaded or quick-connect cylinder attachment
- Integrated technology for future expansion
- Customizable



MSA MILLENIUM CBRN GAS MASK

A Hycar version of the reliable military-style gas mask (MCU-2/P Mask, used by the Air Force in Desert Storm). The mask combines high performance, customized fit, comfort, cost efficiency and is ideal for law enforcement and emergency response personnel.

- Flexible, one piece polyurethane lens with wide field of vision, bonded to a durable super-soft Hycar rubber facepiece
- NIOSH approved for protection against CN and CS tear gas
- Effective against, but does not have approval for OC tear gas
- Effective against biological agents and chemical warfare agents
- Dual-canister mount to allow weapon firing from either shoulder
- Canister provides up to 8 hours service time against CN, CS and OC agents
- Drinking tube to allow fluid ingestion in contaminated atmospheres
- Standard equipment includes a speaking diaphragm for clear, short-range communications
- Features a nosecup to reduce lens fogging in low temperatures or high humidity conditions

MSA MILLENIUM CBRN CANISTER







3M™ SCOTT SAFETY AV-3000 W/ SURESEAL FACEPIECE

Combines superior fit with greater comfort and versatility. Holds NIOSH approvals across a wide variety of applications, including CBRN.

- Top down convertibility-single facepiece for APR, PAPR, supplied air and SCBA applications, including CBRN
- Reverse Reflex faceseal for improved comfort and fit
- Deep, low profile seal for easier interface with PPE
- Dual large mechanical voicemitters as well as extensive electronic options for improved communications for every workplace
- Available with Kevlar, Poly or Rubber head harness

3M™ SCOTT SAFETY 40MM CARTRIDGES AND CANISTERS



3M | SCOTT Fire & Safety

3M™ SCOTT SAFETY AIR-PAK™ X3 PRO

The Air-Pak™ X3 Pro SCBA is built on a proven foundation of redundant safety features to help ensure the security and comfort of today's firefighter.



- Easy to remove harness
- New harness materials offer greater resistance to chemical and water absorption to help minimize contamination
- Reflective webbing
- Natural articulation promotes greater range of motion to the firefighter, while transferring weight to the hips for a more balanced load
- Superior breathablity
- Electronic PAR (ePAR) provides wireless, bi-directional communication between the firefighter and incident command to improve fireground accountability and communications
- New buckle design provides firm hold
- Integrated drag rescue loop
- System integrity alarm provides visual and audible alert
- High flow alarm provides visual and audible alert
- No flow alarm provides visual and audible alert
- "Buddy" lights provide a 360° view of the firefighter's air pressure and PASS status

Honeywell

NORTH®

HONEYWELL OPTI-FIT™ TACTICAL GAS MASK

- Superior field of vision offers an unobstructed view
- Full facepiece constructed of soft silicone for excellent comfort, fit and durability
- Choice of headgear - 5-pt. strap or nylon mesh headnet
- Three-position canister mounting adaptable for various applications
- Anti-scratch coated polycarbonate lens
- Lens meets ANSI Z87.1 standard for impact and penetration resistance
- DIN-threaded 40 mm connectors
- Low breathing resistance
- NIOSH approved with the Model 1688 Canister to provide protection against choloracetophenone (CN), chlorobenzylidene malononitrile (CS) and includes a P100 filter for use against particulates such as pepper spray
- NIOSH approval number TC-14G 0264





HONEYWELL NORTH SAF-T-FIT® P100 PARTICULATE RESPIRATOR

NIOSH-approved P100 protection provides 99.97% particulate efficiency against oil and non-oil based particulates.

- Meets OSHA and EPA filtering facepiece requirements for lead abatement
- Full face seal for secure and comfort fit
- Durable and adjustable straps
- Exhalation valve expels warm air
- Molded cup design
- Incorporates humidity-resistant filter media
- Low breathing resistance
- Lightweight design
- Nose clip is color-coded for visible size recognition
- Latex free
- Multiple size options for wide range and improved fit



AIRIUS AND ARAURA LEVEL IIIA ALSO AVAILABLE

UNITED SHIELD AIRIUS LEVEL II VEST

The latest innovation in WEARABLE body armor.

- NIJ 0101.06 certified Level II armor
- Provides the areal density weight and thinness of leading polyethylene vests with the flexibility and softness of leading aramid vests
- Comes standard with SPA carrier with 'Dry Run' moisture management system to wick away mositure from the body
- The SPA features a 12-point adjustment system, hidden plate pockets, full side coverage, recessed closure system and optional tails
- Weight: 0.63 psf
- Thickness: .22'
- Performance: 9mm v50 - 1705 fps/.357 v50 - 1685 fps

UNITED SHIELD ARAURA LEVEL II VEST

- Weight: 0.99 psf
- Thickness: .25'
- Performance: 9mm v50 - 1729 fps/.357 v50 - 1663 fps

BALLISTICS



UNITED SHIELD LITE TACTICAL VEST

Blends the functionality of a tactical carrier with a lightweight design that's geared for high performance. Features an abrasion resistant outer fabric that provides exceptional durability for extreme situations.

- Sturdy 500D Cordura® nylon outershell exterior construction
- Top loading plate pockets
- Additional pocket for one size smaller rifle plate
- MOLLE compatible webbing on the front, back and sides
- Adjustable shoulder straps
- Adjustable cummerbund with hook/loop closure underneath the front flap
- Bungee lace cummerbund adjustment
- Flat Kanagroo magazine pockets on front flap
- "Man-Down" drag strap in the rear
- Internal straps for adjustable groin protector
- Accepts insertion of United Shield concealable panels



UNITED SHIELD GARRISON VEST

Providing high performance ballistic protection, integrated in a fully functional and versatile design to meet the strategic needs of your specific mission.

- Sturdy 500D Cordura® nylon outershell exterior construction
- Top loading plate pockets
- Additional pocket for one size smaller rifle plate
- MOLLE compatibility on front, back and sides
- Adjustable shoulder straps
- Adjustable cummerbund with hook/loop closure underneath the front flap
- Bungee lace cummerbund adjustment
- Flat Kangaroo magazine pockets on front flap
- "Man-Down" drag strap in the rear
- Internal straps for adjustable groin protector



UNITED SHIELD MOLLE CROSSOVER CARRIER

Ideal for law enforcement officers who have occasional equipment-carrying assignments. Can be easily converted into a ballistic protective vest by allowing insertion of United Shield ballistic panels.

- Durable 500D Cordura® nylon exterior fabric
- Spacer mesh interior fabric improves breathability
- Top loading internal front and back plate pockets
- MOLLE webbing compatibiilty in the front of the carrier
- Adjustable front to back side hook/loop closure
- Internal 4" adjustable elastic cummerbund sewn in the back



UNITED SHIELD DELTA +6H BALLISTIC PLATE

Level III+ stand alone single curve ballistic plate. Ergonomically designed using proven technology affording the wearers excellent stand alone protection against a range of high velocity threats.

- NIJ 0101.06 Certified
- 3.1 lbs. | 10" x 12"

DELTA LITE 6H ALSO AVAILABLE

UNITED SHIELD SIGMA 6H BALLISTIC PLATE

Level III+ stand alone multi-curve ballistic plate. Ergonomically designed using proven technology affording the wearers excellent stand alone protection against a range of high velocity threats.

- NIJ 0101.06 Certified
- 5.8 lbs. | 10" x 12"

SIGMA LITE 6H ALSO AVAILABLE

UNITED SHIELD ZETA 6H BALLISTIC PLATE

Level III+ stand alone single curve ballisitic plate. Ergonomically designed using proven technology affording the wearers excellent stand alone protection against a range of high velocity threats.

- NIJ 0101.06 Certified
- 7.6 lbs. | 10" x 12"

ZETA LITE 6H ALSO AVAILABLE



UNITED SHIELD UNIFORM SHIRT CARRIER

Specially designed to be worn over the dress shirt.

- Uniform shirt design
- Durable 600D Cordura® nylon exterior fabric
- Poly/cotton interior fabric
- Hook/loop shoulder adjustment
- Front adjustable side hook/loop closure
- Two front lower pockets with zipper closure
- Internal tablet pocket with zipper closure
- Front chest pockets with hook/loop closure
- Internal cell phone pocket
- Pen openings
- Shoulder mic tabs
- Bottom internal ballistic opening

ACTIVE SHOOTER

UNITED SHIELD LEVEL IV ACTIVE SHOOTER KIT

Includes:

- (1) PST SC650 helmet
- (2) Zeta 6h NIJ06 certified Stand Alone Ballistic Plates and (1) carrier option
- The Level IV plates are ergonomically designed to offer the user NIJ 0101.06 certified stand alone protection
- Bag included





BALACLAVA

- Fire retardant
- Designed to give a specified level of protection against accidental contact with flame and against certain forms of heat transfer
- One Size

DARK NAVY

EA — ARM 21305-15 (SZ)

ARMADILLO MERINO EPIC SOCK

- Over the calf sock
- Extra long so it can be folded down over the top of the boot
- Elastic arch support system
- Elastic above the ankle for a better fit
- Lightweight high-stretch padding up the shin and across the top of the foot
- Reinforced toe and heel
- Smooth toe seam
- 62% wool, 21% polyamide, 9% polypropylene, 8% elastic
- SM-XL

DARK NAVY

PR — ARM 11511-15-1 (SZ)

ARMADILLO MERINO COUGAR SHORT SLEEVE CREW SHIRT

- Crew neck with generous back length
- Seamless underarm for no chaffing and seamless shoulders designed for load carrying
- Extra strong tread in the stitching and a tag free neckline
- Regular fit
- 100% Merino Wool, Jersey Knit
- SM-4X

DARK NAVY

EA — ARM 21001-15-X

ARMADILLO MERINO JOHNNIES 2 LONG JOHN BOTTOMS

- Flattened seams for increased comfort
- Body hugging fit - comfortable under your uniform
- Tag free waist
- Flatlock stitching
- High stretch stitching
- 100% Merino Wool
- Jersey Knit
- SM-4X

DARK NAVY

EA — ARM 21352-15-(SZ)

ARMADILLO MERINO BOOT SOCK

- Over the calf
- 100% wool next-to-skin and elastic support system
- Reinforced toe and heel
- Smooth toe seam
- 65% Merino Wool, 38% Nylon, 11% Elastane
- SM-XL

DARK NAVY

PR — ARM 11606-15 (SZ)

ARMADILLO MERINO PANTHER LONG SLEEVE CREW NECK SHIRT

- Seamless underarm reducing chaffing
- Raglan sleeve with no seams on the shoulders
- Relaxed fit
- Tag free neckline
- Single needle stitching
- High stretch stitching
- 100% Merino Wool
- Jersey Knit
- SM-4X

DARK NAVY

EA — ARM 21011-15-(SZ)

FR PUBLIC ORDER PANT

- Stud fastening waist
- Zip around lower waist to match length of jacket zip
- Drawcord inside waistband
- Side leg pocket
- Knee darts
- Extra patch of outer cloth at knee
- Ankle tabs with stud adjustment
- 3 under studs penetrate only the outer cloth
- Combine with jacket

			DARK NAVY
EA	YAF	460	(SIZE/HEIGHT)

FR PUBLIC ORDER JACKET

- Flap covering
- Velcro fastening throat tab folds back to loop velcro
- Loop pull on front zip
- 6 cm jetted opening under chest flaps on each side
- Left side only zip fastening map pocket with mobile phone and notebook pocket inside
- 5 belt loops
- Back action pleats allowing 7 cm expansion on each side
- Combine with pant
- SM-3X (Short/Regular/Tall/XTall)
- 4X (Short/Regular/Tall/XTall/XXTall)
- 5X (Regular/Tall/XTall/XXTall)

	DARK NAVY
EA	YAF 771 (SIZE/HEIGHT)

PATROLLING SUSPENDERS

- Outside body: 500 D Nylon
- Nylon complies with US MILSPEC MilaCa43734D
- Webbing complies with US MILSPEC MilaWa17337 and MilaWaAA55301
- Mesh complies with US MILSPEC MilaCa8061

	BLACK
EA	FSL 12-0008

GEAR BELT

- Body is sewn with Type 13, 1-23/32" Nylon
- Climbing buckle (A.K.A. Cobra Buckle), 1.75"
- Nylon complies with US MILSPEC MilaCa43734D
- Webbing complies with US MILSPEC MilaWa17337 and MilaWaAA55301
- Mesh complies with US MILSPEC MilaCa8061

	BLACK
EA	FSL 15-0004





CHEST AND BACK PROTECTOR

- Lightweight, ergonomically designed chest and back protection
- Chest protection: From collar bones to waistline
- Back protection: From shoulder blades to waistline
- Outer shell: Super high impact ABS moulded shell. Ridged design gives excellent protection against impact while keeping weight to a minimum.
- Inner foam: Low-density impact absorbing polyethylene moulded foam reduces weight and allows circulation of air around the product
- Fastenings: 4 Velcro adjustable Nylon straps riveted to the body of the guard. One at each shoulder, two at the waist. Ensuring security and comfort.
- Guards should be worn beneath a compatible flame retardant coverall. The outer moulding offers limited flame spread in accordance with UL-94 HB.
- Certification: Meets the requirements of UK Home Office Centre for Applied Science and Technology Standard 20/07
- Sizes SM-LG

BLACK

PR — DMS CH/BCK (SZ)



SHOULDER AND UPPER ARM GUARDS

- Lightweight, ergonomically designed shoulder and upper arm protection
- Area of protection: The clavicle, the top and point of the shoulder and the upper arm to above the elbow
- Outer shell: Super high impact ABS moulded shell. Ridged design gives excellent protection against impact while keeping weight to a minimum.
- Inner foam: Low-density impact absorbing polyethylene moulded foam reduces weight and allows circulation of air around the product
- Fastenings: 2 cotton covered Velcro adjustable Nylon straps riveted to the body of the guard. One attaches around the shoulder strap of body armour, the other fastens around the upper arm.
- Guards should be worn beneath a compatible flame retardant coverall. The outer moulding offers limited flame spread in accordance with UL-94 HB.
- Certification: Tested and approved to UK Home Office Centre for Applied Science and Technology Standard 20/07 rated
- Sizes XS-XL

BLACK

PR — DMS SHP/ARM (SZ)



FOREARM AND ELBOW GUARDS

- Lightweight, ergonomically designed lower arm protection. Fits the curvature of the arm minimising pressure points at the wrist and elbow. Articulated elbow section ensures freedom of movement.
- Area of protection: The forearm from the wrist to above the elbow
- Outer shell: Super high impact ABS moulded shell. Ridged design gives excellent protection against impact while keeping weight to a minimum.
- Inner foam: Low-density impact absorbing polyehtylene moulded foam reduces weight and allows circulation of air around the product
- Fastenings: 3 cotton covered Velcro adjustable Nylon straps riveted to the body of the guard. Ensuring security and comfort.
- Guards should be worn beneath a compatible flame retardant coverall. The outer moulding offers limited flame spread in accordance with UL-94 HB.
- Certification: Tested and approved to UK Home Office Centre for Applied Science and Technology Standard 20/07 rated
- Sizes XS-XL

BLACK

PR — DMS FRM/040 (SZ)

FEMALE GROIN GUARD

- Lightweight, ergonomically designed female groin protection
- Area of protection: Groin and lower abdomen
- Outer shell: High impact lightweight polypropylene moulding contained within a washable polyester cover
- Inner foam: Low-density impact absorbing foam
- Fastenings: Fully adjustable 2" waist strap. 2 x 1" leg straps pass from the bottom of the guard, between the legs to fasten around the waist strap at the back
- Guards should be worn beneath a compatible flame retardant coverall
- Certification: Tested and approved to UK Home Office Centre for Applied Science and Technology Standard 20/07
- Sizes SM-MD

BLACK

EA — DMS FGG/100 (SZ)



MALE GROIN GUARD

- Lightweight, ergonomically designed male groin protection
- Area of protection: Groin and lower abdomen
- Outer shell: High impact lightweight polypropylene moulding contained within a washable polyester cover
- Inner foam: Low-density impact absorbing foam
- Fastenings: Fully adjustable 2" waist strap. 2 x 1" leg straps pass from the bottom of the guard, between the legs to fasten around the waist strap at the back
- Guards should be worn beneath a compatible flame retardant coverall
- Certification: Tested and approved to UK Home Office Centre for Applied Science and Technology Standard 20/07
- Sizes MD-LG

BLACK

EA — DMS MGG/100 (SZ)



THIGH GUARDS

- Lightweight, ergonomically designed thigh protection
- Area of protection: The front and side of the thighs from close to the hip to just above the knee
- Outer shell: Super high impact ABS moulded shell. Ridged design gives excellent protection against impact while keeping weight to a minimum.
- Inner foam: Low-density impact absorbing polyethylene moulded foam reduces weight and allows circulation of air around the product
- Fastenings: 2 cotton covered Velcro adjustable Nylon straps riveted to the body of the guard. One passes around the thigh, the other attaches to the waist belt. Ensuring security and comfort.
- Guards should be worn beneath a compatible flame retardant coverall. The outer moulding offers limited flame spread in accordance with UL-94 HB.
- Certification: Tested and approved to UK Home Office Centre for Applied Science and Technology Standard 20/07 rated
- Sizes XS-XL

BLACK

PR — DMS THG/050 (SZ)



SHIN AND KNEE PROTECTORS

- Lightweight, ergonomically designed lower leg protection. Fits the curvature of the leg minimising pressure points at the knee and ankle. Articulated knee section ensures freedom of movement.
- Area of protection: The knee and shin to the top of the instep
- Outer shell: Super high impact ABS moulded shell. Ridged design gives excellent protection against impact while keeping weight to a minimum.
- Inner foam: Low-density impact absorbing polyethylene moulded foam reduces weight and allows circulation of air around the product
- Fastenings: 3 cotton covered Velcro adjustable Nylon straps riveted to the body of the guard. Ensuring security and comfort.
- Guards should be worn beneath a compatible flame retardant coverall. The outer moulding offers limited flame spread in accordance with UL-94 HB.
- Certification: Tested and approved to UK Home Office Centre for Applied Science and Technology Standard 20/07 rated
- Sizes XS-XL

BLACK

PR — DMS SHN/100 (SZ)



METATARSAL PROTECTOR

- Lightweight, ergonomically designed instep/metatarsal protection
- Area of protection: The top of the foot from the bottom of the shin/knee guard to the toecap of the boot
- Outer shell: Super high impact ABS moulded shell. Ridged design gives excellent protection against impact while keeping weight to a minimum.
- Inner foam: Low-density impact absorbing polyethylene moulded foam reduces weight and allows circulation of air around the product
- Fastenings: A single Velcro fastening leather strap loops around the boot laces to hold firmly in position
- The outer moulding offers limited flame spread in accordance with UL-94 HB.
- Certification: Tested and approved to UK Home Office Centre for Applied Science and Technology Standard 20/07 rated
- Sizes XS-XL

BLACK

PR — DMS FTPM (SZ)

FORTRESS UNIVERSAL TACTICAL VEST

- Provides full protection to the front, back and sides
- Capable of accepting Level II and IIIA ballistic inserts
- Comes with a gusset sewn top-loading plate pocket that accepts 10 x 12 plates and a heavy-duty operator rescue drag handle
- 360° MOLLE webbing, and front gusset sewn map/tool pocket for quick mission access is fully adjustable in girth and length to fit multiple sizes
- Vest adjustments allows standardization of team equipment and has velcro on the front and rear to accept ID patches
- Accessories include neck, throat, bicep and groin armor
- Sizes SM-XL



NAVY

EA — USI FUTV-SZNV

ID PANELS

- Custom identification panels available for helmets and vests
- Customer can select background color and lettering color
- Vest ID panels will have a Velcro backer to apply to vest. Helmet ID panels will come with both sides of the Velcro attached with a glue backing for helmets.





CALL FOR PRICING/ADDITIONAL INFORMATION



FORTRESS UNIVERSAL PLATE CARRIER

- Provides full protection to the front, back and sides
- Capable of accepting Level II and IIIA ballistic inserts
- Comes with a gusset sewn bottom loading plate pocket that accepts 10 x 12 plates and a heavy-duty operator rescue drag handle
- 360° MOLLE webbing, and front gusset sewn map/tool pocket for quick mission access is fully adjustable in girth and length to fit multiple sizes
- Sizes SM-XL

NAVY

EA — USI FUPC-SZNV



017 SERIES PUBLIC ORDER HELMET

- Thermoplastic shell
- Energy absorbing expanded polystyrene line improves impact protection
- High comfort, flame retardant interior with removable cheek pads for easy cleaning, improved hygiene and longer service life
- Headbands, crown pads and sizing pads for easy fit to individual head shapes and sizes
- High-impact polycarbonate visor with option of anti-mist and anti-scratch coating for improved resistance to fogging and surface abrasion
- Replaceable heavy duty neck curtain - padded for extra comfort and optimum protection
- Four metal gauze audio inserts - resistant to liquid penetration
- Adjustable chinstrap with quick release buckle
- Comply fully with PAS 017: 1995 - the first technical performance standard to be dedicated to public order helmets offering a new higher standard of protection for police and prison officers exposed to front line hazards
- Sizes 00-5

	BLACK, NAVY BLUE
EA	ARG 017T/3 (SIZE/COLOR)



APH05 PUBLIC ORDER HELMET

- Choice of thermoplastic or GRP helmet shells incorporating optically correct, high impact resistant polycarbonate visor with optional anti-mist, anti-scratch coating
- Liquid resistant, metal gauze audio apertures enable local commands to be heard
- Compatible with range of CBRN respirators
- Replaceable neck protector and quick release chin strap with chin cup - accepts high dynamic load with minimum extension and helps to maintain helmet stability
- Range of sizes available to provide optimum fit, with combined impact and padded linings to maximize protection and comfort. Internal fitting accepts radio connection.
- Complies with testing requirements of Home Office Scientific Development Branch Standard 2004, incorporating new tests for impact attenuation of whole helmet and solvent resistance of visor
- Thermoplastic (Sizes 00-5)
- GRP (Sizes 00-6)

	THERMOPLASTIC (BLACK, NAVY BLUE)
EA	ARG APH05T/1 (SIZE/COLOR)

	GRP (BLACK, NAVY BLUE, RED, YELLOW, WHITE)
EA	ARG APH05G/1 (SIZE/COLOR)

RIOT CONTROL HEADSET SYSTEM

- Low profile, single sided headset
- Can be mounted inside riot helmet
- Has the ability to adjust the headset's positon close to his/her ear and provide a noise canceling microphone that would cancel crowd noise, focusing only on the clear transmission of the officer's voice
- Push-To-Talk provides the officer with ease of access to activate when needed yet provide a protective shroud to prevent accidental depression

	BLACK
EA	ATL RCH.ERC.47 (HEADSET SYSTEM)
EA	ATL RCH.P01.47 (PUSH TO TALK ASSEMBLY)
EA	RADIO INTERFACE CABLE



AA50 PUBLIC ORDER GLOVE



- Lightweight
- Black leather
- Elasticated mid-length cuff. Gathered wrist with foam padded lining to prevent ingress of liquids. Compatible with commonly used forearm guards and coveralls.
- Outer material: 0.9-1 mm goatskin leather
- Inner lining: 365 gsm Polyester (Heat resistant to EN659:1996 Annex A)
- Intermediate lining: 0.5 mm Low Density Polyethylene Foam
- Thread: Aramid - flame retardant
- Impact protection: 7-8 mm foam rubber to back of hand & 4 mm foam to back of fingers/thumb
- Abrasion protection: Leather reinforcement to high wear areas of palm/fingers
- Blade cut protection: Aramid loaded reinforcement to palm, fingers and back of hand
- Certification: BS7971-6:2003 Type 2 Level 3
- Sizes 6-13

BLACK

PR — DMS AA50 (SZ)

RIOT ControlBY

- Waterproof aniline fireproof cowhide leather according to DIN/EN 407, level 4
- Anti-cut insert lining according to DIN/EN 388, level 5
- Hard shell knuckle and handback protectors
- Shock absorbing protectors (foam and jelly) on fingers, thumb and wrist
- Fireproof stitching thread and fireproof male and female velcro
- Roller buckle closure with leather strap at wrist for secure fit
- Sizes 5-13

BLACK

PR — MLE 13514SW (SZ)



PUBLIC ORDER - FOOT PROTECTION



HAIX® AIRPOWER XR2

- 8" boot
- Climate system
- Reinforced leather pull tab
- Water resistant sun reflect leather
- Rubber/PU outsole
- Anatomically formed TEXON fleece footbed
- Quality insole
- Composite toe cap
- Metal free puncture protection
- Sizes 5-15 (including 1/2 sizes) (Medium, Wide, Extra Wide)

BLACK

PR — HAI 605118 (SZ)

ORIGINAL S.W.A.T. PUBLIC ORDER BOOT

- 9' boot
- Certified to British Standards BS 7971 2016 Part 5 Footwear for protective clothing and equipment for use in violent situations
- Meets EN ISO 20345:2011 for safety boots
- Composite protective toe cap
- 2.2-2.4mm fire resistant full grain leather
- Waterproof membrane for water, liquid and blood borne pathogen resistance
- LENZI® non-metallic anti-penetration board
- 6mm Poron® XRDMA internal metatarsal protector
- 3M™ Defender fluorochemical finish to assist with fluid run off
- Nomex® flame and heat resistant laces
- Additional PORON® XRDMA in lateral ankle area
- Fire and slip resistant rubber outsole tested [redacted]°C
- Salamander Skin™ toe cap resists abrasion, fire, and liquid fuel
- Sizes: D: 4-15 and EEE: 7-16

BLACK

PR — OSB 114031 BLK (SZ)





AVON C50™ MASK ASSEMBLY

- Based on the U.S. M50/JSGPM and sharing key technologies
- Provides maximum operational flexibility to counter multiple threat scenarios, including CBRN agents, TICs and TIMs
- Offers high protection, outstanding field of vision and superior comfort
- The innovative design features optimize the user's time in the operational area
- Sizes SM-LG

	BLACK
EA	AVO 70501-18X



AVON FM53™ MASK ASSEMBLY

- A multi-role Respiratory Protective Equipment (RPE) System that has been developed specifically for specialist applications where the user needs to respond to ever changing operational conditions
- Provides protection against traditional chemical and biological warfare agents and select TIMs
- Offers both positive pressure SCBA, PAPR and negative pressure APR/capability
- All of the capabilities are available from one mask platform without the need to change components
- Right, left or twin port filter configurations available
- Sizes XS-LG

	BLACK
EA	AVO 72601-250-X



AVON OUTSERT ASSEMBLY

CLEAR OUTSERT

- Flexible polycarbonate outsert that simply attaches to 50 series masks to provide additional impact and scratch resistance in extreme environments.

EA	AVO 70501-156

SUNLIGHT OUTSERT

- Additional protection against high level UV light and flash flares. Constructed from flexible polycarbonate providing additional impact and scratch resistance.

EA	AVO 70501-157



MASK BAG

	BLACK
EA	SFW 44014



CBRNCF50 FILTER

- When combined with an appropriate chemical protective mask, the CBRNCF50 filter canister protects the face, eyes and gastrointestinal tract of the wearer against known chemical and biological agents in aerosol, liquid and vapor form

	BLACK
EA	AVO 72602-2



CTCF50 RIOT AGENT FILTER

- Low profile combination filter containing a pleated high-efficiency filter element
- Specifically designed for removal of riot control agents and tear gases including CS, CN and OC pepper spray
- Pack of 4

	BLACK
PK	AVO 72606-3



INTERLOCKING SHIELDS

- Lightweight personal protective shield
- Can be used individually or locked together to form a continuous barrier
- 4 mm thick clear Makralon Polycarbonate. Offers excellent resistance to impacts, thrown objects and liquids while giving the user an excellent field of vision ahead.
- Handles: Forearm hook and double D handle (optional locking folding handles). Aluminum handles with rubber hand grips. Bolted through the blade and backing plate for maximum strength and security

4'	CLEAR
EA	DMS SLD1200INT
6'	CLEAR
EA	DMS SLD1800INT

POLICE OR SHERIFF ID PANEL AVAILABLE

****ID PANEL IS AN OPTION, NOT STANDARD**

PUBLIC ORDER BATON

- One-piece, solid nylon with moulded rubber grip, retaining strap and locating ring
- 31 mm diameter black Nylon 6
- Grip: Moulded rubber textured grip gives excellent security and control
- Lanyard: 5 mm diameter plaited cord
- 24"

	BLACK
EA	DMS BAT610





SOLO SHIELD

- Lightweight (2.0 kg) personal protective shield
- Forearm loop allows the shield to be retained while leaving both hands free to use other equipment
- 4 mm thick clear Makralon Polycarbonate. Offers excellent resistance to impacts, thrown objects and liquids while giving the user an excellent field of vision ahead.
- Handles: Swivelling steel forearm loop and aluminum grab handle. Bolted through the blade and backing plate for maximum strength and security.
- Shield handles are mounted on a foam/aluminum backing plate which significantly reduces transmission of vibration to the forearm and through the handles
- 650 mm diameter x 4 mm thick

	CLEAR
EA	DMS RSHD

POLICE OR SHERIFF ID PANEL AVAILABLE

****ID PANEL IS AN OPTION, NOT STANDARD**

LEATHER BATON HOLDER

	BLACK
EA	BOS7701-1-BLK



PUBLIC ORDER - FIRE SUPPRESSION

AMEREX HALOTRON I "CLEAN AGENT" EXTINGUISHER



- 9 second discharge
- 6-8 foot range
- 10 H x 3.5 W x 2.63 D
- Stored pressure design
- Dependable drawn steel cylinders
- Durable high gloss polyester powder pain
- All metal valve construction
- Temperature range (-40°F to 120°F)
- EPA approved "Clean Agent" for Class A, E and C hazards
- Low GWP
- Low ODP
- Leaves no residue
- User friendly
- 1.4 LBS

	RED
EA	AMX A384T

LEATHER CARRIER

	BLACK
EA	BOS 7702-1-BLK

COLD FIRE™ TACTICAL CANS

- An environmentally friendly fire extinguishing agent that puts out any fire faster, safer, with less water, less damage to property and less risk to personnel
- Completely 'green' and non-toxic
- Instantly cools everything it touches
- Cools 21x faster than water and works to remove heat, therefore preventing re-igniton
- Encapsulates and breaks down hydrocarbons
- Availablity: 12 oz. and 20 oz. Pistol Grip or Loop Handle Spray Cans, 2L and 6L CFT extinguishers, backpack and fleet kit



12OZ. LOOP HANDLE TACTICAL CAN	
EA	CFT CF302-12TL

20OZ. LOOP HANDLE TACTICAL CAN	
EA	CFT CF302-20TL

2 LITER KIT	
EA	CFT CF302-2LTRKIT

PUBLIC ORDER - LESS THAN LETHAL



COMBINED TACTICAL SYSTEMS AEROSOLS

- Advanced solutions with an array of formulations, sizes and delivery including stream, fog, gel, vapor and Omni-Stream™
- Pepper spray
- Crown management, high volume units
- Omni-Stream™ features a bag on valve (BOV) delivery system allowing the operator to hold the can at any orientation and get consistent stream performance



COMBINED TACTICAL SYSTEMS FLASH BANGS AND STING BALL GRENADES

- Flash Bangs are an ATF controlled Class-C explosive device
- Sting-Ball Grenades are explosive "rubber-ball" style grenades that upon initiation eject rubber balls into a radius surrounding the device



COMBINED TACTICAL SYSTEMS 40MM LAUNCHER

- Multi-Launcher 6.2" Cyl Collapsible Stock
- Lightweight and versatile
- Manufactured using 4140 hardened steel, 6061-T6 mil-spec anodized aluminum and DuPont super tough glass filled nylon



SAGE HAND THROWN MUNITIONS

- 40MM Munitions
- 37MM Rifled Munitions
- 37MM Smooth Bore Munitions

SAGE CHASSIS STOCK SYSTEMS

Each SAGE Enhanced Battle Rifle Chassis System is precison CNC machined from a solid billet of high strength aircraft grade aluminum and is finished with mil-spec hard anodizing. The system increases accuracy and reliablity, reduces perceived recoil, provides ambidextrous sling mounts and multiple Picatinny rails for mounting optics and accessories.





V-LITE™

- 0.8 oz.
- A versatile personal lighting/identification marker
- A simple and intuitive alternative to chemical light sticks
- One button to cycle through the preset functions
- Fully encapsulated to ruggedize the electronics, the flexible silicone body not only protects the good stuff inside but also conforms to curved surfaces
- Mounting is made simple with the V-Lite™ sleeve, providing the operator with a velcro-backed attachment system
- An unnoticeable addition to your helmet during routine operations and low-profile enough to reduce snag hazards during airborne operations
- Modes available: On/Off, Blink/Off, On/Blink/Off, Low/High/Off
- One Size

RED, WHITE, BLUE, ORANGE, GREEN, INFRARED

EA — S&S VL-COLOR01XV



LEATHER WATER BOTTLE CARRIER

BLACK

EA — BOS 7703-1-BLK



VTAC® BROKOS HARNESS

- An ideal tactical load bearing solution
- Complements the 5.11® Brokos belt
- Fully adjustable padded shoulder straps
- MOLLE/5.11 SlickStick® shoulder webbing
- Adaptable rear yoke
- 500D Nylon and aerospace mesh
- Low profile adjustment buckle
- Patch tabs at front and rear
- Removable loop ID panel on back
- One size

BLACK

EA — 511 56105 019



EQUIPMENT BAG

- 80 liter storage
- 6 external zipper pockets
- Protective helmet storage pocket
- Heavy duty bottom
- Cordura nylon with reinforced seams and shoulder straps (backpack or shoulder)

BLACK

EA — DMS 80 LTR



VTAC® BROKOS BELT

- Highly versatile load bearing belt
- Wrap-around MOLLE/5.11 SlickStick® web platform
- Polymer inserts for an ergonomic shape
- Durable, weather resistant 500D Nylon
- Aerospace mesh interior
- Lengths: SM-MD (26.5"), L-XL (33"), 2X-3X (42")

BLACK

EA — 511 58642 019 (SZ)

511 58642 019 2XL/3XL

HOOK & LOOP INNER DUTY BELT

- SM (26-30")
- MD (32-36")
- LG (38-42")
- XL (44-48")



BLACK

EA — BLK 44B7SZBK

CALL 800.331.6707
FOR A QUOTE TODAY!



H&H MEDICAL SWAT-T TOURNIQUET (ORANGE)

Allows a more rapid means to control extremity bleeding and allows application higher into the groin and axilla than other tourniquets.

- Ease of application
- Made with a bright safety orange color for easy identification and application
- Instructions for use are printed on the tourniquet along with the trademark pressure application measure showing just how much pressure to apply to reach occlusion



H&H MEDICAL H*VENT LAMINAR VENTED CHEST DRESSING

Designed to work to relieve pressure from an open chest wound due to air in the chest or bodily fluid.

- A unique multi-directional vented dressing (allows the fluids to "drain towards gravity")
- Helps prevent occlusion
- The unique dome membrane design creates a complete seal around the wound area
- Large vent openings on the H*VENT allows for visual monitoring of the wound
- Proven in internal testing to retain a seal during inhalation and to maintain a sustainable negative pressure (below ambient pressure) within the pleural space
- Lowest profile of any vented chest seal and easy to fold



H&H MEDICAL BLEEDING CONTROL BASIC KIT

Provides first responders with a compact and durable individual hemorrhage control kit to treat bleeding from penetrating and other traumatic injuries.

Kit includes:

- SWAT-T tourniquet
- H&H Mini Compression Bandage
- H&H PriMed Compressed Gauze roll
- Nitrile gloves



NORTH AMERICAN RESCUE COMBAT APPLICATION TOURNIQUET (C-A-T)

The C-A-T® utilizes a durable windlass system with a patented free-moving internal band providing true circumferential pressure to the extremity.

- New single routing buckle for faster application, decreased blood loss, effective slack removal, fewer windlass turns, and simplified training with single protocol application standards
- Includes reinforced windlass, stabilization plate, windlass clip and writeable windlass security strap
- Featuring NAR's signature Red Tip Technology® elliptical tab providing added visual clues during application

NORTH AMERICAN RESCUE

NORTH AMERICAN RESCUE RIGID GEN 7 TOURNIQUET CASES W/ SHIRT SHIELD

Designed to provide personnel with the capability of carrying the life-saving C-A-T® Tourniquet on their person by easily mounting it to their duty/patrol/pistol belt, where it is needed most.

- Includes a Shirt Shield complete with mounting hardware to protect your uniform shirt from undue wear caused by the friction from the windlass clip
- Blade-Tech TekLok Belt Attachment fits up to a 2.25" belt
- Injection molded nylon case to stand up to rugged LE/MIL usage





H&H MEDICAL TECC KIT

Designed to hold enough emergency products to respond to a mass casualty situation.

- Contains everything you need to treat the 3 most preventable causes of traumatic death: blood loss, airway occlusion and sucking chest wound
- Meets the basic requirements for Tactical Emergency Casualty Care



NORTH AMERICAN RESCUE M-FAK MINI FIRST AID KIT

Designed to be the most compact, multi-use IFAK for delivering immediate critical care for penetrating, blast or other traumatic injuries.

Kit includes:

- 1 x C-A-T® (Combat Application Tourniquet®) black
- 1 x 4" Flat ETD™
- 1 x S-rolled gauze (4.5" x 4.1 yd)
- 1 x HyFin® Vent Compact Chest Seal, twin pack
- 1 x pair Bear Claw® nitrile trauma gloves, LG
- Super compact, rugged nylon platform that allows attachment both vertically (MOLLE backing) and horizontally (3" belt loop)
- Clam shell configuration utilizes (2) main sleeves that open on both ends for easy access



NORTH AMERICAN RESCUE PATROL VEHICLE TRAUMA KIT

Desinged to provide personnel with an easily accessible, quick to deploy medical kit from your patrol vehicle.

- One side covers all your agency needs to administer basic first aid and community assistance
- Second side offers a first time combination of basic first aid and basic trauma medical items
- Exterior includes MOLLE-style system to accommodate extra equipment as needed





QUIKCLOT® BELT TRAUMA KIT®

A compact, lightweight, wearable holder that fits up to a 2" belt and can be rotated 90° to make room for other gear. Contents can treat up to one injury.

Includes:

- QuikClot Combat gauze® LE
- SWAT-T™ pressure dressing
- Nitrile gloves



QUIKCLOT® BLEEDING CONTROL BAG®

This bag is integral for responding to a range of bleeding situations. Its innovative design allows it to function in a stand-alone capacity or as part of an overall bleeding control program. Contents can treat up to 12 injuries.

Includes:

- QuikClot Combat gauze® LE
- QuikClot® EMS 4x4 dressings
- QuikClot® EMS rolled gauze
- Tourniquets, C-A-T™ , SOF™ TT-W
- Dressing, TacMed Control™ Wrap
- Nitrile gloves
- Shears, EMS-style



ADS XR150 X-RAY SOURCE

Provides the ultimate option in portability for high powered X-ray machines.

- Weighs less than 5 lbs.
- Penetrates up to 1/2" of steel
- Small size makes the unit easy to position in hard to reach places or to maneuver on a robot arm
- Performance - high penetrating capability, durable, lightweight packing, long battery life
- Simplicity - only one variable to control exposure
- Safety - extremely short exposure time and low leakage
- Spectrum - wide spectrum penetrates both high and low density material in same radiograph



ADS MITHIX PRO EOD HOOK AND LINE TEAM KITS

Designed for EOD, bomb squad, and special operations prodedures.

- High quality components
- Stainless steel hooks
- High-strength marine-grade pulleys
- Low-stretch high grade Kevlar rope and other essential tools made specifically for IED, remote movement and remote handling operations



ADS NEX-RAY®

Offers advanced, portable, lightweight x-ray image capture units designed to obtain accurate, near real-time radiographic imaging.

- Patented technology allows NeX-Ray® to dispense with the use of fragile and heavy glass plates integral to most flat panel imagers
- 2 models available (FPX and MMX)
- Can be operated with Windows XP, 7, or 8 laptops or with Android 4.2 (or later) mobile devices
- NeX-Ray® imagers can be operated in standalone, tethered remote, and wireless modes

ADS TITAN

(1) 12" main barrel
(2) Smooth bore extensions
(1) Rifled extenson
(1) Breech cap
(1) Breech plug
(1) Thread protector



NOW WITH TWO NEW CONFIGURABLE OPTIONS

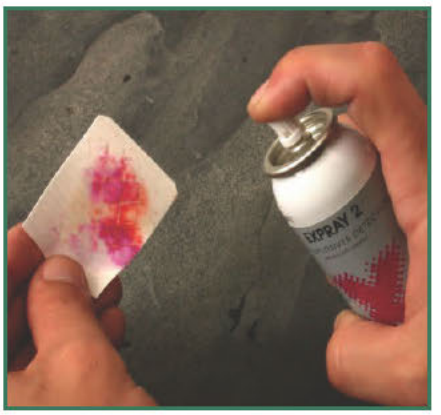
MISTRAL INC.
Member of Mistral Group



MISTRAL SECURITY EXPEN

Ampoule-based technology. Designed for military, EOD, and security personnel primarily for easy carrying and for situations that do not require multiple tests.

- Capabilities: Nitro Aromatic, Nitramines, Ammonium Nitrate, Peroxide, Acetic Anhydride, and much more



MISTRAL SECURITY EXPRAY®

A unique explosive aerosol test technology, Expray®, detects both trace and substance levels of explosives as well as homemade explosive (HME) precursors.

- Capabilities: Nitro Aromatic, Nitro Esters, Nitramines, Inorganic Nitrates and much more



MISTRAL SECURITY TOTAL CONTAINMENT VESSELS (ARC)

Provides full protection against blast and fragmentation with repeated detonation capability.

- Safely contain and transport explosive devices

TACTICAL ELECTRONICS
ELITE TACTICAL CAMERAS & EOD SOLUTIONS





TACTICAL ELECTRONICS 1ST LINE EOD TOOL KIT

Designed to provide EOD operators and bomb technicians with a versatile, lightweight kit that builds upon the capabilities of the Immediate Action Pouch without necessary or wasteful redundancy. Ideal for missions where the user has limited cargo or carry space and where the operator must take weight or dimensions into consideration.

- Small lightweight design
- Can be carried in a cargo pocket or stored in a small compartment
- Ideal for dismounted operations

TACTICAL ELECTRONICS WIRE ATTACK SPECIAL PIERCER PROBES (WASPP) KIT

Specifically designed to allow EOD operators to make non-invasive electrical measurements of wires.

- Includes 10 specialized "bed of nails" piercers with volt meter leads, 10 extensions and 1 roll up carry pouch



TACTICAL ELECTRONICS 2ND LINE EOD TOOL KIT

Customized to equip EOD and bomb technicians with the tools necessary to execute render safe procedures. Allows operators to customize the configuration based on each scenario.

- Comes complete with 6 individually populated tool kits: 1st Line, Immediate Action Pouch, RIP Kit, Detonator Diagnostic Kit, Manual Access Kit and Bit Kit
- All kits fit into one pack with extra room for additional supplies

QINETIQ TALON®

TALON robots are powerful, durable, lightweight tracked vehicles that are widely used for EOD, reconnaissance, communications, sensing, security, defense and rescue. They have all-weather, day/night and amphibious capabilities and can navigate virtually any terrain.

- IOP compliant
- Man-portable, instantly ready for operation
- Fast
- Configurable
- Intuitive
- Outstanding situational awareness: standard 4 color cameras, including night vision, thermal and zoom options
- Withstands repeated decontamination

QINETIQ DRAGON RUNNER® 10

The micro unmanned ground vehicle is lightweight, compact, multi-mission remote platform developed for supporting small unit dismounted operations. When fitted with the Light Weight Modular Arm, it has the ability to investigate and recover or neutralize a potential IED. Day and night sensors allow it to serve as the forward eyes of the team while also delivering remote sensors, emplacing counter-IED charges and more.

- Speed: 4 mph
- Max arm lift: 4.4 lbs.
- Front and rear cameras
- On-board microphone
- Controller: compatible with lightweight radio unit and Gen 2.5 hand controller
- Tough enough to be thrown and survive rough handling and adverse weather

DRAGON RUNNER® 20 ALSO AVAILABLE!"





QINETIQ North America

ICOR MINI-CALIBER®

The lightweight, modular Mini-CALIBER® is a man transport robot for SWAT and EOD operators. Developed for rapid tactical missions, the robot is simple to operate and quick to deploy, providing fast action for searching rooms, hallways, stairwells and confined spaces.

- Includes a manipulator arm on a rotating turret with a 10X zoom camera on the claw and a max arm lift of 15 lbs.
- CBRNE detectors and sensors can be mounted onto the deck of the robot chassis
- Handheld command control unit is portable and intuitive to use
- Clear images are transmitted to the 5.8" LCD daylight readable screen over a wireless RF system

ICOR TECHNOLOGY



ALSO AVAILABLE:



Caliber® T5



Caliber® MK4



MK3 Caliber®



TacticID By. B&W TEK





B&W TEK TACTICID® - GP

A field-ready handheld spectral analysis instrument designed for non-contact forensic analysis. Utilizes proven Raman spectroscopy, allowing users to get real-time actionable identification of unknown chemicals, narcotics, pharmaceutical drugs, explosives and many other substances while reducing operational uncertainty and response time.

- Customized libraries
- Critical component mixture ID
- Indirect contact analysis
- Wi-Fi connectivity
- Touch screen quick notes
- Color-coded result screens
- TacticOne Response™ (24/7/365 emergency support and spectral analysis)

B&W TEK TACTICID® - N

Handheld Raman analyzer for narcotic and pharmaceutical drug identification.

- Comes standard with a comprehensive library of over 1,000 substances
- Critical component mixture ID
- Indirect contact analysis
- Wi-Fi connectivity
- Touch screen quick notes
- Color-coded results screen
- TacticOne Response™ (24/7/365 emergency support and spectral analysis)

MISTRAL SECURITY PDT

A series of individual, presumptive reagent drug tests that help law enforcement officers, drug enforcement agencies and military CID units quickly and easily identify controlled substances while in the field.

- Options: Heroin, LSD, marijuana, cocaine, bath salts and much more



MISTRAL SECURITY PENTEST

An ampoule-based technology that detects trace amounts of drugs as well as bulk amounts.

- Multi-use
- Will not destroy evidence
- Options include: D4D (general screening), Coca, Cannabis, Herosol, LSD, Meth/X, Opiates, and more



MISTRAL INC.
Member of Mistral Group

MISTRAL SECURITY FENTANYL PDT

The only fentanyl test that can distinguish fentanyl from other drugs like meth or amphetamines.

NIGHT VISION



ARMASIGHT PVS7 GEN 3P NIGHT VISION GOGGLES

The most widely recognized and dependable U.S. Military night vision goggle system available.

- Compact, rugged design
- Waterproof
- Ergonomic, simple, easy to operate controls
- Built-in infrared illuminator and flood lens
- Equipped with Automatic Brightness Control (ABC)
- Head or helmet mountable for hands-free usage

AIMPOINT® MICRO T-2

Electronic red dot sighting technology.

- Advanced optical lenses
- Cutting edge lens coatings
- Lightweight sight for extreme conditions
- Excellent night vision compatability

NIGHTOPS TACTICAL PVS-14

A widely recognized monocular night vision device, battle tested by the U.S. Military.

- L-3 Gen 3 Unfilmed technology
- 40 hour runtime
- 1X magnification



THERMAL IMAGING



FLIR BREACH® PTQ136

Thermal imaging monocular. Spots th total darkness.

- Weighing only 7.4 oz. (can be concealed in a pocket or mounted to a helmet with its mini-rail feature)
- On-board recording
- Exceptional vision
- 7 palettes for fast detection of suspects or evidence, day or night
- Digital compass and inclinometer



FLIR THERMOSIGHT® PRO SERII

Thermal imaging weapon sight.

- Exceptional vision
- Built using the new FLIR Boson 1
- Bright, high definition FLCOS display for absolute clarity
- Completely digital for better detection, classification and recovery, day or night
- Powerful and compact hardware is protected by a robust body
- On-board video recording, image capture and storage
- Multiple color palettes
- Digital compass and inclinometer



PELICAN 7600 TACTICAL FLASHLIGHT WITH WAND KIT

- Performance surpassing 900 lumens
- 3 LED colors (white, red, and green)
- Provides high, strobe, medium and low modes
- Full time battery level indication
- USB rechargeable lithium ion battery
- Type III hard anodized finish
- Ingress protected IPX8 submersible



PELICAN 7100 TACTICAL FLASHLIGHT

Compact/high performance flashlight.

- 5" long
- 700 lumens of light output
- High, strobe, medium and low modes
- Full time battery level indication
- USB Lithium Ion rechargeable
- Ingress protected IPX8 submersible

PELICAN 9490 REMOTE AREA LIGHT

- Up to 6,000 lumens (calculated)
- Up to 24 hours of run time
- Intelligent control (allows for various light output levels)
- Maintenace free LED array with 50,000 hour life expectancy
- Full time battery level indication with low level flashing indicator
- 6' deployable mast with 340° rotation
- Multiple deployment positions
- Quick release/ Hot swappable battery design with 12 volt power supply
- Convenient shoulder strap



STREAMLIGHT PROTAC HL® USB FLASHLIGHT

USB rechargeable, 850 lumen tactical flashlight.



- Choice of three user selectable programs
- Multi-fuel capability
- Durable, anodized aluminum construction
- Water resistant sliding metal sleeve protects USB port
- Multi-function, push-button tail switch for one-handed operation
- LED technology impervious to shock with a 50,000 hour lifetime
- Anti-roll head
- IPX4 water resistant
- 1m impact resistance tested

STREAMLIGHT TLR-1® GUN LIGHT

Rail-mounted tactical weapon light.



- 300 lumens
- 2.5 hours regulated run time
- 12,000 candela peak beam intensity
- Rail grip clamp system securely attaches/detaches quickly and safely with no tools
- Powered by two 3-volt CR123 lithium batteries
- Mounts directly to handguns with Glock-style rails and to all MIL-STD-1913 (Picatinny) rails
- Machined aluminum sealed construction with black anodized finish
- IPX7 rated design, waterproof to 1m for 30 minutes

STREAMLIGHT TLR-7® GUN LIGHT

Small and mighty 500 lumen tactial weapon light.



- Runs 1.5 hours
- 4,300 candela
- Custom optic produces a concentrated beam with optimum peripheral illumination
- Uses one CR123A lithium battery
- Safe off feature prevents accidental activation
- Rail grip clamp system securely attaches/ detaches quickly and safely with no tools
- Durable, anodized machined aluminum construction
- IPX7 waterproof to 1m for 30 minutes



SUREFIRE X300U-A

1,000 lumens LED handgun light.

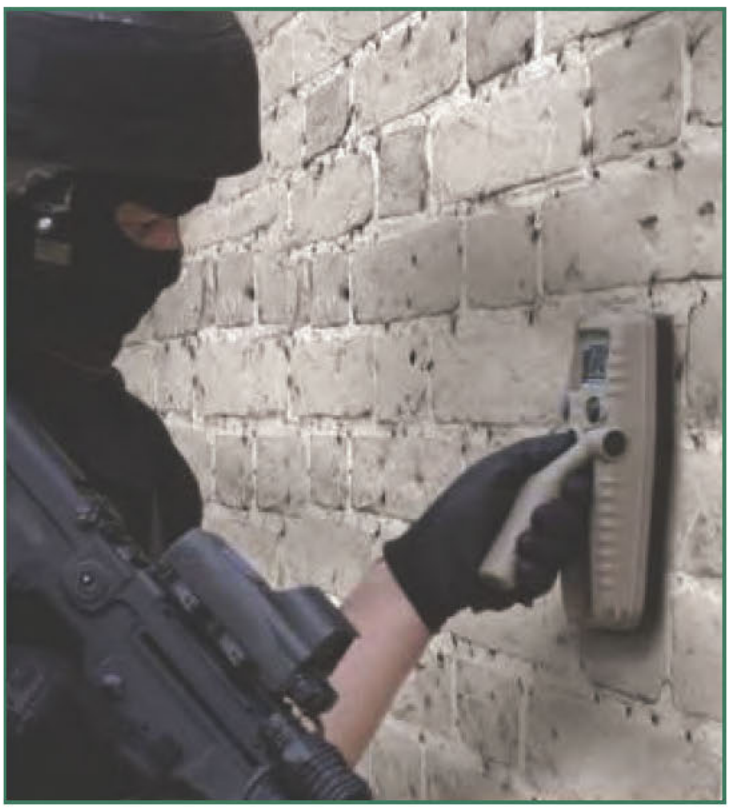
- Custom TIR lens creates smooth, far-reaching light with a larger center spot beam
- Integral ambidextrous momentary-and constant-on switching
- Attaches securely to both universal and picatinny accessory rails
- High-strength aerospace aluminum body, mil-spec hard anodized for extreme durability



SUREFIRE M600DF-BK

1,500 lumen dual fuel rechargeable LED scout light.

- Virtually indestructible ultra-high-output LED generates 1,200 lumens of blinding light with SF123A batteries and 1,500 lumens with included SF18650A rechargeable lithium ion battery charger kit
- TIR lens shapes versatile beam with enough reach and surround light for close-to longer-range operations
- Mil-Spec hard anodized aluminum body, tempered window and O-ring seals make light rugged, durable, and combat ready
- Activation via Z68 momentary/contant-on push button switching with protective shroud



CAMERO
Step into the known

CAMERO XAVER™ 100

Handheld, tactical through-wall detection system. Provides instant critical situational awareness and target acquisition data.

- Potential uses include: Tactical entry/assault, hostage recovery, search and rescue, breaching and force protection
- Reliable detection of moving and static people behind most common wall materials
- 1d imaging information
- Simple user interface and operation requiring no advanced training

CAMERO XAVER™ 400

Compact, tactical through-wall imaging system. Allows for quick location of people hidden by walls and barriers, enabling tactical teams to step into the known and obtain mission-critical information.

- Compact, light and easy to operate
- Ready to go at the push of a button
- Simple user interface with tracking capabilities for intuitive interpretation
- Simultaneous detection of static and moving objects
- Provides information about room dimensions and major infrastructure elements





CMC RESCUE PERSONAL RAPPEL KIT

Lightweight, durable and low profile. Provides everything needed for rappel access or escape for one tactical officer.

Kit includes:

- Black storage bag
- Stealth rope bag
- 8 Link
- Tactical rappel harness
- Black variable anchor strap
- Large edge guard
- Kong Trapezium Quick-Link
- CMC Lifeline - 75' of black 3/8"
- Prusik cord - 5' of blue 7 mm
- Tubular webbing - 20' of black
- (5) black ProTech™ Screw-Lock carabiners



CMC RESCUE TACTICAL TEAM RAPPEL KIT

Provides rope, harnesses, and hardware for two tactical officers moving in vertical environments, where keeping a low profile is a must.

Kit includes:

- Black storage bag
- #2 black rope bag
- Heavy Rescue Organizer™
- (2) 8 Link
- Black variable anchor strap
- (2) tactical rappel harnesses
- Kong Trapezium Quick-Link
- CMC Lifeline - 150' of black 7/16"
- Tubular webbing - 40' (2 z 12') of black
- Large edge guard
- Prusik cord - 10' (2 x 5') of blue 7 mm
- (7) black ProTech™ Screw-Lock carabiners

TACTICAL ELECTRONICS CORE POLE CAMERA

Extend your vision and tactical inspections.

- High-Definition 1280x720p monochrome video
- Longwave infrared (LWIR) thermal imager
- 4 High-intensity white and LED illumination
- Telescopic pole with locking sections
- Lightweight high density graphite pole
- Omni-directional microphone
- Attaches to POLE Grip, or CORE Grip
- Wireless video transmission - 5 GHz
- AES encryption
- WPA2-PSK authentication
- Graphical LCD for status information
- Hardwire video option
- Backlit push buttons
- MicroSD card video recording (32GB)





TACTICAL ELECTRONICS CORE K-9 CAMERA

Transmits real-time HD video back to the handler.

- High-Definition 1280x720p color video
- Longwave infrared (LWIR) thermal imager
- Adjustable high-intensity IR LED illumination
- Push-to-talk two-way audio
- Wireless video transmission - 2.4 GHz
- AES encryption
- Graphical LCD for status information
- Backlit push buttons
- MicroSD card video recording (32GB)

5.11 BREACHING EQUIPMENT

The Heavy Breaching Kit includes four 5.11 breaching tools desgined to defeat any portal quickly and effectively, along with a steel-reinforced, backpack-style Heavy Kit Bag that keeps your breaching tools organized and ready to roll.

- Size: 37" high
- Includes: MultiBreacher, MultiPry, MiniRam, and EdgeBender, Heavy Kit Bag
- Minimizes breach team exposure time
- Durable steel-framed carry pack
- Padded yoke straps
- 400 lb. quick-release buckles
- Removable hood with hook and loop brand closure



TACTICAL ELECTRONICS CORE UNDER DOOR CAMERA

Gain covert visual inspection into rooms behind closed doors.

- 0.26" insertion panel thickness
- Adjustable high-intensity IR LED illumination
- Attaches to POLE Grip or CORE Grip
- Lightweight high density graphite POLE Grip
- Color eyepiece - AMOLED display (CORE Grip)
- Wireless video transmission - 5 GHz
- AES encryption
- WPA2-PSK authentication
- Graphical LCD for status information
- Hardwire video option
- Backlit push buttons
- MicroSD card video recording (32GB)

TACTICAL ELECTRONICS CORE MONITOR

Presents high-definition video from all CORE cameras over an AES encrypted 5 GHz wireless channel.

- Receives high-definition 1280x720p color video on a 5.0" IPS LCD
- Secure pairing with multiple CORE cameras
- Capacitive touchscreen for setup/ configuration
- 1mm Corning Gorilla Glass screen
- Remote camera control for view selection and illumination/dimming
- WPA2-PSK authentication
- Hardwire video option
- Backlit push buttons





TRAINING SERVICES



BSG CBRNE

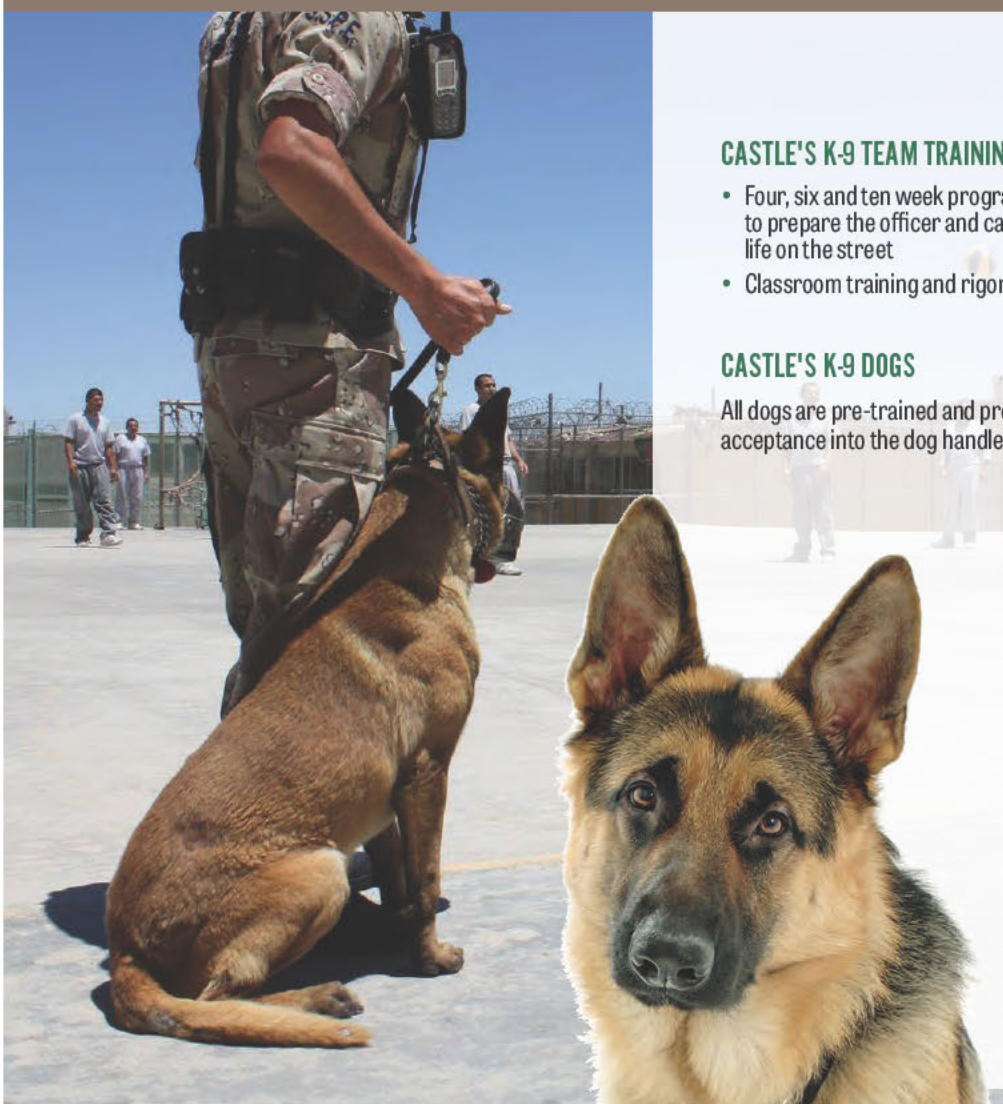
BLACKTHORNE SERVICES GROUP

Provides expertise in CBRNe and related matters. BSG can also branch out to other areas of expertise through their strategic alliances to provide a single point for coordinated consultation on an even larger subject matter.

Training programs include:

- PPE for first responders
- First 100 minutes of RDD, Biological, Chemicals and Explosives response
- Hazardous materials/WMD training
- Illicit and drug lab recognition
- Hazmat rapid intervention teams/fast teams
- Much more!

K9



CASTLE'S K-9 TEAM TRAINING

- Four, six and ten week programs are designed to prepare the officer and canine for everyday life on the street
- Classroom training and rigorous field training

CASTLE'S K-9 DOGS

All dogs are pre-trained and pre-tested before acceptance into the dog handler bonding process

VOHNE LICHE KENNELS

- Selection tested canines
- Narcotic or Explosive trained
- Single or dual purpose

BODY CAMERA

4730

KUSTOM SIGNALS VANTAGE BODY CAMERA

- Flexible data storage solutions (use our cloud or use yours, it is up to you!)
- 30 years of video for law enforcement
- One piece-no cable
- Glove friendly
- Configurable (use only the features you want)
- Rugged design
- IP64 compliant
- 480SD-1080HD capable (and all in between)
- 32GB internal storage
- 120° field of view
- Bookmark button (to mark important events on tape)
- Magnetic mount
- Audio mute

KUSTOM SIGNALS, INC.®



SPEED DETECTION



KUSTOM SIGNALS SMART 650

Speed monitoring awareness radar trailer.

- Kustom Directional RADAR
- 12' high intensity amber LED display
- Flashing overspeed violater alert
- Optional overspeed alerts including 'SLOW', red/blue lightbar, and white LED strobe
- Optional traffic statistics
- 5 year warranty



KUSTOM SIGNALS SMART 850

Speed monitoring awareness radar trailer.

- Kustom Directional RADAR
- 18" high intensity amber LED display
- Flashing overspeed violator alert
- Optional overspeed alerts including "SLOW DOWN", red/blue lightbar, and white LED strobe
- Optional traffic statistics
- Optional solar
- 5 year warranty



KUSTOM SIGNALS VARIABLE MESSAGE SIGN WITH HOMELAND TRAILER

Designed for static and dynamic messages, VMS trailers can be quickly and easily put into place.

- Kustom Directional RADAR
- Amber LED lights provide outstanding visibility
- Hydraulic sign lift
- 4x 2-ton screw leveling jacks
- Removable tongue and 2" ball hitch
- 80W solar panel
- Up to 39 day run time with 6 batteries
- Wi-Fi modem for local wireless programming

3M AUTOMATIC LICENSE PLATE RECOGNITION (ALPR)

3M

ALPR is widely recognized as an effective tool to combat criminal activity, enhance productivity and improve officer safety. Fixed and mobile ALPR systems can help identify certain people and situations:

- Stolen vehicles
- Wanted felons
- Amber alerts
- Sexual predators
- DUI surveillance
- Drug enforcement
- Campus security





GOVERNMENT SECURITY SOLUTIONS

CINTEL ALPR CAMERA

Manufacturer of a full suite of rapidly deployable fixed and mobile ALPR cameras and surveillance products.

CINTEL
Safe. Secure. Simple.





LENCO BEARCAT®

LENCO ARMORED VEHICLES
Protecting Our Nation's Defenders™

Can be used as a SWAT or Military Counter Attack and Rescue vehicle and is often used in hostile Urban Environments.

LDV MOBILE COMMAND CENTERS

LDV

Offers used and new mobile command centers, SWAT trucks and many other specialty vehicle solutions.

GAS DETECTION







MSA ALTAIR® 5X MULTI-GAS DETECTOR

The Altair® 5X is designed with XCell Sensor Technology for faster response and calibration times. XCell Sensors offer superior stability, accuracy and repeatability.

- Easy to use in all applications
- Bluetooth wireless connectivity
- A rugged polycarbonate housing provides unsurpassed durability
- MotionAlert sensor
- InstantAlert feature
- Altair Connect App available on Google Play
- Configurable to meet your needs

MSA
The Safety Company

RAE MULTIRAE WIRELESS, PORTABLE MULTIGAS MONITOR

With the flexibility of up to six gas sensors and the convenience of wireless portability, this multi-gas monitor is versatile and customizable, while delivering real-time access to instrument readings and alarm status from any location. Choose from 25 sensor options including LEL, PID, NDIR, and exotics that can be easily changed in the field. With five built-in alarms, including man down, and wireless connectivity to your command center, MultiRAE delivers vital information for fast incident response.

- Optional integrated wireless
- Dust-tight and waterproof (IP65-rated)
- Onboard gas libraries include 190 VOCs and 55 combustible gases
- Continuous data logging-6 months for 5 sensors 24/7

RAE GAMMARAE II R

A gamma radiation detector and full-range dosimeter in a single instrument. Designed specifically to meet the needs of first responders.

- Two types of sensors for excellent response in high and low dose rate ranges
- Waterproof to IP-67 standards
- Certified for use in Class I, Division 1 hazardous environments
- Top-mounted, invertible display
- Two AA alkaline batteries last up to 600 hours

Honeywell
RAE® SYSTEMS



KROMEK D3S ID

A wearable RIID that gives you the power to make the right decisions about nuclear threats in seconds. A powerful combination of two of Kromek's leading technologies: the non-3He compact thermal neutron detector and its world leading gamma detector, delivering the performance of a RIID in a small, but powerful device, the size of a PRD.

- One of the fastest and most accurate isotope ID devices on the market
- Discreet, wearable, lightweight
- Rapid, visible, audible and tactile alarm settings
- Identifies 17 extra isotopes, 4X faster
- Extensively tested and characterised in multiple DNDO and DARPA programs
- Quick, simple and intuitive to use, no need for specialist training or knowledge
- Built around your operational needs



FLIR®
The World's Sixth Sense®

FLIR IDENTIFINDER® R200

Spectroscopic Personal Radiation Detector (SPRD). Ideal for routine traffic stops or high visibility events and in mass transit or critical infrastructure entry control points.

- Wearable, weighs less than 0.9 lbs.
- Gamma only (R200-G) and gamma/neutron (R200-GN)
- Fully compliant with ANSI N42.32 and N42.48 standards, nuclide identification (≤ 7.5% resolution)
- IP67 and MIL-STD 810G rated enclosure, 1.5m drop-tested on all six sides
- Single-hand operation with 3-button control
- Common user interface with other FLIR raditation detectors
- No consumables or user maintenance



IDENTIFINDER® R300 ALSO AVAILABLE

FLIR IDENTIFINDER® R400

All-Purpose Radionuclide Identification Device (RID)

- Handheld radiation detection and identification
- Intuitive and lightweight (< 3.2 lbs.)
- 3-button interface simplifies operation in high stress situations
- Over 20,000 deployed globally

PPE

DUPONT™ TYCHEM® 2000 SFR

Chemical and secondary flame protection in a lightweight garment. Intended to be worn overy primary flame resistant garments. Also provides an effective barrier against a range of inorganic acids and bases as well as industrial cleaning chemicals and particles.

- Respirator-fit hood lined with Pro-Shield® 6 SFR fabric
- Covered, braided elastic at hood
- Nylon zipper with large metal pull
- Chin flap with double-sided adhesive tape
- Storm flap covers zipper which can be sealed by the wearer with double-sided adhesive strip to prevent intrusion at zipper
- Covered, braided elastic openings at wrist and ankle for tighter fit
- Taped seams

DUPONT®





DUPONT™ TYCHEM® 6000 TF611T

Made of a proprietary barrier film laminated to a Tyvek® substrate. The fabric provides at least 30 minutes of protection against over 180 challenge chemicals including chemical warfare agents and toxic industrial chemicals.

- Strong, durable and lightweight
- Hooded coverall with Elastomeric interface hood for tight fit around respirator
- Rear entry design keeps closure away from direct contact with frontal chemical exposure
- Double storm flap covers zipper which can be secured by the wearer with snaps and hook and loop closure to prevent intrusion at zipper
- Attached dissipative socks with boot flaps
- Attached inner gloves (to be used with appropriate outer gloves)
- Elastic wrist for an optimum fit
- Taped seams provide strong chemical resistance against heavy liquid splashes. A sewn seam is covered with a strip of compatible chemical resistant material through heat sealing

BLAUER RC3® ENSEMBLE

Designed to protect wearers against a broad range of CBRNe threats including liquid and vapor chemicals, radiological and biological particulates, and liquid chemical splash during physically demanding tactical entries, confined space rescue, and US&R missions.

- NFPA 1994 Class 3-R (2018 ed.) certification
- NFPA 1994 Class 4-R (2018 ed.) certification
- NFPA 1992 (2018 ed.) certification
- Breathable GORE CHEMPAK fabric
- Streamlined pattern provides a more tactical fit on the user and better equipment integration
- Durable fabric and seams prevent accidental contamination and provide user confidence
- Ten year shelf life
- Machine washable for multiple uses if not grossly contaminated





Kappler
Know What You're Getting Into.®

KAPPLER DURACHEM® 500

Certified NFPA 1994 protection for both CBRN and Hazmat.

- Includes dual certification to NFPA 1994 for both Class 1 and Class 2
- Provides tactical CBRN protection in non-encapsulating suit
- Rubber gasket fits securely around respirator (eliminates need for taping)
- Rear entry design enhances frontal splash protection



KAPPLER LANTEX® 100

Certified to NFPA 1999 for fentanyl response.

- NFPA 1999 certified Lantex® 100 meets IAB and CDC/NIOSH guidelines for fentanyl protection
- Fabric and seams pass ASTM F1671 blood and viral penetration test
- Breathable protective fabric provides enhanced comfort
- Unique rear entry garment design allows safer doffing, helps prevent cross-contamination
- Soft, flexible rubber gasket around face opening provides secure fit around respirator
- Finger loop features ensures sleeves extend over gloves







LION ERS

LION ready for action

The ERS (Extended Response Suit) protects against lower levels of vapor and liquid concentrations that may be encountered in the Warm Zone when deployed with the proper ensemble. This one piece, front entry suit is breathable for deployment over an extended period of time.

- Durable GORE® CHEMPAK® Selectively Permeable Fabric provides the wearer with protection against TIC's, TIM's, and CWA's below IDLH concentration levels while peforming technical and tactical operations
- Certified to (Warm Zone Operations), NFPA 1994, Class 3 (Toxic Industrial Chemical and Warfare Agent Protection) and NFPA 1992 (Liquid Splash)
- Certifed with variety of face pieces
- Increased mission time and performance due to the breathable selectively permeable membrane
- 24 hour / 3 wash wear life
- Sleek, one-piece, lighweight design with attached hood that easily compacts for storage
- Front-entry design for ease of donning/doffing
- GORE® G9492 inner glove
- Molded face seal that does not require tape and is certified for use with multiple CBRN respirators and masks
- Tapered legs with elasticated cuffs and attached booties for increased funtionality and mobility
- 4 adjustable belt loops to securely wear a duty belt or a PAPR and allow for easy doffing during decontamination

LION MT94™

The MT94™ (Multi-Threat) CBRN ensemble offers first responders advanced protection when facing some of the world's worst chemical and biological threats.

- Limited Hot Zone protection - certified to NFPA 1994, Class 2 and NFPA 1992 for hot zone operations
- GORE® CHEMPAK® Ultra Barrier Fabric provides durable protection against TIC's and CWA's above IDLH concentration levels while also providing improved mobility during tactical and technical operations
- Streamlined design combines durability, mobility and comfort
- Usable for multiple wears and washings, if not exposed or contaminated
- Rugged construction allows you to perform in the most challenging of circumstances
- Certified for use with GORE® G9492™ glove system using GORE® CHEMPAK® Ultra Barrier Fabric



PIP NOMEX HOOD

This NFPA straight cut full face hood is made of 20% Nomex and 80% Lenzing FR, fire resistant 2 ply knit fabrics that are certiifed to NFPA 1971-2007 standard for structural fire fighting.

- 20" in total length with a back gusset that allows it to lay flat around the neck
- Tunneled elastic face opening - 1/2" elastic is encased in fabric to ensure snug and durable fit
- Flatlock seams add strength and extra comfort



APPLICATIONS

- Incident command
- Privacy/scene/evidence protection
- Long-term operations
- Rehab
- Dive rescue

BENEFITS

- 1 person automatic deployment
- Compact storage
- All-weather use
- Pre-installed LED lighting
- Customizable





ZUMRO®
Fast. Simple. Proven.

#1 IN THE INDUSTRY ★

OTHER SIZES & OPTIONS AVAILABLE
PLEASE CALL FOR AN ON-SITE DEMO!



PELTOR®



3M™ PELTOR™ COMTAC™ HEADSETS

Designed to provide warfighters the options needed for successful field hearing protection and combat communications.

- 2-way tactical headset
- Level-dependent surround sound for "talk through"
- Ambidextrous noise-canceling boom mic
- Adjustable sizing

3M™ PELTOR™ TACTICAL 6-S HEADSET

Designed to perceive and localize weak sounds while offering hearing protection in high-noise environments.

- NRR: 19dB
- Small, compact and foldable
- Slim earcup profile
- External earcup microphones help provide situational awareness





ATLANTIC SIGNAL GLADIATOR H TACTICAL HEADSET

Allows an operator to engage and disengage hearing pro at-will while having no impact whatsoever on his ability to RX and TX.

- Earplugs provide up to 23 NRR
- Allows the operator to receive radio communications through his/her facial bones, leaving both ears free to maintain 360° of situational and directional awareness
- Audio transducers are positioned in front of the ears
- Communication systems are customizable

ATLANTIC SIGNAL COMBAT PUSH TO TALK

- Front mounted PTT switch as a secondary actuation switch
- Side mounted switch is quiet and shrouded
- Water resistant

atlantic signal

SAFEWARE IS A PROUD DISTRIBUTOR OF THESE LEADING UNIFORM MANUFACTURERS!

5.11

elbeco

SPIEWAK since 1904

TRU-SPEC





TIMBERLAND PRO® VALOR™ DUTY BOOT

Soft-toe waterproof boots feature outsoles that grip any terrain and lightweight insoles for athletic performance.

- Uppers are black smooth leather and 1200-denier ballistic nylon
- Waterproof membrane
- Mesh lining with antimicrobial treatment for odor control and comfortable feet
- Scotchgard™ protector by 3M for stain resistance
- Bloodborne pathogen-resistant membrane
- Dynamic anti-fatigue technology absorbs shock and returns energy at key zones of the foot for all-day comfort
- Rounded driving moc heel
- Wall-climb toe grip
- Non-marking Timberland PRO® rubber lug outsole is slip-, oil-, and abrasion-resistant



5.11 TACTICAL® A.T.A.C 8" SHIELD CSA/ASTM BOOT

Offers unbeatable puncture, moisture and toe protection for superior safety in the harshest environments. The ATAC Shield Boot keeps you mobile, secure and comfortable at all times.

- Waterproof/breathable BPR membrane
- Side zip functionality
- 5.11 Shock Mitigation System®
- Antibacterial and moisture-wicking lining
- Cushioned insole
- Oil and slip resistant, no-squeak outsole
- Semi-rigid heel and toe reinforcement
- Full grain leather and rugged nylon construction



DANNER ACADIA BOOTS

Made in the USA, the Acadia® features Danner's famous stitchdown construction, providing a more stable platform underfoot and superior durability.

- 8" black
- Waterproof breathable GORE-TEX® lining and a combination upper of 1000 Denier nylon and full-grain leather
- Vibram® Kletterlift outsole provides superior shock absorption and great traction on both wet and dry surfaces

PROPPER® SERIES 100® 8" WATERPROOF SIDE ZIP BOOT

- Polishable full grain leather (black only) with 1000D nylon upper
- Durable, coated, speed lace hardware with 550 paracord lacing
- Fast-rope compatible arch design resists wear from ladders and fast-roping
- Ortholite® sock liner for comfort
- Washable open cell foam inserts contour to your foot for weight distribution and arch support
- Oil- and slip- resistant upper outsole for excellent traction and impact absorption
- Open cell air mesh foam provides full foot air circulation for maximum comfort
- Anti-microbial breathable lining prevents odor and extends the life of the boot
- Triple stitching for durability NATO speed lacing system
- YKK side zipper with zipper guard







HAIX GSG9-S

Developed for and with SRT Teams.

- 8" black
- Waterproof leather
- Footwear liner which will never pull out or wrinkle up over time
- Lightweight foam injected into the sole to provide exceptional shock absorption and superior heat/cold insulation
- Two-zone lacing system

SAFEWARE OFFERS AN EXTENSIVE OFFERING OF DUTY GEAR

GOULD™ &GOODRICH
A PASSION FOR PROTECTION

Including badges, belts, holsters, flashlight holders, magazine cases, radio holders, handcuff holders and much more.



Analysis of Read Data from Massachusetts State Police

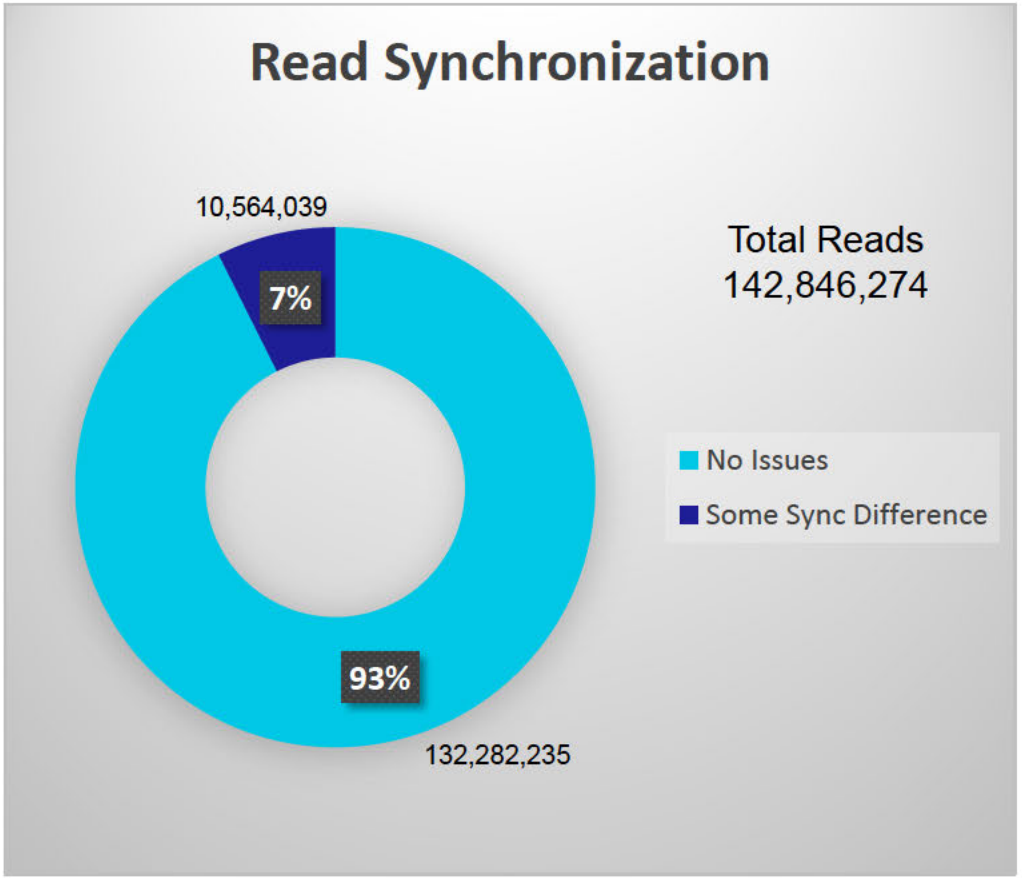
30 November 2020



Confidential

Read Synchronization

- System Scenario:
  - Database
    - Microsoft SQL Server
    - Contains approximately 142 million reads
    - One-year retention period
  - Software
    - BOSS 3
    - First installed: summer 2013
    - Last software update: spring 2018
    - Last annual support agreement: 2018
- This first chart shows the percentage of reads where the camera time is difference than the synchronize time in BOSS. There are a number of reasons for the deviation including but not limited to communication lag, BOSS server is unavailable, network traffic, and the SQL database is unavailable.
- Further analysis will focus on the 7% data.

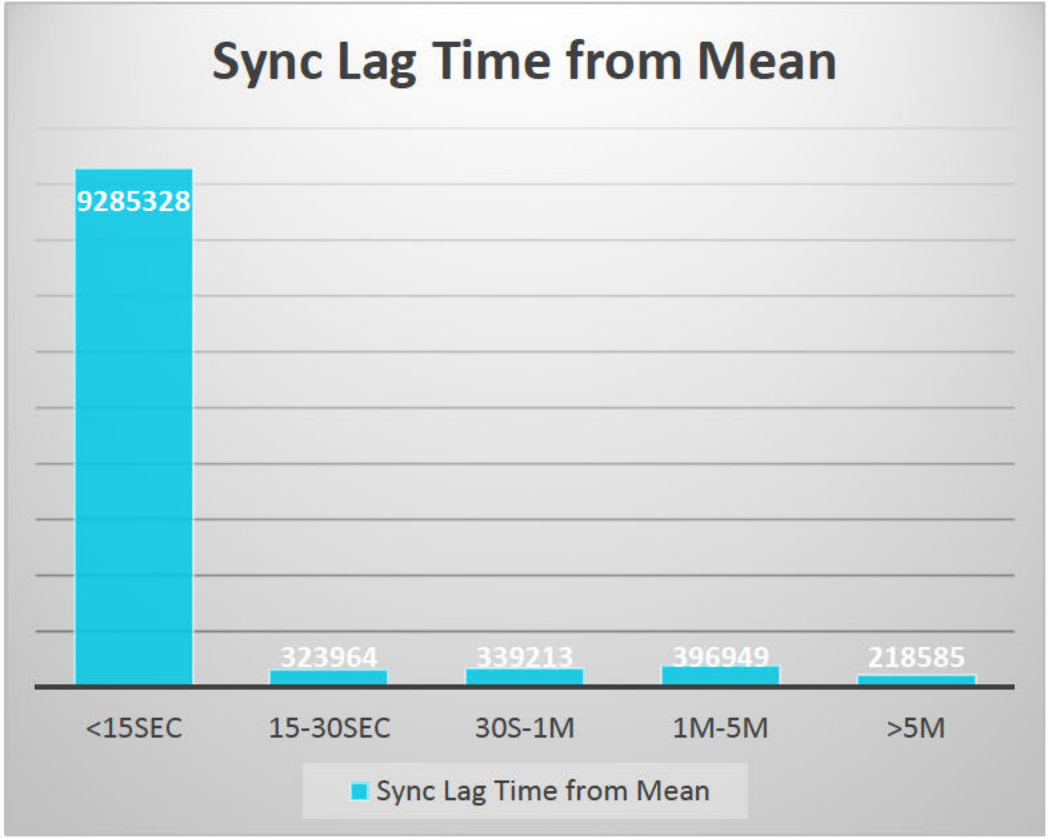


Confidential

Reads with Time Difference

This data represents the 7% data from the total reads where some time difference was identified 4740

- The mean is the average time when the read synchronized that BOSS synchronized with other cameras. This number is important because it gives context to the BOSS service's behavior and thereby accounting for issues with the server.
- Of the 10.5 million reads where the synchronization time is different, 87.9% of that data synchronized within 15 seconds on the mean.
- Of the reads, 94.17% of the data synchronized within a minute of the mean.
- In conclusion, only **0.43%** of the total reads are potentially misaligned with the synchronization. Therefore, we conclude that 99.57% is considered within acceptable synchronization.



Confidential

Summary

There are a number of reasons why the camera time can drift from the BOSS synchronization time. Most of these reasons do not affect the integrity of the read data. These include, but not limited to:

- Communication lags with the network
- BOSS server interruptions
- Bulk cached reads synchronizing all at once
- Database interruptions
- Aged hardware

For these instances, the time captured and recorded by the camera are accurate.

The purpose of the analysis to find signatures in the database that show anomalies that would be considered outside normal interruptions between the camera and the BOSS server. We narrowed the focus by evaluating a subset of reads that exhibit any synchronization time difference. This subset is approximately 7% of the total reads in the system, or 10.5M reads. Within that subset, we calculated an average for each read's sync time (sync mean time) to determine an acceptable deviation between the camera time and BOSS sync time. This was done to account for most BOSS server issues.

Of the subset analysis, approximately 9.95M reads were within one minute of the sync mean time. The remaining 615k reads would be considered potentially misaligned with the synchronization and would need to be evaluated further. This accounts for approximately **0.43%** of the total reads currently in the system. We believe upon initial further analysis that many of these are isolated to specific cameras or camera configurations.

Confidential



PIPS TECHNOLOGY

A NEOLOGY Business

www.pipstechnology.com

Home Office

National ANPR Standards for Policing and Law Enforcement

November 2020

Version: 2.1

1. Executive Summary

These standards articulate the requirements with which the police and other Law Enforcement Agencies (LEA), as detailed at Annex A must comply to access the National ANPR Capability (NAC). These standards do not cover the use of Automatic Number Plate Recognition (ANPR) for any purpose that is not law enforcement and will identify the purposes for which this document shall be applicable. Data from the NAC may not be used for other purposes, however in appropriate circumstances a camera may provide data to both the NAC and organisations other than those listed at Annex A to be managed independently.

This document includes a description of the legal basis for ANPR as well as the applicability of these standards. The standards comprise three main sections: Data Standards, Infrastructure Standards and Data Access and Management Standards. Audit standards and technical requirements are covered in other documents.

Data Standards comprise the security requirements that must be met for the NAC as well as the composition requirements for read data.

Infrastructure Standards cover the end-to-end infrastructure requirements for the NAC, including infrastructure development, cameras, networks, databases, infrastructure access and performance and legal requirements.

Data Access and Management Standards include the management of data within the NAC, including collection, storage, transfer and deletion of data. This section also provides guidance on FOI and Data Protection Act (DPA) enquiries.

The Annexes to this document include password requirements, guidance on investigation categories, the approval process for accessing ANPR data and a list of approved organisations that may access ANPR.

2. Contents

1. Executive Summary 2

Definitions 5

3. Introduction 8

4. Background 9

5. ANPR Legislation 10

6. Applicability 12

7. Part 1: Data Standards 13

7.1. Data Standards Overview 13

7.2. Data Security 13

8. Part 2: Infrastructure Standards 16

9. Part 3: Data Access and Management Standards 28

Annex A: Approved Organisations 38

Annex B: Investigation Categories 40

Major Investigations 40

Serious Investigations 41

Priority and Volume Investigations 43

Annex C: Data Access Requirements 45

Appendix A: Password Requirements 47

Document Revisions

Version 1.1 draft	July 2020	Change ref from CAST to DSTL in 8.14 Clarification at 9.8 re Command and Control Update of links within text
Version 2.0	September 2020	Published with amendments as above
Version 2.1	November 2020	Footnote added re data deletion (para 9.5.1)

Definitions

Acronym	Description
ANPR	Automatic Number Plate Recognition
ANPR system	A collection of cameras, readers components linking to NAS
Audit Standards	National Standards for Compliance and Audit of Law Enforcement ANPR
CCTV	Closed Circuit Television
CAMERA	The device used to capture an ANPR read
CAPTURE RECORD	The record of a vehicle recorded by NAS for a vehicle passing an ANPR camera including the ANPR READ, associated images and meta data.
COMMUNICATIONS LINKS	The connections between the camera, any local infrastructure and the NAS
CONTROLLER	The competent authority which alone or jointly with others determines the means and purposes of the processing of personal data. Part 3 data Protection Act 2018
CCA	Crime and Courts Act 2013
CPIA	Criminal Procedure and Investigations Act 1996 and the CPIA Code of Practice
DPA	Data Protection Act 2018
FOI	Freedom of Information Act 2000
GDPR	General Data Protection Regulation
GSCP	Government Security Classifications Policy – (formerly the Government Protective Marking Scheme (GPMS)
GPS	Global Positioning System
HIT	The report of a match of a vehicle registration mark (VRM) READ with a VRM that is included on a vehicle of interest list (VOI)
ICO Code	ICO Code of Practice for Surveillance Camera Systems

ISO	Information Security Officer – The member of staff with responsibility for ensuring compliance with requirements for IT security
ITHC	IT Health Check – The process for ensuring that security provisions for IT are appropriate and in compliance with requirements that are current at the time of the check.
JCA	Joint Controller Arrangements under provisions of the Data Protection Act 2018-
JPEG	Joint Photographic Expert Group image format
LEA	Law Enforcement Agency – Includes police forces and other agencies undertaking law enforcement activities. For the purpose of this document, LEAs shall only include those organisations listed at Annex A.
MIDAS	Motor Insurance Bureau (MIB) data of uninsured vehicles
MOPI	Code of Practice for the Management of Police Information
NAC	National ANPR Capability includes: • the NAS which is a single national system consisting of the functionality to enable use for operational response, investigation and intelligence purposes and a single national store of data, and, • the National ANPR Infrastructure (NAI) which is a network of ANPR cameras, communications links, firewalls and other related supporting components, that are the responsibility of LEA, that connect to the NAS.
NAI	A network of ANPR cameras, communications links, firewalls and other related supporting components
NAS	National ANPR Service
NASP	National ANPR Standards for Policing first version published in 2013 and replaced by NASPLE recognising the applicability to all law enforcement agencies that access the NAS
NASPLE	National ANPR Standards for Policing and Law Enforcement.
National VOI List	Nationally circulated lists that include stolen vehicles, vehicles requiring an operational response and vehicles within Schengen circulations
NAPS	National Accreditor for Police Systems – Responsible for confirming that police IT systems are in accordance with security requirements and authorising connection to national systems.
Network Connections	The IT links between components of the NAC

NPCC	National Police Chiefs' Council
NPCC Vetting Policy	The NPCC standards for vetting of staff for access to police information
PERSONAL DATA	Means any information relating to an identified or identifiable living individual. 'identifiable living individual' means a living individual who can be identified directly or indirectly, in particular by reference to_ a) an identifier such as name, an identification number, location data or an online identifier, or b) One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual Data Protection Act 2018
PNC	Police National Computer
READ	The interpretation of a VRM by an ANPR system
RIPA	Regulation of Investigatory Powers Act 2000
RIPSA	Regulation of Investigatory Powers (Scotland) Act 2000
Schengen	The Schengen Information System will enable the authorities of signatory countries to have access to reports on persons and objects for the purpose of border checks and controls and other police and customs checks
SMS	A Standards format for text messaging
TSpec	The document prescribing the technical specifications for data within the National ANPR Service (NAS) to comply with the requirements of NASPLE.
VOI	The details of a vehicle that are of interest to law enforcement for operational response or investigation purposes that is included on a list to enable it to be READ and for authorised staff to receive a report of that READ.
VRM	Vehicle Registration Mark

3. Introduction

The Home Office issues these standards in support of the management and use of the National ANPR Service (NAS). ANPR is used by the police and other law enforcement agencies (hereafter referred to as LEAs) for law enforcement purposes. LEAs should use these policy standards to shape technical standards, standard operating procedures and audit standards.

This document covers the use of ANPR within the NAC and will identify for which uses this document shall be applicable. The use of ANPR within the NAC otherwise than in accordance with this document is not permitted.

This document is divided into 3 sections:

- Part 1 – Data Standards, which define the compliance requirements for ANPR Data
- Part 2 – Infrastructure Standards, which define the compliance requirements for ANPR infrastructure
- Part 3 – Data Access and Management Standards, which define the access requirements for LEAs and other organisations that are associated with ANPR data for law enforcement purposes.

4. Background

ANPR technology is used to help detect, deter and disrupt criminality at a local, force, regional and national level. This includes tackling traveling criminals, Organised Crime Groups and terrorists. ANPR provides lines of enquiry and evidence in the investigation of crime and is used by LEAs throughout England, Wales, Scotland and Northern Ireland.

There exists a National Law Enforcement ANPR capability (NAC) which enables LEAs to benefit from operational use of ANPR. The NAC comprises:

- The NAS. This is a single national system comprising standardised functionality to enable use for operational response, investigation and intelligence purposes as well as a single national store of data;
- The National ANPR Infrastructure (NAI), which is a network of ANPR cameras, communications links, firewalls and other related supporting components. Any element of this network that is connected to the NAS shall be the responsibility of the LEA that manages that connection.

4.1 Technical Specifications

Technical specifications for the NAC are detailed within a technical specification document (TSpec). LEAs are required to conform to the requirements of that document.

5. ANPR Legislation

ANPR operates under a complex framework of legislation of general application, including the General Data Protection Regulation (GDPR), the DPA, the Surveillance Camera Code and Common Law.

The National Law Enforcement ANPR capability (NAC) is subject to the Information Commissioner's Office regulatory provisions and regulatory oversight by the Surveillance Camera Commissioner (SCC).[1]

5.1. ANPR Data: Legal Basis

ANPR data from police forces is police information within the meaning of The Code of Practice on the Management of Police Information 2005 (MoPI) made under the Police Act 1996 and Police Act 1997. It may be shared between LEAs in accordance with the provisions of that Code or any other document which applies similar standards in its place, including the National Crime Agency's (NCA) Statement of Information Management Practice (SIMP).

Access to and the retention and management of ANPR data obtained by LEAs must be compatible and consistent with their relevant legal obligations, which include: The Data Protection Legislation (i.e. the General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA));

- ICO Code of Practice for Surveillance Camera Systems (ICO Code);
- College of Policing Approved Professional Practice – Information Management. (MOPI);
- Part 2 of the Protection of Freedoms Act 2012 (PoFA);
- The Surveillance Camera Code issued under Part 2 of PoFA.
- Criminal Procedure and Investigations Act 1996 and Code of Practice issued under Part II of that Act (CPIA);

[1] Section 29(6) of the PoFA includes ANPR as one of a number of surveillance camera systems under the regulatory oversight of the SCC and its associated Home Office code of practice. Relevant authorities (as defined by Section 33 (s33) of PoFA) in England and Wales (including the police) must have regard to the code which provides guidance on the appropriate and effective use of surveillance camera systems, and therefore ANPR

5.2. Use of ANPR for Law Enforcement Purposes

ANPR infrastructure may only be deployed law enforcement purposes as defined in Part 3 of the DPA ; or on grounds of national security. Law Enforcement is defined by the DPA as “the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security”. The Joint Controller Arrangements (JCA).

The JCA details the responsibilities of controllers for compliance with the DPA. The National Police Chiefs’ Council (NPCC) ANPR lead is designated as the lead controller within the JCA for the NAS.

Joint Controllers have determined within the JCA that they will conform to consistent policy and procedures for the elements of the NAC for which their own LEA is responsible and for which they are controller.

5.3. ANPR Audit

The Home Office has also issued a separate document entitled “National Standards for Compliance and Audit of Law Enforcement ANPR” (Audit Standards). This document sets out the requirements for compliance and audit by all LEAs and of the national components of the NAC.

6. Applicability

These standards apply to any NAC operated by LEAs in the UK that connect to or receive data from the NAS.

Where, under an agreement, LEAs receive data from components that are under the ownership or control of other organisations it is the responsibility of the receiving LEA to ensure compliance with the NASPLE.

ANPR cameras that are used solely for speed enforcement are outside the scope of these standards.

ANPR systems that are not operated by LEAs and do not submit data to the NAS are similarly outside the scope of these standards.

6.1. Approved Organisations

An LEA may only connect to, or receive data from, the NAS following approval of the NPCC policing lead for ANPR within the NPCC Crime Operations Committee (NPCC policing lead for ANPR) - an "Approved Organisation".

For an organisation to be designated as an "Approved Organisation" it must be involved in and can lawfully process data for one or more of the following activities:

- National security and counter terrorism
- Law enforcement
    - The prevention and detection of crime
    - The apprehension and prosecution of offenders

In granting access, the NPCC policing lead for ANPR must be satisfied that it is necessary and proportionate for the organisation to be approved.

Approved Organisations must ensure that their organisation complies with the requirements of NASPLE and Compliance and Audit Standards.

References to LEAs within NASPLE includes only "Approved Organisations" unless indicated otherwise. Approved Organisations are listed in Annex A.

In addition to the above purposes LEAs may use the NAS for operational purposes relevant to individual and public safety. E.g Missing persons.

7. Part 1: Data Standards

7.1. Data Standards Overview

Part 1 prescribes the standards with which data must comply for it to be accepted into the NAS.

7.2. Data Security

LEAs have a duty to protect ANPR data to ensure its integrity and to maintain its value for law enforcement purposes. ANPR 'read' data must therefore be attributed a protective marking of OFFICIAL, in accordance with the Government Security Classifications Policy (GSCP).

When in the NAS database, other material could be accessed such that personal details of persons associated with the ANPR READ data may be identified. Once ANPR READ data is available within the NAS, it is personal data in the context of the DPA.

All ANPR data in the NAS, should therefore be managed in accordance with DPA principles and handled as OFFICIAL - SENSITIVE data, in accordance with the GSCP.

Whilst in the custody of, or being transmitted to or from a LEA, ANPR data should be handled in accordance with Part 2 and Part 3 of NASPLE.

Access to data within ANPR systems must be in accordance with Part 3 of NASPLE.

7.3. ANPR Read Records

7.3.1. Composition

An ANPR READ places a VRM at a specific location and time. It is obtained by a camera as part of an automatic number plate reading system. The data components of a record must not be entered manually into the NAS unless for the purposes of correcting a mis-read VRM on the system or by an administrator for testing the connectivity of a camera.

The READs must include VRM, time, location of read and camera identifier and be consistent with the requirements of section 7.4.

7.4. Core Data

7.4.1. Vehicle Registration Mark (Mandatory)

ANPR data must accurately represent VRMs of all vehicles with correctly represented EU and Schengen Community number plates. Systems must accurately record the VRM for vehicles passing within the field of view for each camera. The capture and read rates must be in accordance with the type of camera defined at Section 8.9.

7.4.2. Vehicle Registration Mark – Not Read (Mandatory where functionality is in place)

Where a CAMERA has the capability to record images of vehicles passing within the field of view where no VRM is identified by the system, information will be recorded in the VRM field in accordance with current TSpec.

7.4.3. Time (Mandatory)

System audit provisions must provide evidence of synchronisation at least once every 10 minutes using standard time source techniques in accordance with current TSpec.

Components of ANPR systems must automatically adjust the display of the time to daylight saving time during the period when this is in-force.

7.4.4. Location (Mandatory)

ANPR data must place a read in a location, accurate to within 10 metres. In addition, all fixed-site ANPR cameras must have their GPS co-ordinates accurately recorded to within 5 metres.

7.4.5. Supporting Imagery

In order to assist with assessment of the accuracy of individual read records, ANPR data may include images:

- Plate patch – showing the number plate only, to allow comparison of the visual image with the textual representation interpreted (Mandatory for systems under ownership or control of a LEA)
- Overview Image – showing the vehicle to allow identification of the make, model and colour of the vehicle within the read zone (Optional)
- 'Geo Tagging' - if an accurate GPS Geo Location is available, then this detail may be added to images (Optional)

Should any image be found to exceed prescribed limits for image size, cameras submitting the images must be revised to ensure images obtained are within the limits prescribed within a maximum of 7 days.

All images must be linked to the corresponding read record.

All images recorded must be forwarded to the NAS. Where no overview image has been recorded, the read record must include a reference to identify that no image is recorded.

7.4.6. Record Retention and Deletion

All read records received by LEAs including any associated images must be supplied to the NAS.

All records must be managed and subsequently deleted in accordance Section 9.5.

7.4.7. Camera Performance Evaluation

Camera Performance evaluation, as detailed in Section 8.14 of all components within LEA ANPR systems must be conducted to ensure compliance with the Data Standards. Where performance falls below the Data Standards then this must be corrected and reassessed to confirm that performance conforms to data standards, within 30 days of that issue being identified.

If camera performance issues are not resolved within 30 days of identification, then the feed of data from those cameras must cease until corrected.

8. Part 2: Infrastructure Standards

8.1. Infrastructure Standards Overview

Part 2 prescribes the standards for the components of the NAC, including the operability standards required that are to be used by LEAs connected to the NAS.

8.2. Accreditation

To preserve the integrity of the NAC, all components of infrastructure that connect to the NAS must be assessed to ensure that they do not pose a threat to the NAC and are suitably for handling data up to GSC OFFICIAL level.

8.3. LEA Domain

The assessment of risk to an LEA domain rests with the controller for each LEA, which will normally be discharged by the Information Security Officer (ISO) for that LEA. The level of risk posed should be determined through completion of a Risk Analysis Document and an IT health check (ITHC). Review of compliance with the risk analysis outcomes and the conduct of an ITHC is to be completed annually.

8.4. ANPR Network

The National Accreditor for Police Systems (NAPS) needs to be assured that the local LEA Infrastructure poses no threat to NAC. The NAPS will liaise with the LEA ISO to assess the level of risk posed, as documented through the LEA corporate information risk management and ITHC process.

The NAPS will approve the components of local infrastructure for connection to the ANPR Network. This will be confirmed by the completion of the Code of Connection.

8.5. ANPR Infrastructure Development

A consistent and standardised approach must be applied to infrastructure development within the NAC.

8.5.1. Strategic Assessments

A strategic assessment should be carried out prior to the deployment of an ANPR camera. An assessment should also be carried out prior to receiving ANPR data for onward submission to the NAS, that is received from ANPR systems operated by organisations that are not defined as LEAs. These assessments must identify a need for ANPR at that location for law enforcement purposes.

Where a need is identified, consideration of whether the deployment, or the receipt of ANPR data is appropriate and proportionate. This requires an assessment of the

value for law enforcement purposes taking account of the impact on fundamental rights and freedoms of individuals. Consideration of the legitimate expectations of individual privacy is also required. Strategic assessment should consider:

- National Security and Counter Terrorism,
- Serious, Organised and Major Crime
- Local Crime,
- Community Confidence and Reassurance, Crime Prevention and Reduction.

8.5.2. Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA), which may include consultations with relevant stakeholders, is required for all planned new infrastructure.

The DPIA must include:

- A description of the proposed development
- An assessment of the risks to the fundamental rights and freedoms of individuals – the data subjects.
- Measures to mitigate those risks
- Confirmation of safeguards and security measures to ensure protection of personal data and compliance with the DPA.
- Details of any stakeholder consultation

8.5.3. Information Commissioner's Office Consultation

The NAC may result in high risk to the rights and freedoms of individuals and prior consultation with the Information Commissioner's Office (ICO) may be required before the deployment of any new ANPR infrastructure. When a DPIA identifies a large increase in the number of deployed ANPR infrastructure or where significant privacy risks are identified the ICO should be consulted. (Section 64 DPA)

8.5.4. Strategic Assessment Reviews

LEAs must monitor the continued requirement for a camera to be maintained at a location, or for an LEA to receive data from ANPR systems operated by other organisations. Should the justification for deployment at that location cease, the device must be removed, and the receipt of data must be terminated.

The locations of all cameras and the need to receive data from systems operated by other organisations must be reviewed annually, considering requirements for infrastructure development to ensure that camera deployment or receipt of data remains appropriate and proportionate.

8.6. Vehicle-Mounted Systems

Vehicle-mounted ANPR may only be deployed where any of the following circumstances arise:

- For the purposes of monitoring hits against a list of VOI with the intention that an operational response to the hit will take place, either by staff within the vehicle containing the ANPR system or by others deployed in support of that vehicle for the purpose of providing a response.
- Deployed at locations identified following completion of infrastructure development assessment prior to the deployment of other camera at the location.
- Deployed as a result of Operational tasking processes within an LEA where it has been determined that it is proportionate for short-term deployment of ANPR;
    - In response to identified criminal activity
    - In response to identified community problems
- To support assessment of a location for future more permanent camera deployment in accordance with the infrastructure development procedure
- In support of immediate operational response following report of a crime or incident.

8.7. System Standards

The performance standards for camera shown below are most easily met for vehicles travelling towards a camera, and it is recommended that unless unavoidable, for example in some dual-lane deployments, that this configuration is used in all cases.

8.7.1. Static ANPR Systems

A static ANPR system has been built for the primary purpose of 'capturing' and 'reading' VRMs and is located in a fixed position, with no intention of the system being moved. Except in extreme weather conditions the performance standards for these systems must be achieved at all times. Systems must capture 98% of all VRM that are visible to the human eye[2] and accurately read 95% of captured VRM.

8.7.2. Moveable ANPR Systems

A moveable ANPR system has been built for the primary purpose of 'capturing' and 'reading' VRMs, is located in a fixed position on a temporary basis and may be

[2] 'Visible to the Human eye' should be determined from the viewpoint of the camera within the ANPR system. A number plate visible to a 'human eye' at that location should also be visible by the ANPR system.

moved. Except in extreme weather conditions the performance standards for these systems must be achieved at all times. Systems must capture 98% of all VRM that are visible to the human eye and accurately read 95% of captured VRM.

8.7.3. Multi-Lane ANPR Systems

A Multi-Lane ANPR system has the capability to read VRM for vehicles travelling in multiple lanes of the highway using a single camera. Except in extreme weather conditions the performance standards for these systems must be achieved at all times. For vehicles travelling towards the camera, systems must capture 98% of all VRM that are visible to the human eye and accurately read 95% of captured VRM.

For vehicles travelling away from the camera, the system must capture 90% of all VRM that are visible to the human eye and accurately read 95% of captured VRM.

8.7.4. CCTV Integrated ANPR Systems

A CCTV Integrated ANPR system may operate both as a CCTV camera and as an ANPR camera. The camera should be optimised[3] for the purposes of ANPR when being deployed as a camera. Integrated systems must only provide data to the NAS when in ANPR mode. Except in extreme weather conditions the performance standards for these systems must be achieved at all times when deployed in ANPR mode. CCTV systems may not be optimised to capture ANPR reads therefore systems must capture 85% of all VRM that are visible to the human eye and accurately read 95% of captured VRM.

8.7.5. Mobile ANPR Systems

A mobile ANPR system has been built for the primary purpose of 'capturing' and 'reading' VRMs. These include vehicle-mounted ANPR systems and other portable systems deployed on a temporary basis. Any equipment procured after the publication of version 1 of National ANPR Standards for Policing (NASP) (May 2013) must be live-linked to the NAS.

To achieve the optimum performance requirements, mobile equipment should be capable of night-time and low-light operation. Except in extreme weather conditions the performance standards for these systems must be achieved at all times.

Systems must capture 98% of all VRM that are visible to the human eye and accurately read 95% of captured VRM unless deployed in a moving vehicle, when the system must capture 80% of all VRM that are visible to the human eye and accurately read 95% of captured VRM.

[3] The optimum configuration of CCTV systems differs when used for general CCTV surveillance to when operated as an ANPR reader. It needs to be configured for ANPR use to ensure maximum possible data accuracy

8.7.6. Covert Systems

It is recognised that circumstances may arise where moveable or purpose-built, covert systems are deployed in support of an investigation in circumstances where it is not possible to establish a live-link to the NAS. Deployments of this type that are authorised within provisions of the RIPA or RIPSA are the only circumstances where equipment procured after the publication of version 1 of NASP (May 2013) may not have the capability to live-link to the NAS.

Unless unachievable due the nature of the deployment or in extreme weather conditions, the performance standards for these systems must be achieved at all times. Systems must capture 98% of al VRM that are visible to the human eye and accurately read 95% of captured VRM.

8.8. Camera Access Settings

Unless a camera is designated a 'Restricted Access' camera, all cameras that submit data to NAS must be attributed the settings of 'Open Access', such that all data received from that camera is visible to all users with appropriate permissions to access the data.

With appropriate authority, a camera may be designated a 'Restricted Access' camera. Designation of a camera for 'Restricted Access' may only be authorised by a senior manager. A 'Restricted Access' camera may or may not be covert and the designation of a device for 'Restricted Access' may require authorisation within the provisions of the RIPA or RIPSA.

A record of all authorisations for restricted access must be retained for the duration of the restriction and a period of 2 years thereafter.

8.9. System Capability and Resilience

8.9.1. Image Capture

All cameras under the ownership or control of LEAs must have the capability to capture and record supporting imagery in accordance with section 7.4.5.

There may be circumstances where the shared collection equipment that is owned and managed by a non-LEA organisation is being used that are not enabled for the recording of imagery. In these circumstance, these cameras may be connected to the NAS subject to the standards for ANPR Infrastructure Development.

Supporting Images are important to assist with the accuracy of individual capture records and therefore, where data is received from other a non-LEA organisation without supporting images, provision for upgrading of the system to enable the provision of images should be established.

8.9.2. Schengen Information Systems (SIS)

All ANPR systems must be capable of reading plates that form part of the SCHENGEN community.

8.9.3. Data Storage

The NAS must not allow any data loss.

8.9.4. Local System Resilience

All local ANPR systems must transfer data to the NAS on receipt in local systems from a camera and also have the capacity to retain ANPR reads and their related images for a minimum of 3 and a maximum of 7 days from the time of the ANPR read.

This will provide resilience should the local infrastructure connections, the NAS or communications to the NAS become unavailable and will prevent the loss of data. In the event of a failure to send read records and associated images to the NAS local systems must have the capability to re-send that data.

If for any reason reads from a camera are submitted to the local system more than 7 days after initial capture the reads may be retained on the local system for 24 hours to prevent loss of data, should connection to the NAS become unavailable.

8.9.5. Local system connection and data transfer

Local ANPR systems must not enable connection to or the transfer of data to ANPR systems operated by other LEA for the purposes of searching of data or monitoring of VOI lists.

During the period of any loss of connection to NAS local functionality may provide for basic search of a full or partial VRM and for alerting against the most recent VOI lists received from NAS.

LEAs must not share VOI lists, even in circumstances of NAS unavailability; however, LEAs may share information and intelligence relating to those VOI lists using established intelligence management procedures.

8.9.6. Local system data deletion

Data held on local systems must be deleted within the next 24 hours after the period of 7 days following the time of the read. Where a read is submitted to the local components of NAC more than 7 days after the time of the read by a camera it may be retained for no more than 48 hours in local systems and then deleted within the subsequent 24 hours.

8.9.7. Extended unavailability of NAS

In the unlikely event that connections to the NAS are unavailable for more than 7 days, then deletion of data in accordance with the above provisions may be suspended until such time as connection is restored. This may only be done with specific authority of the controller for the LEA collecting the data and a full written record of the granting of that authority is required.

8.9.8. Mobile ANPR Systems Data Transfer

All ANPR data held on mobile ANPR units that have been unable to transmit their data in real time must be transferred to the NAS within a maximum period of 48 hours from the time of capture except in circumstances where the camera is unable to connect to the local system.

8.9.9. Support and Maintenance

ANPR systems should be commissioned only with an appropriate level of support and maintenance to safeguard against component failure and assist with business change. Local provisions must be in place to ensure that, in the event of any failure of a component of infrastructure that provides communications to the NAS, to prevent loss of data. Reinstatement must be within a period consistent with the ability to retain data locally for that failed component and subject to a maximum period of 72 hours from the time that the component failed.

8.10. System Connectivity

8.10.1. Local ANPR Infrastructure Connectivity to LEA networks

Local ANPR Infrastructure must connect to the LEA network infrastructure to allow user access to the NAS and to support connections to the Police National Computer (PNC) and the NAS.

The security of all infrastructure connections must be managed via an organisation maintained and managed firewall in accordance with that organisation's own policy and the Community Code of Connection and NPCC/Police Scotland Community Security Policy.

8.11. National Databases

NAS must have the capacity to check against the following national databases, as a minimum; PNC; Includes 'Fast Track' 'Extract', 'Schengen' and 'MMC' data.

8.11.1. Response Times

In order to ensure compliance with DPA principles in the circulation of VOI, Real-time matching performance standards must be achieved in 95% of all reads.

The following table summarises maximum response times within the NAC:

System Type	Read to alarm	Number plate read by a camera to delivery to NAS	NAS process to delivery at a LEA for visibility by staff
Static ANPR system	4 sec	2 sec	2 sec
Moveable ANPR system	4 sec	2 sec	2 sec
Multi-Lane ANPR System	4 sec	2 sec	2 sec
CCTV Integrated ANPR system	4 sec	2 sec	2 sec
Mobile ANPR system	6 sec	4 sec	2 sec

8.11.2. Real-Time Data Delivery

In order to ensure operational capability and to support compliance with DPA, local LEA ANPR infrastructure must clearly display the current state of connectivity to the NAS and/or any time when data is not being sent to the NAS. In the event of a communications or systems failure, the LEA infrastructure must buffer that read data and deliver it to the NAS once the communications or failed systems have been restored. The real-time delivery of data is a priority and the delivery of any buffered data should take place in addition to delivery of real-time data.

8.11.3. Search and Export of Data

The NAS must provide for the identification and export of data to enable identification using criteria defined in TSpec.:

The ability to export ANPR data shall be limited to defined users.

In appropriate circumstances a message may be sent to authorised users by means of SMS text. Where SMS is used the information provided will be limited to the VRM, time and location of the read and the name of the list containing the VOI.

Bulk data, including images, required for investigative purposes that is stored under provisions of the Criminal Procedure and Investigation Act 1996 (CPIA) may be exported to an external LEA defined storage area and managed in accordance with local policy.

The NAS must provide for user defined privileges for use of data export functions and data may only be exported by users with those privileges.

8.11.4. Security

The NAC must provide for adequate security measures, including access control, to protect against unauthorised access to the system and data held within it. LEAs must ensure compliance with NAC requirements and are accountable for the security of all components of the NAC that are within their control. LEAs must ensure that individual user privileges are consistent with the requirements of their role and individual level of vetting.

Audit trails must be maintained to record all significant actions taken, including:

- User login,
- Successful and failed database searches, and;
- the addition to, and deletion of data from lists of VOI.

There must be provision within the NAS for users to record the reasons and any required authorisation for their actions. Access to audit trails must also be auditable and restricted to users who require this access as part of their role, as defined within policy.

The security of all LEA components of the NAC must be managed via an LEA. The LEA shall maintain and manage a firewall in accordance with the LEA's own policy, the Community Code of Connection and Community Security Policy. The requirements of the national network connections and GSC as confirmed by the appropriate governance authority in each case.

8.12. Databases

8.12.1. National Database

LEAs that receive VOI lists and updates from a national VOI list shall ensure that this list is loaded on their mobile system at the first opportunity following receipt of that list or update.

8.12.2. Third Party Databases

Where data is provided by a third party (e.g. the MIDAS File as provided from the Motor Insurance database), then there must be measures/procedures to ensure that the data is handled consistent with these standards. The criteria that must be addressed through these procedures include:

- Provisions must be in place to ensure that only the most up-to-date data set is in use.
- Version control and file naming systems must be in place
- Distribution methods must be in accordance with GSC security requirements.

8.13. Lists of Vehicles of Interest

8.13.1. Vehicle of Interest List Purpose

Lists of Vehicles of Interest (VOI) may be maintained by LEAs to support intelligence development, operations and investigations. The contents of a list of VOI will depend upon the purpose of that list, the format for which is detailed in TSpec.

8.13.2. Vehicle of Interest List Information and Access Controls

VOI Lists used for monitoring purposes and that do not require an operational response may include the details defined within the Tspec. When a VOI List is used to support operational response, sufficient information to ensure an appropriate response must be included.

LEA may maintain a VOI list for operational response purposes; however, these lists should only be used in circumstances that do not meet the need to include the information on the PNC. Access permissions for those lists must be restricted to ensure that data access is proportionate in each case.

Special Categories of Data and Criminal Convictions Data as defined by Schedule 1 of the DPA and Articles 9.1 and 10 of GDPR should only be included within a VOI list when it is essential to the purpose of circulation. The LEA circulating the list must ensure that the content and provisions for the access to any such list are appropriate at all times.

8.13.3. Vehicle of Interest List Resilience

The NAS will make lists of VOI available to LEA in order that they can be loaded onto management servers and mobile systems should the live-link to NAS become unavailable.

LEAs must not load VOI lists received from NAS onto any other systems and must establish procedures to ensure that VOI lists loaded onto the management server or mobile systems are current versions of those lists.

8.13.4. Actions required for a Vehicle of Interest List

Any LEA publishing a list of VOI onto NAS will determine access controls for that list. Lists will only be accessible to LEAs where it is proportionate for that accessibility. Where one LEA subscribes to the VOI Lists of another LEA, there is an obligation to monitor the list, assess a 'hit' against the list and respond subject to local resource availability and operational demands.

Logs of the loading of any VOI list onto a mobile system shall be maintained as required by Section 9.10.

8.13.5. Vehicle of Interest List Accuracy

The LEA supplying a VOI list to the NAS must ensure that information within the list is accurate, of current relevance, and is in a format that conforms to the requirements detailed within TSpec. All lists that are supplied must be reviewed on a regular basis by the LEA supplying the list.

8.13.6. Vehicle of Interest List Deletion

A list that is received from an LEA will be deleted from the NAS no later than 28 days after the last date of revision by the LEA that supplied the list.

8.13.7. Vehicle of Interest List Extraction

LEAs will not extract data from a list of VOI for the purposes of creating a composite list from a number of such lists, to be held outside the NAS.

8.14. Performance Evaluation

Performance testing must be consistent with current guidance provided by the Defence Science and Technology Laboratory (DSTL). (DSTL Guidance)

8.14.1. Installation of ANPR Infrastructure

Unless the exceptions for covert systems apply, on installation of any component of ANPR Infrastructure compliance with performance standards detailed within NASPLE must be confirmed and recorded.

Compliance with performance standards is required for both initial installation or on re-installation or re-deployment of any ANPR camera or other component.

8.14.2. Capture Rate Assessment

Any assessment of ‘capture’ rate must be based on not less than 250 consecutive vehicles (or a minimum period of 2 hours) displaying a VRM visible to the human eye passing within the field of view for a camera and in the case of a multi-lane system this applies to each lane covered by that system.

8.14.3. READ Rate Assessment

The READ rate for each type of system must be determined for not less than 250 consecutive ‘captured’ Vehicles displaying a VRM visible to the human eye.

Performance must be assessed for daylight and night time conditions. It is advisable to assess for a range of conditions including; bright daylight (dawn); bright daylight (dusk); overcast daylight and night time.

8.14.4. Performance Evaluation Schedules

The performance of all ANPR systems must be regularly reviewed to ensure conformance with the data standards defined in this document. NAS functionality should be used to monitor continued compliance with required 'capture' rates.

Compliance with the READ rate for a camera should be reviewed at least annually with a sample of not less than 250 consecutive reads. Provisions for performance evaluation must be defined in LEA policy and procedures.

In addition to the annual assessments, the performance standards for all cameras that do not have the capability to provide supporting imagery must be evaluated at no less than 6 monthly intervals. Assessments for this additional assessment shall include a sample of east 50 vehicles passing consecutively within the field of view.

8.14.5. Performance Evaluation of Covert Cameras

Where covert installation of ANPR infrastructure has been authorised within the provisions of RIPA or RIPSA, and the purpose of the installation may be compromised as a result of testing, the testing need not be completed.

8.14.6. Performance Evaluation Logs

A log for all performance evaluation activities must be retained in a form to enable the record of reviews for each component within ANPR systems to be identified and retrieved when required.

9. Part 3: Data Access and Management Standards

9.1. Data Access and Management Standards Overview

Part 3 prescribes the standards required for access to and management of ANPR data within the NAS.

The obligations that arise under the DPA are different depending on the reason for processing of data. It is the responsibility of the controller for the LEA that is processing the data to ensure compliance with relevant parts of the DPA in each case.

9.2. Data Management

9.2.1. Policy

All LEAs that connect to, or have access to, the NAS must have an up to date written policy in place for the access, management and use of ANPR data, including provisions for audit, which must be consistent with Compliance and Audit Standards.

Access to ANPR data must be proportionate to the circumstances of that access and taking account of the impact on the fundamental rights and freedoms of individuals.

9.2.2. Data Access Management

Authorised members of LEAs may access and use data within the NAS to the extent that is compliant with the DPA in the circumstances of each case, without reference to a controller unless otherwise required within the terms of NASPLE.

9.2.3. Shared Collection Equipment

9.2.3.1. Data provision by non-LEAs

NAS may receive data via an LEA from ANPR systems not directly within the control of the LEA in circumstances where it is using shared collection equipment that is owned and managed by a non-LEA organisation.

In these circumstances, the controller for the LEA that initially receives the data and the organisation owning the collection equipment are both controllers who will store data in separate databases that they manage independently. LEA controllers for data received under any such arrangement may manage the data and allow access to the data without reference to the owner, or any other user of the shared collection equipment.

9.2.3.2. Data received directly into NAS

NAS may receive data directly from ANPR systems not within the control of an LEA in circumstances where data is submitted to the NAS using shared collection equipment that is owned and managed by a non-LEA organisation, without the data first being received by a LEA.

The NPCC policing lead for ANPR as controller for data received under any such arrangement may manage the data and allow access to the data without reference to the owner, or any other user, of the shared collection equipment

9.2.3.3. Management of data provided by non-LEAs

In circumstances where a non-LEA has provided data to the NAS, the NPCC policing lead for ANPR and the organisation owning the collection equipment are both controllers who will store data in separate databases that they manage independently.

The NPCC policing lead for ANPR as controller for data received under any such arrangement may manage the data and allow access to the data without reference to the owner, or any other user, of the shared collection equipment.

9.2.3.4. Compliance Agreement

The LEA that receives data from a non-LEA organisation for submission into NAS, or the NPCC policing lead for ANPR in respect of data submitted directly to NAS, must ensure that a formal written-agreement is in place with the owner of the camera and other components of the ANPR infrastructure detailing appropriate arrangements to enable compliance with NASPLE.

9.2.4. Data Extraction from NAS

Where an LEA accesses data within the NAS they are controller for any data extracted from the NAS as a result of that access. Management of all data that is extracted must be in accordance with the provisions within NASPLE and any reports or other documents that include data from NAS must be marked in accordance with the requirements of the Government Security Classifications (GSC). Personal data must only be processed in accordance with the DPA.

9.3. Organisational and User Access to ANPR Data

9.3.1. ANPR Password Policy

Password requirements for access to NAS is based on national Cyber Security Centre guidelines and is applicable to all roles within LEA, third party contractors and suppliers and staff responsible for NAS service management.

Staff will be allocated individual accounts that may only be accessed using a password in a format approved by the national Accreditor to requirements detailed in Appendix A

9.3.2. ANPR Account Management

Staff who are approved to access NAS as both a user and for administrative purposes must be allocated separate accounts such that these functions cannot be achieved using a single log in account. Accounts must be reviewed, suspended or terminated in the following circumstances:

- An account must be suspended if it is not accessed for a period of 90 days. The need for access must be reviewed within the subsequent 7 days. The account may then be reactivated or deleted as appropriate,
- Access permissions must be reviewed within 7 days of a person changing role within an LEA.
- An account must be terminated within a maximum of 48 hours of a person leaving an LEA or partner agency.

9.3.3. Provisions for Data access

Any access to data must be for national security, counter terrorism, investigation and enforcement purposes as defined in Annex B or for the purpose of audit.

Staff within an LEA may be granted access to the extent relevant to their role, in accordance with local LEA policy in an LEA. LEA policy must be consistent with the purposes and standards within this document and the specific requirements at Annex C.

9.3.4. Data Access provision when NAS is unavailable

Data held within the local components of the NAC (Section 8.9) may only be accessed by authorised staff in circumstances where the NAS or communications to the NAS have become unavailable.

9.3.5. Vetting Requirements for access to ANPR data

Staff accessing the NAC are required to have successfully completed vetting to the standards as detailed below unless in exceptional circumstances with express written approval of the NPCC Policing lead for ANPR, as lead controller, approves any vetting process as equivalent to the required standard.

9.3.5.1. Police

Staff within a police service LEA authorised to access ANPR data must have successfully completed Recruitment Vetting (RV) to NPCC vetting standards.

9.3.5.2. Non - Police LEA

Staff within an Approved Organisation that is a non-police LEA authorised to access ANPR data must have current vetting clearance to national non-police personnel vetting (NPPV) Level 2.

9.3.5.3. Partner Agencies

Controllers may allow access to non-police staff in partner agency (e.g. local authority controllers) subject to have them having current vetting clearance to NPPV Level 2, to the extent necessary for their role.

9.3.5.4. Police Service Administration, Monitoring and Audit

Police LEA staff conducting activity in respect of administration, monitoring and audit of the NAS will have a current security clearance to SC level and NPPV to Management Vetting standard.

9.3.5.5. Non-Police LEA Administration, Monitoring and Audit

Non-police LEA staff conducting activity in respect of administration; monitoring and audit of the NAS will have a current security clearance to SC level and NPPV Level 3.

9.3.5.6. National Audit

Staff appointed to any National Audit role must have a minimum current security clearance to Developed Vetting (DV) level and NPPV Level 3.

9.3.5.7. National Administration and Processor Companies

Staff within NAS supplier companies or the Home Office that have access to the NAS for management or administrative purposes will have a current security clearance to SC level and NPPV Level 3.

9.3.6. Authorisation Requirements for access to NAS Data

Where an authorisation for access is required, staff providing that authorisation must ensure that access is proportionate in each case taking account of the DPA and associated principles and that access is in the interest of justice.

9.3.6.1. Authorisation of Staff Access

Each LEA will designate a senior manager who is accountable for the authorisation of staff who may access ANPR data.

9.3.6.2. Role Based Access and Training

Personnel will only be granted access to ANPR data to an extent that is necessary and proportionate to their role. LEAs must ensure that authorised staffs have

completed any required training and are fully aware of the provisions within NASPLE. Authorised staff will have individual access accounts and permissions.

9.3.6.3. Records of Authorised Staff

LEAs will maintain a list of authorised staff and ensure that a persons' authorisation is revised or cancelled as appropriate when they change role or leave the organisation.

9.4. Disclosure and Evidential Use of Data

Data held within or obtained from the NAS may not be used or disclosed for any purposes except those as authorised within NASPLE.

9.4.1. Disclosure schedules

Where ANPR data obtained is retained as material within the meaning of the CPIA (or similar procedures in Scotland), in preparation of disclosure schedules, information relating to ANPR methodology, tactics and camera locations will be recorded on the Schedule of Sensitive Material and may be disclosed to prosecution authorities.

9.4.2. Restrictions on personnel in disclosure of ANPR and in production of evidential materials

Statements of evidence in respect of data within the NAS may only be provided by staff authorised within LEAs to provide ANPR evidence with current access permissions within NAS for that purpose. Subject to the following authorised staff may provide a statement of evidence for any data held within the NAS.

9.4.3. Provisions to safeguard the location of ANPR infrastructure

The order to safeguard the national ANPR infrastructure, apart from data obtained from a Mobile ANPR system, the precise location for an ANPR read obtained from a camera will not be disclosed during an investigation, nor included in evidence unless the controller with responsibility for the camera that recorded the data has been consulted and provided written consent for that disclosure or for evidence to be provided. The following principles apply:

9.4.3.1. Evidential Use of Data

Evidence of an ANPR read will only be included where it is of specific relevance to an investigation and is of material value to any judicial proceedings.

9.4.3.2. Disclosing of Camera Locations in Evidence

Apart from data obtained from a Mobile ANPR system the production of a map or otherwise disclosing the precise location of the camera that recorded an ANPR read is not permitted during any stage of an investigative or prosecution process, unless

specifically authorised by the data controller for the LEA with responsibility for the camera that recorded that data.

9.4.3.3. Information to be included in evidential disclosure

The location of a read will be described in the following decreasing order of preference;

1. The general area of the location (e.g. Town, District, Metropolitan Borough)
2. The postcode (following consultation with the controller with responsibility for the camera that recorded the data, in circumstances where this will identify the precise location of the camera)
3. The name of the road (following consultation with the controller with responsibility for the camera that recorded the data, in circumstances where this will identify the precise location of the camera)
4. The precise location (following consultation with the controller with responsibility for the camera that recorded the data)

9.4.3.4. Disclosure of ANPR data for non-evidential purposes

Unless permitted within section 9.6 of this document, core ANPR read data and any supporting imagery as defined by section 7.4.5., is not to be transferred to other systems, nor disclosed to any third party, including staff from an organisation that is not listed at Annex A, Data may only be disclosed to the data subject in accordance with procedures for dealing with FOI and DPA enquiries in accordance with section 9.12. Data may be shared with an organisation that is not listed at Annex A with the express written authority of the controller with responsibility for the camera that recorded that data.

9.4.3.5. Disclosure to non-Approved Organisations

Where an LEA has an active role in collaboration with another LEA which is not listed at Annex A in the conduct of an investigation, and circumstances consistent with the provisions of Schedule 2 DPA apply, the results of a search of ANPR data may be disclosed to that other LEA with a requirement that it is not further disclosed without the express written authority of the controller for the 'Approved Organisation' collaborating in the investigation.

9.4.3.6. Controller Representations re Disclosure of Camera Locations

In addition to the above, the controller that owns or controls the camera that captures 'read' data will be provided with a specific opportunity to make representation to any court that is to consider an order for information to be disclosed regarding the location of a camera.

9.4.3.7. Recording of Disclosure

In all circumstances where data is disclosed a record must be maintained to include the identity of those disclosing and receiving the data and the reason for and any authorisation of that disclosure.

9.5. Retention and Deletion

9.5.1. Record Retention and Deletion

ANPR READ records must be deleted 12 months[4] after their initial capture, unless retained under provisions of CPIA or similar provisions in Scotland. Retained data may only be accessed in connection with the investigation subject to that retention after a period of 12 months following initial capture.

Records may also be retained for longer than 12 months following a review that identifies a continuing policing purpose for those items of data under provisions of MOPI. These records must be retained and managed in accordance with those provisions. LEAs must establish procedures for the management and review of any data held under these provisions including arrangements for deletion as required.

9.6. Storage of ANPR Data otherwise than in NAS

Data must not be stored outside the NAS except where held in buffer storage in accordance with section 8.9.5 unless for the purpose of retention in accordance with section 9.5.1 or in accordance with section 9.8 below where those requirements cannot be met within the NAS, or it has been extracted as a result of a court order or other lawful authority for the provision of the data.

9.7. Record Amendment

Records that are identified as incorrect for any reason must either be corrected or deleted at the time that they are found to be incorrect.

9.8. Record Deletion from Third Party Systems

ANPR data must be deleted from any computer-based system within 7 days of entry of that data, where an LEA has established any link between the NAS and any other computer-based system for the purposes of:

- Monitoring and the initiation of an operational response to any hit against a list of vehicles of interest or

[4] Read metadata is deleted on day 366 after initial capture. Associated images are deleted the following day. Data may only be accessed up to 12 months after initial capture (Annex C) unless in circumstances of 9.5.1 above.

- More advanced research and analysis purposes in relation to an investigation.
- Entries are included in command and control records

An exception exists for deletion after 7 days when a review has been conducted of the data that it is proposed to be retained which has identified the items of data where a continued policing purpose remains that can only be satisfied by the continued processing of the data within the system external to the NAS.

In this case provisions of MOPI (or similar provisions in Scotland) apply and the relevant items of data may be retained and managed in accordance with those provisions; or

An exception also exists for deletion after 7 days when a review has been conducted into the data that it is proposed to be retained which has confirmed that the items of data are relevant to an investigation. In this case the relevant items of data may be retained, managed and deleted in accordance with the requirements of CPIA.

9.9. Transfer to local systems for basic user access

Data may not be transferred to any local systems external to those required for connection to NAS facilitate basic user access to ANPR data.

9.10. Records of Data Processing, Access and Disclosure

9.10.1. NAS Logging

A log of all automated processing operations will be maintained within NAS to include records of access by administrators and authorised users, data capture, alterations and any search of data or records within NAS. Logs of administrator or user access must include details of the identity of the user together with the justification, date and time of that access and a record of any authorisation relevant to that access.

9.10.2. Mobile Systems Logging

A log recording the details of all lists of VOI that have been loaded onto mobile systems as authorised by section 8.9.8 will be maintained by the LEA that loaded the log onto the mobile systems.

9.10.3. Logging of Access on systems external to NAS

In addition, LEAs are required to maintain a record of any access by their staff to ANPR data, in any external system, to include records of access by administrators and authorised users, data capture, alterations and any search of data or records within NAS. Logs of administrator or user access must include details of the identity of the user together with the justification, date and time of that access and a record of any authorisation relevant to that access in a readily retrievable form.

9.10.4. Logging of Escalation of Investigation Category

LEAs are required to maintain a record of any escalation of an investigation to the category 'Major Investigation' or 'Serious Investigation', including details of the reason for escalation, in a readily retrievable form.

9.10.5. Logging of data Disclosures

Unless disclosure is in accordance with the provisions of the CPIA or similar provisions in Scotland, LEAs will maintain records of all disclosure of ANPR data including the justification, data and time of the disclosure, the identity of the person disclosing the data and the identity of the recipient of the data.

9.10.6. Use of Logs in Disciplinary Proceedings

Logs within NAS and those recorded by an LEA may be used for the purposes of self-monitoring by the controller or the processor, the conduct of internal disciplinary proceedings, in ensuring the integrity and security of personal data and for the purposes of criminal proceedings.

9.10.7. Disclosure of Logs to ICO, SCC and Home Office

Records within NAS and any local records must be made available to the Information Commissioner, the Surveillance Camera Commissioner and the Home Office on request for audit and monitoring purposes.

9.11. Management and Audit of NAS

Audit must be conducted in accordance with National Standards for Compliance and Audit of Law Enforcement ANPR by staff with appropriate security clearance.

LEAs will support all controllers for NAS in the audit and management of NAS.

LEAs will support the national auditor in the monitoring and audit of access to the NAS and will provide relevant information on request.

LEAs will audit the access to NAS by their staff in accordance with Audit Standards and maintain a record of all audits that are undertaken. Details of such audits will be made available to the Information Commissioner, the Surveillance Camera Commissioner and the national auditors on request.

9.12. Freedom of Information Act and Data Protection Act Enquiries

All requests for Information regarding the NAS made to a public authority under the provisions of the Freedom of Information Act 2000 (FOI) will be referred to the relevant controller for consideration and will be managed according to the JCA.

All requests in relation to data held on NAS, made under provision of the DPA, will be referred to the controller for consideration and will be managed according to the

JCA. This includes any subject access requests and requests for erasure or restriction on processing.

Annex A: Approved Organisations

List of Approved Organisations
Avon and Somerset Constabulary
Bedfordshire Police
Border Force
British Transport Police
Cambridgeshire Constabulary
Cheshire Constabulary
City of London Police
Civil Nuclear Constabulary
Cleveland Police
Cumbria Constabulary
Department for Work and Pensions (DWP)
Derbyshire Constabulary
Devon and Cornwall Constabulary
Dorset Police
Driver and Vehicle Licensing Agency (DVLA)
Driver and Vehicle Standards Agency (DVSA)
Durham Constabulary
Dyfed-Powys Police
Environment Agency
Essex Police
Food Standards Agency
Gangmasters and Labour Abuse Authority
Gloucestershire Constabulary
Greater Manchester Police
Gwent Police
Hampshire Constabulary
Hertfordshire Constabulary
H M Revenue & Customs (HMRC)
Humberside Police
Immigration Enforcement
Intelligence Services
Kent Police

Lancashire Constabulary
Leicestershire Constabulary
Lincolnshire Police
Medicines and Healthcare Products Regulatory Agency (MHRA)
Merseyside Police
Metropolitan Police Service
Ministry of Defence Police
National Crime Agency (NCA)
NAFN Data and Intelligence Services facilitating Local Authority Trading Standards investigations
National Vehicle Crime Intelligence Service (NaVCIS)
Norfolk Constabulary
North Wales Police
North Yorkshire Police
Northamptonshire Police
Northumbria Police
Nottinghamshire Police
Police Service of Scotland
Police Service of Northern Ireland (PSNI)
Royal Air Force Police
Royal Military Police
Royal Navy Police
South Wales Police
South Yorkshire Police
Staffordshire Police
Suffolk Constabulary
Surrey Police
Sussex Police
Thames Valley Police
Thurrock National Investigation Service
Warwickshire Police
West Mercia Constabulary
West Midlands Police
West Yorkshire Police
Wiltshire Police

Annex B: Investigation Categories

Investigations within LEAs fall within three main categories, so that there is a consistency of understanding within LEAs as to which investigations should be included within each category. The main categories are:

- Major Investigations
- Serious Investigations
- Priority and Volume Investigations

A consideration of the category of the investigation informs effective management and decision making, including the scope for an investigation and determination of the resources that are to be deployed. These categories provide the framework to support a national policy for retention of, and access to ANPR data. The categorisation of an investigation should be determined taking account of the circumstances in each case, using the below framework as a guide.

Major Investigations

A key characteristic is that Major Investigations should be normally be led by a Nationally Registered Senior Investigating Officer (SIO) within a police force or similarly senior investigator in non-police LEAs.

Designated Major Investigations

Major Investigation Types
Murder
Attempted Murder
Manslaughter
Infanticide
Child Destruction
Kidnapping

Terrorist related crimes

Serious Investigations

Designated Serious Investigations

Serious Investigation Types
Arson
Abduction
Aggravated Burglary dwelling and non-dwelling
Arson High Value or life endangered
Blackmail
Drug Trafficking
Death by Dangerous Driving
Female Genital Mutilation
Fraud and Associated Offences (80hrs + investigation time)
Gross Indecency Child
Perverting Justice
Public order (racially motivated)
Rape
Robbery (Firearms or ABH or more serious injury caused)
Sexual Assault (children under 13)
Threats to Kill
Vulnerable Missing Person

Wounding (S18/20)
Response to incidents of significant public interest / public safety/ public security

Serious Investigation Escalation

Serious Investigations may, with the authority of a senior manager[5] be escalated to the category of Major Investigations.

Investigations that have been escalated to serious from the category of Priority and Volume Investigations may not be further escalated to the category of major Investigation.

Any authority to escalate to the higher category together with the reasons for the grant of that authority must be recorded. Any authority to escalate will take account of the following factors:

Serious Investigation Escalation Factors

Consideration	Examples
Community factors	• Likely to escalate into large scale disorder or critical incident • Has escalated from a previous offence • Sensitivity regarding individuals involved
Offence characteristics	• Aggravating factors of the offence • Vulnerability of victims/witnesses, • Has crossed force or national boundaries • Forms a previously undetected series

[5] an officer of at least superintendent rank in the police or the equivalent level of seniority in a non-police organisation

Offender Characteristics	• Organised crime • Terrorism links • Resistance to police operational strategies • Multiple offenders

Priority and Volume Investigations

Investigations not included within the above categories will be considered as within the remit of Priority and Volume Investigations. This will include investigations into street robbery, burglary and vehicle-related criminality and non-crime issues such as anti-social behaviour, vehicle excise enforcement, road traffic offences, safeguarding and missing persons.

Priority and Volume Investigations may with the authority of manager[6], be escalated to the category of Serious Investigations.

Any authority to escalate to the higher category together with the reasons for the grant of that authority must be recorded and will take account of the following factors:

Priority and Volume Investigations Escalation Factors

Consideration	Examples
Community	• **High risk of critical incident** • **Sensitivity regarding individuals involved**

[6] an officer of at least Inspector rank in the police or the equivalent level of seniority in a non-police organisation

Offence Characteristics	• Aggravating factors of the offence such as: • Hate crime • Weapons used • Injuries sustained • Vulnerability of victims/witnesses, • Priority issue identified within NIM business process. • Series of offences e.g. forensic links to the offender(s) • Complexity of the Investigation
Offender Characteristics	• Criminal history • Resistance to investigative strategies • Prolific offender • Multiple offenders

Annex C: Data Access Requirements

Age of data to be accessed (as required)	Purpose of access to data
	To monitor alarms or receive reports from matches against a list of Vehicles of Interest (VOI) from a NRD for operational response or intelligence purposes.
Real or near real time during the course of monitoring	By any member of staff authorised to access ANPR systems with no additional authority required.
	To research data for 'Priority and Volume Investigation' purposes.
Up to 90 days	By any member of staff in accordance with their authorisation to access ANPR systems.
Over 90 days	By any member of staff in accordance with their authorisation to access ANPR systems with written authority of an Inspector or equivalent staff grade; a) where there has been a significant delay in reporting the offence to be investigated, or; b) new information or evidence has become available, or; c) the investigation is being conducted diligently and expeditiously and is not yet completed.
	To research data for 'Serious Investigation' purposes.
Up to 1 year	By any member of staff in accordance with their authorisation to access ANPR systems.

	To research data for 'National Security', 'Counter Terrorism' or other 'Major Investigation' purposes.
Up to 1 year	By any member of staff in accordance with their authorisation to access ANPR systems.
	To prepare evidential material for information revealed during a previous search of ANPR data.
	By any member of staff in accordance with their authorisation to access ANPR systems with no additional authority required.
	To comply with a written request from the Crown Prosecution Service, the procurator fiscal or on the direction of a court.
	By any member of staff in accordance with their authorisation to access ANPR systems with no additional authority required.
	To research data as part of an investigation into alleged breach of the policing Code of Ethics
	By any member of staff in accordance with their authorisation to access ANPR systems with written authority of a superintendent or equivalent staff grade.

Appendix A: Password Requirements

Password Requirements

Introduction

Purpose

1. The security of NAS requires that users generate an appropriately complex password to protect the National ANPR Capability (NAC) and its data from unauthorised access. The NAS utilises a username and password-based identity and access control for all front-end users.
2. The NAS Password Policy is a procedural part of the information security measures intended to:
    - Protect the Confidentiality, Integrity and Availability of the NAC.
    - Preserve the privacy of all the data and information stored within the NAC environment, ensuring only authorised users are permitted access on a need to know basis.

Procedures

The Purpose of Passwords

3. Passwords are an essential security control to authenticate users and confirm identity and access rights. Passwords protect access to the ANPR data and information in conjunction with the physical and procedural measures of a secure site.
4. Visual recognition of people within a work area, and Photographic ID Cards for sites and buildings, are also an important security layer to protect the NAC.

Limitations

5. The security provided by a password system requires the passwords are known only to the user of the account to which it relates. Thus, a password is vulnerable to compromise whenever it is stored or written down. A user must not disclose their password to anyone including other users and administrators.

Password Requirements

Password creation requirements:

6. Passwords **must** be a minimum length of 8 characters with at least 2 non-alphanumeric characters (e.g. % & ?);
7. Passwords **must not** be stored in any insecure form, users must **disable** password saving in web browsers;
8. Passwords **must not** be based on the following:
   - Months of the year, days of the week or any aspect of dates with which they are personally associated (e.g. birthdays, anniversaries);
   - Family names, initials or car registration numbers;
   - Organisation names, identifiers or references;
9. Good quality passwords should:
   - Not be the same as any of the previous 10 passwords (this will be enforced via the operating system or security solution within NAC);
   - Be unique and only used within the NAC;
10. Password must be changed on suspicion of compromise;
11. Password creation requirements are common for all types of NAC access. If a user has more than one account. For example, a user administrator and system administrator account, different passwords are required for each account;

Expiry terms and Account Lockout

	No of Attempts	*Password expiry*
User/ Role	5	1yr

12. If a user has attempted to log in **5 times** unsuccessfully their account will be:

    a. **Locked out** and **ONLY** unlocked via two alternative processes for use depending upon the business processes of the LEA:
       i. Notify the local User Administrator or,
       ii. Notify the local LEA IT Service Desk.

Forgotten Password Process

13. If a user has forgotten password, A **"I forgot my password"** link is provided on the NAS logon homepage. The system will email a new temporary password to the email address associated with the NAS user account. This temporary password **must** be immediately changed upon first successful login. This will not circumvent the lockout procedure described above.



© Crown copyright 2020

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at www.gov.uk/government/publications and www.npcc.police.uk/anpr

Any enquiries regarding this publication should be sent to us at anpr@homeoffice.gov.uk .

GOV.UK

1. Home (https://www.gov.uk/)
2. Crime, justice and law (https://www.gov.uk/crime-justice-and-law)
3. National ANPR standards (https://www.gov.uk/government/publications/national-anpr-standards)

- Home Office (https://www.gov.uk/government/organisations/home-office)

Guidance

National standards for compliance and audit of law enforcement ANPR - September 2020 (accessible version)

Updated 19 November 2020

Contents

1. Purpose of Compliance and Audit
2. Applicability
3. Audit Governance and Roles
4. Data Standards Audit
5. Infrastructure Standards Audit
6. LEA Local System Audit
7. Vehicle of Interest (VOI) lists Audit
8. Data Access and Management Standards Audit
9. Glossary of Terms, Abbreviations and Definitions
10. Document revisions

Print this page

© Crown copyright 2020

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 (https://www.nationalarchives.gov.uk/doc/open-government-licence/version/3) or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at https://www.gov.uk/government/publications/national-anpr-standards/national-standards-for-compliance-and-audit-of-law-enforcement-anpr-july-2019

1. Purpose of Compliance and Audit

Consistent management of NAS is essential to ensure that data is accurate and to maximise the benefits for law enforcement purposes. Public confidence in the system is essential and robust standards with clear records of compliance with those standards is importance to ensure support for ANPR systems is maintained.

Audit is one part of a larger suite of security controls and measures which includes, governance, physical, personnel, technical and procedural controls. The NAS is designed to provide a security regime that supports and compliments the business and technical needs. It is important that business audit standards, policy and governance are also in place which requires a robust compliance audit regime to be in place.

2. Applicability

These Audit Standards apply to national law enforcement ANPR capability (NAC) operated by the police and other law enforcement agencies (hereinafter called LEA), throughout the UK, that connect to or receive data from the National ANPR Service (NAS).

Audit is conducted with reference to National Standards for Policing and Law Enforcement (NASPLE)

LEAs must ensure compliance by their agency with the requirements of all parts of NASPLE.

3. Audit Governance and Roles

The National Strategic lead as lead controller must ensure that audit standards are in place to provide for effective governance of NAS taking account of threats and risks.

Staff conducting audits must have current security clearance to levels as detailed in NASPLE Part 3.

Staff with user access permissions to NAS may not conduct audits.

LEA must ensure that audit of any access to NAS using administrative permissions is conducted by staff who do not themselves have administrative responsibility for NAS.

3.1 Governance model

The below governance model is in place for NAS:

The National ANPR Strategy Board supports the NPCC Strategic Lead.

The National ANPR Advisory Board advises the NPCC Strategic Lead.

The NAS Service Management reports to the NPCC Strategic Lead.

The National Accreditor reports to the NPCC Strategic Lead.

The National Auditor reports to the NPCC Strategic Lead.

The National Accreditor advises the Security and Data Management within Strategic Board.

The National Auditor advises the Security and Data Management within Strategic Board. 4796

The Security and Data Management within Strategic Board advises the NAS Service Management.

The National Auditor audits the activity of National System Providers and the National Administrator.

The National Auditor monitors the activity of local auditors.

The Service Desk oversees the National System Providers.

The National Administrator supports and advises the Local Administrators.

Local Auditors audit users.

4. Data Standards Audit

Accurate data is essential to ensure legislative compliance and to enable the benefits that can be obtained from ANPR to be optimised. The following elements of NASPLE Part 1 are included for audit.

4.1 Data Security

Every 6 months LEA to review a sample of reports that have been obtained by that LEA from NAS for compliance with the requirements of the Government Security.

Classification Policy (GSCP) requirements for OFFICIAL – SENSITIVE data. (NAS configuration should ensure that all reports are appropriately marked).

4.2 Time

LEAs must record evidence of the accuracy of time recording for all camera that submit data to their management server. Records confirmation of time accuracy must be reviewed at Least once every 7 days. A record of review and any maintenance conducted as a result of the review must be retained for a period of 2 years following the review.

4.3 Location

The accuracy of the recording of location for a read record from all camera with the exception of mobile camera must be confirmed on installation and thereafter reviewed at Least once every 6 months by the LEA manging that camera. A record of all reviews and any maintenance conducted as a result of the review must be retained for a period of 2 years following the review.

4.4 Reporting of Data Standards

Every 12 months LEA must provide the national auditor with a report to include details of the number of cameras operated by the LEA, the number tested during the preceding 12 months, information of the accuracy for recording time and location for each camera tested and details of any maintenance conducted following testing.

5. Infrastructure Standards Audit

5.1 ANPR Infrastructure Development

Compliance with NASPLE Part 2 is important to ensure that ANPR systems are developed and maintained in conformance with relevant legislation and that the benefits that can be obtained from the NAS are optimised. The following elements of NASPLE Part 2 are included for audit.

5.2 Static ANPR Systems

Evidence that the need for deployment is consistent with NASPLE Section 8.6 and performance consistent with NASPLE Section 8.7 on installation and that this has been monitored for each camera and that an annual review for deployment of each camera has been conducted. Evidence of performance evaluation as required by NASPLE Section 8.14 LEAs to retain records of all reviews for a period of 2 years.

5.3 Moveable ANPR Systems

Evidence that the need for deployment is consistent with NASPLE Section 8.6 and performance consistent with NASPLE Section 8.7 on installation and that this has been monitored for each camera. Evidence of performance evaluation as required by NASPLE Section 8.14. LEAs to retain records of all reviews for a period of 2 years.

5.4 Multi Lane ANPR Systems

Evidence that the need for deployment is consistent with NASPLE Section 8.6 and performance consistent with NASPLE Section 8.7 on installation and that this has been monitored for each camera and that an annual review for deployment of each camera has been conducted. Evidence of performance evaluation as required by NASPLE Section 8.14. LEAs to retain records of all reviews for a period of 2 years.

5.5 CCTV Integrated ANPR Systems

Evidence that the need for deployment is consistent with NASPLE Section 8.6 and performance consistent with NASPLE Section 8.7 on installation and that this has been monitored for each camera and that an annual review for deployment of each camera has been conducted. Evidence of performance evaluation as required by NASPLE Section 8.14. LEAs to retain records of all reviews for a period of 2 years.

5.6 Mobile ANPR Systems

Evidence that the need for deployment is consistent with NASPLE Section 8.6 and performance consistent with NASPLE Section 8.7. Evidence of performance evaluation as required by NASPLE Section 8.14. LEAs to retain records of all reviews for a period of 2 years.

5.7 Covert Systems

Audit of deployments of ANPR systems authorised within provisions of the Regulation of Investigatory Powers Act 2000 (RIPA) or the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) to be completed in accordance with arrangements for compliance and review of RIPA and RIPSA deployments as appropriate.

6. LEA Local System Audit

6.1 Local Systems

Audit of local data storage to be completed by the LEA every 6 months to confirm that the period of retention is consistent with NASPLE Part 2 and that data is not transferred or used in other systems except as authorised by NASPLE.

6.2 Mobile Systems Data Transfer

Review of records for transfer of data from Mobile ANPR Systems to be completed by the LEA every 7 days to confirm compliance with NASPLE Part 2. LEAs to retain records of all reviews for a period of 2 years.

6.3 Support and Maintenance

Records for failure of any component of infrastructure to be reviewed by the LEA every 7 days to support compliance with requirements for reinstatement of capability as detailed in NASPLE section 8.14.

7. Vehicle of Interest (VOI) lists Audit

Compliance with the requirement for deletion of lists from NAS 28 days after the latest date of revision to be reviewed by the LEA every 14 days.

Lists held on Mobile ANPR Systems to be reviewed by the LEA at Least once every 7 days to ensure that they remain the current version of any VOI list.

LEA to maintain a record for the review of all VOI lists and retain those records for a period of 2 years.

8. Data Access and Management Standards Audit

8.1 Policy

Annually, the local auditor to confirm that a current written policy is in place in accordance with NASPLE Part 3.

8.2 Audit of provisions for Data Access

The identity of the senior manager as required by NASPLE Section 9.3.6.1 to be confirmed by the local auditor annually

Evidence of the management of staff authorisations and permissions to be audited by the LEA for compliance with authorisation and removal procedures to include:

- annually 5% of all new staff authorisations that have been approved during the previous 12 months
- annually review a sample of staff authorisations where the privileges have changed during the previous 12 months
- all staff who have not accessed NAS for a period of 90 days within the 14 days immediately following the expiry of that period
- all accounts for staff that have left the LEA within 48 hours of them leaving an LEA to ensure that access permissions have been ceased

4799

- annually all staff with administrative access to ensure that this remains appropriate and is not combined with user access permissions
- monthly to review records for all failed ‘log on’ attempts. A record of all reviews conducted to be retained for a period of 2 years

LEA audit to be conducted every 6 months to confirm the deletion of data in accordance with NASPLE with an annual review of 5% of all cases where data is retained beyond standard deletion times to ensure continued retention remains appropriate, both for NAS and other systems.

LEA to audit of instances of data access to ensure access is appropriate within terms of NASPLE with reference to the justification and authority where required as follows:

- LEAs must establish provisions for audit of ANPR data where the period for the search includes data that entered the NAS 90 days or less prior to the search, that is proportionate in each case taking account of their assessment of the potential risk of non-compliance with NASPLE and for the misuse of data. The audit to be completed quarterly[footnote 1]
- to audit 5% of searches across a sample covering 30 consecutive days since the previous audit where those searches cover data that was captured more than 90 days prior to the date of search. The audit to be completed quarterly
- all instances of access to data preserved under provisions of the Criminal Procedure and Investigations Act 1996 (CPIA)

As a minimum, the following elements of data access must be reviewed as part of the audit:

- that any search was properly authorised where required with evidence of authorisation recorded
- that the timescales for the search were appropriate in that they were no greater than was necessary and proportionate in the circumstances of the investigation
- that the reason, purpose and justification for the search was fully recorded within NAS

In respect of access to data preserved under provisions of the CPIA that any access was solely for the investigation for which it was preserved.

LEAs to audit 10% of records of the disclosure of data otherwise than in accordance with CPIA or similar procedures in Scotland in respect of the justification, the date and time of the disclosure and the identification of both the person disclosing and the recipient of the data. (NASPLE section 9.4.3.7)

LEAs are responsible for dealing with any non-compliance with standards that are identified during audit and must report all non-compliance and a copy of the audit report to the national auditor within 28 days of the non-compliance being identified.

All LEAs must maintain a record of audits that are conducted to include:

- a statement of the findings for all audit activity
- a report of the extent of non-compliance
- a report of action taken in relation to non-compliance

4800

Records of audit will be retained for a period of 2 years and made available to the national auditor on request.

8.3 Audit of Changes to Read Records

LEAs to review a sample of changes to ‘read’ records every 6 months to confirm the validity of the change. Records of review to be retained for a period of 2 years.

8.4 Audit of Access by System Providers, National Administrators and Local Auditors

The National Auditor will audit access to NAS by system providers, national administrators and local auditors, reporting details of any audit that is conducted for the information of controllers to the extent determined by those post holders.

The National Auditor will conduct a NAS system audit every 6 months to confirm data is deleted in line with the requirements of NASPLE Part 2.

Audit of access to NAS by a user with ‘Super Administrator’ permissions will be conducted for each occasion that the system is accessed when those permissions are enabled for that user by the National Auditor.

9. Glossary of Terms, Abbreviations and Definitions

ANPR	Automatic Number Plate Recognition
ANPR system	A collection of cameras, readers components linking to NAS
CCTV	Closed Circuit Television
CAMERA	The device used to capture and ANPR read. CPIA Criminal Procedure and Investigations Act 1996
DPA	Data Protection Act 2018
GSC	Government Security Classifications – (formerly the Government Protective Marking Scheme (GPMS))
GPS	Global Positioning System
JPEG	Joint Photographic Expert Group image format
NAS	National ANPR Service
NAC	National Law Enforcement ANPR Capability
NPCC	National Police Chiefs’ Council

NASPLE	National ANPR Standards for Policing and Law Enforcement
LEA	Law Enforcement Agency – Includes police forces and other agencies undertaking law enforcement activities
Read	The interpretation of a VRM by an ANPR system
Schengen	The Schengen Information System will enable the authorities of signatory countries to have access to reports on persons and objects for the purpose of border checks and controls and other police and customs checks
VRM	Vehicle Registration Mark

10. Document revisions

Version 2.0, September 2020: Update of links within text, Minor revision of section 7

---

1. In most cases a sample of 2% of all instances where the period included in the search extends for 90 days or less prior to the date of the search being conducted for a sample of 30 consecutive days in a period since the previous audit (quarterly) is likely to be appropriate. Depending upon the level of risk a lessor or greater sample may be appropriate. The rationale for determining the data sample should be documented in all cases

Print this page

Home Office

National ANPR Service

National ANPR Service
Technical Specifications

Version 3.0
June 2020

Definitions

Acronym	Description
ANPR	Automatic Number Plate Recognition
ANPR system	A collection of cameras, readers components linking to NAS
CCTV	Closed Circuit Television
CAMERA	The device used to capture an ANPR read
CAPTURE RECORD	The record of a vehicle recorded by NAS for a vehicle passing an ANPR camera including the ANPR READ, associated images and meta data.
COMMUNICATIONS LINKS	The connections between the camera, any local infrastructure and the NAS
CONTROLLER	The competent authority which alone or jointly with others determines the means and purposes of the processing of personal data. Part 3 data Protection Act 2018
CPIA	Criminal Procedure and Investigations Act 1996 and the CPIA Code of Practice
DPA	Data Protection Act 2018
FOI	Freedom of Information Act 2000
GDPR	General Data Protection Regulations
GSC	Government Security Classifications – (formerly the Government Protective Marking Scheme (GPMS)
GPS	Global Positioning System
HIT	The report of a match of a vehicle registration mark (VRM) READ with a VRM that is included on a vehicle of interest list (VOI)
ISO	Information Security Officer – The member of staff with responsibility for ensuring compliance with requirements for IT security
ITHC	IT Health Check – The process for ensuring that security provisions for IT are appropriate and in compliance with requirements that are current at the time of the check.
JCA	Joint Controller Agreement under provisions of the Data Protection Act 2018-
JPEG	Joint Photographic Expert Group image format

LEA	Law Enforcement Agency – Includes police forces and other agencies undertaking law enforcement activities. For the purpose of this document, LEAs shall only include those organisations listed at Annex A.
MIDAS	Motor Insurance Bureau (MIB) data of uninsured vehicles
MOPI	Code of Practice for the Management of Police Information
NAC	National ANPR Capability includes: • the NAS which is a single national system consisting of the functionality to enable use for operational response, investigation and intelligence purposes and a single national store of data, and, • the National ANPR Infrastructure (NAI) which is a network of ANPR cameras, communications links, firewalls and other related supporting components, that are the responsibility of LEA, that connect to the NAS.
NAI	A network of ANPR cameras, communications links, firewalls and other related supporting components
NAS	National ANPR Service
NASP	National ANPR Standards for Policing first version published in 2013 and replaced by NASPLE recognising the applicability to all law enforcement agencies that access the NAS
NASPLE	National ANPR Standards for Policing and Law Enforcement.
National VOI List	Nationally circulated lists that include stolen vehicles, vehicles requiring an operational response and vehicles within Schengen circulations
NAPS	National Accreditor for Police Systems – Responsible for confirming that police IT systems are in accordance with security requirements and authorising connection to national systems.
Network Connections	The IT links between components of the NAC
NPCC	National Police Chiefs' Council
NPCC Vetting Policy	The NPCC standards for vetting of staff for access to police information

PERSONAL DATA	Means any information relating to an identified or identifiable living individual. 'identifiable living individual' means a living individual who can be identified directly or indirectly, in particular by reference to_ a) an identifier such as name, an identification number, location data or an online identifier, or b) One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual Data Protection Act 2018
PNC	Police National Computer
READ	The interpretation of a VRM by an ANPR system
RIPA	Regulation of Investigatory Powers Act 2000
RIPSA	Regulation of Investigatory Powers (Scotland) Act 2000
Schengen	The Schengen Information System will enable the authorities of signatory countries to have access to reports on persons and objects for the purpose of border checks and controls and other police and customs checks
SMS	A Standards format for text messaging
VOI	The details of a vehicle that are of interest to law enforcement for operational response or investigation purposes that is included on a list to enable it to be READ and for authorised staff to receive a report of that READ.
VRM	Vehicle Registration Mark

1 Introduction

This document prescribes the technical specifications for data within the National ANPR Service (NAS). National ANPR Standards for Policing and Law Enforcement (NASPLE) set out the standards that are required for the National ANPR Capability (NAC) to ensure compliance with relevant legislation in the operation and use of law enforcement ANPR. The information within this document is intended to support compliance and consistency in the operation and management of NAS by the police and other law enforcement organisations (hereafter referred to as LEA).

2 ANPR Read Records

2.1 System Testing

The only number that may be entered into any component of the NAS for the purpose of testing connectivity is QQ111QQQ.

2.2 Core Data Components

2.2.1 Vehicle Registration Mark (VRM) (Mandatory)

Where a camera has the capability to record images of vehicles passing within the field of view where no VRM is identified by the system, 'QQQQQQQ'1 must be recorded within the VRM field.

The required format must conform to the Standard Coding Format UTF-8character set. The VRM must contain no spaces.

2.2.2 Time (Mandatory)

Recorded and synchronised using standard time source techniques to Greenwich Mean Time (GMT) plus 0 (+0) at least once every 10 minutes, with accuracy to stratum level 3.

The required format is 'dd/mm/yyyy hh:mm:ss', in 24 hour format.

2.2.3 Location (Mandatory)

ANPR data must place a read in a location, accurate to within 10 metres. This location should have been ascertained through a Global Positioning System (GPS) device. In addition, all fixed-site ANPR cameras must have their GPS co-ordinates accurately recorded to within 5 metres.

[1] Some ANPR cameras can detect the presence of a vehicle where no VRM is visible and the use of 'QQQQQQQ' ensures that these vehicles are traceable in the database with a format that will not be attributed to a genuine VRM.

The required format for recording a location is latitude and longitude in decimal degrees.

When a mobile ANPR system is unable to deliver an accurate GPS coordinate for a read, the GPS field must be populated with N0000000 E00000000.

2.2.4 Supporting imagery

Plate patch – showing the number plate only, (Mandatory for systems under ownership or control of an LEA).

A plate patch must be in JPEG format, 120x60 pixels and be no more than 3kB in size.

Overview – showing the vehicle in the context of the read zone (Optional).

An overview image must be in JPEG format, no more than 25kB in size.

Where images obtained by a camera exceed 3Kb for a plate patch or 25KB for an overview, these must be adjusted prior to forwarding to the NAS.

'Geo Tagging', if an accurate GPS Geo Location is available, then this detail may be added to images using Exif (Exchangeable image file format) (Optional

Other metadata

Column	Format	Mandatory	Details
Feed ID	Numeric	Yes	2 character code as used by the Police National Computer (PNC) Also known as 'Force ID'
Source ID	Numeric	Yes	Short integer (range 1 to 9999)
NRD ID	Numeric	Yes	Short integer (range 0 to 9999) (NRD ID zero (0) must be used to denote VRMs entered manually by an administrator of the ANPR system.)
Lane ID	Alphanumeric	No	Optional text description
'Alias' ID	Alphanumeric	No	Optional textual description that does not disclose the exact location of a NRD
Username	String	Yes	Username of operator using the ANPR system. When deployed in other circumstances, use 'Unattended'.
Preset ID	Integer	No	Short integer Default value is 0 Used to indicate direction of travel on multi-lane CCTV cameras.

3 Data storage and management

3.1 Data loss and resilience

The NAS must not allow any data loss and be configured to provide to provide resilient capability.

3.2 Local system retention and deletion

Local components of NAC must be configured to enable retention of any data received from a camera at more than 7 days for a maximum of 48 hours and for deletion of that data within the following 24 hours.

3.3 Mobile Data Transfer

Local capability must be in place to support transfer of data from mobile ANPR units to the NAS within 48 hours of capture by the camera within the mobile system.

4 National Databases

The NAS must have the technical capability to run the following national databases, as a minimum - PNC; Includes 'Fast Track' 'Extract', 'Schengen' and 'MMC' data.

PNC Extract File

The PNC Extract File is available to forces at least three times every 24 hours and should be loaded onto the mobile systems opportunity following receipt. All ANPR reads must match against the PNC Extract File should the live link to the PNC be unavailable.

5 Vehicle of Interest (VOI) Lists

VOI lists in NAS will be referenced to the LEA that creates and manages the list. In order to support the display of symbols within vehicle mounted systems the file name will be in accordance with the reference list at Annex A.

The following character mapping is to be used. All lists of VOI must conform to the following template, **(Mandatory elements shown in bold text)**:

NB: Entries in 'Standard Words' section must match **exactly** those in the template for uploading into NAS

Column	Description	Standard Words	Comment
1	**VRM**		No spaces, Alphanumeric characters only
2	MAKE		
3	MODEL		
4	COLOUR		
5	**ACTION**	Stop Assess No Alert	Action can include a requirement to STOP the vehicle and take action as described Or To assess in the context at the time the vehicle comes to notice to determine action. Or No Alert only to be used when a VOI list is submitted for monitoring purposes with no intention that any action is taken when the vehicle comes to notice
6	**WARNING MARKERS**	No Warning Known Warnings Present	Generally, PNC ACTion should be used if warning markers are present. For VOI lists, 'No Warning Known' is most applicable. If it is essential to use a VOI list and warning markers are present then 'Warnings Present' should be used with the agreed PNC abbreviation (max of 3) entered as the first words separated only by a space in the Information /Action field. (field 9)

Column	Description	Standard Words	Comment
7	**REASON**	Intel Serious Crime Cloned Low Crime Drugs Intel Sexual Intel Low Crime Offender management Impaired Driving Documents Disqualified Other No Insurance DO NOT USE No MOT – Do NOT USE No Tax – Do NOT USE No Keeper – Do NOT USE LEA P1 LEA P2 LEA P3 LEA P4 LEA P5 LEA P6	Only one reason code per entry No Insurance, No MOT, No Tax and No Keeper MUST NOT be used as a REASON to create a VOI list entry. If intelligence relates to one of these categories, then DOCUMENTS must be used. They are included in the template solely for the use of nationally populated lists to support NAS functionality.
8	INTEL 3X5X2		Enter grading without X or spaces
9	**INFORMATION/ ACTION**	Free Text – Maximum of 198 characters including spaces and punctuation. Carriage return must not be used	Brief free text sufficient to add extra value and detail for the person dealing with activation.
10	**LEA AND AREA**		Include Force Name/ Area (BCU/Division letter/ other LEA ref
11	**START DATE**	Provide date in format [dd/mm/yyyy]	
12	**WEED DATE**	Provide date in format [dd/mm/yyyy];	Entries will be weeded on date specified
13	PNC ID		
14	**GSC marking**	OFFICIAL (or) OFFICIAL-SENSITIVE	Only one marker to be used
15	CAD		
16	**CONTACT**	Provide details of 24hour point of contact for enquiries if vehicle stopped	

6 Real Time Matching

The NAS must provide real-time matching to PNC and other lists of VOI for all ANPR reads.

The system response time from a Vehicle Registration Mark (VRM) being captured by a camera to the hit notification response being delivered to a specific operator must not exceed 4 seconds for static, moveable, dual lane and CCTV Integrated systems, and 6 seconds for mobile ANPR systems.

To allow for this end-to-end performance requirement, the camera must deliver ANPR reads to the NAS within 2 seconds of capture for static, moveable, dual lane and CCTV ANPR Integrated systems and within 4 seconds of capture for mobile ANPR systems.

The NAS must process that read against the PNC and other VOI databases and deliver any resultant match notification to the operator within 2 seconds of receipt of the read by the NAS for all systems.

7 Real Time Delivery of Data

Local LEA ANPR infrastructure must clearly display the current state of connectivity to the NAS and/or any time when data is not being sent to the NAS. In the event of a communications or systems failure, the LEA infrastructure must buffer that read data and deliver it to the NAS once the communications or failed systems have been restored. The real-time delivery of data is a priority and the delivery of any buffered data should take place in addition to delivery of real-time data.

8 Search and Export of Data

The NAS must provide for the identification and export of data to enable identification using any of the following criteria:

- Vehicle Registration Mark (VRM);
- Date and time parameters;
- by camera identification;
- by location co-ordinates;
- by ‘geo plotting’
- direction of travel (desirable)

9 Interoperability

Systems must enable interoperability between LEAs and the NAS to allow:

- Real-time matching of reads against lists of VOI and the real-time delivery of hits
- Remote research in accordance with prevailing researching guidelines
- NAS read searching for national data searches and data mining in accordance with the NAS Business Rules, as defined within current NASPLE
- Distribution of lists of vehicles of interest to the NAS
- Transfer of data and all associated images between LEA ANPR Infrastructure and the NAS.

Vehicle of Interest List (VOI) Naming Convention

In order to display the name of the organisation creating the VOI list within symbols in vehicle mounted systems, character mapping is required. A VOI list file name will begin with the organisations PNC ID followed by an underscore (for example 07_Cheshire VOI List); the agreed force abbreviation will be displayed in the bottom 'white' section of the VOI symbol (in this example CHESH would be displayed). The following character mapping is to be used:

Character at start of VOI File name followed by underscore	***Display in bottom white section of VOI symbol***
52	**A&S**
40	**BEDS**
93	**BTP**
35	**CAMBS**
07	**CHESH**
48	**COLP**
59	**CNC**
17	**CLEV**
03	**CMBRIA**
30	**DERBYS**
50	**D&C**
55	**DORSET**
94	**DVLA**
201	**DVSA**
11	**DURHAM**
63	**DPP**
42	**ESSEX**
53	**GLOS**
06	**GMP**
61	**GWENT**
44	**HANTS**
41	**HERTS**
88	**LEA**
16	**HUMB**
46	**KENT**
04	**LANCS**
33	**LEICS**
32	**LINCS**
05	**MERPOL**
02	**METPOL**
24	**MOD**
36	**NFOLK**
60	**NWP**
12	**NYP**
34	**NHANTS**
10	**NORPOL**
31	**NOTTS**
90	**PSOS**

98	**PSNI**
62	**SWP**
14	**SYP**
21	**STAFFS**
37	**SFFOLK**
45	**SURREY**
47	**SUSSEX**
43	**TVP**
23	**WARWCK**
22	**WMERCA**
20	**WMIDS**
13	**WYP**
54	**WILTS**
LEA	**LEA**
TUTELAGE	**TULAGE**
MIDASGOLD	**MIBGLD**
TRIVIUM	**TRVIUM**

© Crown copyright 2020

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at anpr@homeoffice.gov.uk



PIPS TECHNOLOGY™
DETECTION INNOVATION



PAGIS Administrator's Manual

Version 2.14

Updated 4/10/2020

NEOLOGY MOBILITY TECHNOLOGIES

Table of Contents

Table of Contents 2

NOTICES 4

Technical Support 4

Design Changes 4

Trademarks 4

Copyright 4

Version 4

INTRODUCTION 5

1.1 Dual Lens Color and Infrared Camera 5

1.1.1 Available Products 5

1.2 Using This Manual 6

SCREEN REFERENCE 7

2.1 The PAGIS Software Login Screen 7

2.1.1 Logging on with the Default Administrative Account 7

2.2 Main Screen - Live View 8

2.2.1 Getting Started in PAGIS 8

2.3 The PAGIS Navigation Buttons 9

2.3.1 Camera Control Buttons 9

2.3.2 GPS Indicators 10

2.3.3 Camera Firmware Update (Restricted Users) 10

2.3.4 Day/Night Mode 10

2.4 Begin Shift 11

2.4.1 Sync via USB Thumb drive (or Local Source) 11

2.4.2 Sync via Wireless Network 11

2.4.3 PAGIS Auto-Sync Settings 11

2.4.4 Begin Shift – Additional Information 11

2.5 End Shift 11

2.5.1 Sync to BOSS 11

2.6 Cam Mode Button 12

2.6.1 Camera Modes 12

2.7 Taking a Picture 12

2.8 Search Entry Screen 13

2.8.1 Searching Synchronized Hotlists for License Plates 13

2.8.2 Searching Locally Stored Reads and Hits 13

2.8.2.1 Searching for a Match 14

2.8.3 Wild Card Symbols 14

2.8.4 Manually Adding a Plate to PAGIS 15

2.8.4.1 ADD VLP Query 15

2.8.4.2 ADD VRM Report Screen 15

2.9 The Review Screen 16

2.9.1 Summary Review Section 16

2.9.2 Review Navigation Buttons 16

2.9.3 Reads 17

2.9.3.1 Reads Result Screen Navigation Buttons 17

2.9.3.2 Interactive Buttons – Reads Screen 17

2.9.4 Hits 18

2.9.4.1 Hit Screen Attributes 18

2.9.4.2 Hit Screen Function Buttons 19

2.9.4.3 Interactive Buttons – Hits Screen 19

2.9.4.4 Set Disposition – Additional Detail 19

2.9.4.5 Add Intel – Additional Detail 20

2.9.5 Misreads 20

2.9.5.1 Marking a Record as a Misread: 21

2.9.6 Audits 22

2.9.7 Targets 22

2.9.7.1 The Targets Screen 23

2.9.7.2 Targets Screen Navigation Buttons 23

2.9.8 Databases 24

2.9.8.1 Databases Screen Functions 24

2.9.8.2 Databases Screen Navigation Buttons 24

2.9.8.3 Databases Edit- “Manual Reports” 25

ADMIN SETTINGS 26

3.1 Sync Options Screen 26

3.1.1 Synchronization Types 26

3.1.1.1 Synchronization to Disk (Local Storage) 27

3.1.1.2 Synchronization with BOSS 27

3.1.1.3 Sync to “Instation” (Formerly BOF2 and BOF3) 28

3.1.2 Global Sync Options 29

3.2 PAGIS Privacy Settings (Local Data Retention) 30

3.3 Language 31

3.4 Location 31

3.5 Users 32

3.5.1 User Privileges ____ 32
3.6 Sound ____ 33
3.6.1 Configuration Buttons ____ 33
3.7 System ____ 34
3.8 Rules ____ 35
3.8.1 Rules – Additional Clarifications ____ 35
3.9 OCR ____ 36
3.10 External ____ 37
3.10.1 XML Datastream Ports ____ 37
3.11 Cameras ____ 38
3.11.1 Checking the Connection ____ 38
3.11.2 Troubleshooting Camera Connections ____ 38
3.11.3 Configuring the Cameras in PAGIS ____ 39
3.12 Cam Setup ____ 40
3.12.1 Cam Setup Navigation Buttons ____ 40
3.13 Configs (Camera View Modes) ____ 41
3.13.1 Configs Navigation Buttons ____ 41
3.13.2 Reviewing and Modifying Existing Modes ____ 42
3.13.3 Adding a New Camera Mode ____ 43
3.14 Info ____ 44
3.15 Camera Firmware Update, (Admin) ____ 44
PAGIS INSTALLATION GUIDE ____ 45
4.1 PAGIS System Requirements ____ 45
4.2 PAGIS Prerequisites ____ 45
4.2.2 PAGIS Software Installation (MDC) ____ 46
4.2.3 PAGIS Software Installation (Mobile Processor) ____ 47
TROUBLESHOOTING TIPS ____ 48
5.1 Troubleshooting & Tips ____ 48
5.1.1 PAGIS with NetMotion VPN ____ 48
5.1.2 Cisco VPN Client: ____ 48
5.1.3 Microsoft .NET 3.5 Installation ____ 48
5.1.4 Firewall Settings for Client-Server Installations ____ 48
PAGIS/BOSS3 CONFIGURATION ____ 49
6.1 Creating a New Device in BOSS3 ____ 49
6.2 Enabling a New Mobile System in BOSS3 ____ 49
6.3 Assigning Ownership to a Device in BOSS3 ____ 49
6.4 Assigning Hotlists to a Device in BOSS3 ____ 50
PAGIS/BOSS4 CONFIGURATION ____ 50
7.1 Creating a New Device in BOSS4 ____ 50
7.2 Enabling a New Mobile System in BOSS4 ____ 50
7.3 Assigning Ownership to a Device in BOSS4 ____ 51
7.4 Assigning Hotlists to a Device in BOSS4 ____ 51
APPENDIX A: THE GLOSSARY ____ 52
APPENDIX B: PAGIS SOFTWARE DATABASE FILE ____ 53
APPENDIX C: FAQ ____ 55
APPENDIX D: XML DATASTREAM ____ 60

4818

NOTICES

The information within this manual is authorized for distribution to customers, authorized service center personnel, and distributors of Neology. Every effort has been made to supply correct information. However, Neology assumes neither responsibility for its use, nor for any infringements of patents or other rights of third parties, which may result from its use. No license is granted by the manufacturer under any patent or patent rights. Neology reserves the right to modify and update the equipment at any time without prior notice. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means to a third party without the prior consent of the copyright holder. The manufacturer's warranty will be invalidated if untrained personnel operate the equipment or if any attempt is made to service the equipment by unauthorized personnel.

This manual contains confidential and proprietary information and should not be redistributed except as needed for proper use and maintenance of the agency's Mobile ALPR system.

Technical Support

Service of this equipment by replacement of parts, on-site repair, routine maintenance inspection, and scheduled remote support session is available. Please contact PIPS Technology's ALPR Technical Support.
Phone: 833-PIPS-LPR (833-747-7577), Option 2
Support Team Email: Support@PIPSTechnology.com
For Customers in Europe, Middle East and Africa: Support@PIPSTechnology.co.uk
Web: www.pipstechnology.com
Fax: 858-391-0264
Corporate Office: 13520 Evening Creek Drive Suite 460. San Diego, CA 92128

Design Changes

Neology reserves the right to change the design of any product from time to time without notice and with no obligation to make corresponding changes in products previously manufactured.

Trademarks

PIPS Technology™ is a trademark of Neology Inc., and either registered or pending registrations in several jurisdictions. Windows, Windows 7, Windows 8, Window 10, and .NET are all trademarks of the Microsoft Corporation. Other trademarks and registered trademarks are the property of their respective owners.

Copyright

The Neology / PIPS Technology PAGIS Software is copyright of Neology. All rights reserved. This product contains confidential and trade secret information of Neology and is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portions of it, may result in civil and criminal penalties.

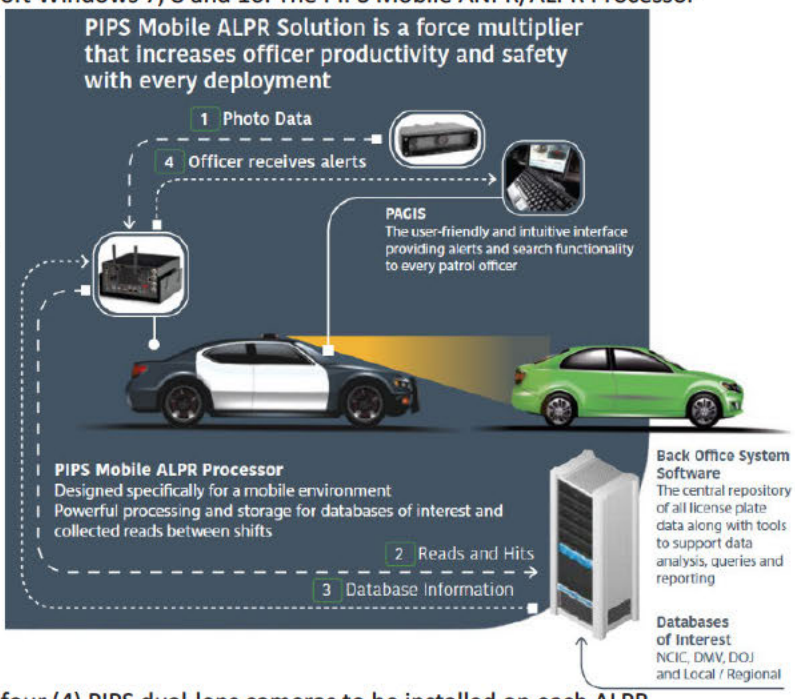
Version

This manual demonstrates the attributes of the Neology / PIPS Technology PAGIS Software Version 2.14 and was last updated in March 2020.

INTRODUCTION

PIPS Technology's Automated License Plate Recognition (ALPR) software solution called PAGIS utilizes dual-channel, dual-lens, cameras to "read" plates. Our software is optimized to run on the Mobile Processor itself or in conjunction with a mobile data computer (MDC). Our mobile software is compatible with Microsoft Windows 7, 8 and 10. The PIPS Mobile ANPR/ALPR Processor comes equipped with Microsoft Windows 7 Embedded.

The PAGIS Software processes the infrared plate image provided by any of the cameras and then interprets the plate number through Optical Character Recognition (OCR) via the mobile processor. The PAGIS application then searches for any matches of the plate with those listed in the databases, or "hotlists," distributed from the PIPS Back Office System Software (BOSS) or other external sources.



WARNING: To reduce the risks associated with impact, which if not avoided, could result in serious injury or death: Do Not interact with the ALPR system while driving in hazardous situations. The PIPS mobile camera series and License Plate Capture Software are not intended for use in hazardous environments, so that the User and/or others are not put at risk for personal injury and/or property damage.

1.1 Dual Lens Color and Infrared Camera

The PIPS Technology Mobile ALPR System allows for a maximum of four (4) PIPS dual-lens cameras to be installed on each ALPR vehicle provided that the vehicle supports the additional mounting equipment.

Each dual-lens mobile camera uses visible light to take color overview pictures of the vehicle and uses infrared (IR) illumination to capture the license plate's alphanumeric characters. IR illumination offers the best capture performance of reflective license plate characters for the following reasons:

- State issued license plates are designed to be highly reflective to IR light.
- Cameras using IR capture technology do not depend on the presence of visible light to function.
- Cameras using IR capture technology are not negatively impacted by the effects of headlights, solar glare, or total darkness.
- IR light penetrates rain and fog better than visible light.
- Due to these attributes, the system can be used 24 hours a day, seven days a week.

1.1.1 Available Products

Additional information about this and other PIPS Technology applications, cameras, and solutions are available on the PIPS web site: http://www.pipstechnology.com

1.2 Using This Manual

The section overview of this software manual is as follows:

Section 1: The Introduction and Basics

Section 2: PAGIS User's Section: Explains screen function and User Operations in the PAGIS Software

Section 3: Troubleshooting Tips

Section 4: Software Administrator's Guide: Explains how to install and configure the PAGIS Software

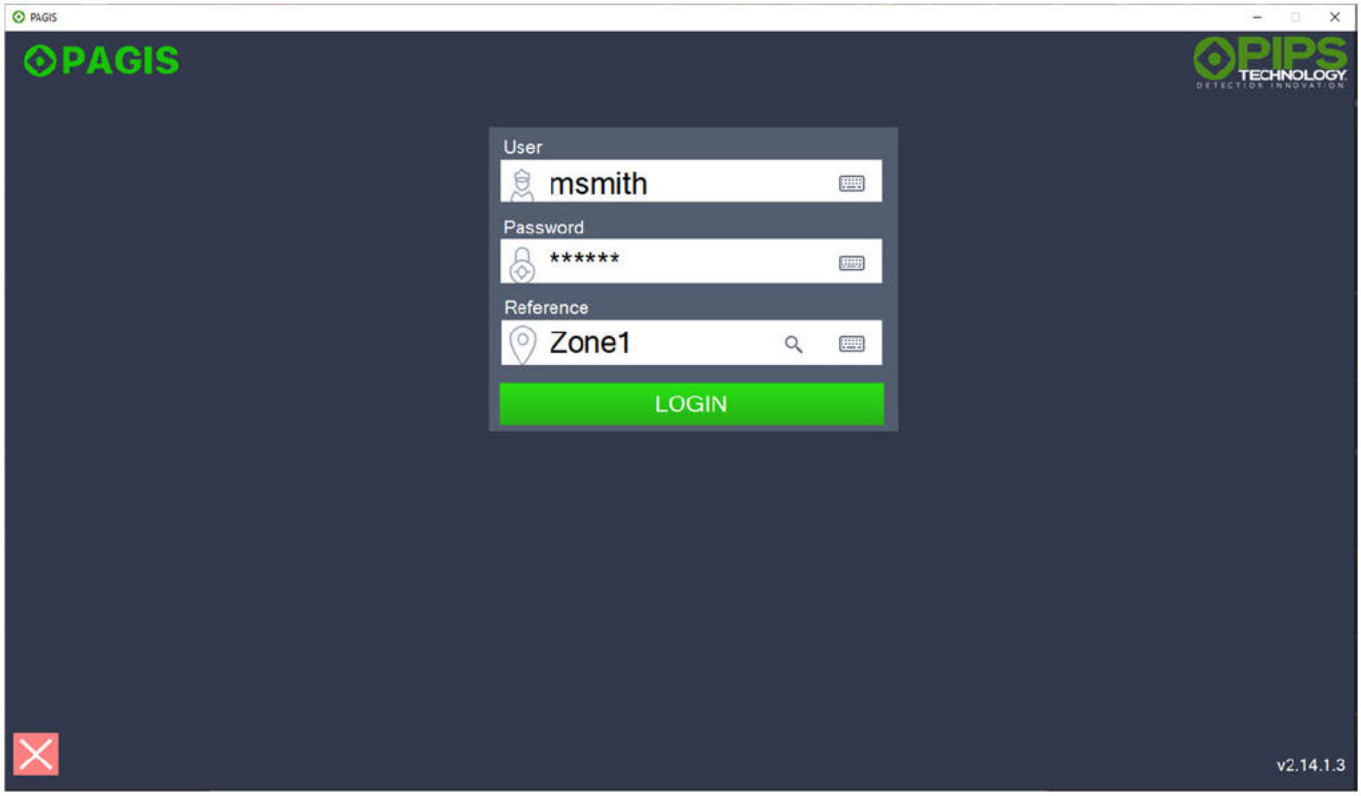
Section 5: Additional Information and Troubleshooting Tips

Section 6: Initial BOSS configuration for new PAGIS devices (MDCs)

Appendices: Additional features and details

SCREEN REFERENCE

This section guides the user through the PAGIS Software screens and the available options. Screens are grouped according to function. When a button is grayed out or missing, the option is not available, or no information has been accrued to activate it.



2.1 The PAGIS Software Login Screen

The PAGIS Software allows users with various access privileges to use the same MDC. For users with touch screen monitors, the Keypad button immediately to the right of any text box gives the user access to an on-screen keyboard for data entry.

User Field: The alphanumeric string assigned to identify the user. Usernames are not case sensitive.
Password Field: Password of the assigned user logging in. Passwords are case sensitive.
Reference Field: This is an optional field utilized to fit a number of use cases. A user can manually enter a reference at logon, leave the field blank, or select list of unique tags that will be associated with all data captured while logged in. If the Administrator has configured a default reference tags, that information will be displayed automatically. Otherwise, it will be blank.
Login Button: Submits the username and password to attempt a login.
Exit Button: By clicking the X icon in the lower left-hand corner, the user can exit/close the PAGIS Software.

2.1.1 Logging on with the Default Administrative Account

The PAGIS Software includes a default administrative account that can be used for the initial configuration. To do so, simply click the **Login** button with the User and Password fields blank.

NOTE: System Administrators are strongly encouraged to configure users for PAGIS just before, or soon after the installation and setup. PAGIS users accounts are created and maintained in BOSS. Once Users are established by the BOSS System Administrator, the default user account is automatically disabled. Best practices are to be certain at least one User account has administrative privileges.

2.2 Main Screen - Live View

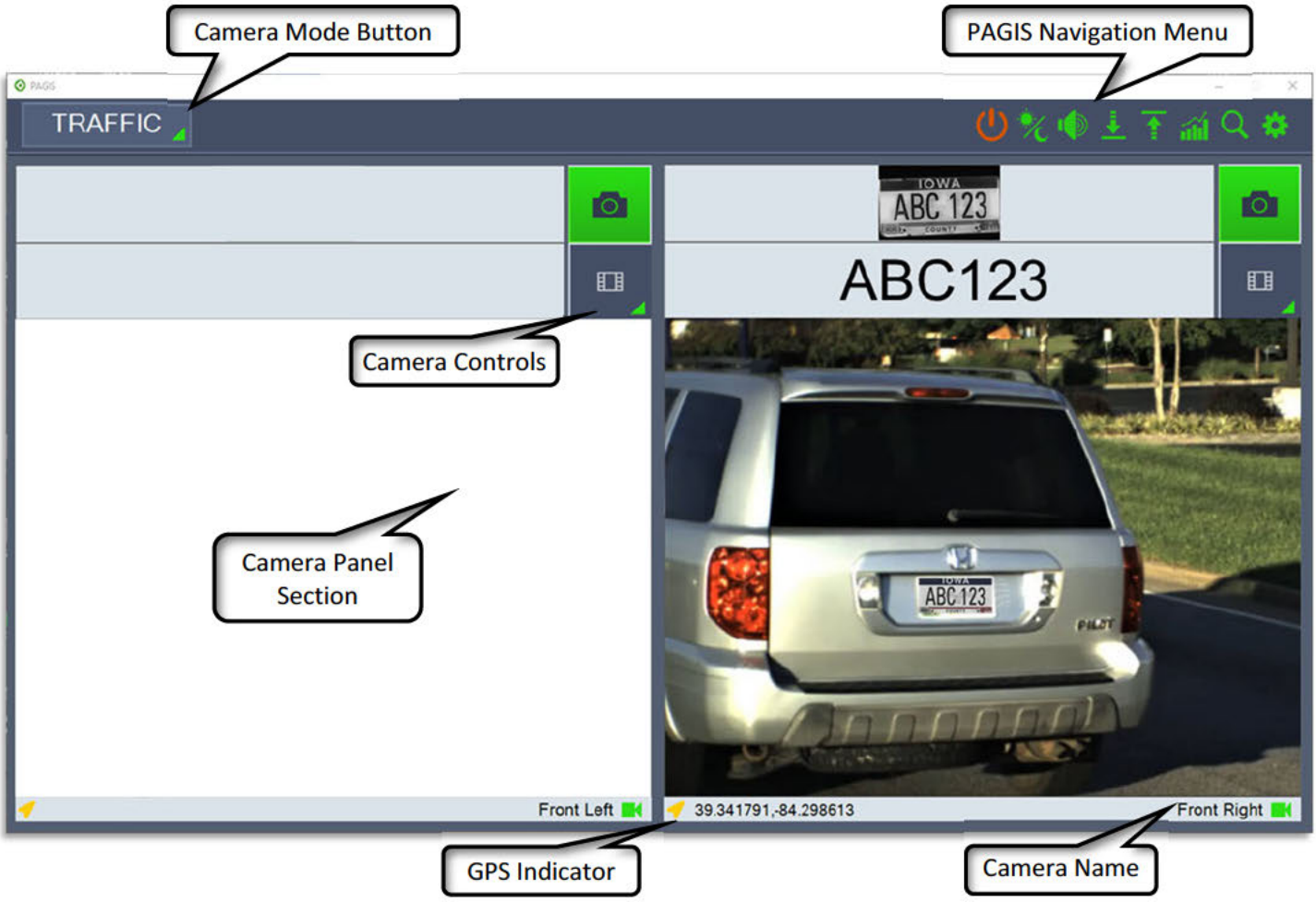
Upon a successful login, the user will see the Main screen (Live View). This is the default view and starting place of all PAGIS Software features. (NOTE: Access to features is based on user group rights established in BOSS.)

The Main Screen is also the place users will monitor read images and ALPR "hits". At the initial startup of the system it is normal to see only a blank/grey screen for a few seconds. Once a connection has been established with the mobile cameras, white boxes will be displayed showing the live-feed camera panels. At this point, the system is ready to capture reads/plates.

2.2.1 Getting Started in PAGIS

By default, PAGIS loads into a static view. This means live video will not automatically appear in the camera panels (white boxes) until a plate has be captured or the user selects one of the live feed options.

Once a plate is "seen" by a camera assigned to the current viewing mode (Traffic vs Parking), it will display the captured information in the corresponding camera panel. Each plate capture is also accompanied by a short "Beep" to audibly alert the user a read has taken place. (NOTE: If the user is in the Traffic Mode at the time a parking camera reads a plate, there will be a sound effect, but no plate image will be displayed on screen unless that plate is on a synchronized Hotlist or until the user switches to Parking Mode.)



2.3 The PAGIS Navigation Buttons

4824

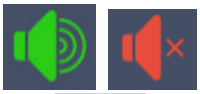
This section provides a quick reference guide to the available navigation buttons of the Live View screen.



The Camera Mode button is located in the upper left corner and is used to switch between the configured camera modes. Once configured, the name will change to a selected mode. The default values are “ALL”, “Traffic” and “Parking”.



The Logoff button is located in the upper right of the window. When selected, the user will be logged out of PAGIS and return to the login screen.



The Sound button is located to the right of the Logoff button. When selected, this button with toggle the PAGIS system sounds On and Off.



Day/Nite mode switches PAGIS between day & night mode screen skins.



The Begin Shift Synchronization button is located to the right of the Sound button. When selected, this will reach out to the BOSS server to download users, hotlists, and other system settings.



The End Shift Synchronization button is located to the right of the Begin Shift Button. When selected, this will upload any previously unsent reads, images, and audits to the BOSS server.



The Statistics/Review button is located to the right of the End Shift Button. When selected the user is able to review Databases/Hotlists, Reads, Targets, and other PAGIS information.



The Search button is located to the right of the Review Button. When selected the user can search his/her reads as well as manually add a license plate to a temporary hotlist.



The Admin/Settings button is located in the upper right corner of the screen. This button is only viewable to Admin level users and allows for system configuration changes and setup.



Firmware update icon will atomically appear when PAGIS detects a new firmware is available for the P720 mobile cameras. All user types are notified, but only Admins can apply the update.

2.3.1 Camera Control Buttons

The dual-lens cameras can capture both color and an infrared image. Formerly, there were a total of three buttons that allowed the user to view the IR and color feed as well as capture a picture directly from PAGIS. Now there is a toggle button to switch between color and IR views and a separate button to take a picture. These buttons are displayed on the main Live Screen as shown below:



The Camera View Selector button: This is the default state at login showing the Static View. (**NOTE**: PAGIS does not automatically display a life feed.)



Color View: by clicking on the Camera View Selector button once, the user will switch to the Color View Mode. This displays the current view of the color camera and will time out after 60 seconds.



IR View: by clicking on the Camera View Selector button twice, the user will switch to the Infrared (IR) View Mode. This displays the current view of the IR camera and will time out after 60 seconds.



The Take Pic button: Just above the Camera View Selector button is the “Take Pic” button. This button allows the user to quickly take a picture from the camera currently viewed.

2.3.2 GPS Indicators

GPS is stamped on each read and hit as capture events take place by the system. The signal strength and location indicators are located underneath the camera panels at the bottom of the Live Screen.

39.341788,-84.298518 Shows an example of the Location Indicator displaying the Lat/Long on the most recent read

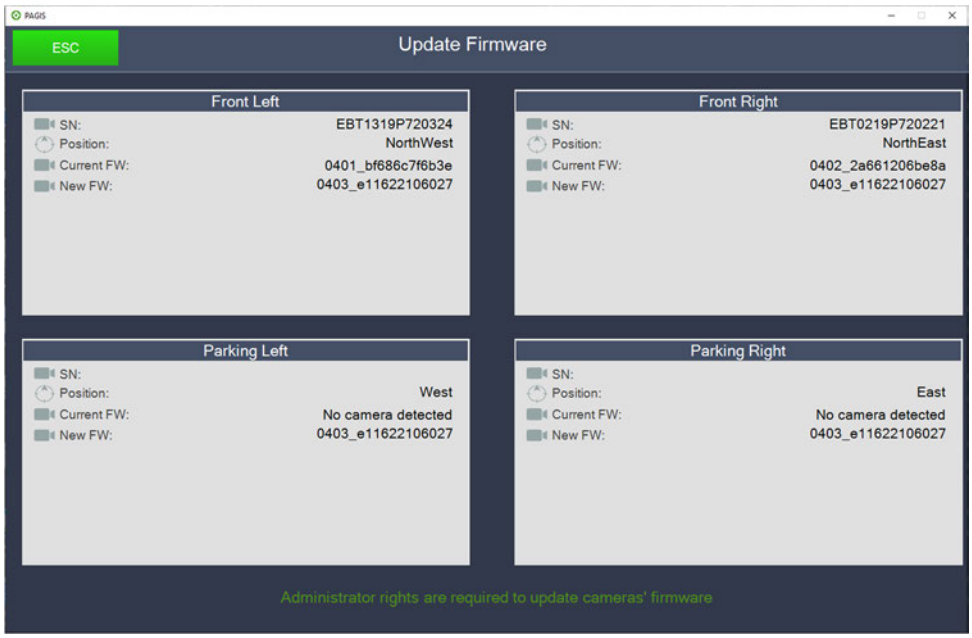
A green or yellow indicator shows a strong or medium strength GPS lock.

A red indicator shows there is no available GPS information.

2.3.3 Camera Firmware Update (Restricted Users)

Camera firmware update provides a means for PIPS to update the camera software to enhance and or correct camera performance. The frimware icon will only apper when update is avialable.

- The firmware update process only updates camera that are attached and function on the mobile processor.
- Restricted PAGIS users are only notified and displayed update information, only a PAGIS administrator can apply the FW update.

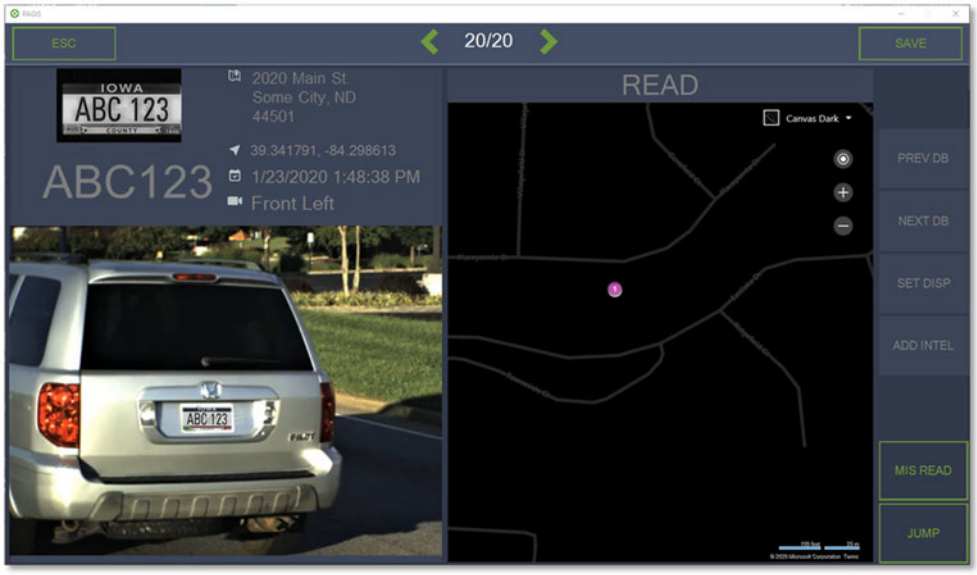


Firmware Updater Window List.

- Title “Camera Name”.
- Camera serial number.
- Position.
- Current FW version.
- New FW version available.

2.3.4 Day/Night Mode

Day/Night mode changes PAGIS user interface skins to a darker appearance to reduce illuminating the vehicle interior.



2.4 Begin Shift

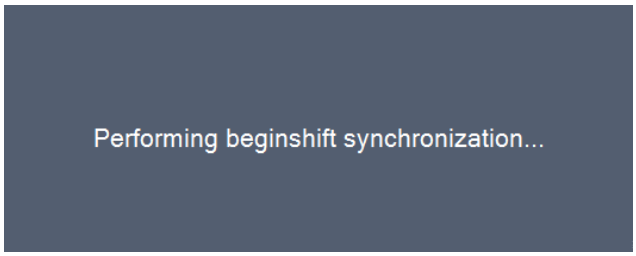
Begin Shift is thought of as the first step for all PAGIS users. From the Live View Screen, the PAGIS user must click the Begin Shift button twice. Once to select the function and once more to launch the Sync. With most agencies, this action utilizes a wireless network to import all the necessary data used during a shift (Hotlists, Dispositions, and Targets) directly from the BOSS Server. However, agencies can also configure their systems to perform this function via Thumb drive or a local source file.

2.4.1 Sync via USB Thumb drive (or Local Source)

Depending on the agency network, some alter the default PAGIS/BOSS configuration mode to use a USB Thumb drive or locally stored file on the MDC/Laptop instead of the wireless Sync. In order to synchronize effectively, the user must first confirm he/she has access to the source location before initiating Begin Shift. **NOTE**: All synchronizations using this method must be performed manually. To learn more about this process, refer to the "Client Tools" section of the BOSS Manual.

2.4.2 Sync via Wireless Network

Synchronizations over a wireless network provide the agency with additional automated features. Best practices recommend the user manually launch Begin Shift from the Live View Screen at the beginning of every patrol shift. However, it is possible for users to allow PAGIS to synchronize via its auto-sync settings. When a manual Begin Shift is launched, the Main View Screen removes the camera feeds and displays a status window of the Sync process. Once the Begin Shift operation is complete, PAGIS will return to the normal Main View Screen.





2.4.3 PAGIS Auto-Sync Settings

PAGIS auto-sync settings are best thought of as how PAGIS receives additional updates and maintains the downloaded ALPR data throughout the entire patrol shift. This prevents the need for the officer to manually perform Begin Shift functions multiple times a day. The auto-sync occurs every 30 seconds and receives data in small batches. The batches are not to exceed 1MB in size for every minute of download. In addition to receiving data, the auto-sync function also uploads a copy of data collected by PAGIS and sends it to BOSS for reporting/processing.

2.4.4 Begin Shift – Additional Information

By default, the synchronizations in PAGIS receive only what has been changed to the ALPR data since the last Sync. Meaning, if some plates have been removed from a Hotlist and others have been added, the system will only transfer that data instead of downloading the entire Hotlist each time the Begin Shift is launched. This helps to reduce the amount of data transferred over the agency's network. **NOTE**: Begin and End Shift synchronization, as well as all auto-sync features, are dependent upon stable communication to the BOSS server via an active data connection.

2.5 End Shift

End Shift in PAGIS is the process in which all the collected ALPR data (Reads, Hits, and Images) from the recent shift is uploaded to the BOSS server and cleared from the local cache. As with Begin Shift, the agency has two options. They can choose to Sync via USB Thumb drive or via wireless connection. Best practices recommend users perform an End Shift Sync at the end of every patrol.

2.5.1 Sync to BOSS

At the end of every shift, the accrued ALPR data should be exported to BOSS. Just like with Begin Shift, the user must click the button twice to launch it (once to select it and once more to execute the Sync). During the Sync, PAGIS uploads any Reads, Hits, and Images not already synchronized to BOSS and purges these items from the local cache on the MDC's hard drive. Completing an End Shift also removes any VLP entries manually added to PAGIS during the shift.

2.6 Cam Mode Button

Clicking the Cam Mode button in the upper left corner of the Live View Screen allows the user to cycle through the different camera modes configured by the PAGIS Administrator. Changing the camera mode changes which cameras are displayed on the Main Screen.

2.6.1 Camera Modes

By default, PAGIS provides "Parking" and "Traffic" as the two configuration modes. Users often switch these modes to suit their current use-case. For example, an officer in a parking lot will often switch the mode to "Parking" so s/he can see the parking cameras on the Live View Screen. They can then switch back to "Traffic" when monitoring city streets.

2.7 Taking a Picture

The PAGIS software has ability to quickly take a picture from one of the currently displayed ALPR cameras on the Live Screen. The user only needs to click on the Take Pic button.



To Take a Picture:

1. From the Live View Screen, press the Take Pic button from the desired camera
2. The image taken will be displayed
3. Enter a description of the picture in the text field at the bottom of the screen
4. Press Save to save the picture or Escape to cancel. Either action will return you to Live View.

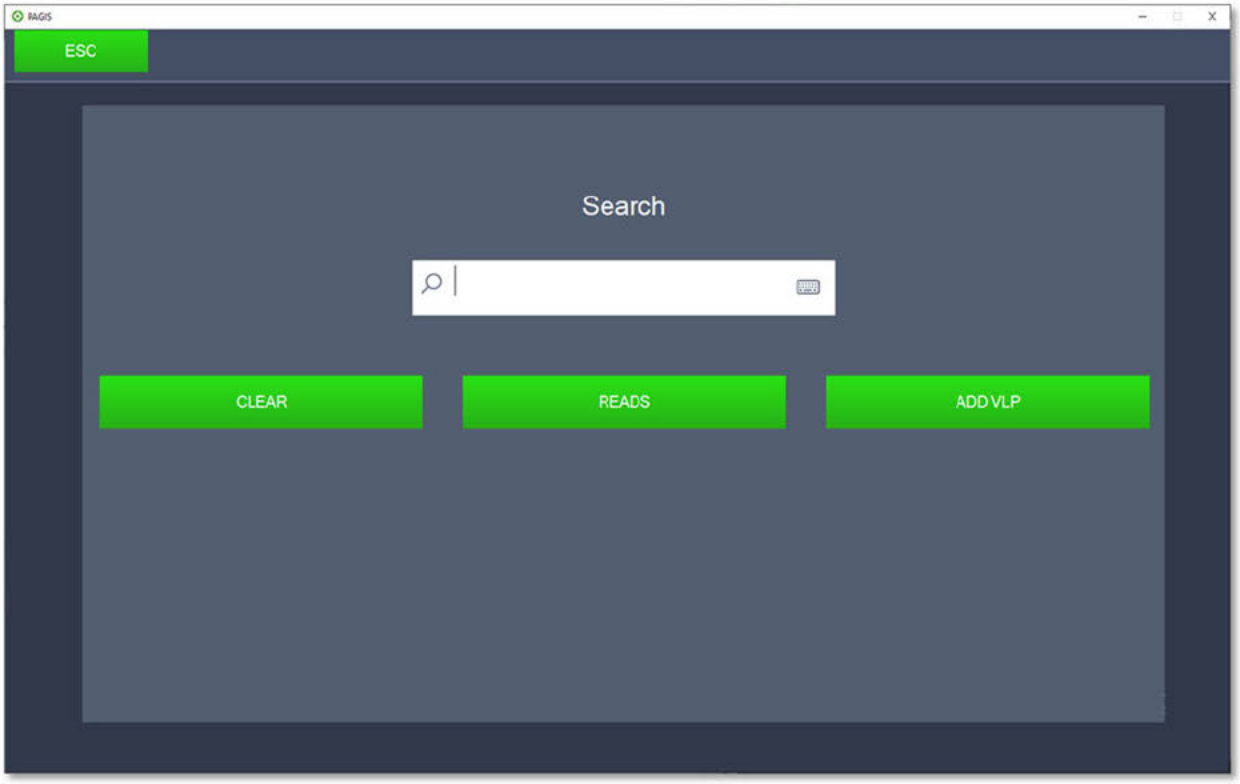
NOTE: The picture will Not be saved if a description/note is not entered in the text box.

To View the Saved Images:

1. Navigate to the Review menu in PAGIS
2. Select Audits
3. The user will be able to see a thumbnail of the image and the saved text/note
4. In order to review the saved images at a later time, the user will need to run the Audit Report from BOSS.

2.8 Search Entry Screen

Pressing the Search button icon from the Live View screen or SEARCH from the Databases window allows the user to search all manually entered plates as well as all BOSS synchronized databases (Hotlists) for license plate and target information. Users can also search all locally stored reads/images accrued since the last End Shift by clicking the Reads button instead of pressing the Enter key.



2.8.1 Searching Synchronized Hotlists for License Plates

By entering a vehicle license plate number (VLP) and pressing the Enter key or the ADD VLP button, the user can quickly search all the stored plate information locally collected as well as the information from all synchronized hotlists distributed from the BOSS server. **NOTE**: Hotlists can only be searched by entering complete VLPs. Wildcards and partial plate numbers will not return results.

Search Box: The text field used to enter the desired plate search via alphanumeric characters and/or wild card symbols.

Clear Button: Clears the contents of the search box.

Driver's License Info: The search field can also check the Hotlists for any DL information stored (Not available all countries).

Reads Button: This button searches for a match from all the reads/hits locally stored on the MDC/Laptop.

ADD VLP: Searches all locally stored hotlists for the plate and if there's no match, allows the user to add the plate to the "Manual Reports" alert list for use in the field. **NOTE**: All manual entries are cleared with each End Shift

ESC: The Escape button allows the user to exit to the Main/ Live View screen.

2.8.2 Searching Locally Stored Reads and Hits

As mentioned previously, this search function allows users to find reads and hits directly from their recent patrols using the search field and the Reads button. These searches pull only the reads and hits locally gathered/stored since the last time the user completed an End Shift. **NOTE**: The search results are specific to each Windows User Profile and do NOT pull images from the BOSS server.

2.8.2.1 Searching for a Match

4829

- From the Search field, users may enter a plate (or partial plate with wildcards) and then click the READS button.
- Results are displayed with the data gathered at the time the read was taken (See example below).
- Each result should display the infrared (IR) image of the plate as well as the color overlay of the vehicle for review.
- Each result shows the GPS data, Closest address point, Time and Date, and the Camera that read the plate.
- If there are multiple results, the user can cycle through them by clicking the left and right navigation arrows.



2.8.3 Wild Card Symbols

The use of wild card symbols in the Search box allows greater flexibility for the user, but may return a larger set of results.

- Wild card searches performed using the asterisk (*) designates an unknown number of characters.
- Wild card searches performed using the underscore (_) indicates a single missing or unknown character.
- Searches can be performed using one, both or no wild card symbols.

Example: The officer received an alert from Dispatch looking for a vehicle plate containing the letter J and the number 8 separated by one character. Because the officer doesn't know how many characters there are before or after the J and 8, he enters *J_8* in the search box to review all possible matches of J and 8 separated by only one digit.

2.8.4 Manually Adding a Plate to PAGIS

PAGIS allows users to manually add a plate of interest directly into the software as needed. Once saved, these entries are stored as part of the Manual Reports alert list and work just like any other Hotlist synchronized from the BOSS server.
NOTE: These additions are designed to be temporary and are cleared from the software with each End Shift.

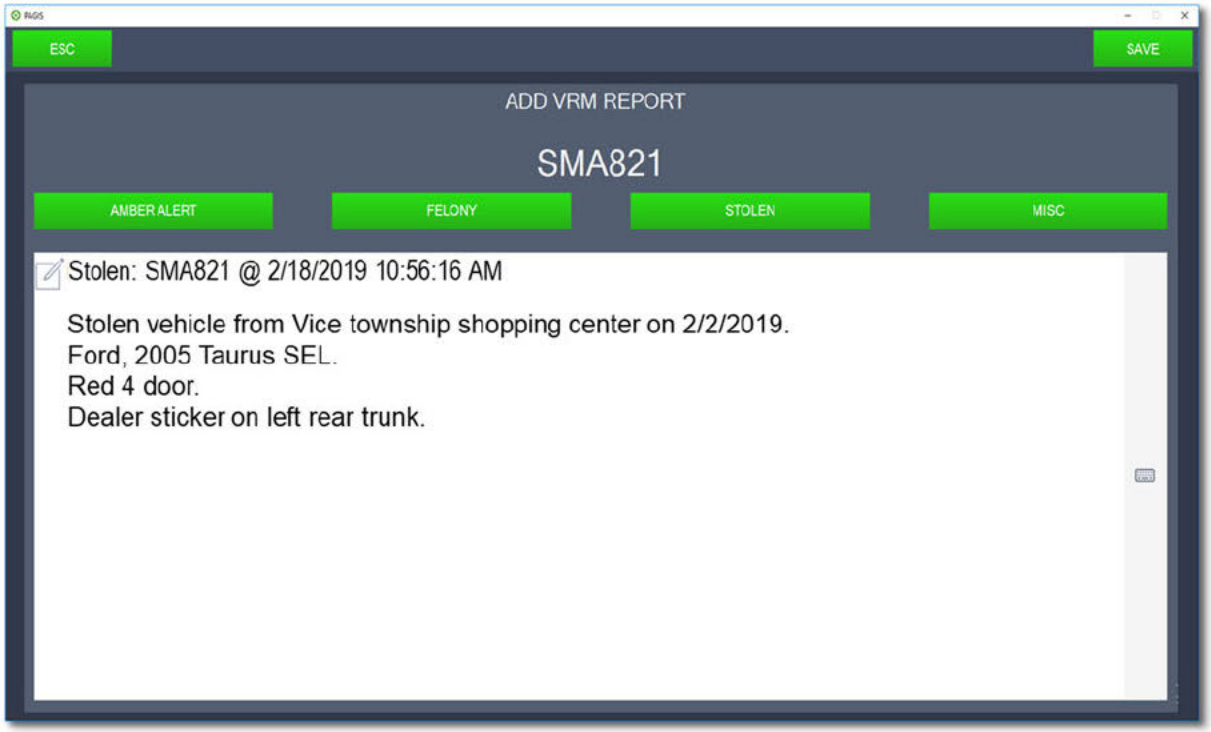
2.8.4.1 ADD VLP Query

Before an entry is added to the Manual Reports Hotlist in PAGIS, the software searches all stored databases for a match. If a match occurs, a message will display under the search box showing which Hotlist(s) it has been found in. If the VLP query does not return a match, the "ADD VRM REPORT" screen appears.



2.8.4.2 ADD VRM Report Screen

If the desired plate does not already reside in another Hotlist, the ADD VRM Report Screen becomes accessible to the user.



1. From the Search Entry Screen, enter the desired plate to add.
2. Click the ADD VLP button. If no match is found on any other hotlist, the "Add VRM Report" screen will appear.
3. Click to select the applicable alert type (AMBER ALERT , FELONY , STOLEN , or MISC)
4. Either leave the default information or add additional detail.
5. Click Save at the top right to add the plate to the Manual Entries Hotlist

2.9 The Review Screen

4831

PAGIS allows users to review all locally stored data from one easy location. Clicking the Review icon from the Main Screen launches Review. This screen is divided into the Summary View Chart and sub-section navigation buttons to the right.



2.9.1 Summary Review Section

The Summary View Chart is divided into five categories and allows a user to review the information collected during their shift at a glance.

Total Reads: Shows the total number of Reads/Hits synced to BOSS and the total number of reads captured during the shift.
Reads: Shows the total number of reads synced to BOSS and the total number of reads captured during the shift.
Hits: Shows the total number of hits synced to BOSS and the total number captured during the shift.
Misreads: Shows the total number of reads marked as a "misread" synced to BOSS and the total marked during the shift.
Audits: Shows the total number of audits synced to BOSS and the total number of audits during the shift.
Targets: Shows only the number of targets downloaded from BOSS.
(NOTE: The Sync value will always be zero for customers using Disk Sync mode/Client Tools.)

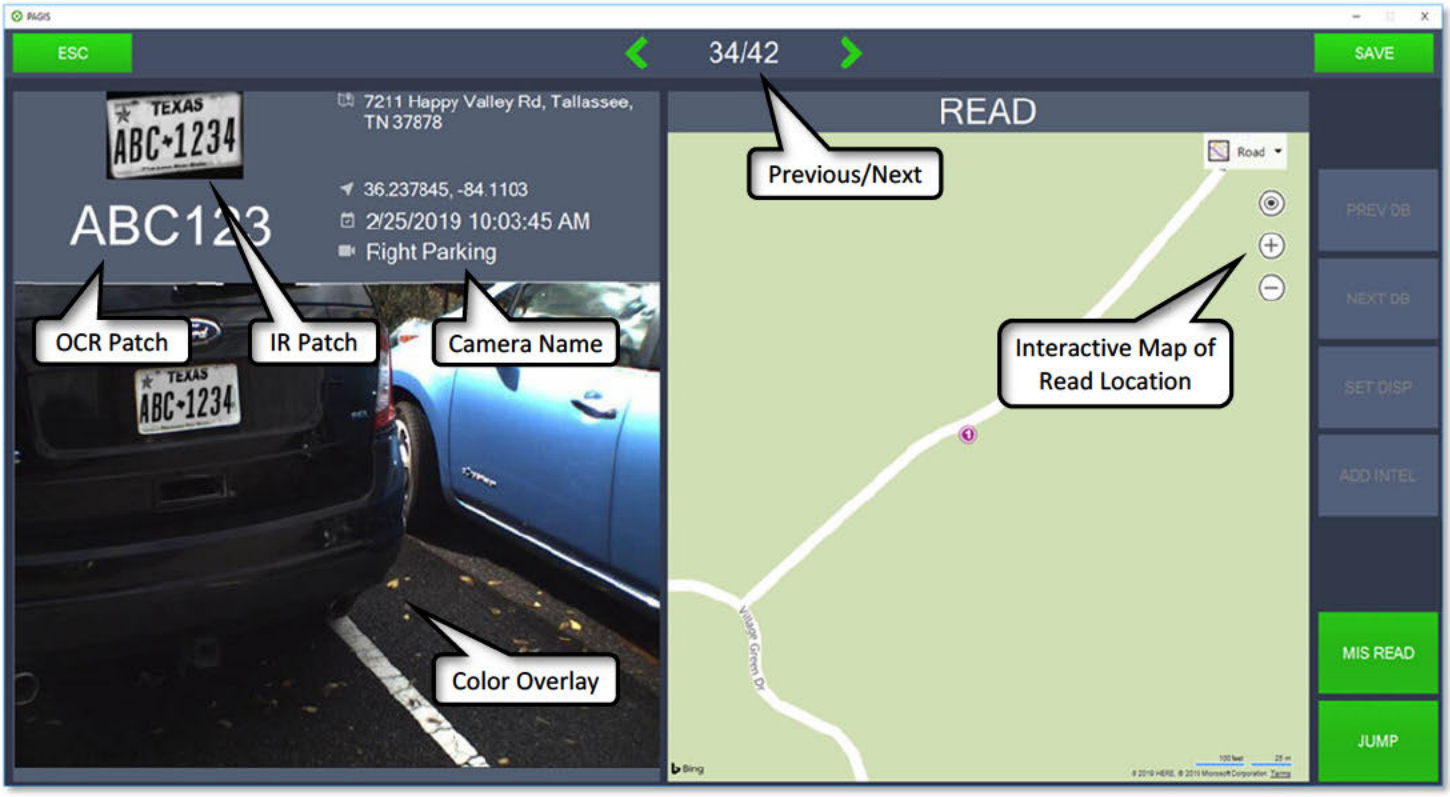
2.9.2 Review Navigation Buttons

The navigation buttons allow the user to review specific sets of information gathered during the shift.

Reads: Review all plate detections that have occurred since the last End Shift synchronization.
Hits: Review the hit alerts for Vehicle License Plate (VLP) reads that matched a Hotlist.
Misreads: Review reads and/or hits that have been manually flagged during the shift as misreads, where the plate number in the image does not match the OCR interpretation of the plate (e.g., a letter O misread as a Q or zero).
Audits: Review failed and successful logons, any manual data entered during the shift, pictures taken and all manual license plate searches.
Targets: Review targets that have been synchronized/downloaded from Boss.
Databases: Review all the Hotlists currently distributed to this PAGIS laptop/MDC.
Esc: Returns the user to the previous screen.

2.9.3 Reads

From the Main Screen, the user can review his or her accumulated Reads (those gathered since the last End Shift was completed) by clicking on the Review icon and then selecting the Reads Navigation button. The Read Review Screen is divided into two main sections. The left side displays the information gathered at the time of the read and the right side displays an interactive map of the GPS location.



NOTE: Buttons that are greyed out indicate options that are not available in the current view. For example, the Reads and Hits review screens share the same layout but different on-screen options.

2.9.3.1 Reads Result Screen Navigation Buttons



Read Count: The left number is the current record. The right number is the total available for review.

Next/Previous button: The arrows on either side of the read count allow the user to navigate back and forth to review reads/results.



MisRead button: When the button is green it indicates the record has NOT been edited as a Misread by a user. Once a Misread is saved, this button will turn grey and the record title will update.



Jump button: Allows the user to "jump" to a specific record without the need to navigate one record at a time using the Next/Previous buttons.



Save button: Apply any changes/edits and return to the Main Screen.



Escape button: Returns the user to the Main Screen.

2.9.3.2 Interactive Buttons – Reads Screen

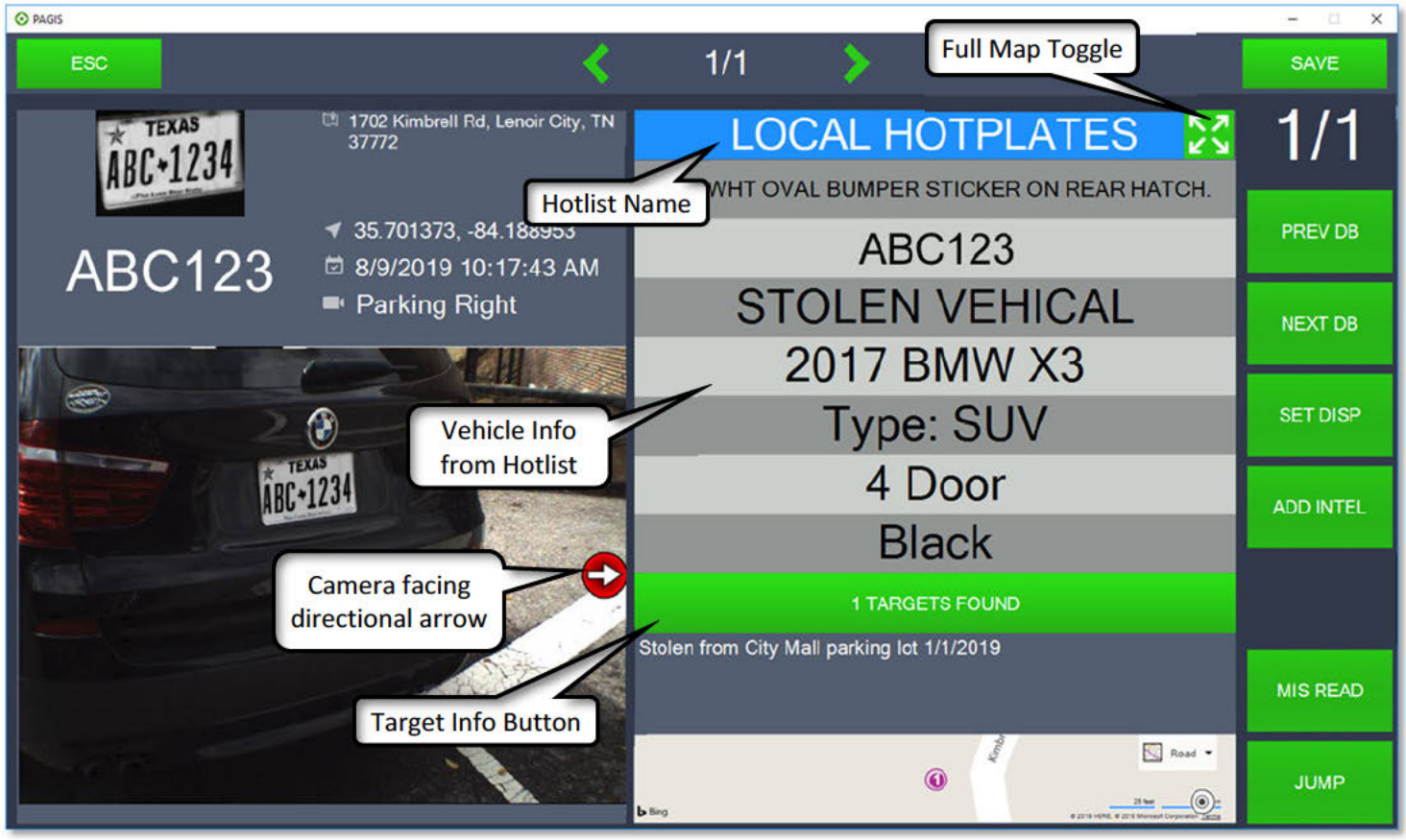
From the Reads Review, the user can interact with the following:

- IR Patch: The user can click on the IR "Patch" plate image to open a full-screen view.
- OCR Patch: The user can click on the OCR "Patch" image to edit the license plate number if necessary/Misread.
- Color OV Image: The user can click on the color image to open a full-screen view.
- Map: The user can manipulate the interactive map of the read location (Map Type, Scroll, and Zoom).

2.9.4 Hits

Users can manually access the Hits Section by first selecting the Review icon from the Live View Screen and then clicking the Hits Button. The Hits Screen is also divided into two main sections. The left side displays the information gathered from the ALPR equipment during the read. And the right side displays the information provided by the associated alert list.

NOTE: Each time a VLP matches a Database value (a license plate read by the system matches a Hotlist entry), PAGIS plays an audible tone and automatically displays the Hit Screen to alert the user.



2.9.4.1 Hit Screen Attributes

Hit Count and Navigation Buttons: Displays the total Hit count as well as the Next/Previous navigation buttons.

IR Patch Image: A thumbnail image of the license plate from the IR camera.

OCR Text: The character string the OCR engine generated from the current plate.

GPS Location: The GPS coordinates at the time of the hit. (If a GPS device is not attached, the Lat/Long is displayed as 0,0).

Date and Timestamp: The date and time when the read/hit was captured.

Overview Image: The overview image of the vehicle from the Color Camera. (**NOTE**: Color images require visible light)

Camera Name: The name of the camera that captured the read ("Right Parking" in the screenshot).

Hotlist Name: This is the name of the Hotlist or "Database" where the plate was matched.

Target Button: When available, this indicates a person of interest is associated with the Hit and opens the Targets Screen.

Vehicle Information: The area of grey bars will display the related vehicle information from the Hotlist. Any information added manually by the user will appear in the Text Box near the bottom of the screen.

Interactive Map: Shows the location the Hit took place. Users can access full-screen view by clicking the map or the toggle .

2.9.4.2 Hit Screen Function Buttons



The Hit Count Indicator: shows how many Hotlists the current Hit has registered against.



Previous DB button: This button moves the user to the previous Database/Hotlist that produced a Hit.



Next DB button: Pressing this button moves the user to the next Database/Hotlist that produced a Hit.



The Set Disposition button: prompts the user to report the disposition of the hit by selecting one of the approved codes assigned in BOSS by the Administrator.



The Add Intel button: allows the user to add additional information regarding the current Hit.



The Misread button: allows the user to flag the Hit as a misread.



The Jump button: Allows the user to "jump" to a specific Hit instead of navigating one at a time.

2.9.4.3 Interactive Buttons – Hits Screen

- IR Patch: The user can click on the IR "Patch" image to open a full-screen view.
- OCR Patch: The user can click on the OCR "Patch" image to edit the license plate number if necessary/Misread.
- Target Button: Shows associated person(s) of interest and opens the Targets Screen.
- Color OV Image: The user can click on the color image to open a full-screen view.
- Map: The user can manipulate the interactive map of the read location (Map Type, Scroll, and Zoom).

2.9.4.4 Set Disposition – Additional Detail

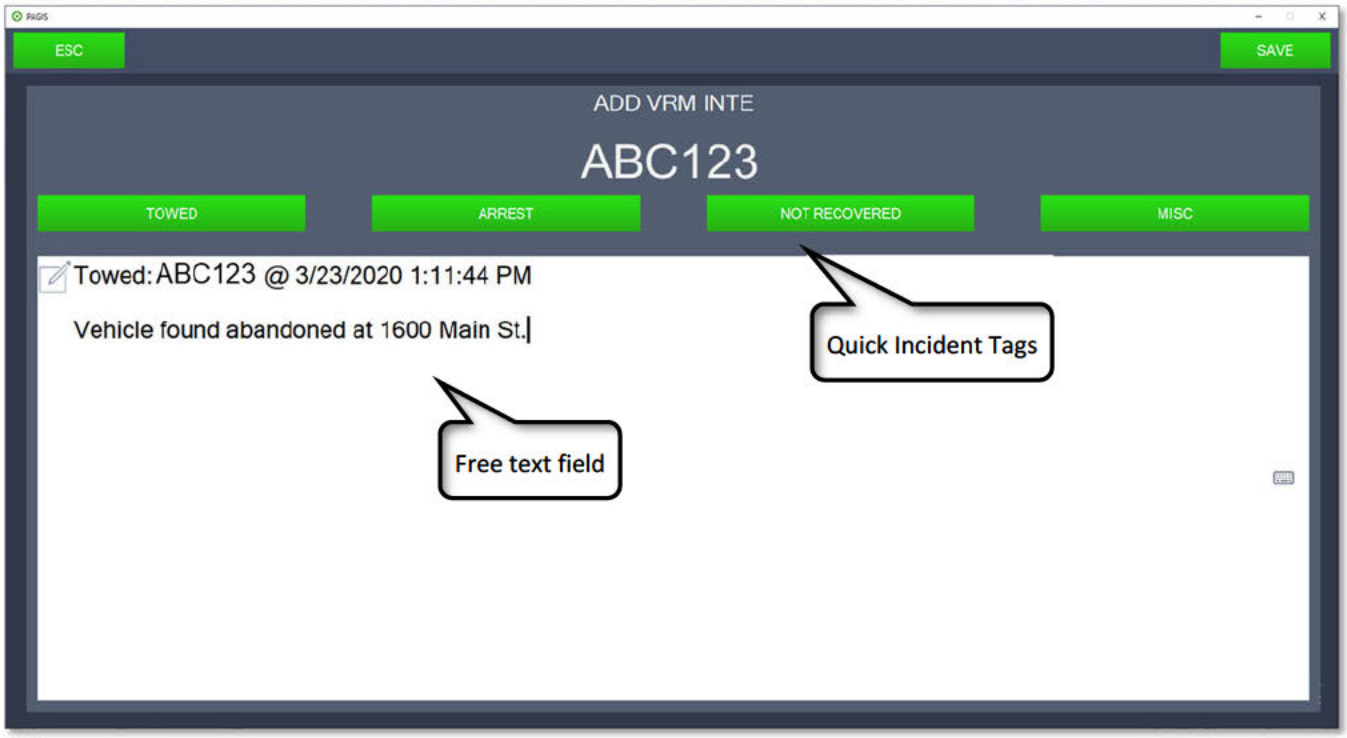


PAGIS allows for additional information to be added to a record in the form of a Disposition. Once Hits are flagged with a disposition code, the Agency is capable of running a "Reads Statistics by Disposition Report" in BOSS. Thus, providing valuable metrics and understanding to leadership in regard to their ALPR Enterprise.

When the "Set Disp" button is selected, the user is prompted to choose from a list of predefined values set by the Agency/BOSS Administrator. Once a disposition is selected and Saved, the disposition is reported to BOSS and will also show up in the Hits Review Screen text box in PAGIS on the next alert notification.

2.9.4.5 Add Intel – Additional Detail

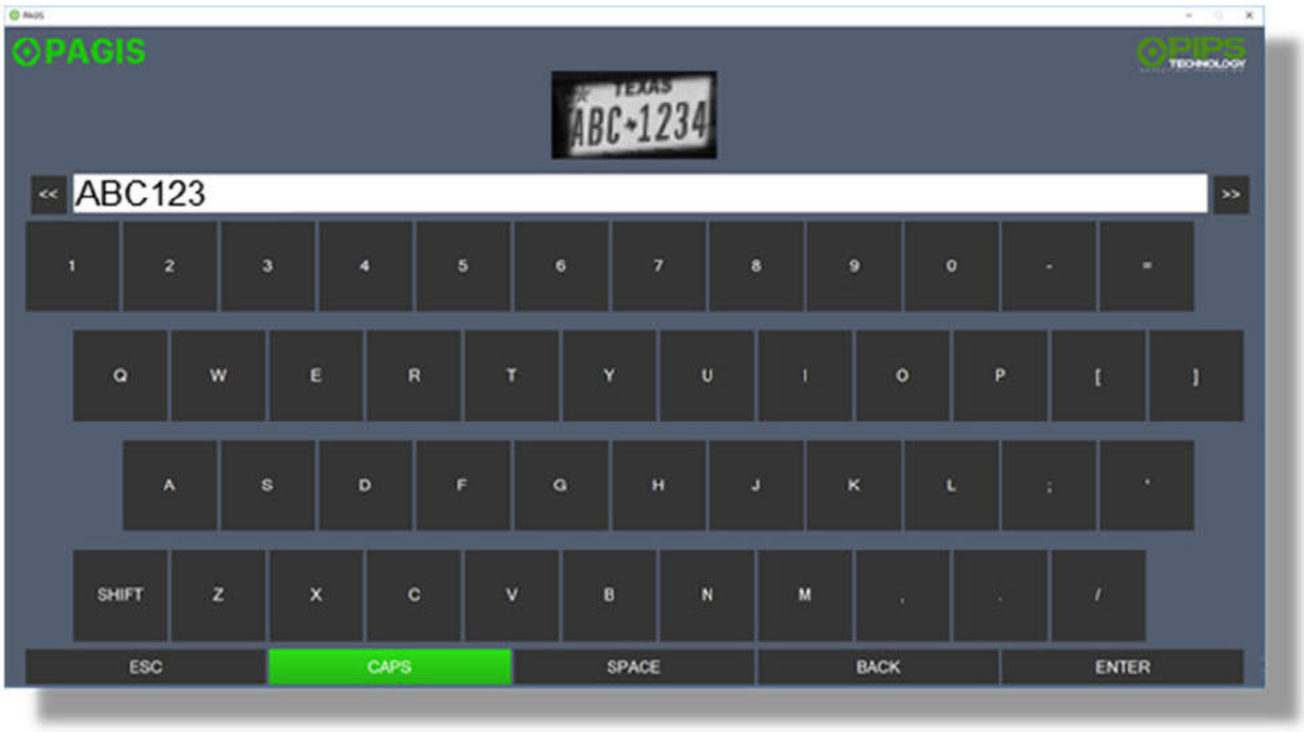
The Add Intel button launches the Intel screen. The user is prompted to assign one of four values: Towed, Arrest, Not Recovered, and Misc. by clicking the associated button at the top of the screen. The user may also enter additional detail regarding the license plate/vehicle. After clicking the Save button, the intel will now appear in the Hits Screen text box.



2.9.5 Misreads

PAGIS allows the user to mark Reads and Hits with incorrect OCR translations as a Misread. This is most commonly done by Agencies for Hits only as users typically don't have time to review every single Read from their shift. Once an errant Hit is corrected, the system updates the record to show it as a Misread and thus improves Agency Hit Reporting.

Correcting a plate read can be accomplished by clicking on the "OCR Patch" in either the Hits or Reads review screen. When the user clicks on the OCR Patch, the OCR Edit Screen opens and allows the user to update the Vehicle License Plate (VLP) data.



2.9.5.1 Marking a Record as a Misread:

The user can mark a record as a Misread from both Reads or Hits Review Screen. Each user can either simply flag the record as a Misread or update the OCR Patch information. **NOTE**: This ability is only available until the user has performed an End Shift function.

Manually Flagging a Read or Hit as a Misread:

1. Navigate to either the Reads or Hits Review Screen
2. Click on the Misread button on the Right
3. Click Save
4. Take note that the record title has now changed from “Read” to “Misread”

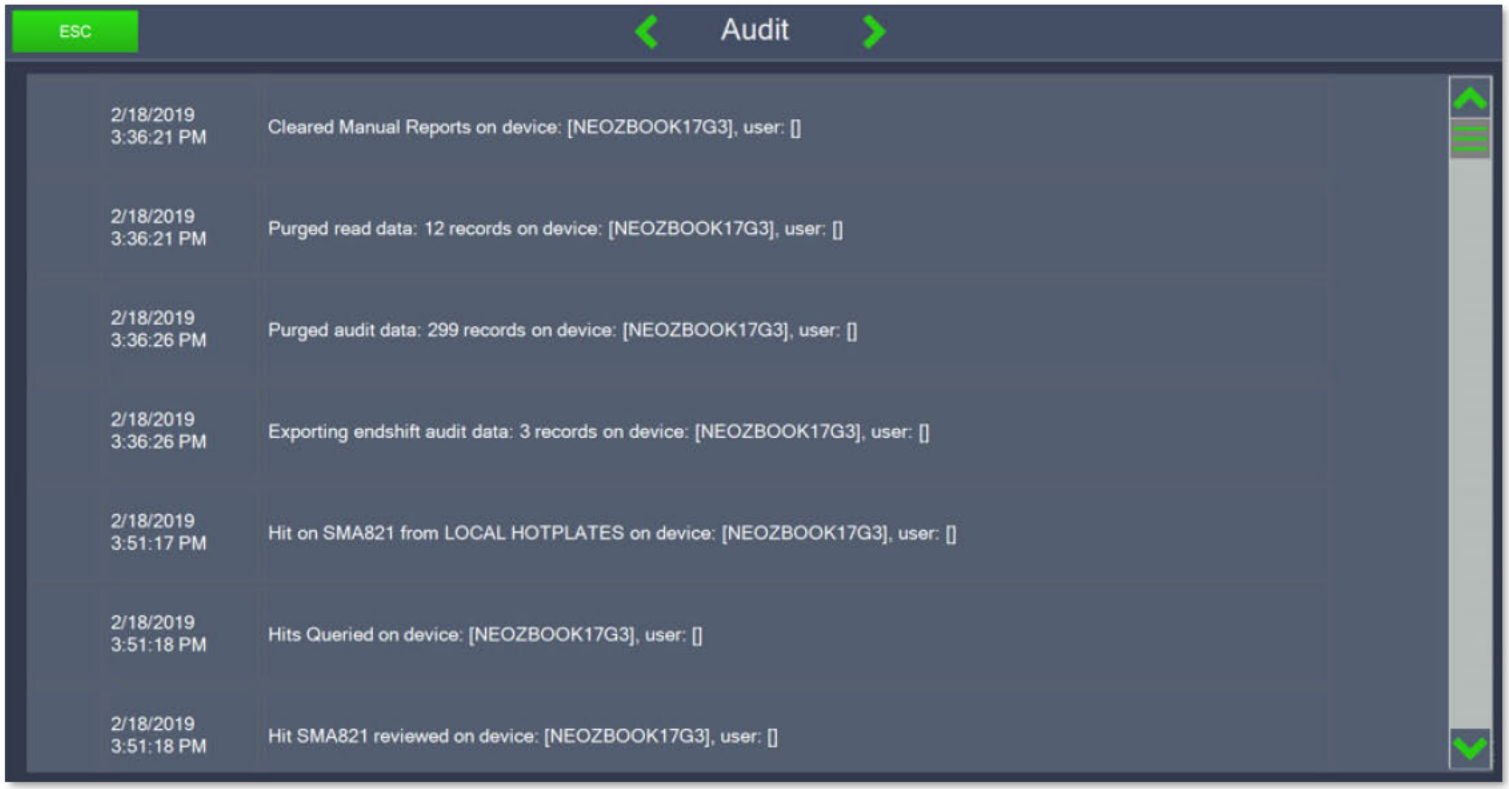
Updating the Read/Hit OCR Patch:

1. Navigate to either the Reads or Hits Review Screen
2. Click on the OCR Patch (Text just under the IR Plate Image)
3. Use the keyboard or on-screen keypad to update the Vehicle License Plate Number
4. Click the Enter Button to Save the changes (and exit back to the Review Screen)
5. When the user saves the changes to the OCR Patch, the record (Read/Hit) is automatically flagged as a Misread

2.9.6 Audits

PAGIS logs both user and key system activity during each use of the software. The audit log captures various information like Read searches, synchronizations, hits, and user login attempts. The Audit Report is viewed in PAGIS by navigating to the Review section and selecting “AUDITS”.

NOTE: Performing an End Shift or syncing the database clears the current log.



2.9.7 Targets

PAGIS has the ability to display information regarding Persons of Interest in response to a Hit alert. Targets are created by BOSS/Hotlist Administrators, and typically provide detailed information about owners of a registered vehicles. When configured, Target data is always linked to unique VLP data (a specific License Plate). If PAGIS registers a Hit on a Plate with a target ID, the Target Information Button is displayed in the Hit Alert window and allows the user to access the Target Screen.



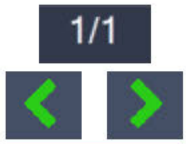
2.9.7.1 The Targets Screen

When a PAGIS user clicks the Target Information Button from a Hit Alert, the Targets Screen opens. This screen displays the information from the BOSS server about the Person(s) of Interest matched to the Hit (license plate).



2.9.7.2 Targets Screen Navigation Buttons

If a Hit alert has more than one Target associated with it, the PAGIS user can navigate all Target information with the buttons described below:



Target Count: The left number is the current record. The right number is the total available for review.

Next/Previous button: Arrows on either side of the target count allow the user to navigate back and forth to review the various targets.



Jump button: Allows the user to "jump" to a specific record without the need to navigate one record at a time using the Next/Previous buttons.

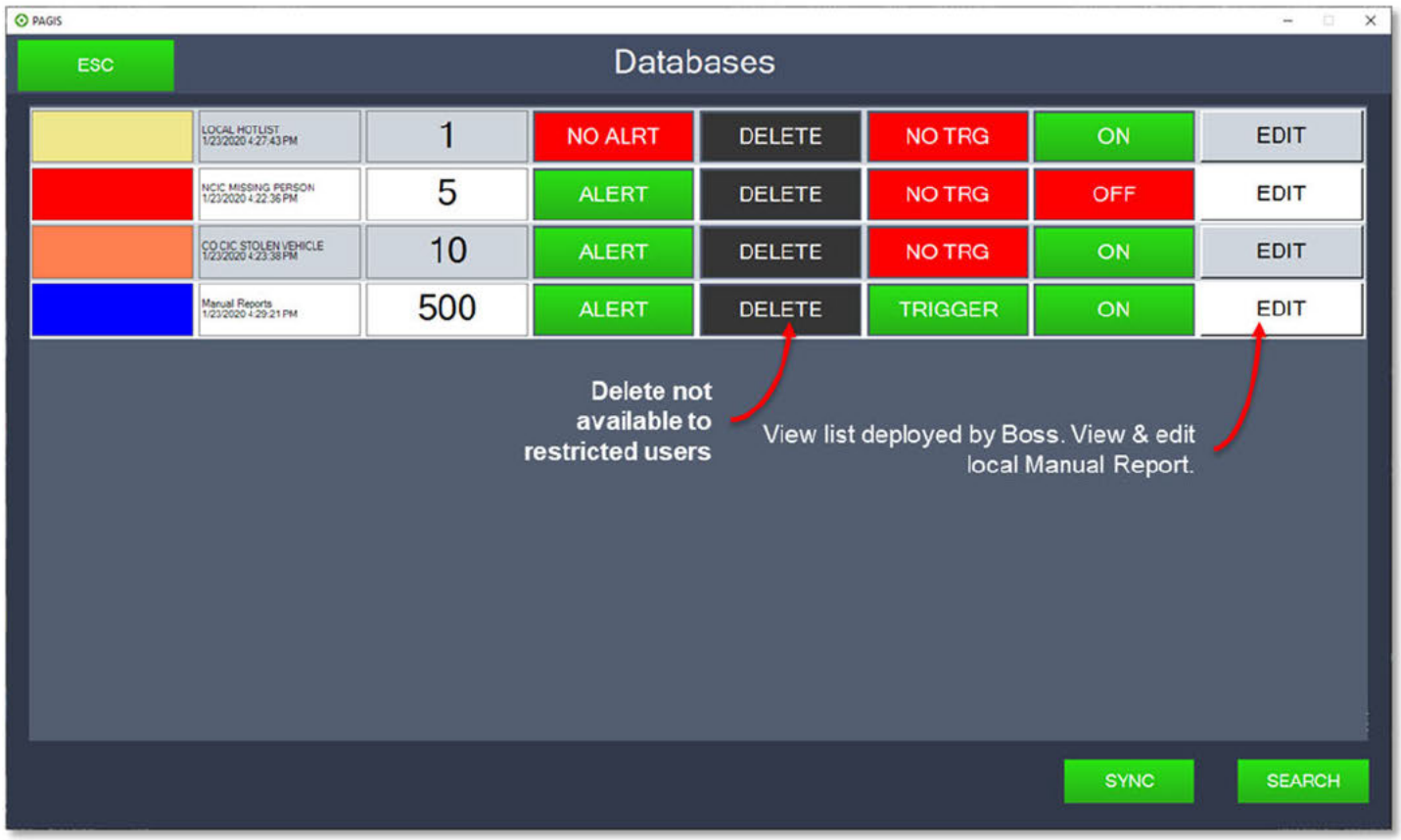


Close button: Returns the user to the previous screen.

2.9.8 Databases

Users can review Hotlists in PAGIS by navigating to the Review section and selecting "DATABASES" on the right. From the Databases Screen, users can toggle Hotlists functions On and Off based on their rights.

NOTE: User rights and Hotlist attributes are configured in BOSS.



2.9.8.1 Databases Screen Functions

Hotlist Color Code: The color attributed to each Hotlist by the BOSS Administrator.

Hotlist Name: The name of the Hotlist given by the BOSS Administrator. Also shows the time/date of the last synchronization.

Hotlist Priority: The priority of the Hotlist assigned by the BOSS Administrator. The lower the number between 1 and 999, the higher the priority. If a plate resides on multiple Hotlists, the list with the higher priority will be displayed first.

Alert Button: Toggles audible alerts On and Off for each Hotlist until the next synchronization.

Delete Button: Based on user rights, allows the user to temporarily delete a Hotlist from PAGIS until the next synchronization. To delete a hotlist, the user must click the button twice (it turns green and then deletes the list).

Trigger Button: Toggles external triggers On and Off. An example of an external trigger is a light bar.

On/Off Button: Disables and enables each Hotlist (each Hotlist is set to On by default).

Edit: View and edit localy created hotplates with a given hotlist, Hotlist/Hotplates deployed via BOSS can only be viewed.

NOTE: Hotlist settings altered in PAGIS will be reset to their default configuration during the next Sync or End Shift. The default configurations are assigned by the BOSS Server/Administrator.

2.9.8.2 Databases Screen Navigation Buttons

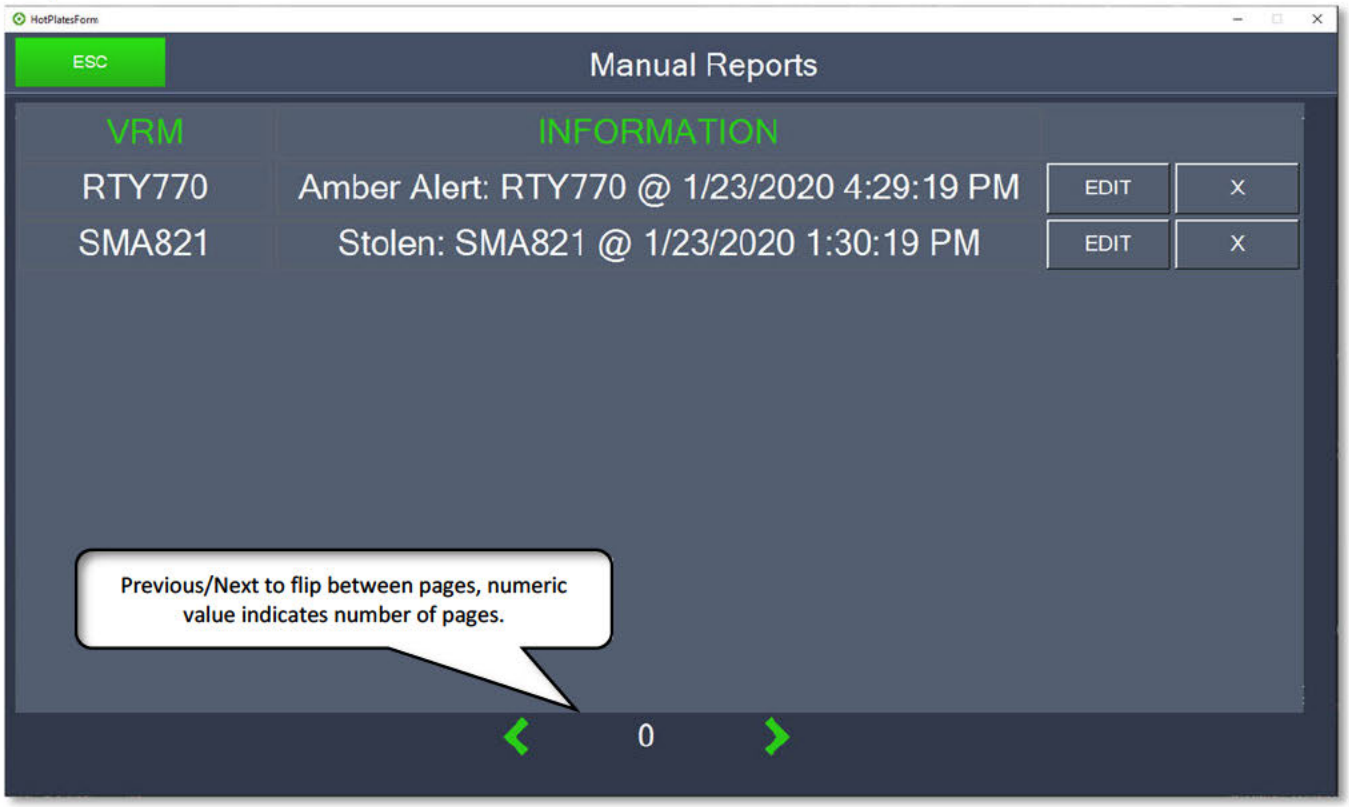
SYNC — **Sync button**: Synchronizes PAGIS with the BOSS server in order to update the Hotlists.

SEARCH — **Search button**: Open the Search Entry Screen (See section 2.8 for more information).

2.9.8.3 Databases Edit- “Manual Reports”

Editing Hotlist has two function based on origin of hotlist.

- Hotlist deployed to PAGIS via BOSS cannot be edited, only the hotplates list can be viewed. Editing/updates are indented to be managed via BOSS.
- Hotlist created in PAGIS, i.e. “Manual Reports” can be managed by PAGIS users, allowing for changes or deletion of the hotplates contained within the hotlist.



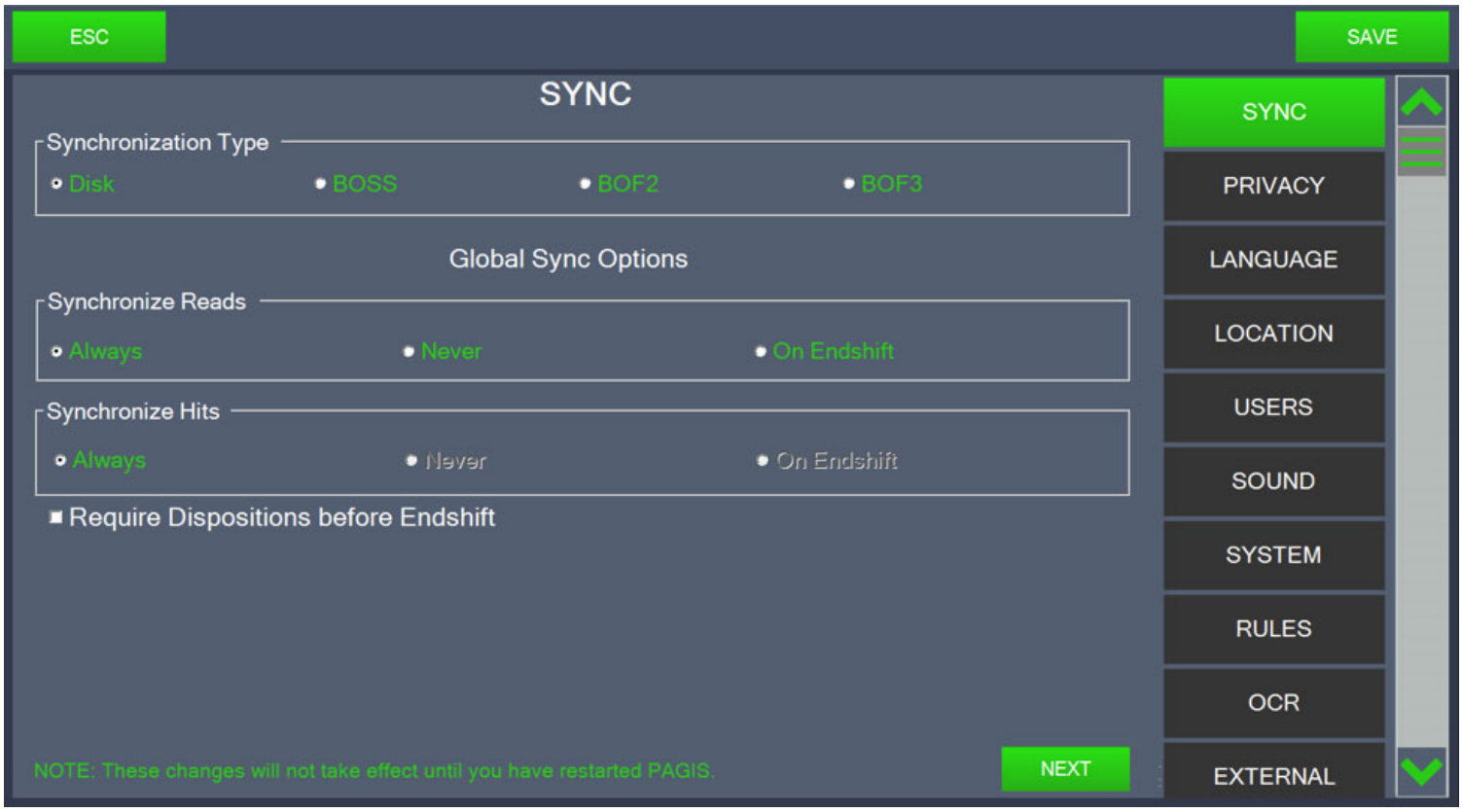
EDIT Button: Make changes to the indicustly hotplate information including licanse plate nuamber.
X Button: Remove indivualy hotlist from hotlist.
Previous/Next Button: Scroll thought lising of hotplates contaned within the hotlist. The numeric value indicates the number of pages.

ADMIN SETTINGS

The Settings Menu is the central location for configuring PAGIS Software functions endpoint by endpoint. Users with Admin level rights in PAGIS can see and click on the Settings Button from the Live View Screen. Launching Settings opens the menu to the Sync Options Screen by default. **NOTE**: Users without Admin level access will not see this icon on the Live View Screen.

3.1 Sync Options Screen

As mentioned previously in sections 2.4 and 2.5, PAGIS uses various sync options to store, update, and synchronize ALPR data to and from the BOSS server. On the Sync Screen, Administrators configure the synchronization method and options.
NOTE: Configuration changes will not take effect until they are saved and the PAGIS Software has been restarted.



3.1.1 Synchronization Types

- **Disk**: Uses local storage of Sync files in conjuction with a USB flashdrive to manually Sync to and from BOSS.
- **BOSS**: Uses a wireless data network to Sync files to and from the BOSS server.
- **BOF2**: Used predominantly in Europe (see regional guide for support).
- **BOF3**: Used predominantly in Europe (see regional guide for support).

3.1.1.1 Synchronization to Disk (Local Storage)

4842

Sync to Disk is a manual two-part process most commonly used with a USB Thumb drive. To use Begin Shift, the user accesses a centralized terminal (Ex. Patrol Room PC) to download the files from BOSS and then inserts the Thumb drive in the laptop to perform Begin Shift. At the end of the day, the user then Performs End Shift from the laptop/MDC connected to the Thumb drive and uploads those files to BOSS via the central terminal (See the "Client Tools" section of the BOSS Manual).
NOTE: From the Sync Menu, select "Disk" and click the Next button at the bottom to configure the drive location.

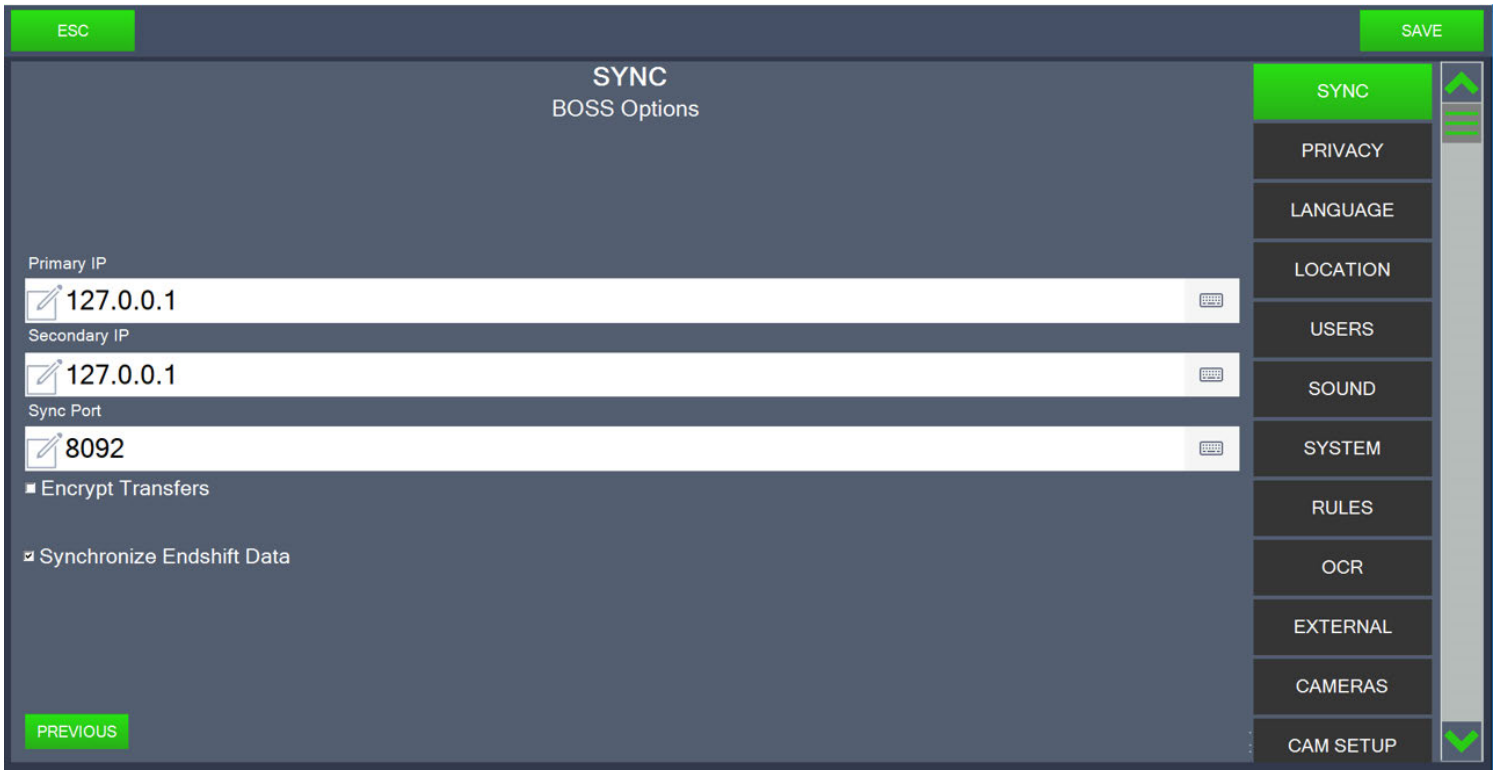


- **Delete Beginshift Data on Sync**: The sync folder on the Flash Drive is deleted once all Begin Shift data has been imported to PAGIS. This is on by default to help prevent false alerts.
- **Encrypt Endshift Data**: All uploaded End Shift data created in PAGIS is encrypted. This is off by default.
- **Copy Endshift Data on Sync**: If unchecked, no End Shift data will be transferred from PAGIS to the Drive location.
- **Keep Only Updated Databases**: Removes any Hotlists from PAGIS that were not updated during Begin Shift as "outdated". This is off by default.

Sync to Disk Setup:
In the text box, enter the drive path or letter to be used with Disk Sync. Folder name is not required as PAGIS creates the required folder(s). Once entered, select the desired options and then click the Previous button. Click Save to retain the settings.

3.1.1.2 Synchronization with BOSS

Sync to BOSS is a streamlined method for updating ALPR data to the field units and the server. Additionally, selecting this option enables the PAGIS auto-sync features that synchronize data throughout the shift without user involvement. However, this does require a stable data connection as well as some network configuration before it can be utilized.



Sync to BOSS Screen:

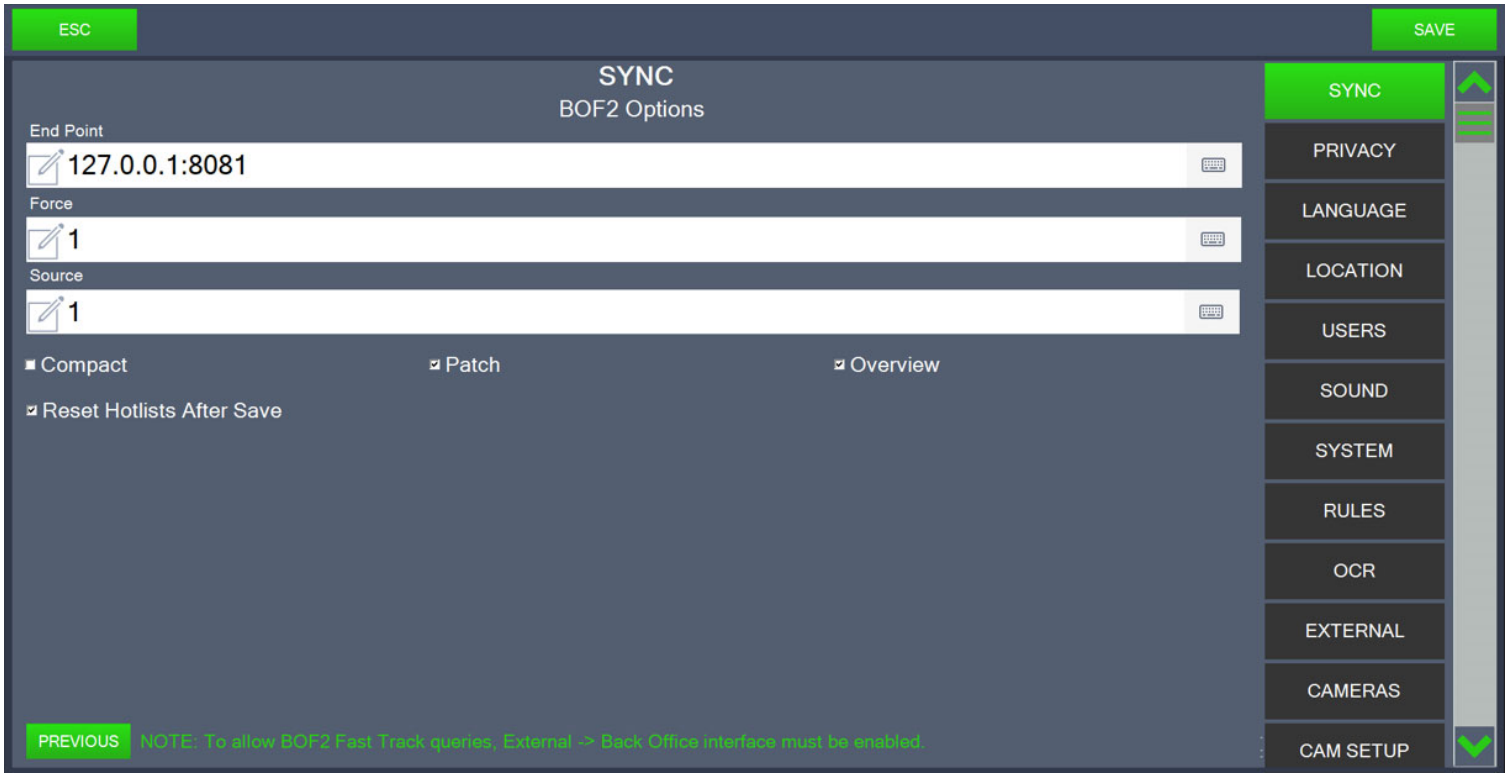
- **Primary IP**: The IP address of the BOSS server. This can also be the DNS name (**NOTE**: using DNS adds an additional failure point via the Domain Controllers and is not recommended as the best option).
- **Secondary IP**: Used for a secondary IP in cases where users switch from a cellular network to a Domain APN thus routing to BOSS from either an internal or external IP. This field can be left blank or with the primary IP as well.
- **Encrypt Transfers**: When enabled, data transfers to BOSS will be encrypted.
- **Synchronize Endshift Data**: On by default, this enables PAGIS to sync to BOSS when End Shift is performed by the user.

Sync to BOSS Prerequisites:
To establish the wireless sync to BOSS, the Agency Network Administrator will need to open TCP 8092 to the BOSS server as well as define the internal and/or external IP address(es).

Sync to BOSS Setup:
From the Sync Settings Menu, the Admin must select the BOSS option and click the Next button. Then s/he will update the Primary and Secondary IP fields as necessary and de/select any options. Once configured, click the Previous button and then click Save to retain the changes. (For more information on PAGIS Auto-Sync settings, refer to section 2.4.3)
NOTE: After synchronizing to BOSS, data is flagged in the database to prevent duplicate values on future synchronizations.

3.1.1.3 Sync to "Instation" (Formerly BOF2 and BOF3)

The Instation software was formerly known as BOF2 & BOF3 and was developed by Anite PLC. It is a web-based Back Office software suite used in European markets to provide similar features as the PIPS BOSS server and UI Client.
NOTE: These options are NOT used in the Domestic United States.

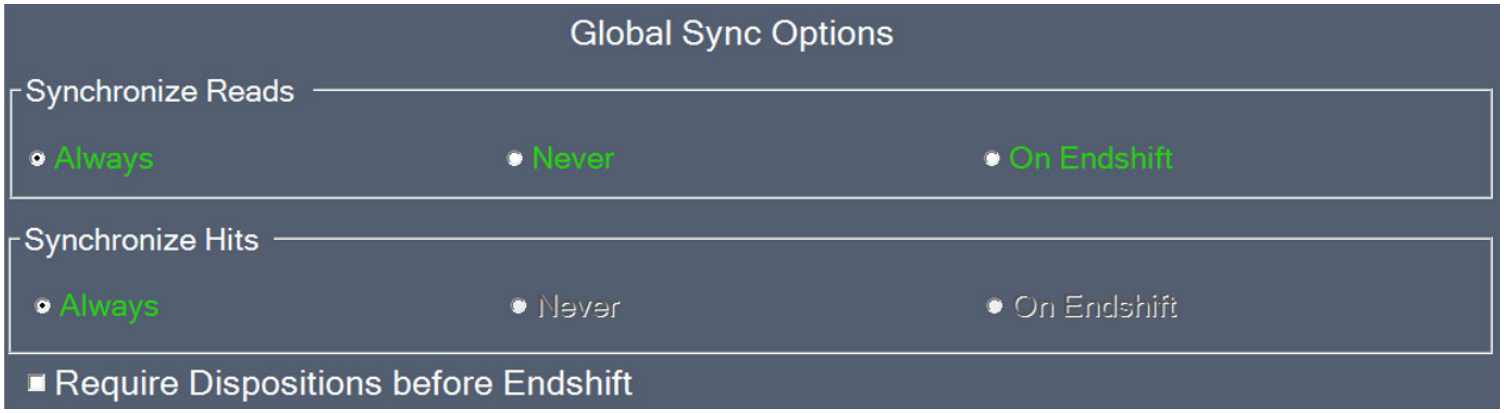


- **End Point**: The IP Address of the Instaion website. Format must be [IP Address:Port]
- **Force/Source**: Unique codes assigned to each police force.
- **Compact**: This option minimizes data transfer to Instation. Images will be deselected by default when in use.
- **Patch**: Refers to the image of the plate pulled from the read. This is on by default.
- **Overview**: Refers to the color overlay image from the read. This is on by default.
- **Reset Hotlists After Save**: When the software syncs to Instation, this will reset the hotlist tracking.

3.1.2 Global Sync Options

4844

Global Sync settings control how PAGIS synchronizes ALPR data during Begin and End Shift cycles and applies to both manually launched synchronizations as well as Auto-Sync functions. The two sections are Synchronize Reads and Synchronize Hits.



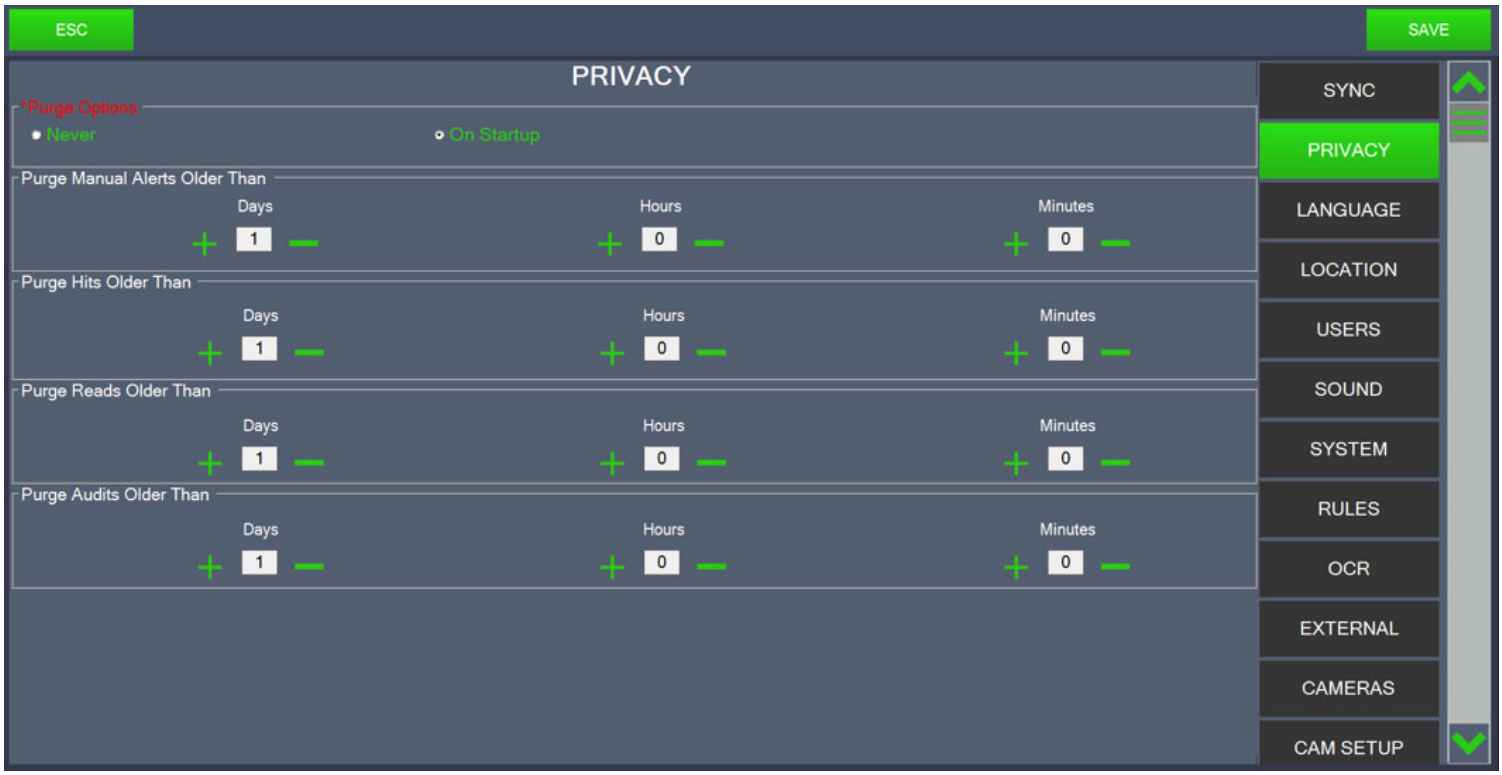
NOTE: All Hits are Reads, but not all Reads are Hits. A "hit" is a read that coincides with an Alert List. Due to this, the Options selected in the "Synchronize Reads" section dictate what options are available in the "Synchronize Hits" section. Unavailable options are greyed out.

- **Always**: Reads and Hits are synchronized to BOSS as close to real-time as the data network and PC processing allow.
- **Never:** The information gathered during the shift will be "sanitized" with each launch of End Shift. The corresponding data and images will NOT be sent to the BOSS server.
- **On End Shift**: Synchronization to BOSS will only occur when the user manually launches End Shift.
- **Require Dispositions before Endshift**: Requires the user to select a disposition code for each Hit registered in the PAGIS software since the last End Shift was completed before the Synchronization is processed.

3.2 PAGIS Privacy Settings (Local Data Retention)

4845

Although most commonly configured in BOSS, the PAGIS Software allows the Admin to configure the data retention settings for the local endpoint by minutes, hours, or days. This feature ensures the data captured/stored on the MDC is sanitized by the software itself (this is important for customers without BOSS). **NOTE**: To enable the Privacy settings, the Admin must select the "On Startup" purge option and then set at least one value in each row. Rows left with all Zero will not be sanitized or purged.



- **Never**: Selected by default, this option disables the PAGIS privacy settings and uses only those set in BOSS.
- **On Startup**: This option must be selected in order to enable the PAGIS privacy settings. Once enabled, PAGIS looks to purge/sanitize the system each time it's launched or restarted.
- **Purge Manual Alerts Older Than**: Controls how frequently all of the Databases/Hotlists in PAGIS are purged. The purge rate is calculated from the timestamp of the Hotlist. Once the retention value is surpassed, the Hotlist is deleted. Hotlists distributed from BOSS will be re-downloaded on the next Sync.
- **Purge Hits Older Than**: Controls how frequently all Hits in PAGIS are purged. The purge rate is calculated from the timestamp of read. Once the retention value is surpassed, the Hit is removed the next time PAGIS is restarted.
- **Purge Reads Older Than**: Controls how frequently all Reads in PAGIS are purged. The purge rate is calculated from the timestamp of read. Once the retention value is surpassed, the Read is removed the next time PAGIS is restarted.
- **Purge Audits Older Than**: Controls how frequently all Audits in PAGIS are purged. The purge rate is calculated from the timestamp of audit. Once the retention value is surpassed, the audit is removed the next time PAGIS is restarted.

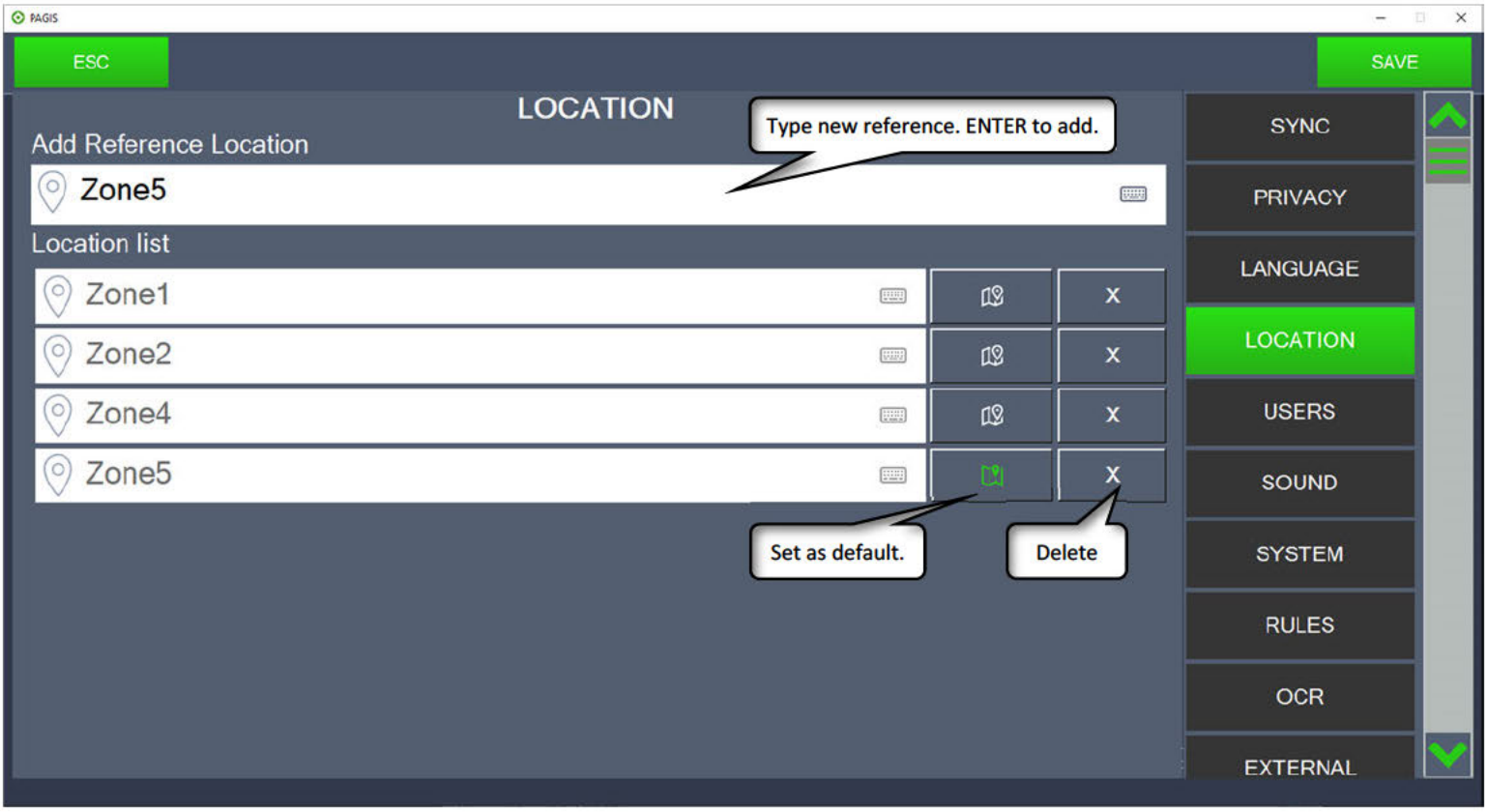
NOTE: Once the hits, reads, databases, or audits have been purged, they can no loner be viewed in the PAGIS software.

3.3 Language

The Language screen allows the Admin to change the language assignment used in the PAGIS Software. Available languages are listed in the drop-down list and are added during the installation process.

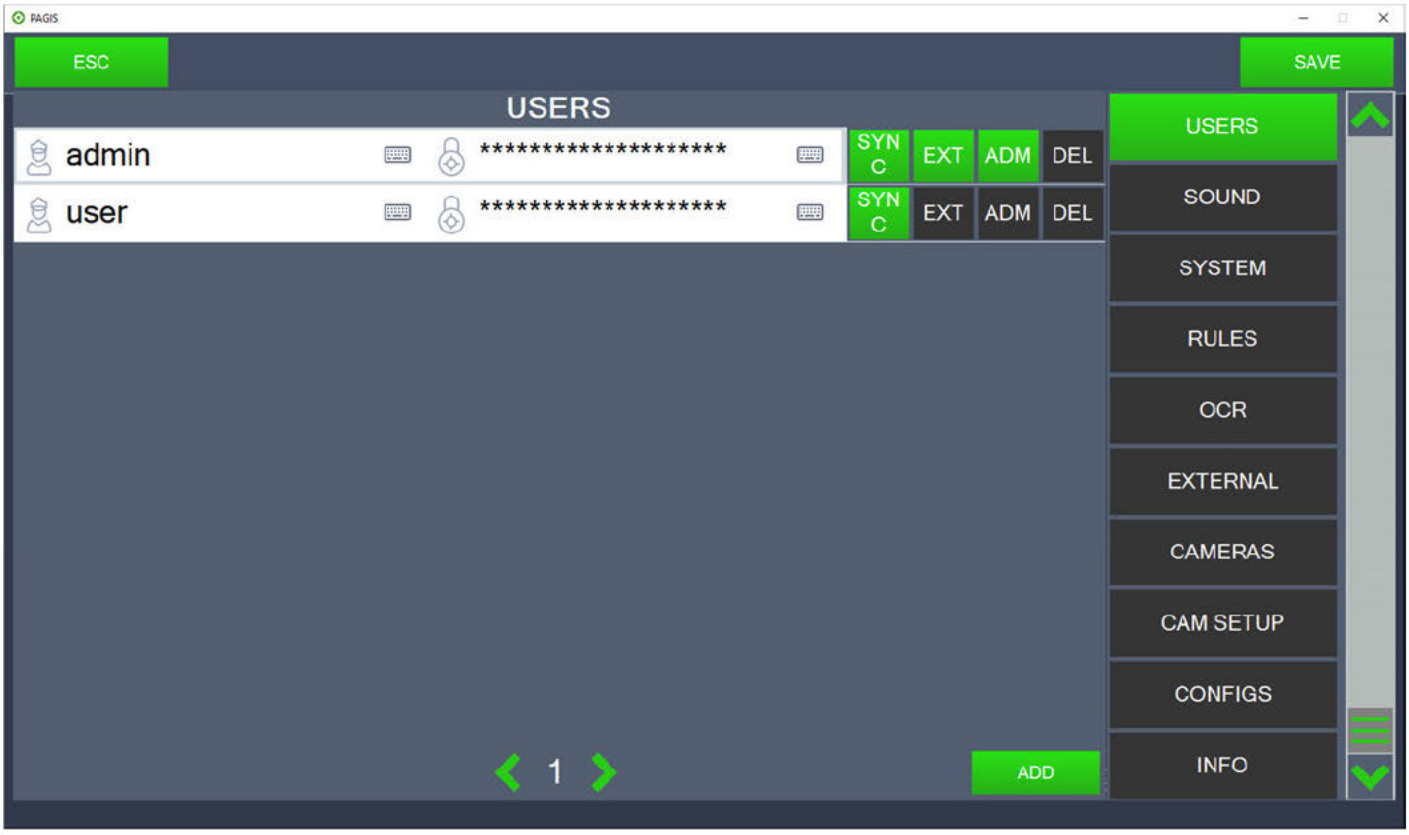
3.4 Location

Updates to the location field will auto-fill the “Reference” section of the PAGIS Login Screen. These are often used to specify a patrol region (Examples: “North Patrol” or “A2”). Once designated all reads/hits will show this designation. Muiltiple “Referance” location can be added, the available list can then be selected from the login screen.



3.5 Users

User accounts, credentials, and rights are generally administered from BOSS and then distributed to the MDC. However, PAGIS does allow for Administrators to add and delete users as well as set their privileges directly from PAGIS.



NOTE: Adding user directly in PAGIS should be limited to customers not utilizing a BOSS server. User accounts created directly in PAGIS by customers with BOSS will be overwritten/removed during the next sync.

Adding a User in PAGIS:

1. From the Admin Screen, select the Users Button on the Right
2. Click the Add Button ADD
3. Enter the case sensitive username in the Username Field (max of 15 alphanumeric characters)
4. Enter the case sensitive password in the Password Field (max of 15 alphanumeric characters)
5. Select the User's privileges
6. Click the Save Button SAVE

3.5.1 User Privileges

These are the "rights" the new user will have in the PAGIS software (When selected, each button turns green).

SYNC — **Sync:** Allows users to synchronize data.

EXT — **External**: Allows the user to access external databases.

ADM — **Admin**: Provides the user Admin rights and allows him/her to configure the PAGIS Software.

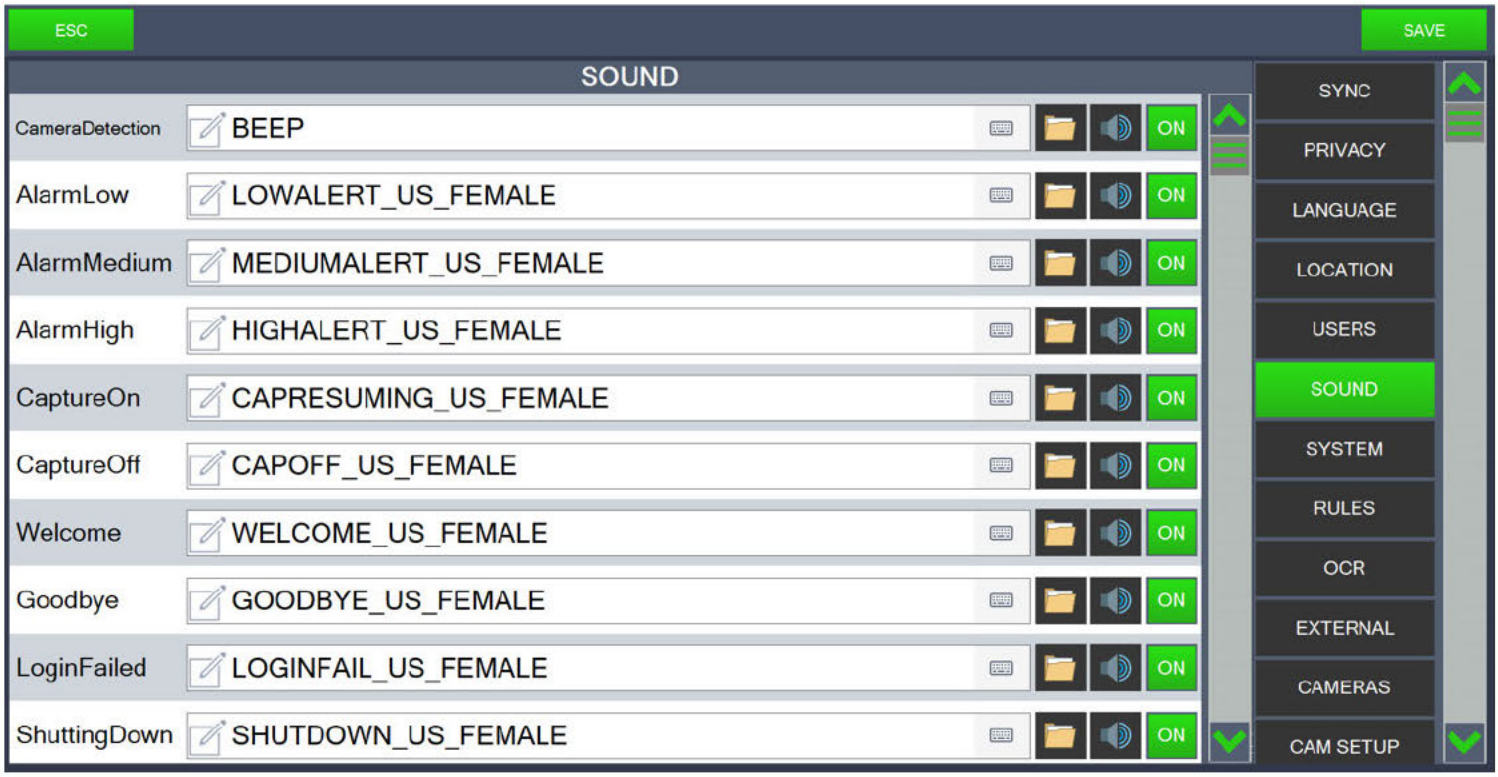
DEL — **Delete**: Allows the Admin to delete a User from the list. Click once to select and the save button to delete.

NOTE: Creating a new user in PAGIS automatically deactivates the default user account settings (Section 2.1.1).

3.6 Sound

4848

Sounds in PAGIS mirror the user or software activity (Ex. Login, Audible alert from a "Hit", and Logout) and are On by default. PAGIS Administrators can adjust the sounds from the available presets and/or load unique .wav files onto each MDC for custom use. **NOTE**: The default storage path is C:\Program Files (x86)\PIPS Technology, Inc\PAGIS2\sounds



3.6.1 Configuration Buttons

The sounds listed on the configuration screen can be altered or updated by PAGIS administrators using the buttons below. **NOTE**: Changes to any sounds must be saved before they can be played in PAGIS.



Click to browse to the sounds folder. This is used to select a new sound file.



Click to Test/Play the selected sound.



Shows the status of that sound. Click to turn each sound Off.

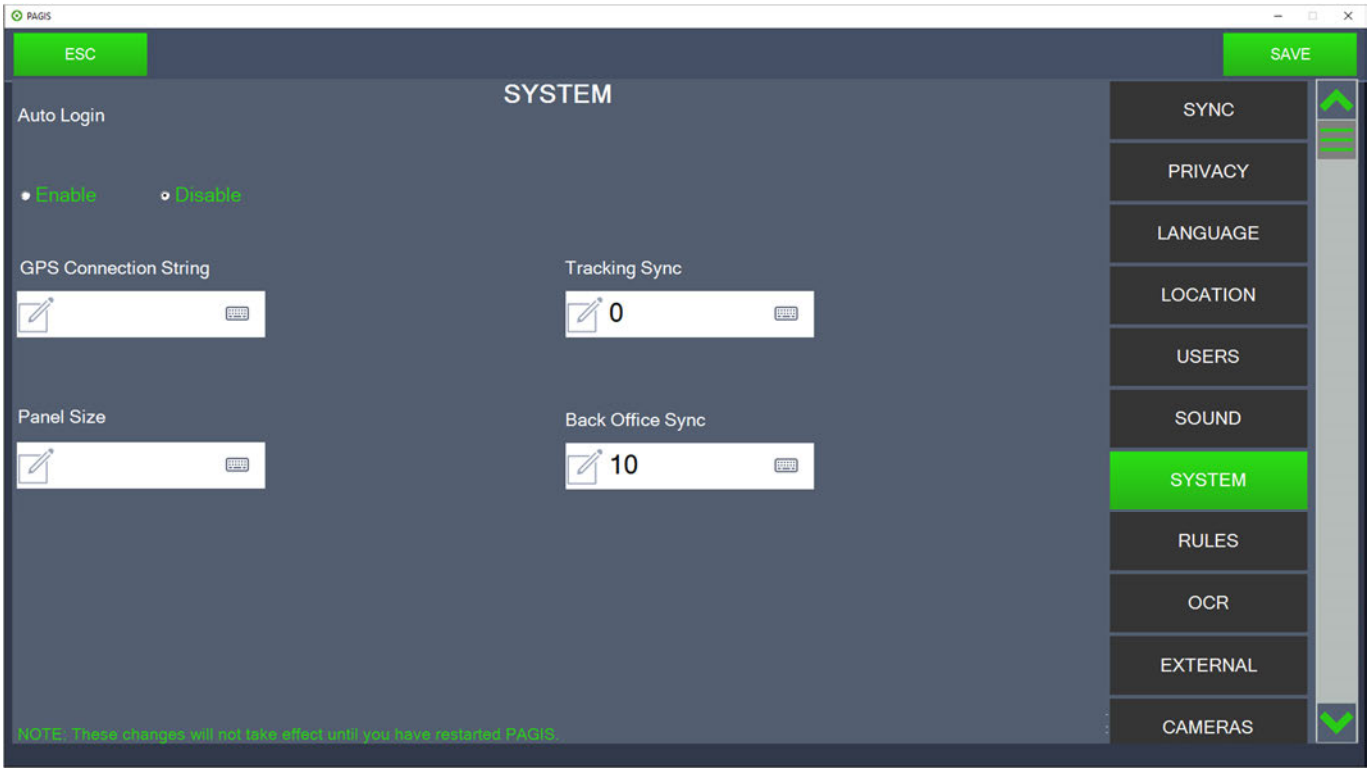


Shows the status of that sound. Click to turn each sound On.

3.7 System

4849

The System screen determines external system connections. The primary external connection is the GPS antenna. The GPS connection string will accept TCP/IP ports or COM port designations. This section also contains control of the PAGIS "Auto Login" feature (which is set to Off by default).

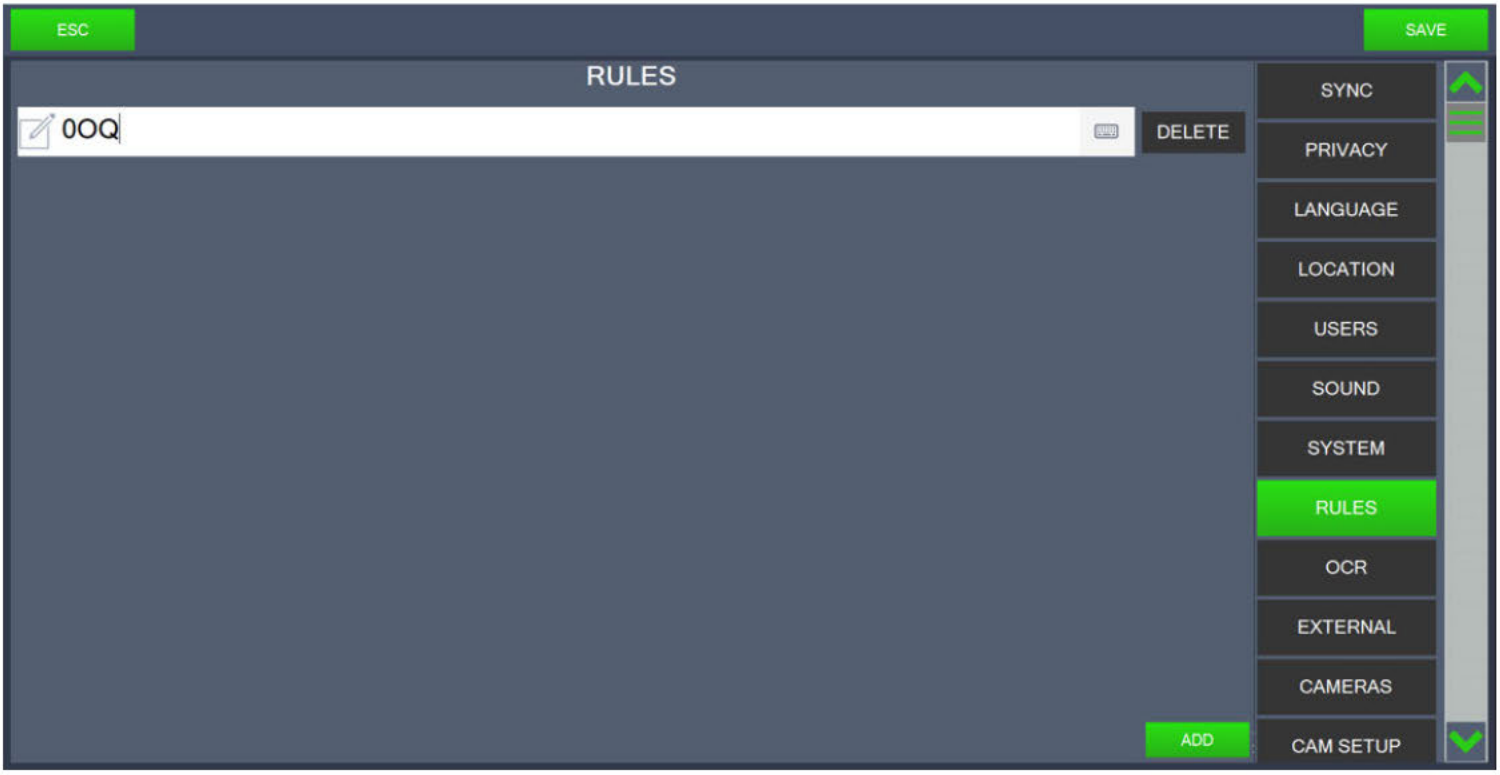


- **Auto Login**: Enabling this feature will ignore existing user account information and login to PAGIS as the Admin. This feature is recommended only for unattended use (Speed-Trailer applications and Covert Drop and Go deployments).
- **GPS Connection String**: This value is utilized by PAGIS to acquire the GPS feed from its source. The default is traditionally either blank (no entry) or 6.
- **Tracking Sync**: Controls the sync intervals in (Sec.) that PAGIS communicates with BOSS4 to update tracking status. Default off=Zero, values can range from 1-9999. BOSS4 Back Office Software requiered for this feature.
- **Panel Size**: Controls the resolution of the color image displayed on the Live View Screen. By default this is blank as PAGIS controls the aspect ratio. However a PAGIS Admin can assign custom resolutions in WxL format (720x1024) to assist with non-standard dispalys.
- **Back Office Sync**: This setting controls the sync timing that PAGIS sends data back to BOSS3/BOSS4, Timing is in (Sec.), default is 10sec, values can range from 0-9999.

NOTE: All changes must be saved and will not take effect until PAGIS is restarted.

3.8 Rules

Rules in PAGIS allow Administrators to force the software to process plate reads in specific ways. For example, in states that allow for both O and 0 (zero) on their license plates, a rule can be set to read any zero as an O and any O as a zero. This provides PAGIS greater flexibility to the standard OCR functions.



Adding a Rule to PAGIS:

1. Click the Add Button ADD
2. Enter the desired alphanumeric characters (Ex. 0 and O) into the text field
3. Click the Save Button SAVE at the top right of the screen

Deleting a Rule:

1. Locate the rule to be removed from PAGIS
2. Click the Delete Button DELETE to the right of the rule (It will turn green when selected)
3. Click the Save Button to complete the removal

3.8.1 Rules – Additional Clarifications

1. Rules are processed based on the first character entered. So in order to read any O as a zero, the Admin will need to add rule "O0". And in order to read any zero as an O, a second rule must be entered as "0O".
2. Rules are NOT designed to overhaul OCR function. Any consistently misread values should first be brought the attention of PIPS Support for review. And only those cases where further adjustments to the OCR software are impossible would rules be recommended.
3. Adding rules to PAGIS will make it less likely to miss a Hit Alert. However, it will increase the number of Hit Notifications that require the Officer to visually confirm the OCR read ("IR Patch") and the Hotlist Alert match.

3.9 OCR

The OCR Section in PAGIS provides Administrators some additional options on how they would like PAGIS to process plate reads.



- **JPEG Images**: On by default, this forces PAGIS to use compressed .JPG images instead of the full resolution Bitmap images each time a read is taken. This settings minimizes data storage requirements and preserves MDC drive space.
- **Inverse Plates**: Off by default, this setting is only used in States where plates with light color lettering over a dark background are prevalent. Enabling this option increases processing load and should remian disabled unless required.
- **Square Plates**: Off by default, this setting adjusts the read area plates that are square instead of retangular.
- **Disable Duplicate Read**: On by default, this setting helps PAGIS prevent duplicate plate reads. If a VLP is read by more than one camera within a short period, the duplicate read is ignored. This minimizes data storage requirements and improves overall system metrics related to numbers of Hits and Reads.

NOTE: Once changes are made, the Admin must click the Save Button SAVE button in the upper right corner to retain them.

3.10 External

The External Screen allows the Admin to connect PAGIS to an external database or device via XML Datastream. This feature is Off by default and any changes must be saved before they will be available.



Enabling the Datastream:

1. Click the Off Button OFF to toggle to On ON
2. Click the Save button in the upper right corner
3. Close and reopen PAGIS

NOTE: Enabling this feature will reduce the overall performance of the PAGIS Software.

3.10.1 XML Datastream Ports

Administrators will need to configure their external device or database to utilize two specific TCP ports:

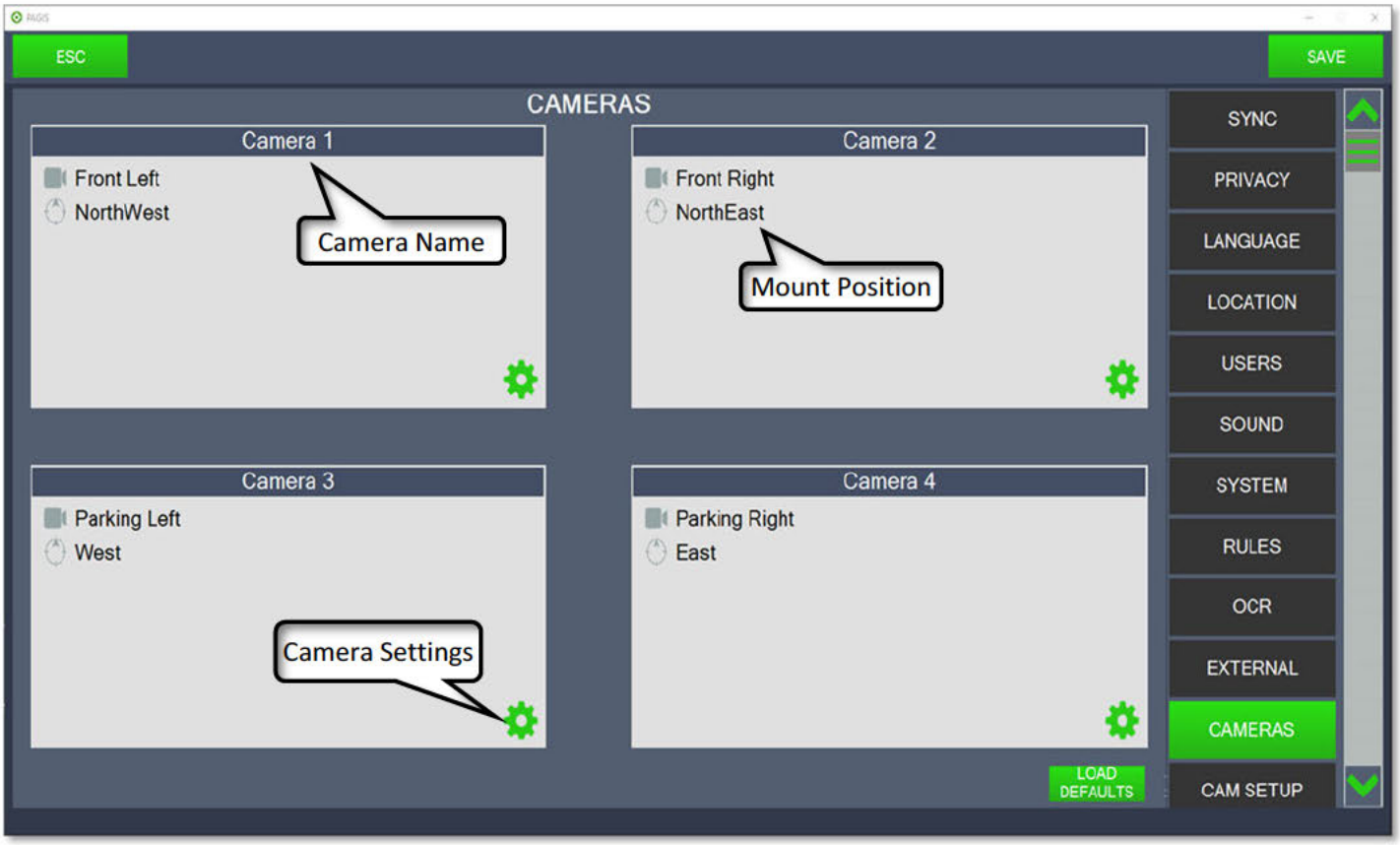
1. Query Port: TCP 7000
2. XML Datastream/Heartbeat: TCP 10100

NOTE: Greater detail on the XML Datastream can be found in Appendix D

3.11 Cameras

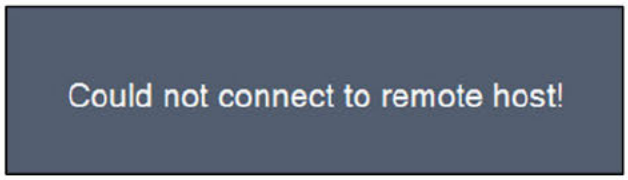
The Cameras Section provides the Administrator the means to add/delete, identify, and configure the ALPR cameras. Although the PAGIS Software comes preloaded with a default layout, best practices advise the Admin to fully review, and completely configure at least one MDC by hand in order to tailor the setup for the Agency's unique attributes.

IMPORTANT: The configuration steps completed here will dictate the available camera mode options in the Configs Section.



3.11.1 Checking the Connection

In order to configure the cameras, the PAGIS Software and the SX Processor (Black Box) must be able to communicate. If they cannot, the Administrator will receive the error message below as soon as he or she clicks on the Cameras Button CAMERAS indicating that PAGIS cannot "see" the cameras.



3.11.2 Troubleshooting Camera Connections

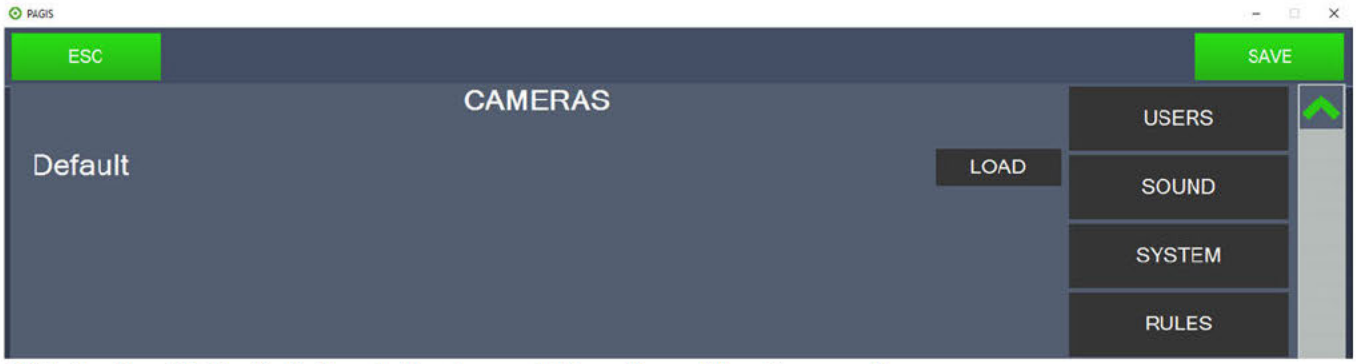
The most common troubleshooting steps have been included below for convenience. If these don't resovle the issue, please contact PIPS Support for additional assistance. **NOTE**: For more information see Appendix C – The Mobile FAQ

1. Start the vehicle and confirm power to the Processor. Confirm the SX switch, and any added in-line switch, is set to On.
2. Confirm the network adapter settings on the laptop match the proper Static IP scheme for the SX Processor in use.
3. Disable the local Windows Firewall, VPN software, and any real-time monitoring software one at a time.
4. Use a different network cable ensuring it's properly seating in NIC port on the SX as well as the MDC or Docking Station.
5. Docking Stations can also impede communication. Test by removing the laptop from thhe dock, directly connect the network cord to the laptop, and then reconfigure the network adapter settings as needed.

3.11.3 Configuring the Cameras in PAGIS

This section will assist with the general configuration of the cameras. Administrators can begin by selecting the Settings Icon to edit each of the existing cameras or by selecting the Load Defaults Button LOAD DEFAULTS. This manual will start with Load Defaults.

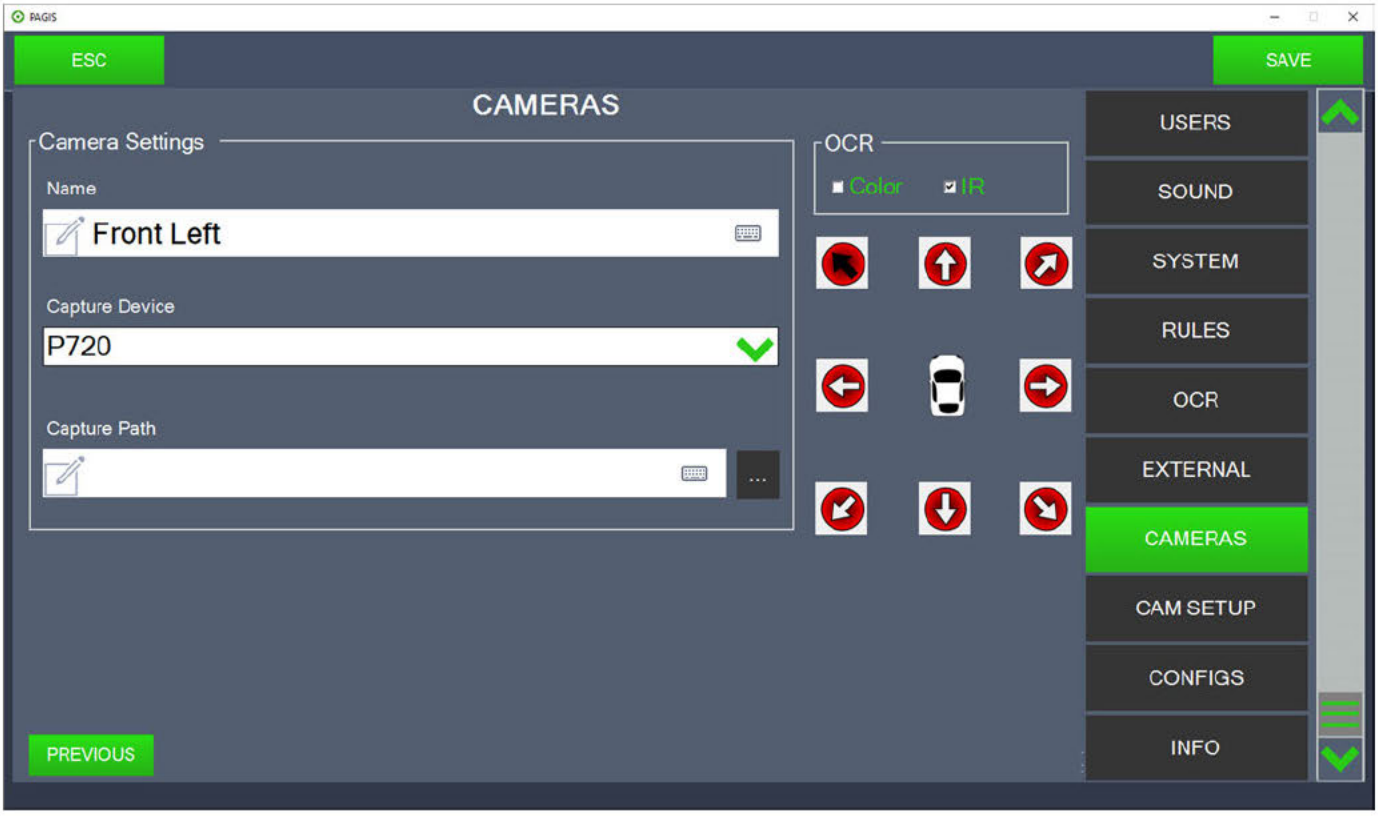
Gettings Started – Load Defaults:



1. Click the Load Defaults Button in the lower right portion of the Cameras Screen
2. Locate "Default" and click the Load Button LOAD
3. Once it's selected (and turned Green), click the Save Button (This returns the Admin to the Cameras Screen)
4. Click the Settings Icon to inspect and configure each camera one at a time

The Camera Settings (Edit) Screen:

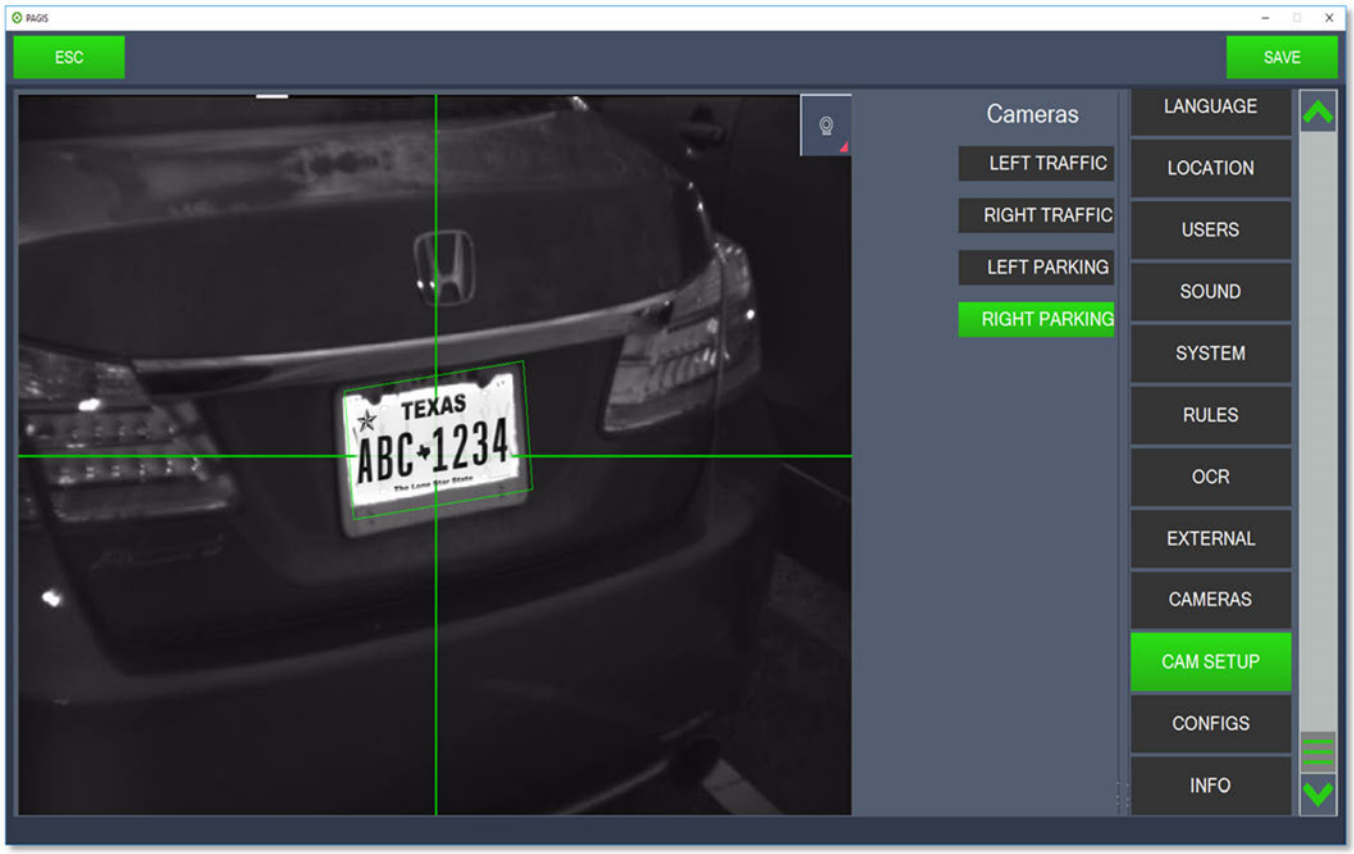
This provides the Admin a single screen to edit the name, confirm the capture device, assign camera position, and confirm OCR.



1. Confirm/Update the Camera Name **NOTE**: Use Camera Names with 11 characters or less to avoid various UI anomalies
2. Confirm the "Capture Device" field was auto-detected. If not, use the drop down to select the only Pxxx value on the list
3. Leave "Capture Path" blank (This is an optional field)
4. Select the camera mount position indicating the direction the camera is facing. The arrows turn black when selected
5. Ensure the OCR is set to IR. The color camera is used for OCR in only rare situations and will increase system load as well as the likelihood of false alerts. Use this setting with caution
6. Click the Save Button to retain the changes

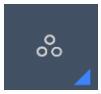
3.12 Cam Setup

The Cam Setup Screen presents Administrators with a live preview of the configured cameras. This section also allows the Admin to switch view modes from Color to IR to ensure the system is functioning properly. **NOTE**: This screen can also be utilized as a means to align newly mounted cameras when RDP access to the SX Processor is limited or unknown.



3.12.1 Cam Setup Navigation Buttons

The Admin may view the output of each camera by clicking on the camera name. When a camera is selected, the button will turn green to indicate it has been selected. In order to switch view modes, the Admin must use the following buttons:



Color View: The Color View Mode is the default view when the Admin first enters Cam Setup. This displays a live preview of the color camera.

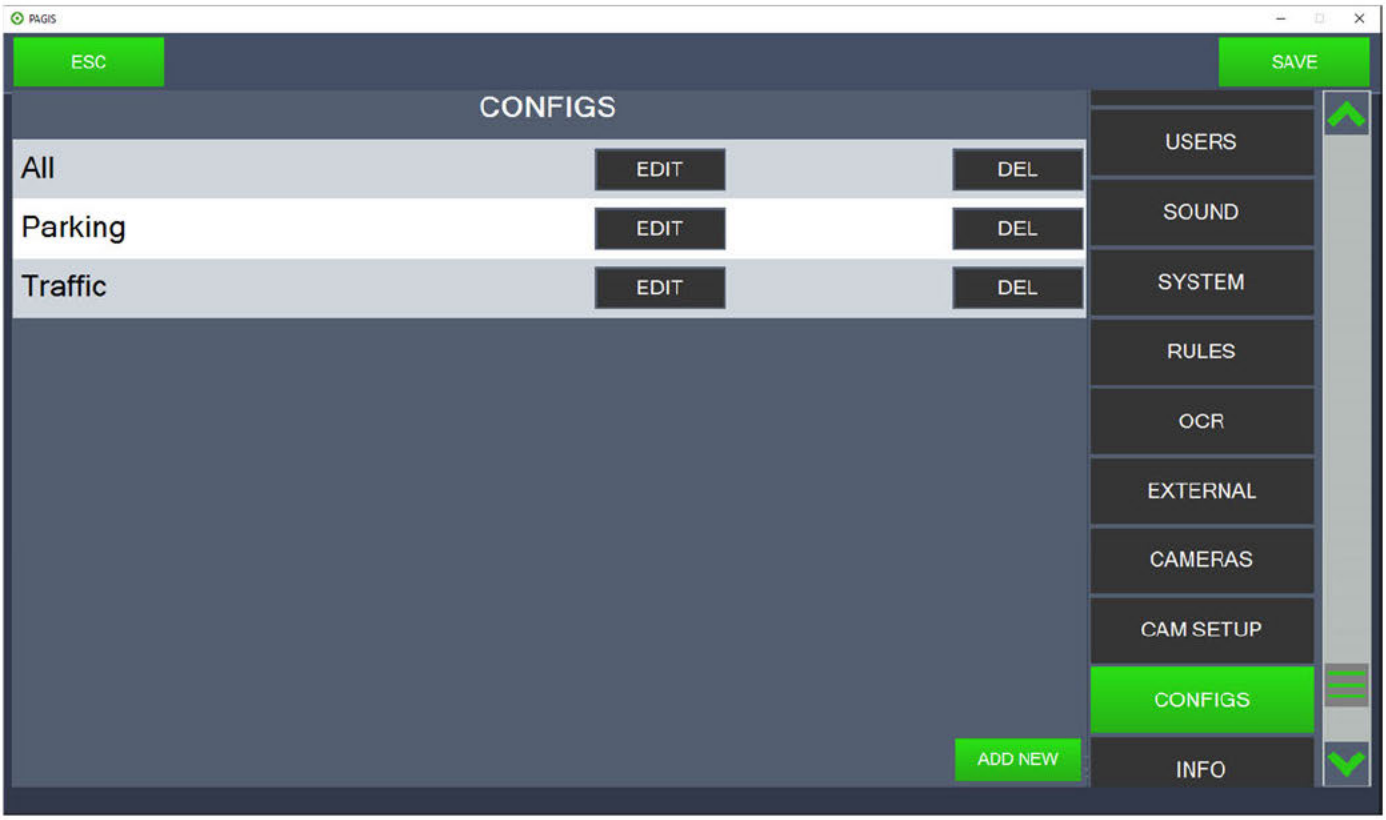


IR View: By clicking on the Camera View Selector button, the Admin will switch to the Infrared (IR) View Mode. This displays a live preview of the IR camera.

NOTE: Unlike the main Live View Screen, the camera feed shown on the Cam Setup page will not time out when in use. This feature makes it easier for the Administrator to review and align the mobile cameras.

3.13 Configs (Camera View Modes)

The Configs Screen allows the Admin to construct how the cameras will be displayed on the Live View Screen for the user. This section also allows agencies to create multiple viewing configurations to meet specific environmental needs or to add greater functionality to the software. By default, the Configs layout provides the agency with three camera modes, “ALL”, “Traffic” and “Parking”. All mode dipalys the front two cameras and rear two are activated, Traffic mode only displays the front two cameras and rear cameras are off, Parking mode only displays rear two cameras and front cameras are off.



3.13.1 Configs Navigation Buttons

To properly configure the camera modes used in PAGIS, the Admin will navigate this section with the following:



To delete a config/camera mode, click the DEL button to select it (turns Green) and then click Save



To review, edit, or modify a camera mode, click the EDIT button



To preserve changes or finalize a deletion, click the SAVE button

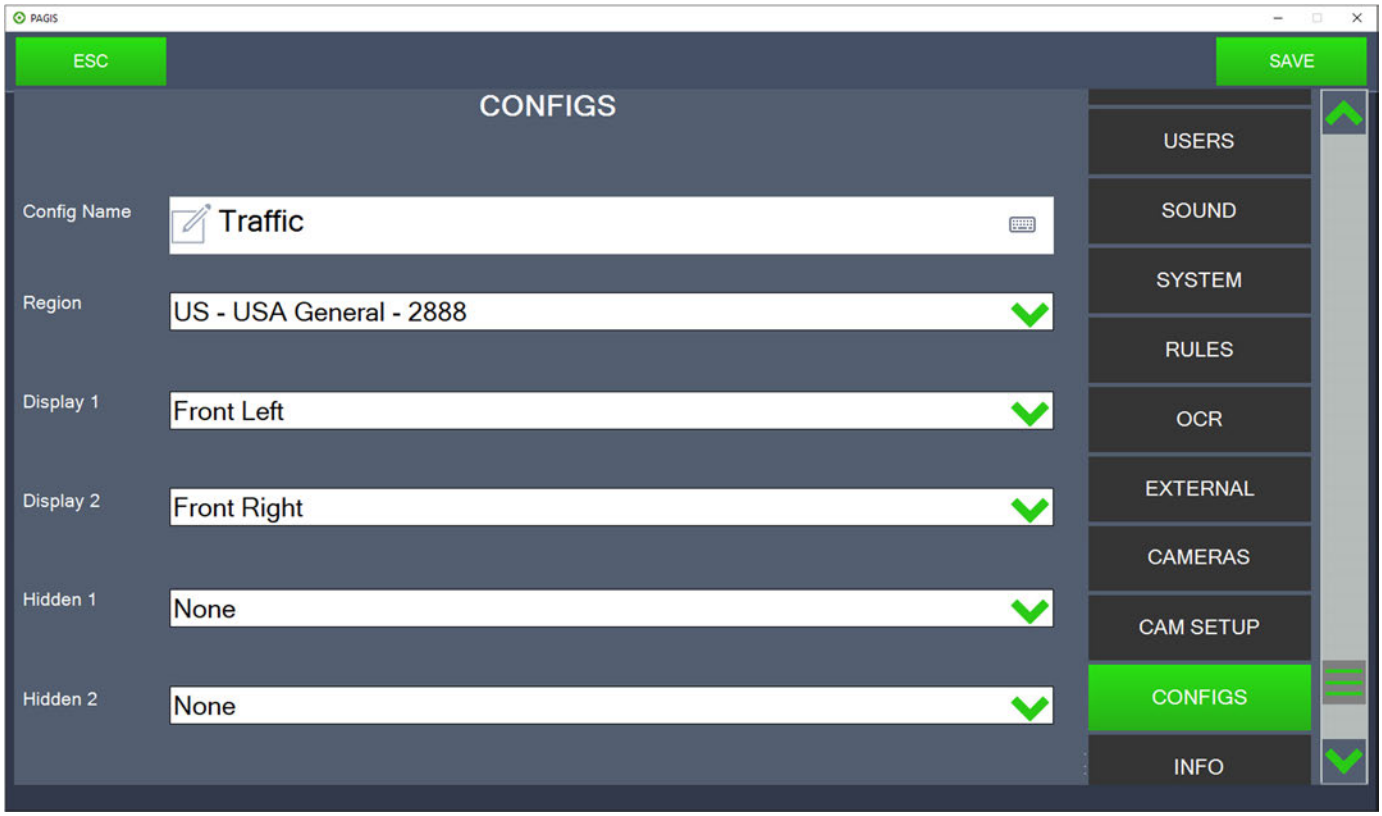


To add a new camera mode, click the ADD NEW button

NOTE: The number of Configs equals the number of Camera Modes available to the user from the Live View Screen. Each camera mode untilizes the Config name established in this section. Users cycle through the modes on the Live View Screen by clicking the Mode Selection Button in the upper left corner.

3.13.2 Reviewing and Modifying Existing Modes

When getting started, most Administrators will begin by simply modifying the existing camera modes or “configs”. The following example will demonstrate the standard configuration of a four-camera mobile unit.



1. Click the EDIT Button EDIT from the main Configs Screen to modify a mode
2. Review/Update the name of the Mode **NOTE**: The name should be intuitive for all users as this becomes the label of the mode selection button on the Live View Screen
3. Click the drop down arrow on the Region field to select the best local option (Adds additional accuracy to OCR)
4. Confirm the camera listed in the Display 1 field. This camera will be displayed on the left side of the Live View Screen
5. Confirm the camera listed in the Display 2 field. This camera will be displayed on the right side of the Live View Screen
6. Confirm the Hidden 1 field shows one of the other cameras not listed in the Display fields
7. Confirm the Hidden 2 field shows the last available camera not yet listed (Leave field as “NONE” for 3-cam systems)
8. Click the Save button to retain the changes
9. Click the Configs Button from the menu to access the other Mode(s)
10. Perform steps 1-8 for all Configs/Camera Modes available

NOTE: Cameras listed in the Hidden fields will function, perform OCR, and capture plate reads, but they will not be displayed to the user while in the named camera mode (unless a Hit is detected opening the Alert Screen). For ALPR units with more than two cameras, best practices dictate the Admin utilize these fields.

3.13.3 Adding a New Camera Mode

When the two default modes provided in the PAGIS software do not offer the agency all the functionality desired, the Administrator can use the Configs Screen to add additional camera modes. For example, if officers request a mode to view only the cameras on the left side of the vehicle while stopped on the side of the road, the PAGIS Adminstrator can build that functionality from this screen.



1. Enter a name for the new Mode (Ex. “Left Side”)
2. Click the drop down arrow on the Region field to select the best local option (Adds additional accuracy to OCR)
3. Confirm the camera listed in the Display 1 field. This camera will be displayed on the left side of the Live View Screen
4. Confirm the camera listed in the Display 2 field. This camera will be displayed on the right side of the Live View Screen
5. Confirm the Hidden 1 field shows one of the other cameras not listed in the Display fields
6. Confirm the Hidden 2 field shows the last available camera not yet listed (Leave field as “NONE” for 3-cam systems)
7. Click the Save button to retain the changes

3.14 Info

4859

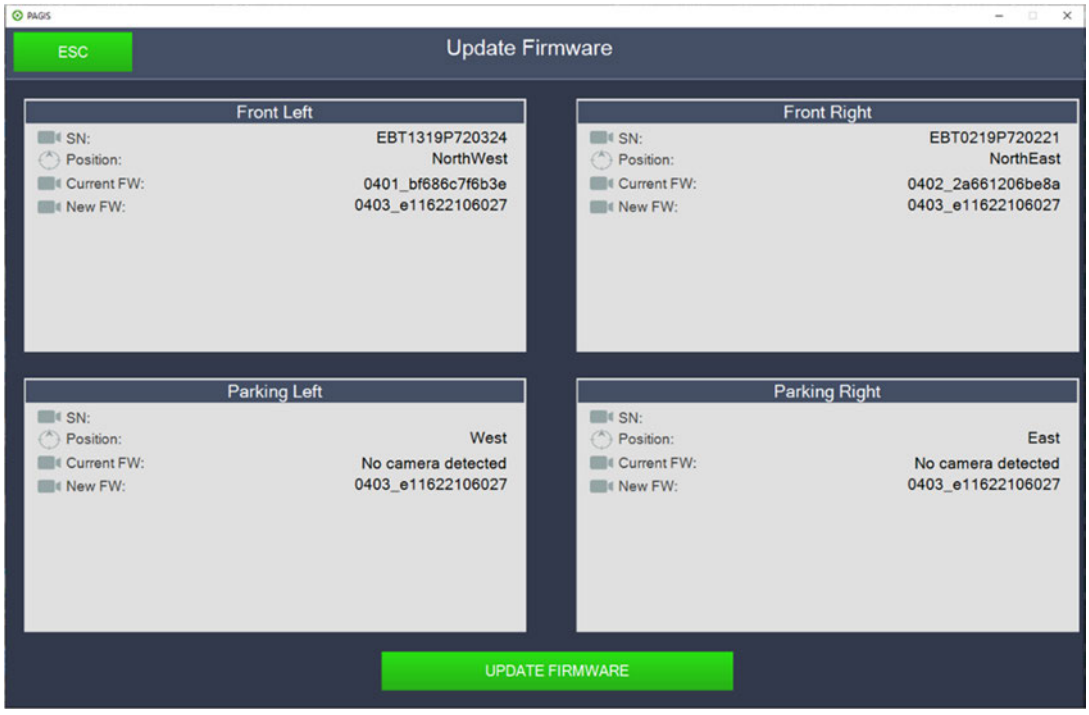
The Info screen displays additional information including the version number of the current installation. This information is helpful when contacting Technical Support.



3.15 Camera Firmware Update, (Admin)

Camera firmware update provides a means for PIPS to update the camera software to enhance and or correct camera performance. The frimware icon  will only apper when a update is avialable.

- The firmware update process only updates camera that are attached and function on the mobile processor.
- Administrator must log into PAGIS and apply the FW update. The update process takes around 4min and should not be interrupted or risk permanently damaging the cameras, PAGIS will return to normal opertaion after update.
- Once the "UPDATE FIRMWARE" button is clicked PAGIS will switch to full gray screen with message indicating "Camera Firmware is Updating", during this process you'll will notice small command windows opening on top of PAGIS, these windows represent the firmware being applied to each active camera so you may notice one or server depending. Once completed a message will appear "Firmware Updated Successfully" then PAGIS will return to normal operation.
- After FW completion and return to "Live View", its requiered to cycle thought the "Cam Mods" to refresh cameras.



Firmware Updater Window List.

- Title "Camera Name".
- Camera serial number.
- Position.
- Current FW version.
- New FW version available.

4.1 PAGIS System Requirements

The PAGIS Software requires the following minimum system requirements for the mobile data computer:

- Intel I3 CPU at 2.0 GHz or higher.
- Windows Operating System (Win7-Win10).
- Microsoft .NET Framework 3.5.
- 8 GB of RAM.
- At least 1 GB of free disk space.
- SVGA display with a minimum resolution of 800 x 600 pixels.
- Available 10/100 Ethernet port.
- Keyboard and mouse, or a touch screen monitor.
- Internet access needed for mapping and Firmware update.

4.2 PAGIS Prerequisites

Prerequisites:

1. Ability to install software.
2. Ability to configure the network adapter.
3. PAGIS 2.12 and above are only compatible with SX4 and SX4e Processors.

Network Adapter Settings:

The PIPS mobile processor operates based on a static IP and is preassigned the IP address of 192.168.200.201. When connecting laptop/MDC to the PIPS mobile processor your computer must be on the same IP network as the mobile processor, in fact the connecting compute must adopt one octet lower than the assigned IP of the PIPS processor in order for MDC installed PAGIS to connect to the mobile processor and receive data from the ALPR cameras. Below are the steps to configure your computer.

1. Navigate to Adapter Options in Windows and right click on the adapter and select properties.
2. Click to select IPv4 and click Properties
3. Click the radio button “Use the following IP Address” to set the Static IP address.
4. Enter 192.168.200.200 in “IP address” section.
5. Enter 255.255.255.0 in “Subnet mask” section.
6. Either leave the “Default gateway” blank or enter 192.168.200.201.
7. Click OK to save changes.

NOTE: The Mobile processor is pre-configured to relay its camera data connection to the .200 IP address, using alternative IP’s on Laptops will result in the software’s failure to communicate with the cameras.

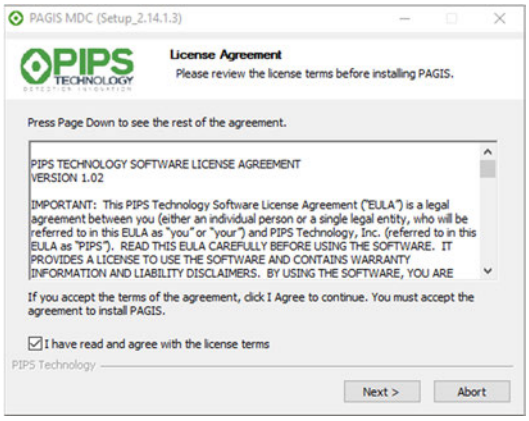
4.2.2 PAGIS Software Installation (MDC)

4861

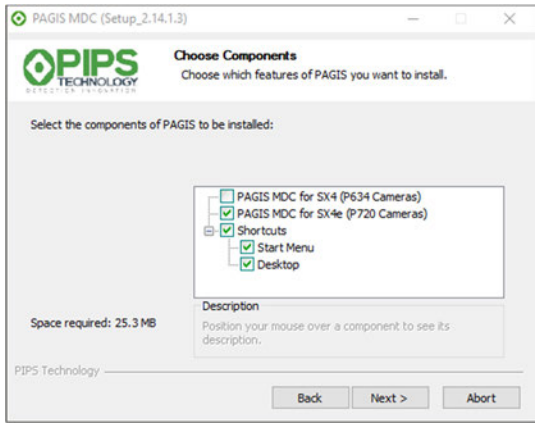
1. If PAGIS exist on your computer, it must be version 2.9 or 2.12 for installer to update. If your version of PAGIS is older it is recommended you “EndShift” any existing data, then uninstall PAGIS.
2. It is recommended you “EndShift” any existing data if upgrading a previous version of PAGIS.
3. Prior to software installation, take the time to figure out what version of PIPS mobile processor you have as the software installation requires you to select so it can properly configure the camera settings based on processor type. PAGIS version 2.14 supports processor versions SX4 & SX4e only, you can either look at the product tag located on the processor or look at the camera IO ports on the back of the processor, if the 4 camera IO ports are vertically arranged RJ45’s then it’s a SX4e, if they are vertically arranged circular shaped “LEMO” connectors then it’s a SX4. Horizonal arranged circular shaped “LEMO” connectors is a SX3 and is not compatible with PAGIS 2.14.
4. When upgrading to PAGIS V2.14.x.x also requires that the PIPS mobile processor be updated to same version in order to take advantage of Firmware update.



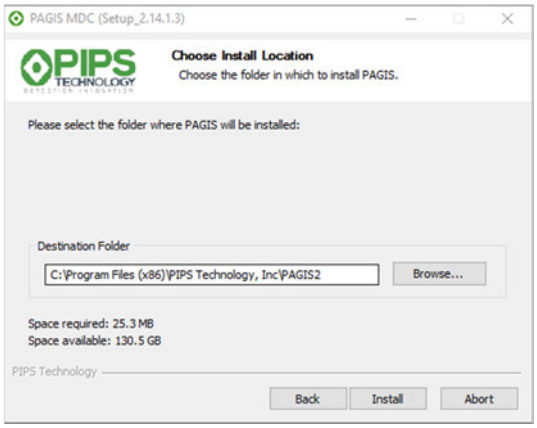
5. Place the PAGIS installer on your computer’s desktop, “PAGIS_Setup_MDC_2.14.x.x.exe”.
6. Right click the PAGIS installer executable and select “Run as administrator”.



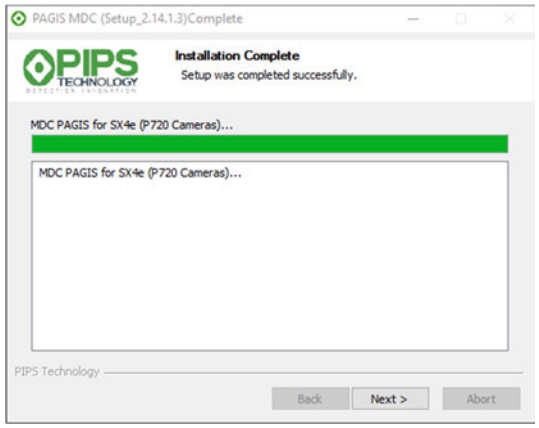
7. Check the license agreement box, then click Next.



8. Select the mobile processor type and alter “Shortcuts” if needed. Next to continue.



9. Confirm path if upgrading, click Install to proceed.



10. Installation Compete, Next to proceed.
11. Click Finish.
12. Click Yes to reboot if you would like to test PAGIS auto start at login if selected during installation, otherwise click No as its not required for PAGIS to run.

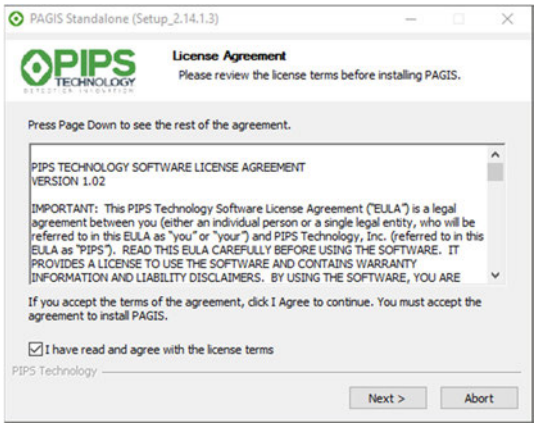
Note: See Appendix A for terminology definitions.

4.2.3 PAGIS Software Installation (Mobile Processor)

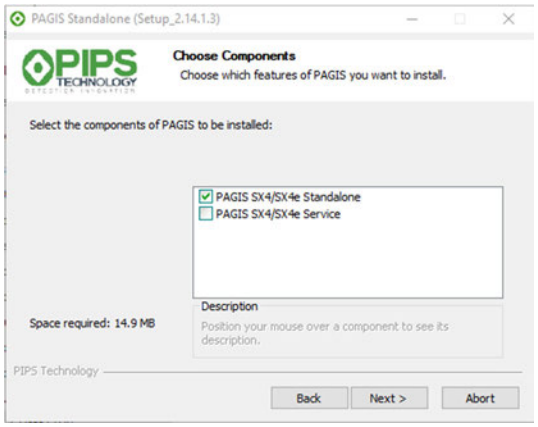
1. PAGIS v2.14.x.x updater is only compatible with PIPS mobile processors SX4 & SX4e.
2. The PAGIS updater only updates existing versions of PAGIS on mobile processor, version 2.9 and newer.
3. Update required for both “Standalone” & “Service/VPRelay” to support some of the newer features.
4. The processor must be in its respective mode to update that option as the folder path are hidden when not active, see “Change Mode” in SX4 or SX4e manual.



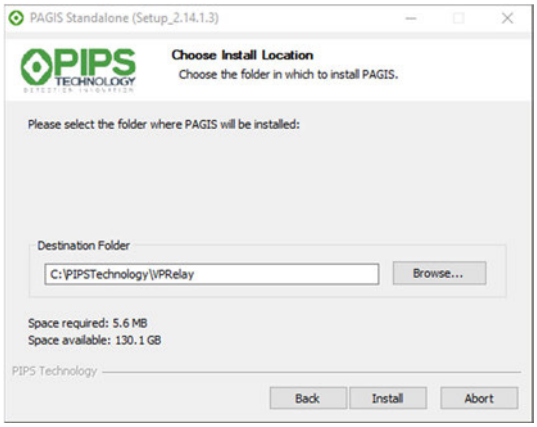
5. Remote desktop into processor or utilize attached monitor/keyboard.
6. Place the updater in C:\PIPSTechnology folder on the PIPS mobile processor.
7. Execute PAGIS Updater.



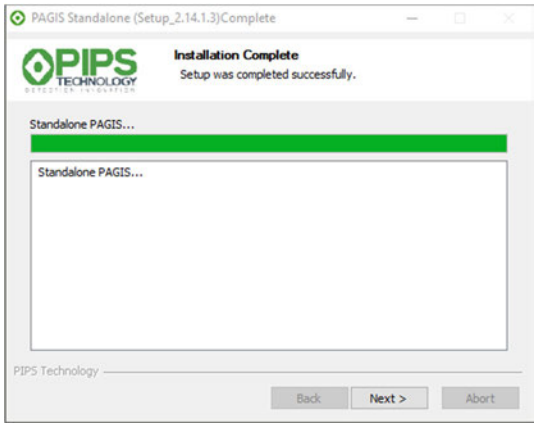
8. Check the license agreement box, then click Next.



9. Select option to update, next to continue.
   - Standalone= PAGIS login from Processor.
   - Service= PAGIS login from connected Laptop.



10. Change the default path presented by updater, see below.
    - For “Service” C:\PIPSTechnology\VPRelay.
    - For “Standalone” C:\PIPSTechnology\Standalone.



11. Installation Compete, Next to proceed.
12. Click Finish.
13. Click Yes to reboot.

Note: See Appendix A for terminology definitions.

TROUBLESHOOTING TIPS

This section provides some basic troubleshooting tips and information

5.1 Troubleshooting & Tips

- The first login to PAGIS after the new install of an unconfigured version does not require a username or password. Simply click Login to be granted Admin access to the software.
- A good means to test the communication from the MDC to BOSS is ping or telnet (over TCP 8092) through the command prompt.
- A good means to test the communication from the MDC to the SX Processor is ping or telnet (over TCP 9000) via command prompt.
- For many other troubleshooting tips, see Appendix C – Frequently Asked Questions

5.1.1 PAGIS with NetMotion VPN

Agencies utilizing NetMotion VPN software on the MDC will need to apply the following passthrough steps:

1. Login to the NetMotion server as administrator
2. Click Settings > Then select Client > Select Global Client Settings > Then select Passthrough List
3. Click the “Add…” button on the right > Select “Network Address”
4. Enter the following settings (as shown):
    A. IP address:192.168.200.0 (the zero is correct, it's an IP address “range”) Subnet Mask: 255.255.255.0.
    B. Keep all other settings default (as shown) and click OK.
5. The MDC must then disconnect from NetMotion and reconnect again for the settings to be applied locally.

5.1.2 Cisco VPN Client:

Make sure Stateful Firewall is unchecked and "Allow Local LAN".

5.1.3 Microsoft .NET 3.5 Installation

The PAGIS Software requires Microsoft .NET Framework 3.5 specifically. If the MDC doesn’t have .NET, it can be downloaded from the Microsoft website.

5.1.4 Firewall Settings for Client-Server Installations

For client-server installations, the Windows Firewall needs to allow the SX Processor and the MDC to communicate. If the MDC is maintained by a Network Administrator, he or she should be contacted before making changes to the firewall. The command prompt commands for the exceptions are below

Option 1: Allow Microsoft Windows Version 8 or newer to auto-detect the launch of the PAGIS.exe application and use the wizard to add the PAGIS.EXE to the exception list (making note of Public or Private Network settings as necessary).

Option 2: Add PAGIS to the exception list manually by browsing to the install path of PAGIS. The default is below for reference: C:\Program Files (x86)\PIPS Technology, Inc\PAGIS2\PAGIS.exe

Option 3: Add the communication ports manually:
TCP in/out 8092 = Pagis sync port to BOSS back office software.
TCP in/out 9000 = Mobile processor camera feed port.
TCP in/out 9001 = Mobile processor camera snapshot port.
TCP in/out 32023 = Mobile processor camera setup port.
TCP in/out 10000 = Mobile processor data capture port.
NOTE: XML Datastream uses TCP 10100 and TCP 7000

PAGIS/BOSS3 CONFIGURATION 4864

In order for the PAGIS software to function properly, the device must be built, enabled, and configured in BOSS3 before being deployed for service in the field.

6.1 Creating a New Device in BOSS3

Once network communication to BOSS3 has been established from the vehicle, the new device must be "built" or added to the Device List in BOSS3 before it can be used. The approved way to do this, is to simply perform a Begin Shift from the PAGIS software. **NOTE**: The computer name is what will be displayed in BOSS as device name.

1. At the PAGIS Live View Screen, click the Begin Shift button once to select it, and then click again to launch the sync.
2. If the laptop has previously been setup to communicate with BOSS and is already enabled, the sync transfer window should appear in the middle of the Live View Screen.
3. If this is a new/disabled device, a message indicating "HttpStatusCode" will be displayed.
4. This indicates the BOSS3 server has received the sync request but has rejected it due to device status.
5. Once the BOSS Admin has enabled the device, the Status Code error will not appear again, and syncs should complete as configured in BOSS3.

6.2 Enabling a New Mobile System in BOSS3

Installing PAGIS and configuring the network settings is only the first step in making the ALPR unit operational. Once PAGIS is configured to work with or on the SX Processor and the mobile cameras, it must then be enabled in BOSS3 before synchronizations can take place. **NOTE**: By default, every new device recognized by the BOSS3 server is disabled until the Admin enables it. This is done for security.

1. Log into the BOSS3 UI Client Software with Admin privileges.
2. Click the Admin button on the left to expand the options.
3. Click the Devices button. The new device should now be listed to the right.
4. Click the name of the Device to select it. (This will open the device details screen)
5. Click the Edit button at the bottom of the window.
6. Click the Enable button from the Edit window.
7. This will enable the device and return the Admin to the Device List.

NOTE: If desired, the Admin can re-enter the Edit window to assign an alternate name in BOSS3 for the new device. The Admin will need to update the "Description" field and then click the Save button. Agencies commonly use this field to signify the Unit number, Car name, or Patrol Shift. The "Name" field is the device/host name and cannot be edited in BOSS3.

NOTE: Once the Device is enabled the Admin needs to assign ownership and hotlist distribution.

6.3 Assigning Ownership to a Device in BOSS3

Every new device added to BOSS3 allows for Admin level access into PAGIS without the use of a username or password. In order to password protect the PAGIS software, the BOSS Administrator must assign "Owners" to the device in BOSS3.
NOTE: For more detail on Users, User Groups, Sites, and Roles, refer to the BOSS3 manual.

1. Login to the BOSS3 UI with Admin credentials.
2. Click the Admin button on the Left to expand the options.
3. Click Devices to review the list.
4. Click on the Device Name to open the device details screen.
5. Click on the Edit button.
6. Locate the "Owners" field. Click the Select button to the right.
7. Check the box(es) for the appropriate Site(s)/User Group(s). **NOTE**: This tells BOSS3 which sets of users will have rights to login to PAGIS from this specific device.
8. Notice the Select button has changed to a Save button. Click Save to retain changes.
9. Confirm the changes show in the Owners Field.
10. Click the Save button at the top left of the Edit window.

6.4 Assigning Hotlists to a Device in BOSS3

In order for the PAGIS users to receive alerts, one or more of the stored hotlists in BOSS3 must be distributed to the new device. **NOTE**: For more information on building and configuring Hotlists, refer to the BOSS3 manual.

1. Login to the BOSS3 UI with Admin credentials.
2. Click the Admin button on the Left to expand the options.
3. Click the “Hotlists” button to review the list of configured alert lists.
4. Click the Hotlist Name to select the first alert list. This will open the Details screen.
5. Click the Edit button at the bottom of the window.
6. Locate the “Deployment” field. Then click the Select button to the right.
7. Check the box next to the name of the new device.
8. Notice the Select button has changed to a Save button. Click Save to retain the changes.
9. Confirm the changes show in the Deployment Field.
10. Click the Save button at the top left of the Edit window.
11. Perform these steps again for all remaining Hotlists necessary for this device.

PAGIS/BOSS4 CONFIGURATION

In order for the PAGIS software to function properly, the device must be built, enabled, and configured in BOSS4 before being deployed for service in the field.

7.1 Creating a New Device in BOSS4

Once network communication to BOSS4 has been established from the vehicle, the new device must be “built” or added to the Device List in BOSS4 before it can be used. The approved way to do this, is to simply perform a Begin Shift from the PAGIS software. **NOTE**: The computer name is what will be displayed in BOSS as device name.

1. At the PAGIS Live View Screen, click the Begin Shift button once to select it, and then click again to launch the sync.
2. If the computer has previously been setup to communicate with BOSS and is already enabled, the sync transfer window should appear in the middle of the Live View Screen.
3. If this is a new/disabled device, a message indicating “HttpStatusCode” will be displayed.
4. This indicates the BOSS4 server has received the sync request but has rejected it due to device status.
5. Once the BOSS Admin has enabled the device, the Status Code error will not appear again, and syncs should complete as configured in BOSS4.

7.2 Enabling a New Mobile System in BOSS4

Installing PAGIS and configuring the network settings is only the first step in making the ALPR unit operational. Once PAGIS is configured to work with or on the SX Processor and the mobile cameras, it must then be enabled in BOSS4 before synchronizations can take place. **NOTE**: By default, every new device recognized by the BOSS4 server is disabled until the Admin enables it. This is done for security.

1. Log into the BOSS4 URL with Admin privileges.
2. Navigate to the Resources pulldown menu.
3. Select Devices from the menu options. The new device should now be listed.
4. Click the name of the Device to select it. (This will open the device details windows on the left)
5. Click the Enable slide toggle to enable device, located in upper right of device edit window then click save.
6. This will enable the device, synchronization between BOSS4 and PAGIS is allowed.

NOTE: Once the Device is enabled the Admin needs to assign ownership and hotlist distribution.

7.3 Assigning Ownership to a Device in BOSS4

Every new device added to BOSS4 allows for Admin level access into PAGIS without the use of a username or password. In order to password protect the PAGIS software, the BOSS Administrator must assign “Owners” to the device in BOSS4.

NOTE: For more detail on Users, User Groups, Sites, and Roles, refer to the BOSS4 manual.

1. Login to the BOSS4 URL with Admin credentials.
2. Navigate to the Resources pulldown menu.
3. Select Devices from the menu options. The new device should now be listed.
4. Click the name of the Device to select it. (This will open the device details windows on the left)
5. Locate the “Owner” field. Click in the Owner filed, and a list of all available Groups will appear.
6. Select group by clicking on it, it will then automatically be added to owners, see list below “Owner”.
7. To add mode groups, repeat step 15.
8. Confirm the changes show in the Owner Field.
9. Click the Save button at the bottom right of the Edit window.

7.4 Assigning Hotlists to a Device in BOSS4

In order for the PAGIS users to receive alerts, one or more of the stored hotlists in BOSS4 must be distributed to the new device.

NOTE: For more information on building and configuring Hotlists, refer to the BOSS4 manual.

1. Login to the BOSS4 URL with Admin credentials.
2. Navigate to the System pulldown menu.
3. Select Hotlists from the menu options
4. Click the Hotlist Name to select the first alert list. This will open the Details screen.
5. Locate the “Deployment” field.
6. Check the box next to the name of the new device listed.
7. Click the Save button at the bottom right of the Edit window.
8. Perform these steps again for all remaining Hotlists necessary for this device.

APPENDIX A: THE GLOSSARY

4867

ALPR/ANPR	"Automatic License Plate Recognition/Automatic Number Plate Recognition".
BOSS	"Back Office System Software". This is the ALPR server.
GPS	"Global Positioning System".
GUI	"Graphical User Interface".
Hotlist	A database or list that contains vehicle license plates of interest ("alert list").
IR	Infrared light.
License Plate	Also called a tag or number plate.
MDC	"Mobile Data Computer". This is the tablet or laptop in the vehicle.
OCR	"Optical Character Recognition" (also referred to as a "cardet").
OS	"Operating System".
PAGIS	This is the License Plate Capture Software most commonly used in an ALPR vehicle.
Service	Operation mode of the PAGIS software. Service or "VPRelay" is used to refer to PAGIS instance that is running directly on the PIPS mobile processor without a GUI interface, this mode is intended to run in conjunction with MDC version of PAGIS installed on laptop connected via Ethernet.
Standalone	Operation mode of the PAGIS software. Standalone is used to refer to PAGIS instance that is running directly on the PIPS mobile processor with a GUI interface. Same a "Service"
SX	SX is a short notation referencing PIPS's mobile processor, commonly the SX is followed by the generation number of the processor, i.e. SX3, SX4 & SX4e.
UI	A "User Interface" is the means in which the user can access and navigate the software.
USB Flash Drive	Also called a thumb drive or memory stick.
VLP	"Vehicle License Plate".
VPN	"Virtually Protected Network".
VPRelay	Operation mode of the PAGIS software. VPRelay or "Service" is used to refer to PAGIS instance that is running directly on the PIPS mobile processor without a GUI interface, this mode is intended to run in conjunction with MDC versions of PAGIS installed on laptop connected via Ethernet.
Whitelist	Opposite of a standard BOSS Hotlist. This is a list of license plates that should not trigger an alert.

APPENDIX B: PAGIS SOFTWARE DATABASE FILE

This section is used to configure the PAGIS Software when it's not being used with the Back Office System Software (BOSS). Comma-separated value (CSV) format is the only format the PAGIS Software supports for importing data into the vehicles for the purpose of matching against the captured license plate data. PAGIS will support CSV files with any number of columns, called "fields", as long as the first field is the VLP (Vehicle License Plate). **NOTE**: The CSV format is standard ASCII.

Example CSV Files:

1. *ABC123, Red, Ford, Explorer, 1996, WANTED XYZ456, Blue, Audi, A4, 2001, MURDER*
2. *45ABC234, Vehicle wanted in associated with a kidnapping on 12/5/2005 995BD233, Vehicle reported stolen from Liz's Lounge at 6am on 12/1/2005*
3. *UIO223 ABC123*

General Function:

PAGIS calls/utilizes files in pairs. Each database in PAGIS is created using two files; a CSV file, and an INI configuration file. Without both of these files, the database will not load and PAGIS will not "see" it. Each CSV file/hotlist must have the exact same name as the INI configuration file. Example: Stolen.ini and Stolen.csv will work. Stolen.ini and Plates.csv will not.

Reading an INI Configuration File

Lines that appear in brackets [] are called "Headings". The labels that appear inside the headings, are called "values". Values will always contain an equal sign (=). If a line starts with a semicolon, it is considered to be a comment and is not read by the software. There is no limit to the number of comments in the INI file.

The [SETTINGS] Heading

The values in the Settings heading are: NumFiles, DbName, DbColor, Priority, Covert, Alarm, and NumFields.

- NumFiles: Determines how many database files the system should split the specified hotlist into. Generally, this value is set to 1. But for larger hotlists (200,000+ lines), a number of 2-5 may be more desirable.
- DbName: Tells the PAGIS Software what the displayed name of the hotlist should be.
- DbColor: Sets the display color of the hotlist. This is merely an esthetic setting and not a functional setting. The right-hand side of the equal sign is the HEX value representing the ARGB values for the color. If this value is unknown, the Admin should simply leave this line out of the file.
- Priority: Designates the priority of this hotlist in relation to other hotlists in the system. The highest priority database is 1 and the lowest is 999. **NOTE**: if a plate resides on multiple lists the higher priority will be alerted first.
- Covert: Determines whether standard PAGIS Software users are alerted when a hit is made from the database. Covert database can be used for hotlists that are included for information-gathering purposes rather than eliciting user intervention. The system can also be configured to notify via email or SMS message when a hit is made from a covert hotlist.
- Alarm: Sets the audible alert to be played in PAGIS when a hit is made from the hotlist. Values for Alarm are LOW, MED, HIGH
- NumFields: Indicates how many fields (columns) are in the CSV file. If this value is less than the actual number of fields in a file, then the additional fields are placed in the general information area. This value also determines the number of headings of the [Field x] present in the file. For example, if NumFields=2 then there will be two additional headings, [Field 0] and [Field 1]. **NOTE**: Adding "Creation =" will place the timestamp the hotlist was added to the Begin Shift file.

The [FIELD X] Heading

Under the Field heading, there are two configurable values, “Name” and “PAGIS”.

- Name: Tells the system what the name of this field is. If no name is specified, then no name given to the field. The format is Name = <field>
- PAGIS: Specifies how to display the field in the GUI/PAGIS Software.
    - If no value is defined, the field is placed as general information.
    - Values 1-5 represent special fields for the PAGIS Software that translate to the information being displayed in a box of its own when a hit is processed.
    - A value of 6 represents an ID number to cross reference the vehicle from the hotlist with a person from the wanted list.
    - A value of 7 is identical to leaving the value undefined.

Sample INI Configuration File

[Settings] NumFiles=1
DbName=Stolen Vehicles DbColor=ffffff00 Priority=5 Covert=False Alarm=MED NumFields=8
;PAGIS Values
;0 is VRM / VLP (Not User Definable, always Field 0)
;1 is Special Field 1
;2 is Special Field 2
;3 is Special Field 3
;4 is Special Field 4
;5 is Special Field 5
;6 is ID Number (PNC ID, Drivers License, Social Security Number, etc.)
;7 is General Info (Default for all undefined fields) [Field 0]
PAGIS=VRM

Sample INI Configuration File

[Field 0] Name=VRM
[Field 1] Name=Color
PAGIS=3 [Field 2]
Name=Make PAGIS=1
[Field 3] Name=Model
PAGIS=2 [Field 4]
Name=Action PAGIS=4
[Field 5] Name=Warning
PAGIS=5 [Field 6]
Name=PNCID PAGIS=6
[Field 7] Name=Intelligence PAGIS=7

APPENDIX C: FAQ

Q: **HOW DO I ENTER A SUPPORT CASE?**
A: We have a webform you can use here, you can email our Support Team at Support@PIPSTechnology.com, or you can call us on the phone Monday-Friday 8am to 4pm Central Time (9am-5pm Eastern) at (833) 747-7577 Option 2.

Q: **HOW DO WE CREATE USERS IN PAGIS?**
A: The agency BOSS Administrator creates all users, both for BOSS and for PAGIS. Once the user is created in BOSS, the Admin would click the user's name to select/edit the user. Then click the Advanced button and update the PAGIS specific password. Please note that the username and password fields are both case sensitive and the PAGIS users need to be added to a group with the Role that allows them to use PAGIS/LPCS.

If you have any further questions, please feel free to enter a request for support here.

Q: **WHERE DO USERS CHANGE THEIR LOGIN PASSWORD IN PAGIS?**
A: User passwords are created and updated in BOSS via the UI client software. For the majority of our customers using both the PAGIS Software and BOSS, any user accounts or passwords created in the PAGIS Software itself will be overwritten by the user information defined in BOSS during the next sync.

If you have any further questions, please feel free to enter a request for support here.

Q: **HOW DO WE REQUEST AN RMA REPAIR?**
A: To assist with this, please navigate here to review our RMA procedure as well as to download the request form. Please keep in mind that once submitted, all repairs are reviewed for age of equipment and warranty status before final processing takes place. Additionally, incomplete forms and those without much detail often result in processing delays.

If you have any further questions, please feel free to enter a request for support here.

Q: **WE GOT NEW MDC LAPTOPS IN THE PATROL CARS, HOW DO WE ADD THOSE DEVICES TO BOSS?**
Q: **HOW DO WE EDIT THE DEVICE NAMES IN BOSS?**
A: The initial device template/skeleton is automatically created in BOSS the first time the device attempts to Sync from the field. Devices should NEVER be created manually. For PAGIS laptops, this is done after PAGIS is installed and configured and Begin Shift is launched. However, if the agency would like to organize the device list by updating the "Device Name" field, those steps are below:
1. Login to the BOSS UI with Admin rights
2. Navigate to Admin > Devices
3. Click on a device name to select it > Click Edit
4. Update the name of the device in the "Description" field (Name field cannot be altered)
5. Click Save > This will take you back to the Device Summary List. The "Device Name" field should show the new name

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **WE HAVE A NEW MOBILE COMPUTER/MDC THAT'S NOT SYNCING WITH BOSS.**
Q: **WE KEEP SEEING AN HTTP_STATUS_CODE ERROR WHEN RUNNING BEGIN SHIFT.**
A: This error most commonly means that a new device in the field (laptop/tablet) can "see" the BOSS server, but that it hasn't been enabled yet to "talk" with it. Follow the general steps below to address this issue:
1. The agency BOSS Administrator will need to login to the BOSS UI client and Select Admin
2. Then select Devices and from there, left click on the device/computer name of that MDC to edit it
3. Once in the Edit screen, Enable the device. This will take you back to the Device List.
4. Click the name to edit the device again. Now assign users/Owners and save.
NOTE: The Select button becomes a Save button when selecting which Groups/Users should have access to login to this device
5. Once that is done, navigate to Admin > Hotlists
6. From here, click on each hotlist one at a time to distribute them to the new device being sure to Save the changes next to the Distribution field. Note again that the Select button becomes a Save button. And there's another Save button at the top left of

the edit window.
7. After this is complete, perform Begin Shift from the field unit/MDC and confirm there are no further errors. [4871]

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **NEW PAGIS USER CAN'T LOGIN BUT OTHERS CAN.**
Q: **USERS CAN LOGIN TO PAGIS WITH NO CREDENTIALS AT ALL.**
A: Entry or login to the PAGIS software in the field is partially controlled by the Device settings in BOSS. The users themselves must also be properly setup with an LPCS/PAGIS password. To check the current device settings/ access, perform the following steps:
1. Login to BOSS UI (with Administrator rights)
2. Select the Admin Section
3. Select Devices and then Select the Device in question by PC name
4. Once selected click on the Edit button near the bottom
5. Locate and inspect the "Owners" Field (this is a list of users/groups that have access to login to the device)
NOTE: If this field is blank, the device is in an open configuration mode allowing admin level access simply by clicking login (any credentials would also be accepted).
6. To update the device owners, click the "Select" button next to the Owners field (notice it changes to a Save button)
7. Check which Users/Groups of Users should be able to login to PAGIS from this device
8. Click the Save button next to the field
9. And then click Save in the upper left portion of the Edit window
10. Have a previous user or Admin login to PAGIS and perform Begin Shift to sync the new data
11. A PAGIS Admin can confirm by navigating to Admin, Admin, and then Users to review the list
12. Another test would be to have the new user attempt to login

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **WHEN USERS LOGIN TO PAGIS, THEY ONLY SEE A GREY SCREEN.**
Q: **CAMERAS AREN'T SHOWING UP IN PAGIS ANYMORE.**
SEE ALSO: "THE LINK LIGHTS ON OUR ALPR COMPUTER/MDC WON'T TURN ON OR FLASH"
A: Below are some basic troubleshooting steps you'll want to follow before creating a support ticket.
1. Doublecheck the physical power switch on the black box/Processor is On. In many vehicles, there is also an in-line switch in the front of the vehicle that needs to be switched On. When the units are properly powered and on, you should see lights and hear fans running.
2. Confirm that the network adapter settings on the laptop match the proper Static IP scheme for the SX Processor in use. The older scheme is 192.200… and the newer scheme is 192.168…. NOTE: the adapter status in Windows should say "unidentified network". If it says "cable unplugged" the laptop can't "see" the SX.
3. If the power and Static IP settings are good and things still aren't working, test further by disabling the three main software related culprits. Turn off/bypass the local Windows firewall, antivirus, and VPN software one at a time.
4. If you're still not able to see the camera feed after that, you may want to use a different network cable as those can get damaged over time and then confirm that the cord is properly plugged into the ports.
5. If the network cord from the SX Processor is routed through a docking station, then it's possible the dock is preventing the traffic. You should contact the dock's manufacturer for the most recent firmware. To test for this, remove the laptop from the dock, directly connect the network cord to the laptop, and then reconfigure the network adapter settings (remove the static settings from the dock's adapter/ and assign the static IP to the laptop's NIC adapter).

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.
Q: **THE LEFT FRONT CAMERA ON OUR ALPR VEHICLE IS NO LONGER SHOWING IN PAGIS**?
Q: **HOW DO WE TROUBLESHOOT MOBILE CAMERAS**?
A: Below are the main troubleshooting steps to test the camera(s) and cable(s) on a system where only one or two cameras are no longer displaying images.
Step 1: Confirm MDC/SX communication - steps shown in section "Cameras aren't showing up in PAGIS anymore."
Step 2: Access the SX Processor – RDP or directly connect a monitor, keyboard, and mouse to the SX. Contact PIPS Support for

help with RDP if the credentials are unknown to the agency.
Step 3: Confirm camera activity – Launch Tools. Then open P6Utility or Mobile Toolkit. Check the camera feeds/function by switching the Input menu to the camera(s) in question
Step 4: Unplug and Reattach the Camera Cables – Note, the cables DO NOT TWIST. The metal locking nut on the cable slides back about a millimeter and the cable comes straight out. Do this at the SX Processor and the Camera. You may need to remove the camera from the mount in order to unplug the cable successfully (most brackets use a #3.5 Hex/Allen Wrench)
Step 5: Swap Port on SX Processor – At the SX Processor, swap the camera cables from the non-working camera to a port with a working port (Take care to note the swap so the cables get back to their original ports). If the camera outage stays at the port site, the issue is most likely the capture card on the SX Processor and will require RMA (Example: working Left cam is swapped to port of non-working Right cam and no longer functions. AND the previous non-working Right cam starts working once it's plugged into the Left cam's port). If the fault/error stays with the camera regardless of SX port, continue to Step 6.
Step 6: Physically Swap Camera Locations – Once all other items are checked, move the camera itself to a working position in order to test the cable. (Example: physically move Left cam to the Right cam position on the top of the vehicle) Connect the cable at the new position and test feed in Tools > P6Utility/Mobile Toolkit. If the camera works at the new location, the issue is most likely a bad cable. If the camera still does not work, the issue is most likely a faulty camera in need of repair/RMA.

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **WE'RE NO LONGER GETTING GPS IN PAGIS.**
Q: **WE'RE NOT SEEING GPS DATA FROM SOME OF OUR FIELD UNITS IN BOSS.**
A: Below are the basic troubleshooting steps for checking the GPS of field units:
1. Login to PAGIS (as Admin)
2. Navigate to Admin section, then click the Admin button
3. Select "System" on the left pane
4. Confirm/Set the button at top to "Default"
5. Remove any value(s) stored in the GPS Connection String field. Leave '5' in the Computer String.
6. Click the Save button to retain changes made.
7. Close PAGIS fully and relaunch and log back in to test (Note: GPS will only show with test reads/hits)
8. For versions of PAGIS 2.9 and up, test with a GPS Connection String of 6 if the blank field doesn't work. Save the changes. Log out. Close the software and then relaunch to test.

Please be advised, that some GPS issues can be caused by local or domain firewall settings, antivirus software, or any other software package monitoring/transmitting network data. To test these, disable or bypass those software options on the MDC and retest.

If these initial troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **HOW DO I INSTALL THE PAGIS SOFTWARE?**
Q: **I JUST LOADED PAGIS ON A MACHINE AND IT CRASHES WITH A .DLL ERROR WHEN I TRY TO LAUNCH IT.**
A: The most common installation of PAGIS is Client/Server or "VPRelay Mode". The .dll error is caused by the installer not being run from the HDD and/or the wrong install option being selected (Example: SupeRex instead of MDC). The best practices for the installation are below. (Note, this does not cover MDC or PAGIS configuration, only the act of installation)
1. Always copy the installer over to the HDD/Desktop of the MDC. Never run it from a thumb-drive or network share
2. Regardless of how you're logged in to Windows, right click the installer and select "run as Admin" or "run with elevated privileges"
3. Continue through the message/error about OS compatibility
4. Click next on the wizard and then be sure to select the MDC option (to use with VPRelay)
5. After that, it's next, next, next, finish the reboot is not necessary

If these steps did not resolve the issue, please feel free to enter a request for support here.

Q: **USERS ARE GETTING HITS/ALERTS ON PREVIOUSLY RECOVERED STOLEN PLATES.**
Q: **USERS AREN'T GETTING HITS FROM KNOWN ACTIVE PLATES.**

Q: **THE HOTLISTS IN PAGIS DON'T SHOW TODAY'S DATE.**
Q: **THE HOTLISTS AREN'T SYNCING WITH BEGIN/END SHIFT.** 4873
A: Whether it's from data latency or just use over time, the local file structure can get some minor corruption and will need to be refreshed. The steps below show the best practices:
1. Login to Windows with Admin rights (ability to uninstall/delete software)
2. Login to PAGIS and perform an End Shift
3. When complete without error, Logout of PAGIS and then Exit/Close the program
NOTE: If the End Shift fails or displays an error, contact Support for additional assistance.
4. If there were no errors, locate the PAGIS icon on the desktop.
5. Right click on the icon and select "Open File Location" (This should open a window where the program was installed)
6. Scroll up and locate the folder labeled "data". Double-click it to open it
7. Select and delete everything in here EXCEPT for "Attributes.db"
8. Once that's complete, Login to the PAGIS software again
9. Perform a Begin Shift. This will pull down fresh data from the server
NOTE: Once complete, the files in the data subfolder as well as the Databases section of PAGIS should be restored.

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **IS PAGIS COMPATIBLE WITH OUR NEW WINDOWS 10 LAPTOPS?**
A: Although there's a warning about compatibility during the install of PAGIS on any Windows OS after XP, it is compatible with all them. However, we have seen errors occur when agencies copy and paste folder structures from previous installations. This of course is not recommended.

Q: **THE LINK LIGHTS ON OUR ALPR COMPUTER/MDC WON'T TURN ON OR FLASH.**
Q: **OUR WINDOWS 10 MDC WAS WORKING BUT HAS STOPPED COMMUNICATING TO THE SX PROCESSOR.**
A: There are many variables with troubleshooting any network connection. And the connection from the ALPR computer to the SX Processor is no different. The following troubleshooting list highlights the most common:
1. The physical network cord is bad/damaged.
A: Test with a different cable and confirm that it is plugged in fully

2. The network adapters are not configured or have incorrect static IPs
A: Confirm the Static IP scheme in use and properly configure the network adapters

3. Local and/or Domain Firewall rules have prevented the flow of communication
A: Disable or bypass these and test again

4. VPN, Anti-Spyware, Antivirus, or other monitoring software has blocked communication
A: Disable or bypass these one at a time and test after each to find the culprit(s)

5. Docking Station Firmware can be incompatible with some newer computers or become corrupt
A: Test by running the network cord straight to the MDC and then configuring the network adapters (NOTE: It would also be a good idea to contact station manufacturer to see what the latest firmware version is and upgrade as necessary)

6. The NIC Drivers have become corrupt
A: Update the specific Networking drivers in use on the MDC through the Device Manager in Windows

7. Turn off all power saving settings of the Ethernet Adapter in the device manager
A: Uncheck "Allow the computer to turn off this device to save power"

8. Check for Windows 10 update 1709 and 1803 as this update will not allow the NIC and Cellular Aircard to run simultaneously
A: Settings > Update and Security > Windows Update > "Update History" link – if there, see the steps in the FAQ

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **AS SOON AS WE DOCK OUR MDC, WE LOSE CONNECTION TO THE WIRELESS.**
Q: **OUR WINDOWS 10 LAPTOP LOSES CONNECTION TO THE INTERNET WHEN THE NETWORK CABLE IS PLUGGED IN.**
Q: **OUR MDC HAS MICROSOFT VERSION 1709 OR 1803 AND CAN'T CONNECT TO WIFI WHEN DOCKED.**
A: Microsoft Updates (1709 and 1803) prevent the Wireless connection as soon as a Network cable is plugged into the device. This also occurs for MDCs/laptops that are docked (where the Network cable from the SX Processor is run through the docking station). As of January 2019, the steps to correct this are below.
WIN10 version 1803
1. Open Regedit
2. Expand HKEY_LOCAL_MACHINE
3. Navigate to Software > Policies > Microsoft > WcmSvc > Local
4. Right click on Local > Hover over New > Select "DWORD (32-bit)"
5. Name the new value "fMinimizeConnections"
6. Right click the on the new name > select Modify > Set value data to 1 (leave base Hex) > Click OK
7. Reboot Windows and test

WIN10 version 1709 - Microsoft fixed this with Update KB 4284822. But if you still have issues, the registry steps are below:
1. Open Regedit
2. Navigate to HKEY_LOCAL_MACHINE > Software > Policies > Microsoft > WcmSvc > Local
3. Right click on Local > Hover over New > Select "DWORD (32-bit)"
4. Name the new value "fMinimizeConnections"
5. Right click the on the new name > select Modify > Set value data to 0 (leave base Hex) > Click OK
6. Then Navigate to HKEY_LOCAL_MACHINE\Software\Microsoft\Wcmsvc
7. Right click on Wcmsvc > Hover over New > Select DWORD (32-bit)
8. Name the value "IgnoreNonRoutableEthernet"
9. Right click on the new value > Modify > Set value data to 1 (leave base in Hex) > OK
10. Reboot Win10 and test

If the steps above did not resolve the issue, you may need to address this with Microsoft. Their support site is here.

APPENDIX D: XML DATASTREAM

Overview

The XML Datastream can be used to push the current data from a running PAGIS system to another application. The data available via the Datastream includes reads, hits and current images. The connection to the Datastream is a TCP/IP socket (default port: 10100). When initially connecting, an XML packet is passed to the PAGIS Software to subscribe to the Datastream. The data connection is configured as "push only" and doesn't allow receipt of additional external data. The current image stream is pushed periodically whereas reads and hits are passed as close to real-time as possible.

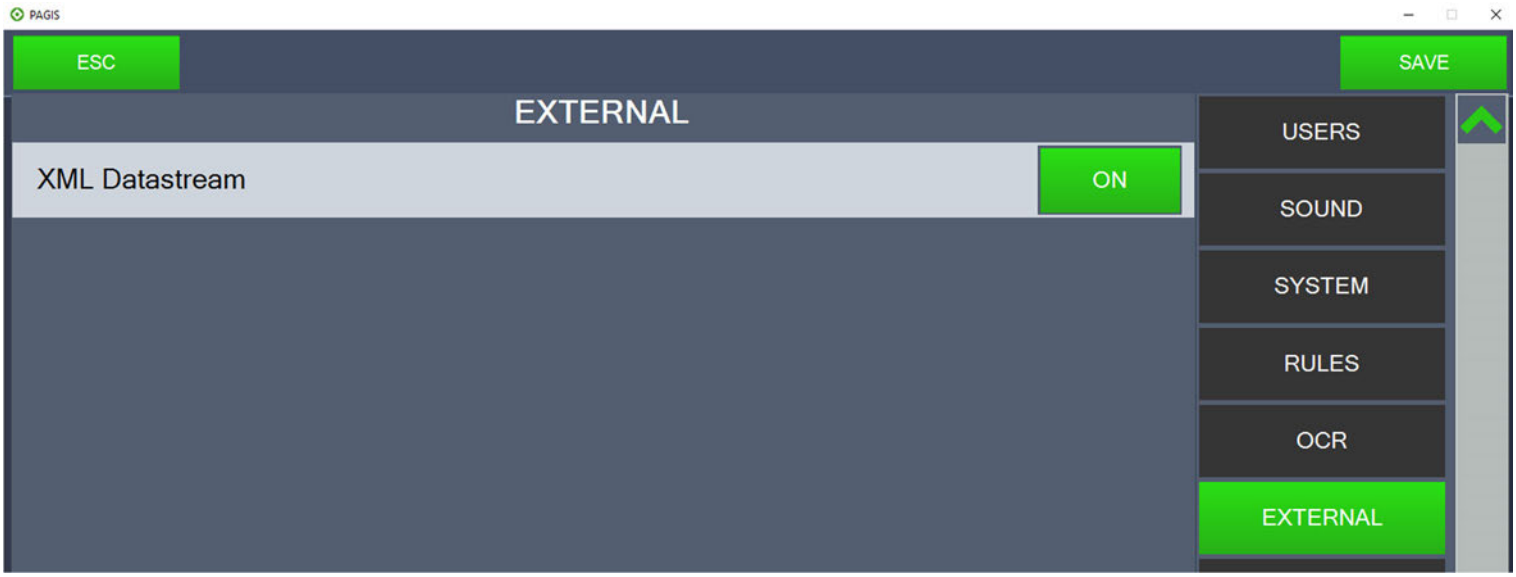
PAGIS Port

By default, the PAGIS.exe.config file has a key for defining the port number for the XML Datastream. The default value is 10100. This setting does not need to be changed unless the default port is unavailable.
The key has the following format:

```
<!--XML Datastream Settings/-->
<add key="XML.Datastream.Port" value="10100"/>
```

PAGIS Admin Setting

To utilize this feature, the XML Datastream needs to be enabled in PAGIS. To do this, navigate to Settings > Admin > External. The "XML Datastream" option should be turned on as shown in the image below and then saved.



XML Subscription

When initially connecting to PAGIS, the Datastream subscriber will receive only a Heartbeat XML packet (see example below) until PAGIS receives a subscription packet from the subscriber. The properly formed subscription packet defines the specific data that the subscriber wishes to receive.

Heartbeat XML Packet

The Heartbeat Packet is sent once every 10 seconds. The purpose of the heartbeat packet is to let the subscriber know that the communications channel is working between PAGIS and the subscriber. The timestamp is sent in the format of "`YYYY-MM-DDThh:mm:ss`".

Sample of the Subscription XML Packet

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-heartbeat>
  <timestamp>2011-10-13T09:41:56Z</timestamp>
</pips-datastream-heartbeat>
```

Subscription XML Packet

A properly formed subscription packet will have all of the data being requested from PAGIS. To receive a specific datatype, a tag must be added to the subscription to define the desired datatype. The valid entries for datatype are: Reads, Hits, and CurrentImage.

- Subscribing to Reads will send all plates that are detected by PAGIS regardless of whether or not it has an associated hit.
- Subscribing to Hits will send all plates detected by PAGIS that are on a hotlist and the associated Read data for that Hit.
- Subscribing to the CurrentImage Datastream offers two additional attributes that may be passed as well. The "camera" attribute can be set to determine which camera the image is coming from. If no value is passed for "camera" the value defaults to zero. The "milliseconds" attribute determines how long the system waits between sending the current image. The default value for milliseconds is 1000. If a value of zero is sent, the system will send a single snapshot.

Sample of the Subscription XML Packet

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-subscription>
  <datatype>Reads</datatype>
  <datatype>Hits</datatype>
  <datatype>HitTrigger</datatype>
  <datatype camera="0" milliseconds="1000">CurrentImage</datatype>
</pips-datastream-subscription>
```

HitTrigger

The HitTrigger packet is used to alert other systems that a hit has occurred on the PAGIS system. The packet is greatly simplified from the Reads/Hits XML packet and only contains the license plate text, timestamp and a description of the hit. The description will contain the name of the hotlist that originated the hit and may be used to send additional information.

Sample of the HitTrigger XML Packet

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-hittrigger>
  <timestamp>2011-10-13T09:41:56Z</timestamp>
  <vrm>SBX989</vrm>
  <hotList name='Alpha'>
    <field1><![CDATA[This is Alpha Field 1]]></field1>
    <field2><![CDATA[This is Alpha Field 2]]></field2>
    <field3><![CDATA[This is Alpha Field 3]]></field3>
    <field4><![CDATA[This is Alpha Field 4]]></field4>
    <field5><![CDATA[This is Alpha Field 5]]></field5>
  </hotList>
</pips-datastream-hittrigger>
```

Reads/Hits XML Packet

The Reads/Hits packet contains information about the plate that was detected. This information includes:

- Source – The device that detected the plate
- Camera – The camera on the device that detected the plate
- Read – The Information about the plate that was captured
- VRM – The plate translated to text
- Timestamp – When the read occurred
- GPS – The location coordinates where the read took place
- ImagesPatch – The image of plate in infrared (IR)
- Overview – The image of scene/car in Color
- Hits – The associated hotlist(s) data

Sample of the Current Image XML Packet

NOTE: The Current/Live Image XML Packet contains the current image from the camera. It is sent every 5 seconds.

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-currentimage>
  <timestamp>2011-10-13T09:41:56</timestamp>
  <data>(Image data here)</data>
</pips-datastream-currentimage>
```

Sample Read with Hits XML

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-reads>
  <reads>
    <source>
      <name>PAGIS_90210</name>
      <software name="PAGIS" version="2.6.8" />
      <camera name="Front Left">
        <read>
          <state>TN</state>
          <vrm>SBX989</vrm>
          <confidence>97.5</confidence>
          <timestamp>2011-09-30T09:30:10Z</timestamp>
          <username><![CDATA[shronski]]></username>
          <gps>
            <latitude>-87.4567</latitude>
            <longitude>98.7654</longitude>
          </gps>
          <images>
            <image name='Patch'>
              <type>IR</type>
              <data>

<![CDATA[/9j/4AAQSkZJRgABAQAAAQABA.....................................................................
.....................................................................................................
..... /9k=]]>
              </data>
            </image>
            <image name='Overview'>
              <type>Color</type>
              <data>

<![CDATA[/9j/4AAQSkZJRgABAQAAAQABAAD..................................................................
.....................................................................................................
.... //2Q==]]>
              </data>
            </image>
          </images>
          <misread>0</misread>
          <manual>0</manual>
          <hits>
            <hotList name='Alpha'>
              <field1><![CDATA[This is Alpha Field 1]]></field1>
              <field2><![CDATA[This is Alpha Field 2]]></field2>
              <field3><![CDATA[This is Alpha Field 3]]></field3>
              <field4><![CDATA[This is Alpha Field 4]]></field4>
              <field5><![CDATA[This is Alpha Field 5]]></field5>
            </hotList>
            <hotList name='Beta'>
              <field1><![CDATA[This is Beta Field 1]]></field1>
              <field2><![CDATA[This is Beta Field 2]]></field2>
              <field3><![CDATA[This is Beta Field 3]]></field3>
              <field4><![CDATA[This is Beta Field 4]]></field4>
              <field5><![CDATA[This is Beta Field 5]]></field5>
            </hotList>
          </hits>
        </read>
      </camera>
    </source>
  </reads>
</pips-datastream-reads>
```



PIPS TECHNOLOGY™

DETECTION INNOVATION



PAGIS User's Manual

Version 2.14

Updated 3/30/2020

NEOLOGY MOBILITY TECHNOLOGIES

Table of Contents

Table of Contents 2

NOTICES 3

Technical Support 3

Design Changes 3

Trademarks 3

Copyright 3

Version 3

INTRODUCTION 4

1.1 Dual Lens Color and Infrared Camera 4

1.1.1 Available Products 4

1.2 Using This Manual 5

SCREEN REFERENCE 6

2.1 The PAGIS Software Login Screen 6

2.1.1 Logging on with the Default Administrative Account 6

2.2 Main Screen - Live View 7

2.2.1 Getting Started in PAGIS 7

2.3 The PAGIS Navigation Buttons 8

2.3.1 Camera Control Buttons 8

2.3.2 GPS Indicators 9

2.3.3 Camera Firmware Update (Restricted Users) 9

2.3.4 Day/Night Mode 9

2.4 Begin Shift 10

2.4.1 Sync via USB Thumb drive (or Local Source) 10

2.4.2 Sync via Wireless Network 10

2.4.3 PAGIS Auto-Sync Settings 10

2.4.4 Begin Shift – Additional Information 10

2.5 End Shift 10

2.5.1 Sync to BOSS 10

2.6 Cam Mode Button 11

2.6.1 Camera Modes 11

2.7 Taking a Picture 11

2.8 Search Entry Screen 12

2.8.1 Searching Synchronized Hotlists for License Plates 12

2.8.2 Searching Locally Stored Reads and Hits 12

2.8.2.1 Searching for a Match 13

2.8.3 Wild Card Symbols 13

2.8.4 Manually Adding a Plate to PAGIS 14

2.8.4.1 ADD VLP Query 14

2.8.4.2 ADD VRM Report Screen 14

2.9 The Review Screen 15

2.9.1 Summary Review Section 15

2.9.2 Review Navigation Buttons 15

2.9.3 Reads 16

2.9.3.1 Reads Result Screen Navigation Buttons 16

2.9.3.2 Interactive Buttons – Reads Screen 16

2.9.4 Hits 17

2.9.4.1 Hit Screen Attributes 17

2.9.4.2 Hit Screen Function Buttons 18

2.9.4.3 Interactive Buttons – Hits Screen 18

2.9.4.4 Set Disposition – Additional Detail 18

2.9.4.5 Add Intel – Additional Detail 19

2.9.5 Misreads 19

2.9.5.1 Marking a Record as a Misread: 20

2.9.6 Audits 21

2.9.7 Targets 21

2.9.7.1 The Targets Screen 22

2.9.7.2 Targets Screen Navigation Buttons 22

2.9.8 Databases 23

2.9.8.1 Databases Screen Functions 23

2.9.8.2 Databases Screen Navigation Buttons 23

2.9.8.3 Databases Edit- “Manual Reports” 24

TROUBLESHOOTING TIPS 25

3.1 Troubleshooting & Tips 25

3.1.1 PAGIS with NetMotion VPN 25

3.1.2 Cisco VPN Client: 25

3.1.3 Microsoft .NET 3.5 Installation 25

3.1.4 Firewall Settings for Client-Server Installations 25

APPENDIX A: THE GLOSSARY 26

APPENDIX B: PAGIS SOFTWARE DATABASE FILE 27

APPENDIX C: FAQ 29

NOTICES

The information within this manual is authorized for distribution to customers, authorized service center personnel, and distributors of Neology. Every effort has been made to supply correct information. However, Neology assumes neither responsibility for its use, nor for any infringements of patents or other rights of third parties, which may result from its use. No license is granted by the manufacturer under any patent or patent rights. Neology reserves the right to modify and update the equipment at any time without prior notice. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means to a third party without the prior consent of the copyright holder. The manufacturer's warranty will be invalidated if untrained personnel operate the equipment or if any attempt is made to service the equipment by unauthorized personnel.

This manual contains confidential and proprietary information and should not be redistributed except as needed for proper use and maintenance of the agency's Mobile ALPR system.

Technical Support

Service of this equipment by replacement of parts, on-site repair, routine maintenance inspection, and scheduled remote support session is available. Please contact PIPS Technology's ALPR Technical Support.
Phone: 833-PIPS-LPR (833-747-7577), Option 2
Support Team Email: Support@PIPSTechnology.com
For Customers in Europe, Middle East and Africa: Support@PIPSTechnology.co.uk
Web: www.pipstechnology.com
Fax: 858-391-0264
Corporate Office: 13520 Evening Creek Drive Suite 460. San Diego, CA 92128

Design Changes

Neology reserves the right to change the design of any product from time to time without notice and with no obligation to make corresponding changes in products previously manufactured.

Trademarks

PIPS Technology™ is a trademark of Neology Inc., and either registered or pending registrations in several jurisdictions. Windows, Windows 7, Windows 8, Window 10, and .NET are all trademarks of the Microsoft Corporation. Other trademarks and registered trademarks are the property of their respective owners.

Copyright

The Neology / PIPS Technology PAGIS Software is copyright of Neology. All rights reserved. This product contains confidential and trade secret information of Neology and is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portions of it, may result in civil and criminal penalties.

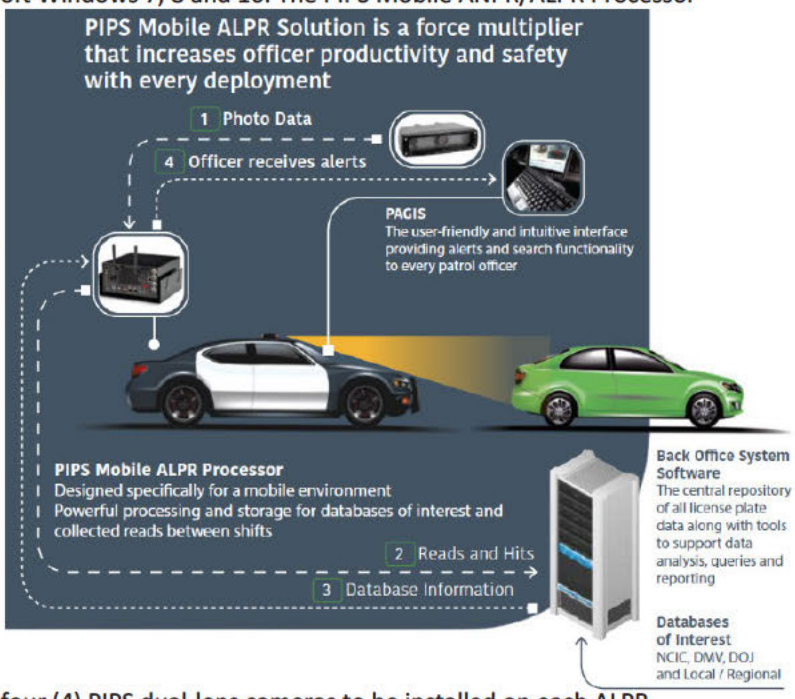
Version

This manual demonstrates the attributes of the Neology / PIPS Technology PAGIS Software Version 2.14 and was last updated in March 2020.

INTRODUCTION

PIPS Technology's Automated License Plate Recognition (ALPR) software solution called PAGIS utilizes dual-channel, dual-lens, cameras to "read" plates. Our software is optimized to run on the Mobile Processor itself or in conjunction with a mobile data computer (MDC). Our mobile software is compatible with Microsoft Windows 7, 8 and 10. The PIPS Mobile ANPR/ALPR Processor comes equipped with Microsoft Windows 7 Embedded.

The PAGIS Software processes the infrared plate image provided by any of the cameras and then interprets the plate number through Optical Character Recognition (OCR) via the mobile processor. The PAGIS application then searches for any matches of the plate with those listed in the databases, or "hotlists," distributed from the PIPS Back Office System Software (BOSS) or other external sources.



WARNING: To reduce the risks associated with impact, which if not avoided, could result in serious injury or death: Do Not interact with the ALPR system while driving in hazardous situations. The PIPS mobile camera series and License Plate Capture Software are not intended for use in hazardous environments, so that the User and/or others are not put at risk for personal injury and/or property damage.

1.1 Dual Lens Color and Infrared Camera

The PIPS Technology Mobile ALPR System allows for a maximum of four (4) PIPS dual-lens cameras to be installed on each ALPR vehicle provided that the vehicle supports the additional mounting equipment.

Each dual-lens mobile camera uses visible light to take color overview pictures of the vehicle and uses infrared (IR) illumination to capture the license plate's alphanumeric characters. IR illumination offers the best capture performance of reflective license plate characters for the following reasons:

- State issued license plates are designed to be highly reflective to IR light.
- Cameras using IR capture technology do not depend on the presence of visible light to function.
- Cameras using IR capture technology are not negatively impacted by the effects of headlights, solar glare, or total darkness.
- IR light penetrates rain and fog better than visible light.
- Due to these attributes, the system can be used 24 hours a day, seven days a week.

1.1.1 Available Products

Additional information about this and other PIPS Technology applications, cameras, and solutions are available on the PIPS web site: http://www.pipstechnology.com

1.2 Using This Manual

The section overview of this software manual are as follows:

Section 1: The Introduction and Basics

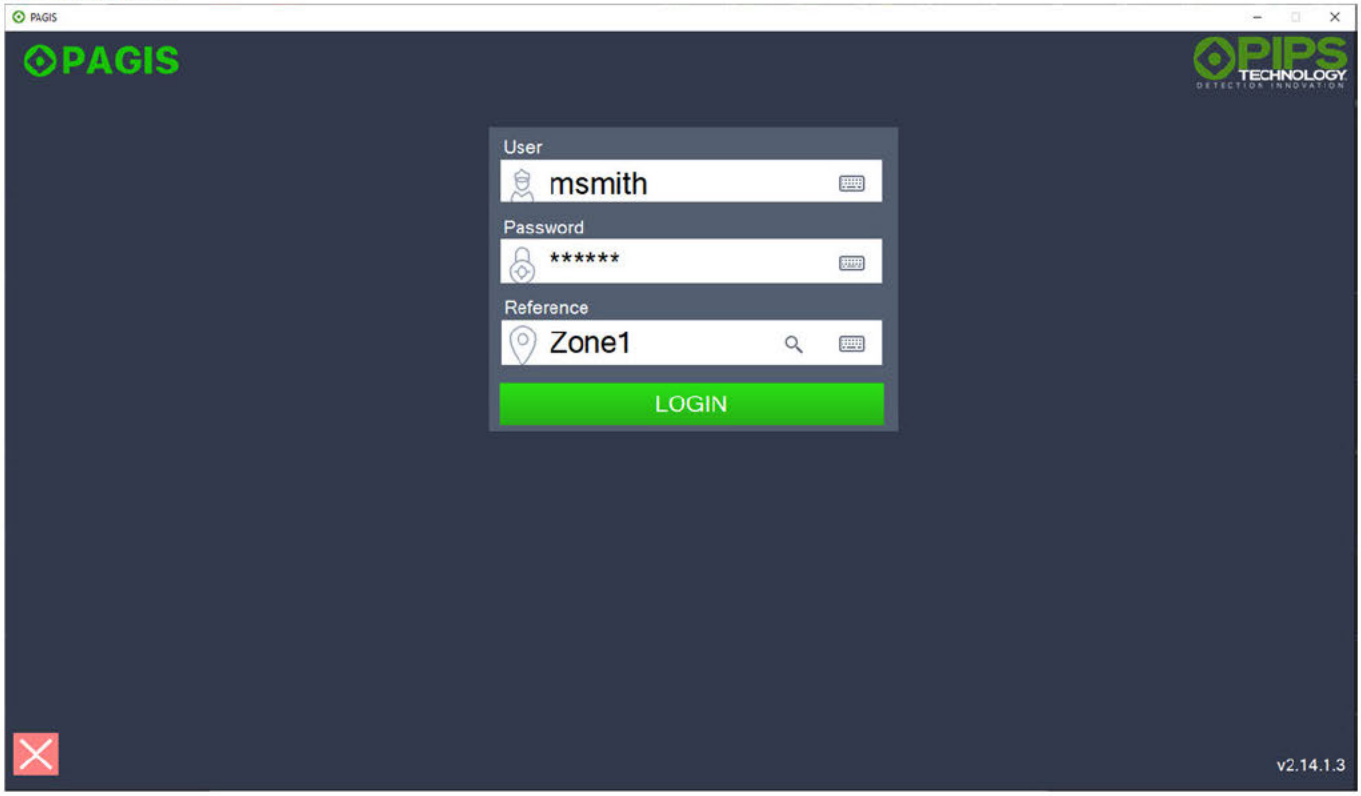
Section 2: PAGIS User's Section: Explains screen function and User Operations in the PAGIS Software

Section 3: Troubleshooting Tips

Appendices: Additional features and details

SCREEN REFERENCE

This section guides the user through the PAGIS Software screens and the available options. Screens are grouped according to function. When a button is grayed out or missing, the option is not available, or no information has been accrued to activate it.



2.1 The PAGIS Software Login Screen

The PAGIS Software allows users with various access privileges to use the same MDC. For users with touch screen monitors, the Keypad button immediately to the right of any text box gives the user access to an on-screen keyboard for data entry.

User Field: The alphanumeric string assigned to identify the user. Usernames are not case sensitive.
Password Field: Password of the assigned user logging in. Passwords are case sensitive.
Reference Field: This is an optional field utilized to fit a number of use cases. A user can manually enter a reference at logon, leave the field blank, or select list of unique tags that will be associated with all data captured while logged in. If the Administrator has configured a default reference tags, that information will be displayed automatically. Otherwise, it will be blank.
Login Button: Submits the username and password to attempt a login.
Exit Button: By clicking the X icon in the lower left-hand corner, the user can exit/close the PAGIS Software.

2.1.1 Logging on with the Default Administrative Account

The PAGIS Software includes a default administrative account that can be used for the initial configuration. To do so, simply click the **Login** button with the User and Password fields blank.

NOTE: System Administrators are strongly encouraged to configure users for PAGIS just before, or soon after the installation and setup. PAGIS users accounts are created and maintained in BOSS. Once Users are established by the BOSS System Administrator, the default user account is automatically disabled. Best practices are to be certain at least one User account has administrative privileges.

2.2 Main Screen - Live View

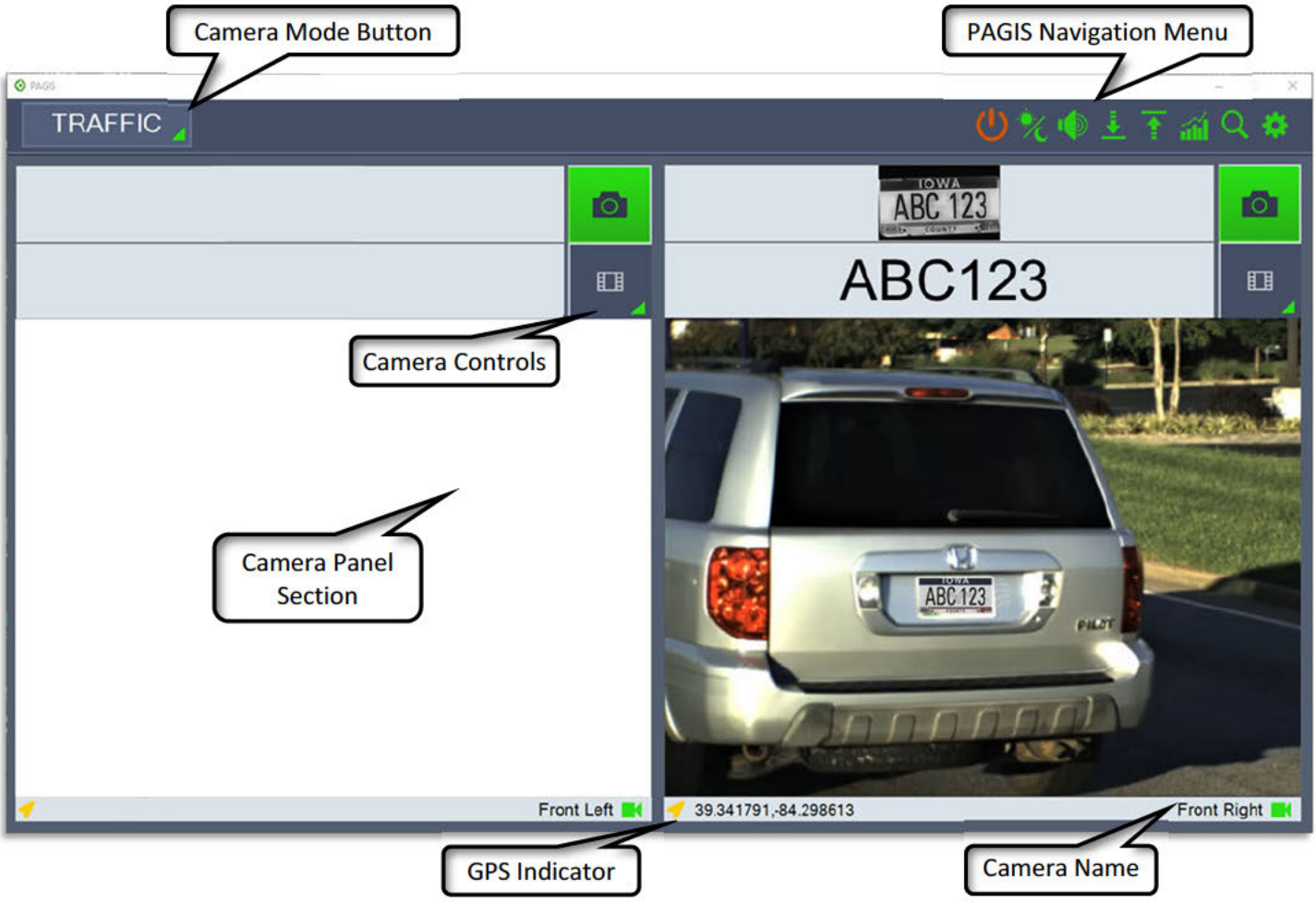
Upon a successful login, the user will see the Main screen (Live View). This is the default view and starting place of all PAGIS Software features. (NOTE: Access to features is based on user group rights established in BOSS.)

The Main Screen is also the place users will monitor read images and ALPR "hits". At the initial startup of the system it is normal to see only a blank/grey screen for a few seconds. Once a connection has been established with the mobile cameras, white boxes will be displayed showing the live-feed camera panels. At this point, the system is ready to capture reads/plates.

2.2.1 Getting Started in PAGIS

By default, PAGIS loads into a static view. This means live video will not automatically appear in the camera panels (white boxes) until a plate has be captured or the user selects one of the live feed options.

Once a plate is "seen" by a camera assigned to the current viewing mode (Traffic vs Parking), it will display the captured information in the corresponding camera panel. Each plate capture is also accompanied by a short "Beep" to audibly alert the user a read has taken place. (NOTE: If the user is in the Traffic Mode at the time a parking camera reads a plate, there will be a sound effect, but no plate image will be displayed on screen unless that plate is on a synchronized Hotlist or until the user switches to Parking Mode.)



2.3 The PAGIS Navigation Buttons

4885

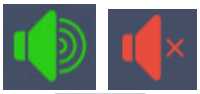
This section provides a quick reference guide to the available navigation buttons of the Live View screen.



The Camera Mode button is located in the upper left corner and is used to switch between the configured camera modes. Once configured, the name will change to a selected mode. The default values are “ALL”, “Traffic” and “Parking”.



The Logoff button is located in the upper right of the window. When selected, the user will be logged out of PAGIS and return to the login screen.



The Sound button is located to the right of the Logoff button. When selected, this button with toggle the PAGIS system sounds On and Off.



Day/Nite mode switches PAGIS between day & night mode screen skins.



The Begin Shift Synchronization button is located to the right of the Sound button. When selected, this will reach out to the BOSS server to download users, hotlists, and other system settings.



The End Shift Synchronization button is located to the right of the Begin Shift Button. When selected, this will upload any previously unsent reads, images, and audits to the BOSS server.



The Statistics/Review button is located to the right of the End Shift Button. When selected the user is able to review Databases/Hotlists, Reads, Targets, and other PAGIS information.



The Search button is located to the right of the Review Button. When selected the user can search his/her reads as well as manually add a license plate to a temporary hotlist.



The Admin/Settings button is located in the upper right corner of the screen. This button is only viewable to Admin level users and allows for system configuration changes and setup.



Firmware update icon will atomically appear when PAGIS detects a new firmware is available for the P720 mobile cameras. All user types are notified, but only Admins can apply the update.

2.3.1 Camera Control Buttons

The dual-lens cameras can capture both color and an infrared image. Formerly, there were a total of three buttons that allowed the user to view the IR and color feed as well as capture a picture directly from PAGIS. Now there is a toggle button to switch between color and IR views and a separate button to take a picture. These buttons are displayed on the main Live Screen as shown below:



The Camera View Selector button: This is the default state at login showing the Static View. (**NOTE**: PAGIS does not automatically display a life feed.)



Color View: by clicking on the Camera View Selector button once, the user will switch to the Color View Mode. This displays the current view of the color camera and will time out after 60 seconds.



IR View: by clicking on the Camera View Selector button twice, the user will switch to the Infrared (IR) View Mode. This displays the current view of the IR camera and will time out after 60 seconds.



The Take Pic button: Just above the Camera View Selector button is the “Take Pic” button. This button allows the user to quickly take a picture from the camera currently viewed.

2.3.2 GPS Indicators

GPS is stamped on each read and hit as capture events take place by the system. The signal strength and location indicators are located underneath the camera panels at the bottom of the Live Screen.

39.341788,-84.298518 Shows an example of the Location Indicator displaying the Lat/Long on the most recent read

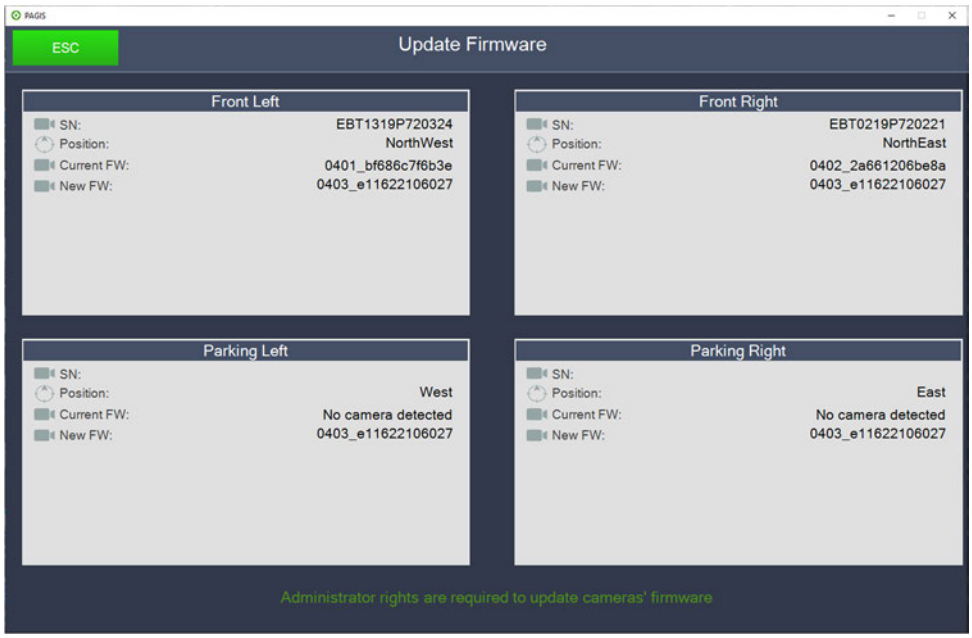
A green or yellow indicator shows a strong or medium strength GPS lock.

A red indicator shows there is no available GPS information.

2.3.3 Camera Firmware Update (Restricted Users)

Camera firmware update provides a means for PIPS to update the camera software to enhance and or correct camera performance. The frimware icon will only apper when update is avialable.

- The firmware update process only updates camera that are attached and function on the mobile processor.
- Restricted PAGIS users are only notified and displayed update information, only a PAGIS administrator can apply the FW update.

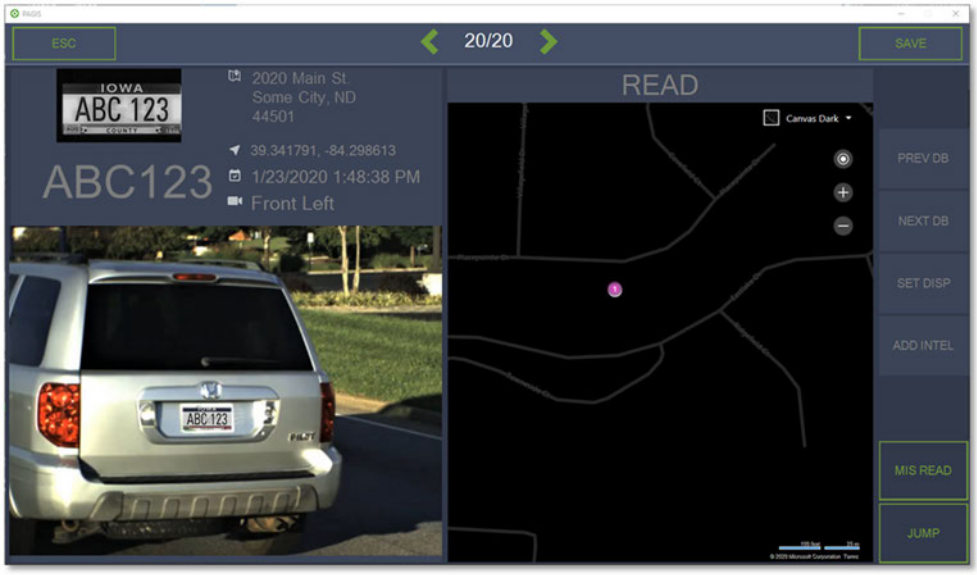


Firmware Updater Window List.

- Title “Camera Name”.
- Camera serial number.
- Position.
- Current FW version.
- New FW version available.

2.3.4 Day/Night Mode

Day/Night mode changes PAGIS user interface skins to a darker appearance to reduce illuminating the vehicle interior.



2.4 Begin Shift

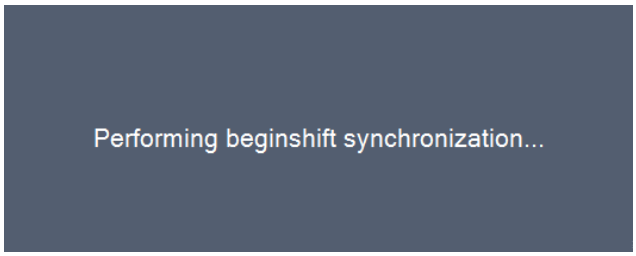
Begin Shift is thought of as the first step for all PAGIS users. From the Live View Screen, the PAGIS user must click the Begin Shift button twice. Once to select the function and once more to launch the Sync. With most agencies, this action utilizes a wireless network to import all the necessary data used during a shift (Hotlists, Dispositions, and Targets) directly from the BOSS Server. However, agencies can also configure their systems to perform this function via Thumb drive or a local source file.

2.4.1 Sync via USB Thumb drive (or Local Source)

Depending on the agency network, some alter the default PAGIS/BOSS configuration mode to use a USB Thumb drive or locally stored file on the MDC/Laptop instead of the wireless Sync. In order to synchronize effectively, the user must first confirm he/she has access to the source location before initiating Begin Shift. **NOTE**: All synchronizations using this method must be performed manually. To learn more about this process, refer to the "Client Tools" section of the BOSS Manual.

2.4.2 Sync via Wireless Network

Synchronizations over a wireless network provide the agency with additional automated features. Best practices recommend the user manually launch Begin Shift from the Live View Screen at the beginning of every patrol shift. However, it is possible for users to allow PAGIS to synchronize via its auto-sync settings. When a manual Begin Shift is launched, the Main View Screen removes the camera feeds and displays a status window of the Sync process. Once the Begin Shift operation is complete, PAGIS will return to the normal Main View Screen.





2.4.3 PAGIS Auto-Sync Settings

PAGIS auto-sync settings are best thought of as how PAGIS receives additional updates and maintains the downloaded ALPR data throughout the entire patrol shift. This prevents the need for the officer to manually perform Begin Shift functions multiple times a day. The auto-sync occurs every 30 seconds and receives data in small batches. The batches are not to exceed 1MB in size for every minute of download. In addition to receiving data, the auto-sync function also uploads a copy of data collected by PAGIS and sends it to BOSS for reporting/processing.

2.4.4 Begin Shift – Additional Information

By default, the synchronizations in PAGIS receive only what has been changed to the ALPR data since the last Sync. Meaning, if some plates have been removed from a Hotlist and others have been added, the system will only transfer that data instead of downloading the entire Hotlist each time the Begin Shift is launched. This helps to reduce the amount of data transferred over the agency's network. **NOTE**: Begin and End Shift synchronization, as well as all auto-sync features, are dependent upon stable communication to the BOSS server via an active data connection.

2.5 End Shift

End Shift in PAGIS is the process in which all the collected ALPR data (Reads, Hits, and Images) from the recent shift is uploaded to the BOSS server and cleared from the local cache. As with Begin Shift, the agency has two options. They can choose to Sync via USB Thumb drive or via wireless connection. Best practices recommend users perform an End Shift Sync at the end of every patrol.

2.5.1 Sync to BOSS

At the end of every shift, the accrued ALPR data should be exported to BOSS. Just like with Begin Shift, the user must click the button twice to launch it (once to select it and once more to execute the Sync). During the Sync, PAGIS uploads any Reads, Hits, and Images not already synchronized to BOSS and purges these items from the local cache on the MDC's hard drive. Completing an End Shift also removes any VLP entries manually added to PAGIS during the shift.

2.6 Cam Mode Button

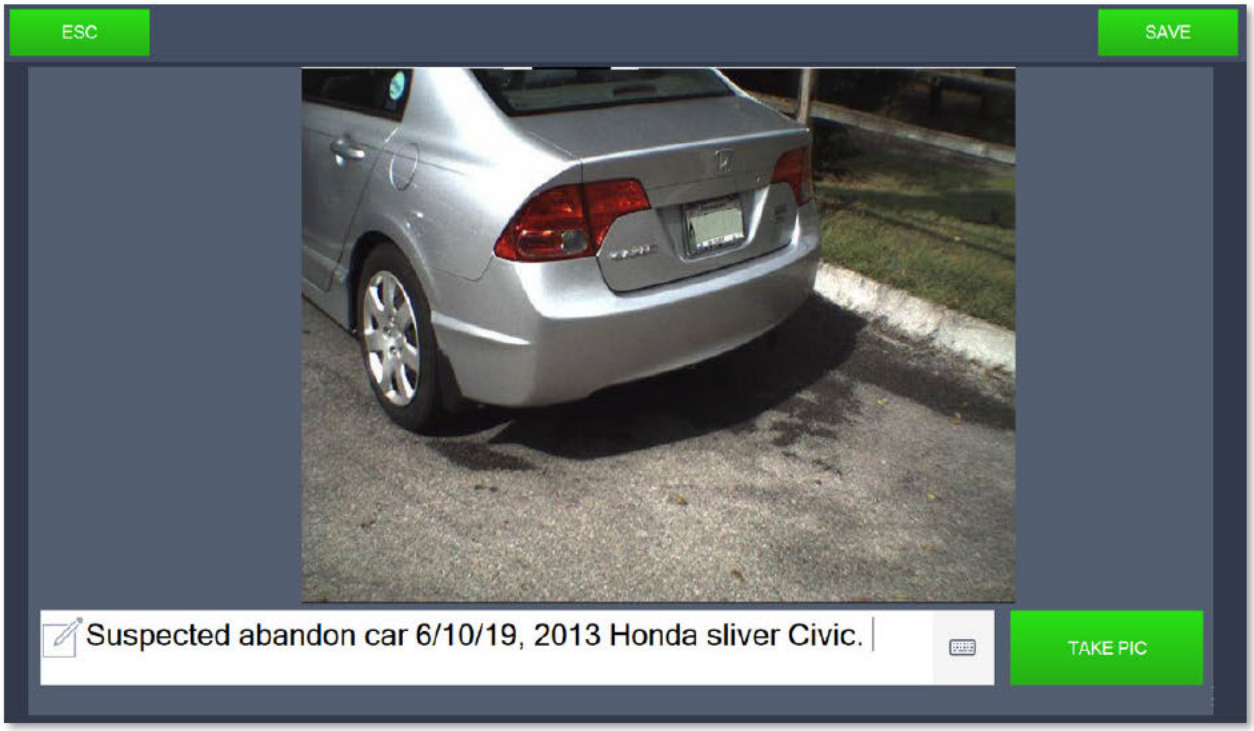
Clicking the Cam Mode button in the upper left corner of the Live View Screen allows the user to cycle through the different camera modes configured by the PAGIS Administrator. Changing the camera mode changes which cameras are displayed on the Main Screen.

2.6.1 Camera Modes

By default, PAGIS provides "Parking" and "Traffic" as the two configuration modes. Users often switch these modes to suit their current use-case. For example, an officer in a parking lot will often switch the mode to "Parking" so s/he can see the parking cameras on the Live View Screen. They can then switch back to "Traffic" when monitoring city streets.

2.7 Taking a Picture

The PAGIS software has ability to quickly take a picture from one of the currently displayed ALPR cameras on the Live Screen. The user only needs to click on the Take Pic button.



To Take a Picture:

1. From the Live View Screen, press the Take Pic button from the desired camera
2. The image taken will be displayed
3. Enter a description of the picture in the text field at the bottom of the screen
4. Press Save to save the picture or Escape to cancel. Either action will return you to Live View.

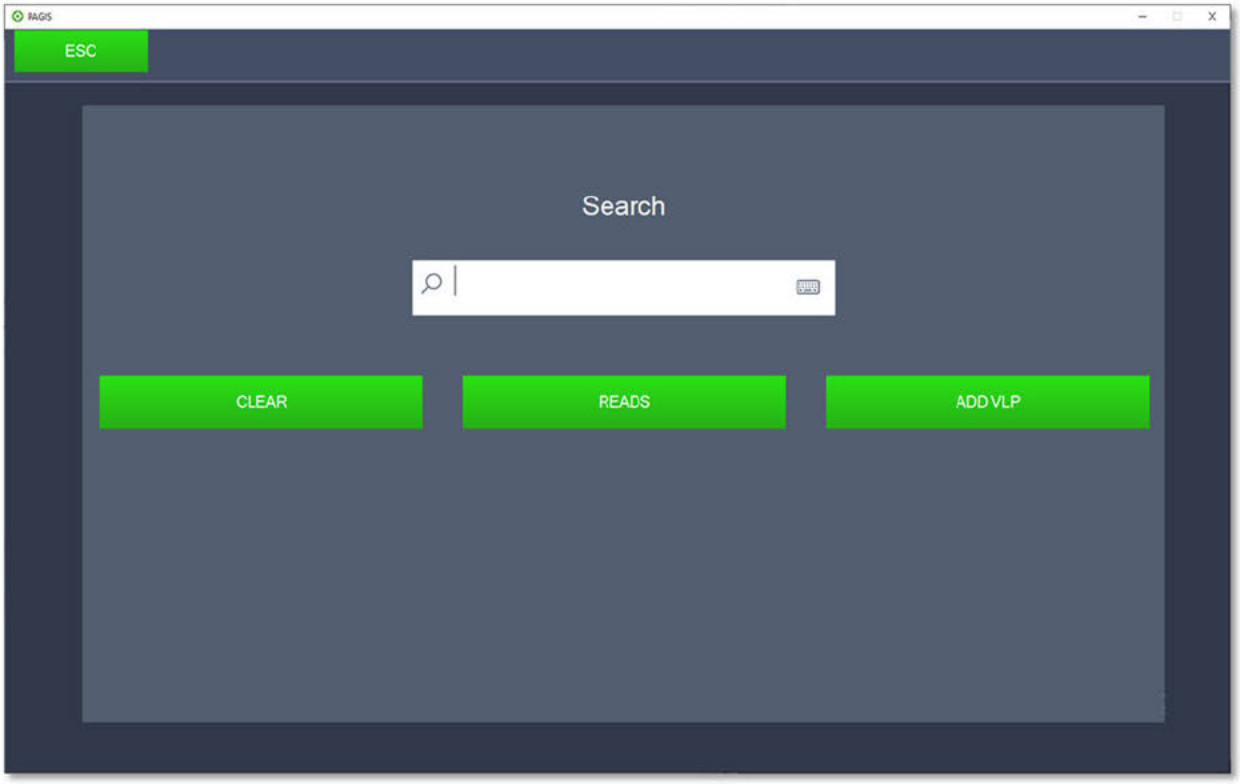
NOTE: The picture will Not be saved if a description/note is not entered in the text box.

To View the Saved Images:

1. Navigate to the Review menu in PAGIS
2. Select Audits
3. The user will be able to see a thumbnail of the image and the saved text/note
4. In order to review the saved images at a later time, the user will need to run the Audit Report from BOSS.

2.8 Search Entry Screen

Pressing the Search button icon from the Live View screen or SEARCH from the Databases window allows the user to search all manually entered plates as well as all BOSS synchronized databases (Hotlists) for license plate and target information. Users can also search all locally stored reads/images accrued since the last End Shift by clicking the Reads button instead of pressing the Enter key.



2.8.1 Searching Synchronized Hotlists for License Plates

By entering a vehicle license plate number (VLP) and pressing the Enter key or the ADD VLP button, the user can quickly search all the stored plate information locally collected as well as the information from all synchronized hotlists distributed from the BOSS server. **NOTE**: Hotlists can only be searched by entering complete VLPs. Wildcards and partial plate numbers will not return results.

Search Box: The text field used to enter the desired plate search via alphanumeric characters and/or wild card symbols.

Clear Button: Clears the contents of the search box.

Driver's License Info: The search field can also check the Hotlists for any DL information stored (Not available all countries).

Reads Button: This button searches for a match from all the reads/hits locally stored on the MDC/Laptop.

ADD VLP: Searches all locally stored hotlists for the plate and if there's no match, allows the user to add the plate to the "Manual Reports" alert list for use in the field. **NOTE**: All manual entries are cleared with each End Shift

ESC: The Escape button allows the user to exit to the Main/ Live View screen.

2.8.2 Searching Locally Stored Reads and Hits

As mentioned previously, this search function allows users to find reads and hits directly from their recent patrols using the search field and the Reads button. These searches pull only the reads and hits locally gathered/stored since the last time the user completed an End Shift. **NOTE**: The search results are specific to each Windows User Profile and do NOT pull images from the BOSS server.

2.8.2.1 Searching for a Match

4890

- From the Search field, users may enter a plate (or partial plate with wildcards) and then click the **READS** button.
- Results are displayed with the data gathered at the time the read was taken (See example below).
- Each result should display the infrared (IR) image of the plate as well as the color overlay of the vehicle for review.
- Each result shows the GPS data, Closest address point, Time and Date, and the Camera that read the plate.
- If there are multiple results, the user can cycle through them by clicking the left and right navigation arrows.



2.8.3 Wild Card Symbols

The use of wild card symbols in the Search box allows greater flexibility for the user, but may return a larger set of results.

- Wild card searches performed using the asterisk (*) designates an unknown number of characters.
- Wild card searches performed using the underscore (_) indicates a single missing or unknown character.
- Searches can be performed using one, both or no wild card symbols.

Example: The officer received an alert from Dispatch looking for a vehicle plate containing the letter J and the number 8 separated by one character. Because the officer doesn't know how many characters there are before or after the J and 8, he enters *J_8* in the search box to review all possible matches of J and 8 separated by only one digit.

2.8.4 Manually Adding a Plate to PAGIS

PAGIS allows users to manually add a plate of interest directly into the software as needed. Once saved, these entries are stored as part of the Manual Reports alert list and work just like any other Hotlist synchronized from the BOSS server.
NOTE: These additions are designed to be temporary and are cleared from the software with each End Shift.

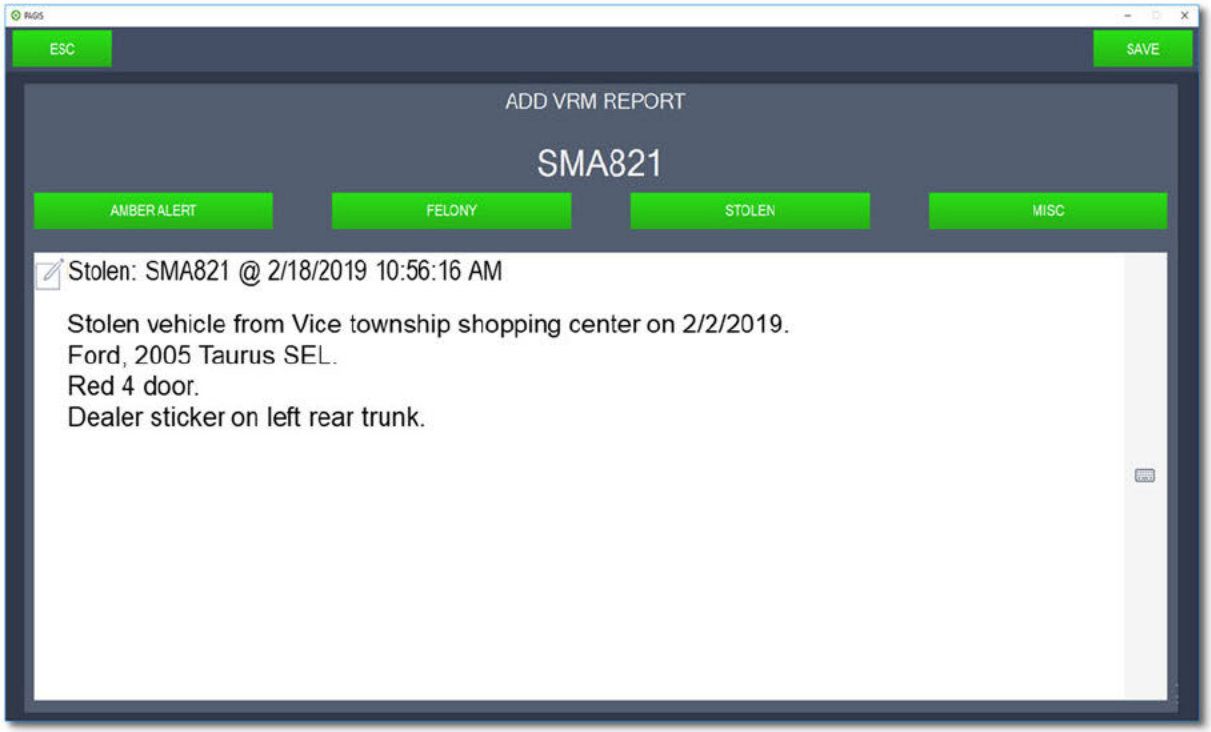
2.8.4.1 ADD VLP Query

Before an entry is added to the Manual Reports Hotlist in PAGIS, the software searches all stored databases for a match. If a match occurs, a message will display under the search box showing which Hotlist(s) it has been found in. If the VLP query does not return a match, the "ADD VRM REPORT" screen appears.



2.8.4.2 ADD VRM Report Screen

If the desired plate does not already reside in another Hotlist, the ADD VRM Report Screen becomes accessible to the user.



1. From the Search Entry Screen, enter the desired plate to add.
2. Click the ADD VLP button. If no match is found on any other hotlist, the "Add VRM Report" screen will appear.
3. Click to select the applicable alert type (AMBER ALERT , FELONY , STOLEN , or MISC)
4. Either leave the default information or add additional detail.
5. Click Save at the top right to add the plate to the Manual Entries Hotlist

2.9 The Review Screen

4892

PAGIS allows users to review all locally stored data from one easy location. Clicking the Review icon from the Main Screen launches Review. This screen is divided into the Summary View Chart and sub-section navigation buttons to the right.



2.9.1 Summary Review Section

The Summary View Chart is divided into five categories and allows a user to review the information collected during their shift at a glance.

Total Reads: Shows the total number of Reads/Hits synced to BOSS and the total number of reads captured during the shift.
Reads: Shows the total number of reads synced to BOSS and the total number of reads captured during the shift.
Hits: Shows the total number of hits synced to BOSS and the total number captured during the shift.
Misreads: Shows the total number of reads marked as a "misread" synced to BOSS and the total marked during the shift.
Audits: Shows the total number of audits synced to BOSS and the total number of audits during the shift.
Targets: Shows only the number of targets downloaded from BOSS.
(NOTE: The Sync value will always be zero for customers using Disk Sync mode/Client Tools.)

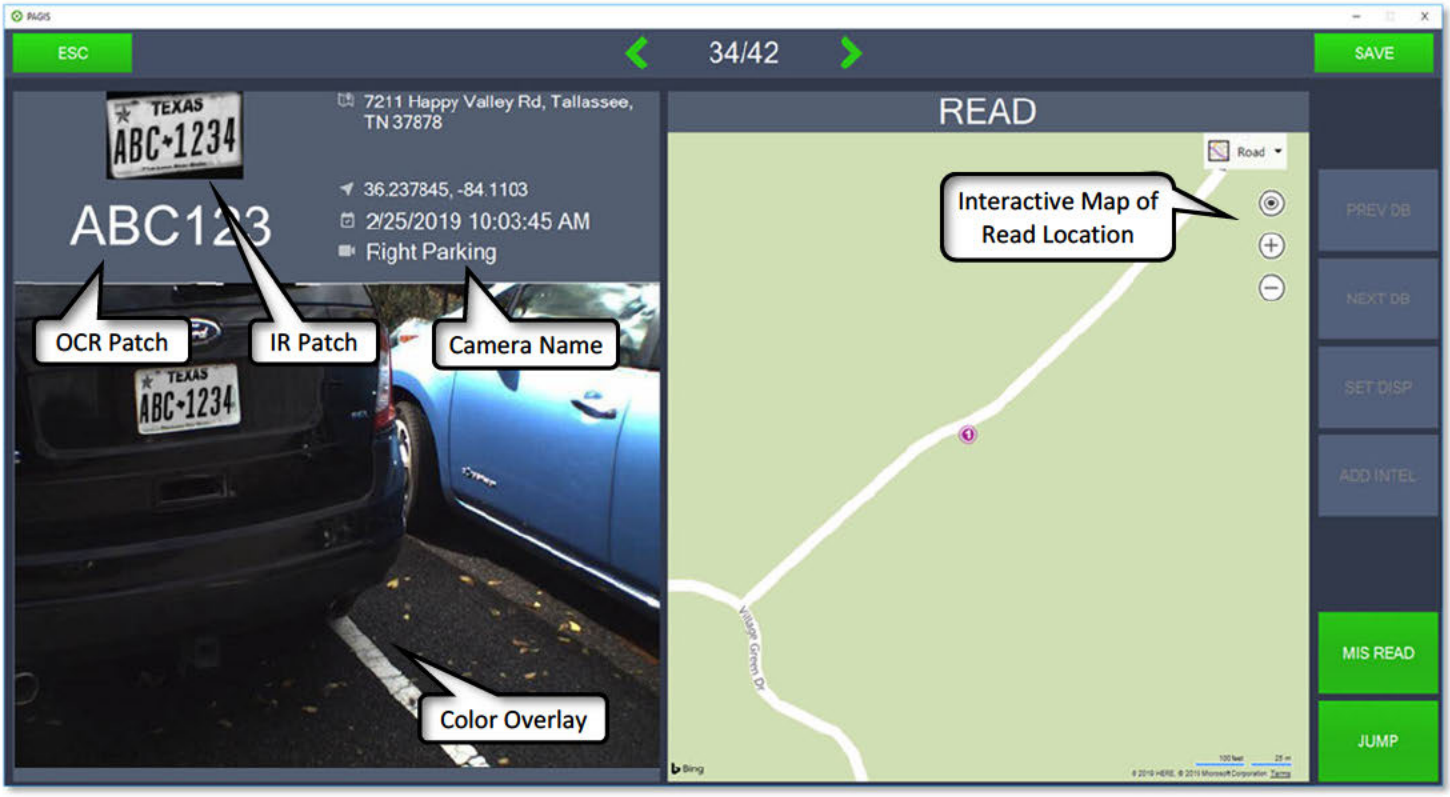
2.9.2 Review Navigation Buttons

The navigation buttons allow the user to review specific sets of information gathered during the shift.

Reads: Review all plate detections that have occurred since the last End Shift synchronization.
Hits: Review the hit alerts for Vehicle License Plate (VLP) reads that matched a Hotlist.
Misreads: Review reads and/or hits that have been manually flagged during the shift as misreads, where the plate number in the image does not match the OCR interpretation of the plate (e.g., a letter O misread as a Q or zero).
Audits: Review failed and successful logons, any manual data entered during the shift, pictures taken and all manual license plate searches.
Targets: Review targets that have been synchronized/downloaded from Boss.
Databases: Review all the Hotlists currently distributed to this PAGIS laptop/MDC.
Esc: Returns the user to the previous screen.

2.9.3 Reads

From the Main Screen, the user can review his or her accumulated Reads (those gathered since the last End Shift was completed) by clicking on the Review icon and then selecting the Reads Navigation button. The Read Review Screen is divided into two main sections. The left side displays the information gathered at the time of the read and the right side displays an interactive map of the GPS location.



NOTE: Buttons that are greyed out indicate options that are not available in the current view. For example, the Reads and Hits review screens share the same layout but different on-screen options.

2.9.3.1 Reads Result Screen Navigation Buttons



Read Count: The left number is the current record. The right number is the total available for review.

Next/Previous button: The arrows on either side of the read count allow the user to navigate back and forth to review reads/results.



MisRead button: When the button is green it indicates the record has NOT been edited as a Misread by a user. Once a Misread is saved, this button will turn grey and the record title will update.



Jump button: Allows the user to "jump" to a specific record without the need to navigate one record at a time using the Next/Previous buttons.



Save button: Apply any changes/edits and return to the Main Screen.



Escape button: Returns the user to the Main Screen.

2.9.3.2 Interactive Buttons – Reads Screen

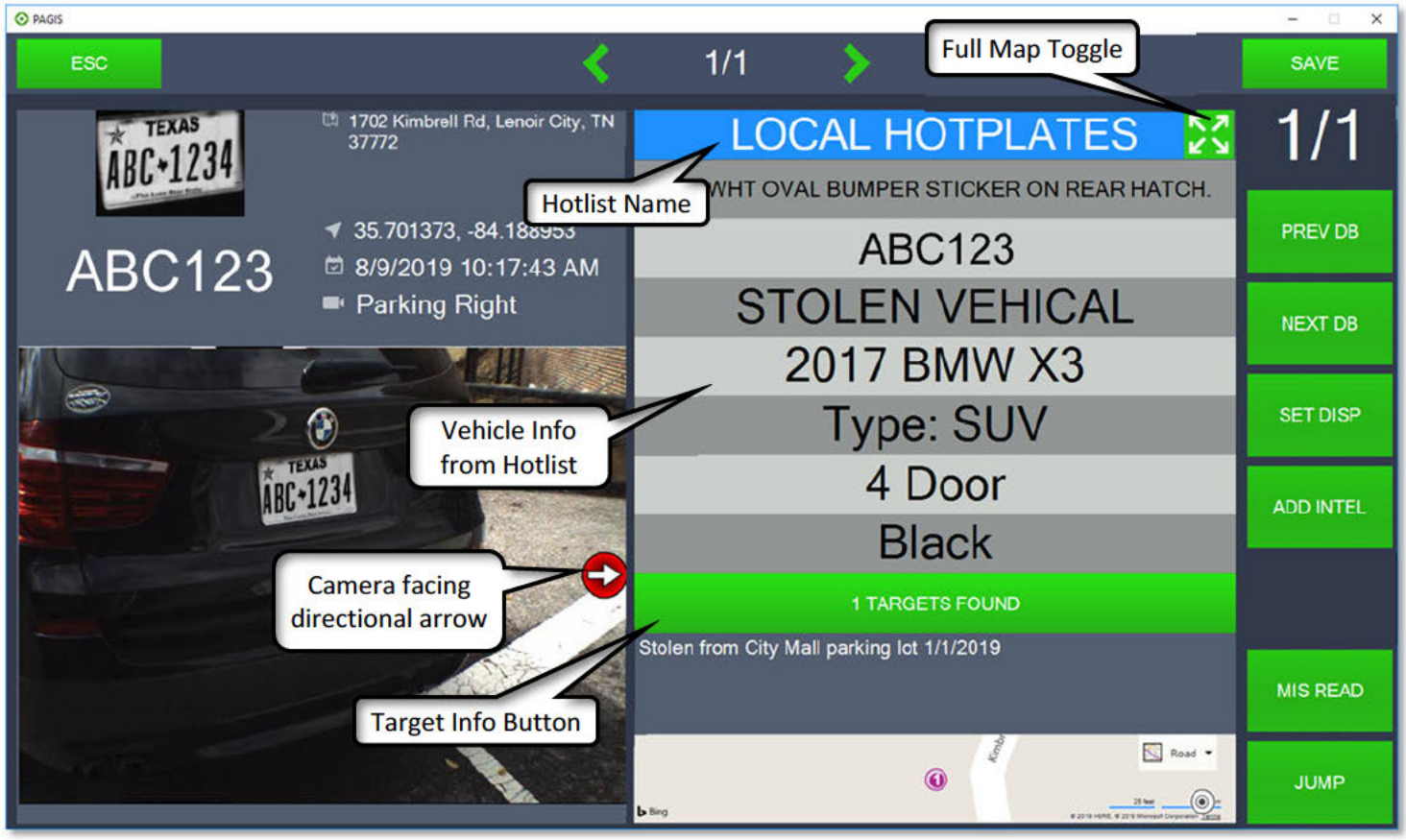
From the Reads Review, the user can interact with the following:

- IR Patch: The user can click on the IR "Patch" plate image to open a full-screen view.
- OCR Patch: The user can click on the OCR "Patch" image to edit the license plate number if necessary/Misread.
- Color OV Image: The user can click on the color image to open a full-screen view.
- Map: The user can manipulate the interactive map of the read location (Map Type, Scroll, and Zoom).

2.9.4 Hits

Users can manually access the Hits Section by first selecting the Review icon from the Live View Screen and then clicking the Hits Button. The Hits Screen is also divided into two main sections. The left side displays the information gathered from the ALPR equipment during the read. And the right side displays the information provided by the associated alert list.

NOTE: Each time a VLP matches a Database value (a license plate read by the system matches a Hotlist entry), PAGIS plays an audible tone and automatically displays the Hit Screen to alert the user.



2.9.4.1 Hit Screen Attributes

Hit Count and Navigation Buttons: Displays the total Hit count as well as the Next/Previous navigation buttons.
IR Patch Image: A thumbnail image of the license plate from the IR camera.
OCR Text: The character string the OCR engine generated from the current plate.
GPS Location: The GPS coordinates at the time of the hit. (If a GPS device is not attached, the Lat/Long is displayed as 0,0).
Date and Timestamp: The date and time when the read/hit was captured.
Overview Image: The overview image of the vehicle from the Color Camera. (**NOTE**: Color images require visible light)
Camera Name: The name of the camera that captured the read ("Right Parking" in the screenshot).
Hotlist Name: This is the name of the Hotlist or "Database" where the plate was matched.
Target Button: When available, this indicates a person of interest is associated with the Hit and opens the Targets Screen.
Vehicle Information: The area of grey bars will display the related vehicle information from the Hotlist. Any information added manually by the user will appear in the Text Box near the bottom of the screen.
Interactive Map: Shows the location the Hit took place. Users can access full-screen view by clicking the map or the toggle .

2.9.4.2 Hit Screen Function Buttons



The Hit Count Indicator: shows how many Hotlists the current Hit has registered against.



Previous DB button: This button moves the user to the previous Database/Hotlist that produced a Hit.



Next DB button: Pressing this button moves the user to the next Database/Hotlist that produced a Hit.



The Set Disposition button: prompts the user to report the disposition of the hit by selecting one of the approved codes assigned in BOSS by the Administrator.



The Add Intel button: allows the user to add additional information regarding the current Hit.



The Misread button: allows the user to flag the Hit as a misread.



The Jump button: Allows the user to "jump" to a specific Hit instead of navigating one at a time.

2.9.4.3 Interactive Buttons – Hits Screen

- IR Patch: The user can click on the IR "Patch" image to open a full-screen view.
- OCR Patch: The user can click on the OCR "Patch" image to edit the license plate number if necessary/Misread.
- Target Button: Shows associated person(s) of interest and opens the Targets Screen.
- Color OV Image: The user can click on the color image to open a full-screen view.
- Map: The user can manipulate the interactive map of the read location (Map Type, Scroll, and Zoom).

2.9.4.4 Set Disposition – Additional Detail

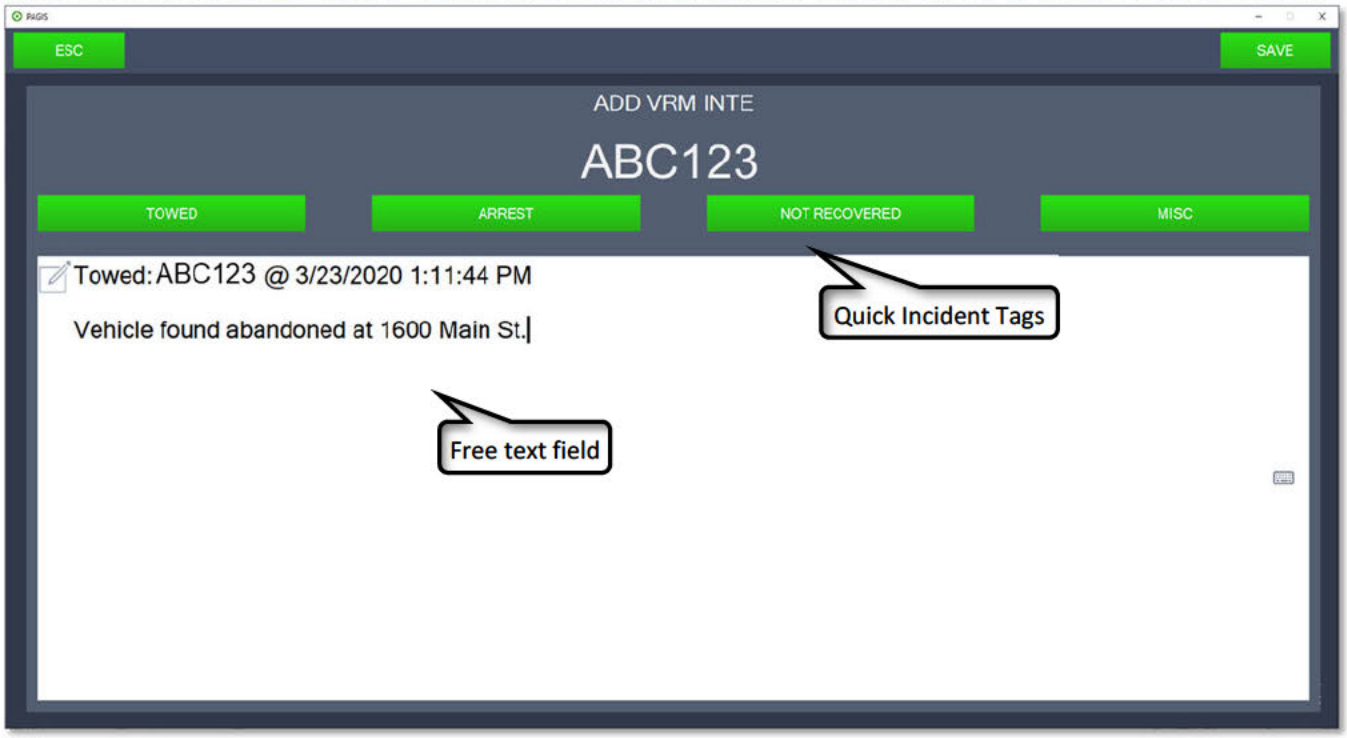


PAGIS allows for additional information to be added to a record in the form of a Disposition. Once Hits are flagged with a disposition code, the Agency is capable of running a "Reads Statistics by Disposition Report" in BOSS. Thus, providing valuable metrics and understanding to leadership in regard to their ALPR Enterprise.

When the "Set Disp" button is selected, the user is prompted to choose from a list of predefined values set by the Agency/BOSS Administrator. Once a disposition is selected and Saved, the disposition is reported to BOSS and will also show up in the Hits Review Screen text box in PAGIS on the next alert notification.

2.9.4.5 Add Intel – Additional Detail

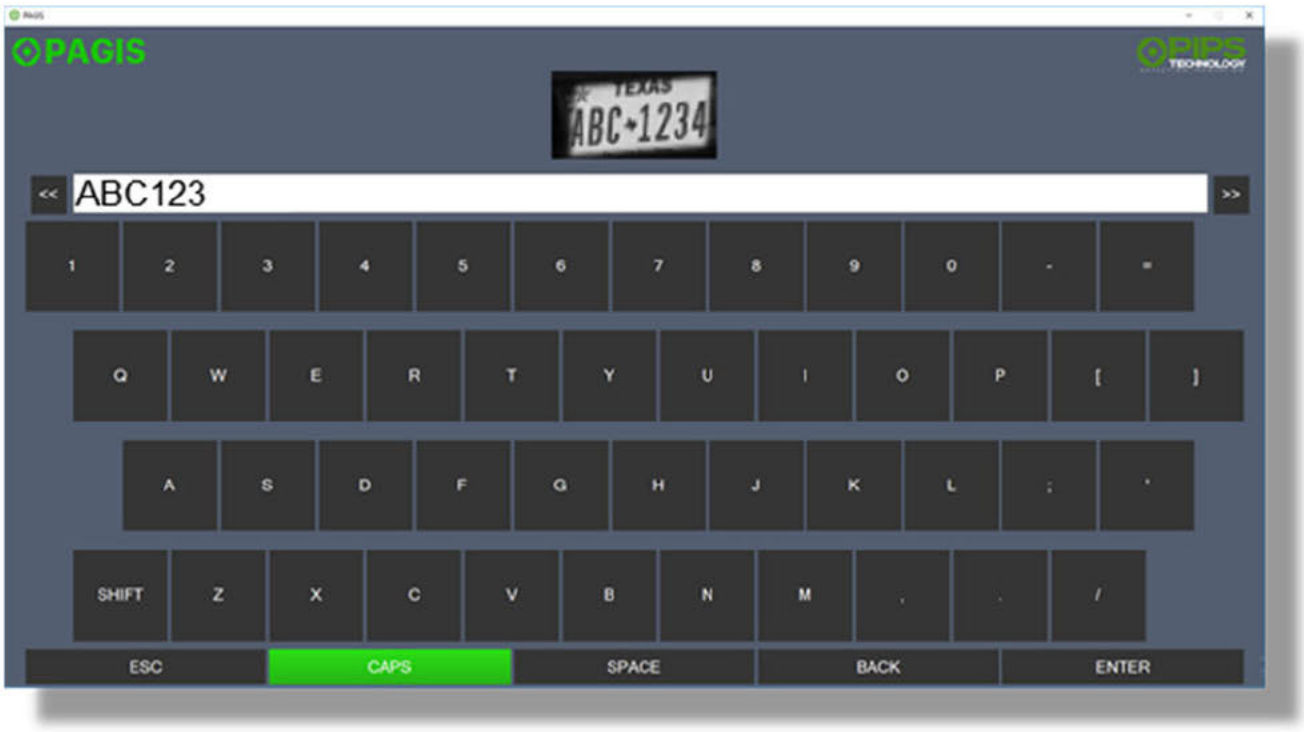
The Add Intel button launches the Intel screen. The user is prompted to assign one of four values: Towed, Arrest, Not Recovered, and Misc. by clicking the associated button at the top of the screen. The user may also enter additional detail regarding the license plate/vehicle. After clicking the Save button, the intel will now appear in the Hits Screen text box.



2.9.5 Misreads

PAGIS allows the user to mark Reads and Hits with incorrect OCR translations as a Misread. This is most commonly done by Agencies for Hits only as users typically don't have time to review every single Read from their shift. Once an errant Hit is corrected, the system updates the record to show it as a Misread and thus improves Agency Hit Reporting.

Correcting a plate read can be accomplished by clicking on the "OCR Patch" in either the Hits or Reads review screen. When the user clicks on the OCR Patch, the OCR Edit Screen opens and allows the user to update the Vehicle License Plate (VLP) data.



2.9.5.1 Marking a Record as a Misread:

The user can mark a record as a Misread from both Reads or Hits Review Screen. Each user can either simply flag the record as a Misread or update the OCR Patch information. **NOTE**: This ability is only available until the user has performed an End Shift function.

Manually Flagging a Read or Hit as a Misread:

1. Navigate to either the Reads or Hits Review Screen
2. Click on the Misread button on the Right
3. Click Save
4. Take note that the record title has now changed from “Read” to “Misread”

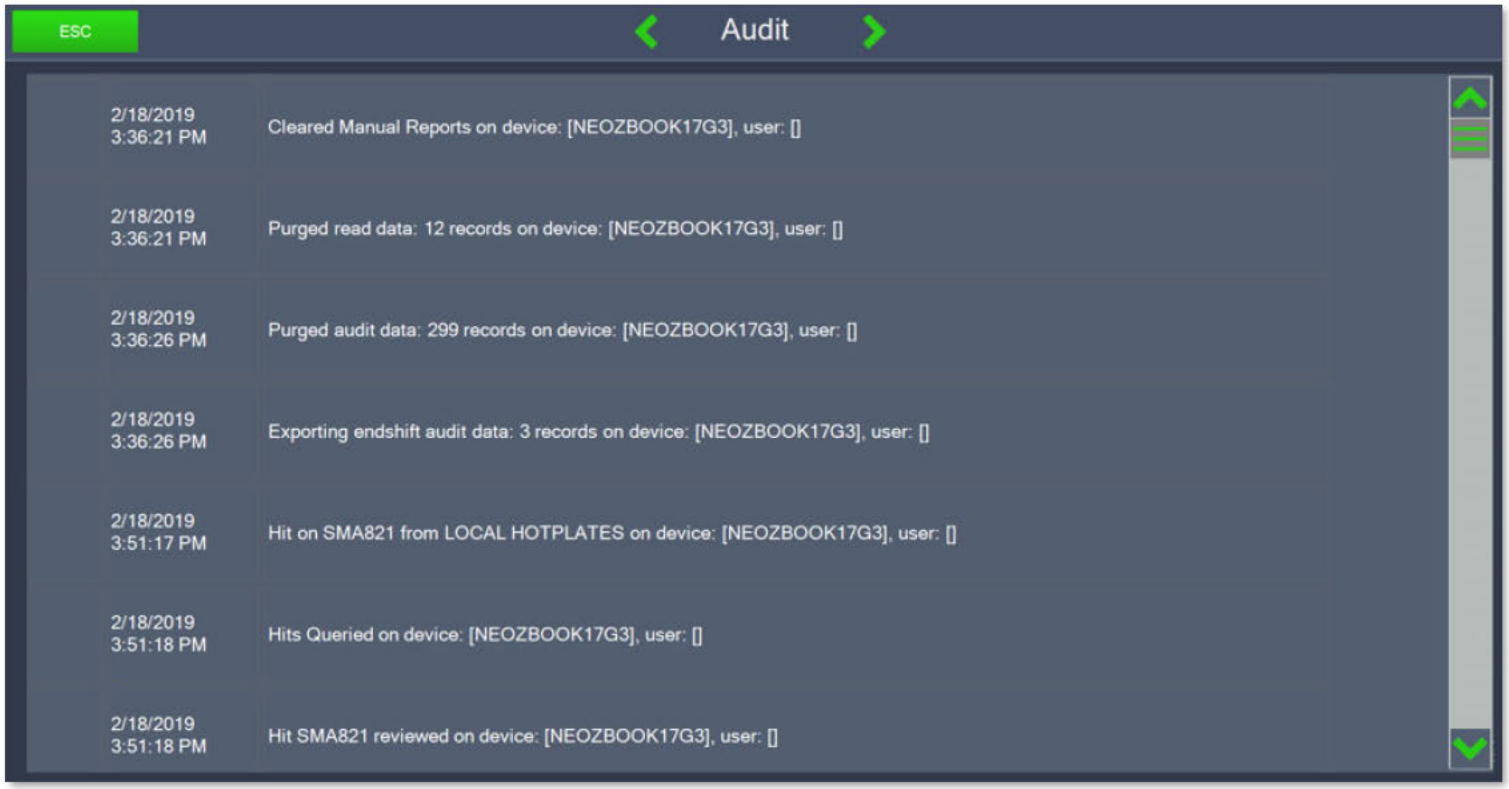
Updating the Read/Hit OCR Patch:

1. Navigate to either the Reads or Hits Review Screen
2. Click on the OCR Patch (Text just under the IR Plate Image)
3. Use the keyboard or on-screen keypad to update the Vehicle License Plate Number
4. Click the Enter Button to Save the changes (and exit back to the Review Screen)
5. When the user saves the changes to the OCR Patch, the record (Read/Hit) is automatically flagged as a Misread

2.9.6 Audits

PAGIS logs both user and key system activity during each use of the software. The audit log captures various information like Read searches, synchronizations, hits, and user login attempts. The Audit Report is viewed in PAGIS by navigating to the Review section and selecting “AUDITS”.

NOTE: Performing an End Shift or syncing the database clears the current log.



2.9.7 Targets

PAGIS has the ability to display information regarding Persons of Interest in response to a Hit alert. Targets are created by BOSS/Hotlist Administrators, and typically provide detailed information about owners of a registered vehicles. When configured, Target data is always linked to unique VLP data (a specific License Plate). If PAGIS registers a Hit on a Plate with a target ID, the Target Information Button is displayed in the Hit Alert window and allows the user to access the Target Screen.



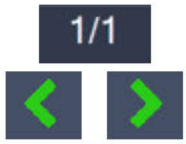
2.9.7.1 The Targets Screen

When a PAGIS user clicks the Target Information Button from a Hit Alert, the Targets Screen opens. This screen displays the information from the BOSS server about the Person(s) of Interest matched to the Hit (license plate).



2.9.7.2 Targets Screen Navigation Buttons

If a Hit alert has more than one Target associated with it, the PAGIS user can navigate all Target information with the buttons described below:



Target Count: The left number is the current record. The right number is the total available for review.

Next/Previous button: Arrows on either side of the target count allow the user to navigate back and forth to review the various targets.



Jump button: Allows the user to "jump" to a specific record without the need to navigate one record at a time using the Next/Previous buttons.

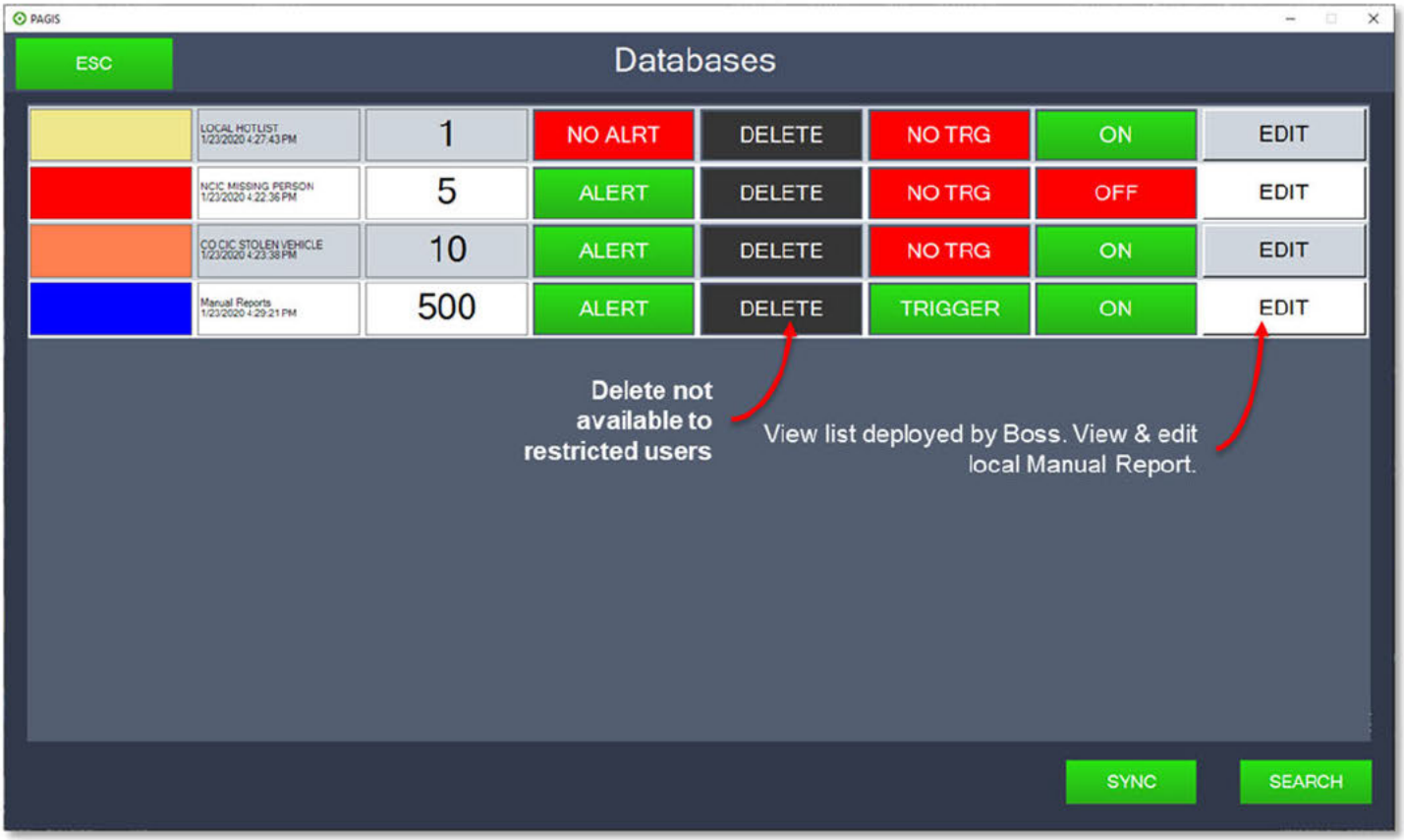


Close button: Returns the user to the previous screen.

2.9.8 Databases

Users can review Hotlists in PAGIS by navigating to the Review section and selecting "DATABASES" on the right. From the Databases Screen, users can toggle Hotlists functions On and Off based on their rights.

NOTE: User rights and Hotlist attributes are configured in BOSS.



2.9.8.1 Databases Screen Functions

Hotlist Color Code: The color attributed to each Hotlist by the BOSS Administrator.

Hotlist Name: The name of the Hotlist given by the BOSS Administrator. Also shows the time/date of the last synchronization.

Hotlist Priority: The priority of the Hotlist assigned by the BOSS Administrator. The lower the number between 1 and 999, the higher the priority. If a plate resides on multiple Hotlists, the list with the higher priority will be displayed first.

Alert Button: Toggles audible alerts On and Off for each Hotlist until the next synchronization.

Delete Button: Based on user rights, allows the user to temporarily delete a Hotlist from PAGIS until the next synchronization. To delete a hotlist, the user must click the button twice (it turns green and then deletes the list).

Trigger Button: Toggles external triggers On and Off. An example of an external trigger is a light bar.

On/Off Button: Disables and enables each Hotlist (each Hotlist is set to On by default).

Edit: View and edit localy created hotplates with a given hotlist, Hotlist/Hotplates deployed via BOSS can only be viewed.

NOTE: Hotlist settings altered in PAGIS will be reset to their default configuration during the next Sync or End Shift. The default configurations are assigned by the BOSS Server/Administrator.

2.9.8.2 Databases Screen Navigation Buttons

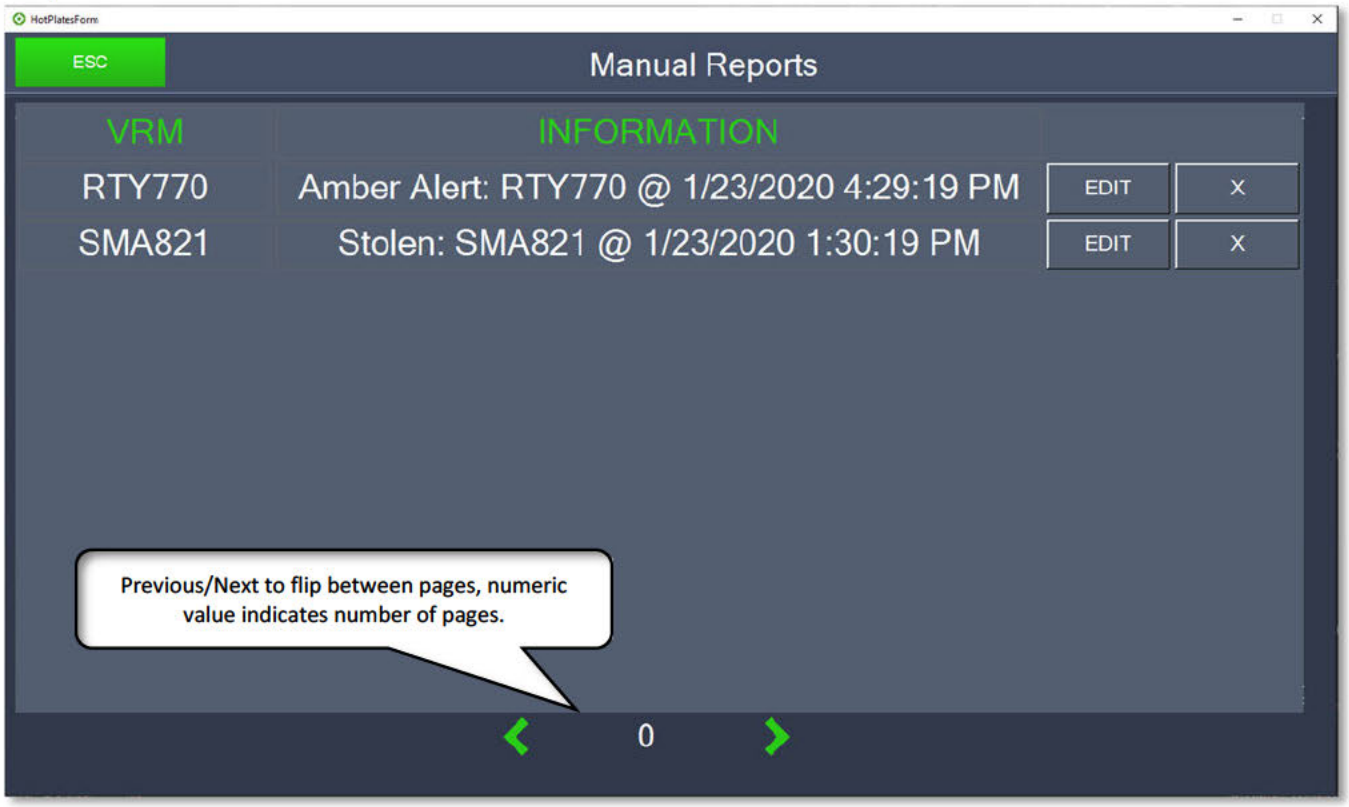
SYNC — **Sync button**: Synchronizes PAGIS with the BOSS server in order to update the Hotlists.

SEARCH — **Search button**: Open the Search Entry Screen (See section 2.8 for more information).

2.9.8.3 Databases Edit- “Manual Reports”

Editing Hotlist has two function based on origin of hotlist.

- Hotlist deployed to PAGIS via BOSS cannot be edited, only the hotplates list can be viewed. Editing/updates are indented to be managed via BOSS.
- Hotlist created in PAGIS, i.e. “Manual Reports” can be managed by PAGIS users, allowing for changes or deletion of the hotplates contained within the hotlist.



EDIT Button: Make changes to the indicustly hotplate information including licanse plate nuamber.
X Button: Remove indivualy hotlist from hotlist.
Previous/Next Button: Scroll thought lising of hotplates contaned within the hotlist. The numeric value indicates the number of pages.

TROUBLESHOOTING TIPS

This section provides some basic troubleshooting tips and information

3.1 Troubleshooting & Tips

- The first login to PAGIS after the new install of an unconfigured version does not require a username or password. Simply click Login to be granted Admin access to the software.
- A good means to test the communication from the MDC to BOSS is ping or telnet (over TCP 8092) through the command prompt.
- A good means to test the communication from the MDC to the SX Processor is ping or telnet (over TCP 9000) via command prompt.
- For many other troubleshooting tips, see Appendix C – Frequently Asked Questions

3.1.1 PAGIS with NetMotion VPN

Agencies utilizing NetMotion VPN software on the MDC will need to apply the following passthrough steps:

1. Login to the NetMotion server as administrator
2. Click Settings > Then select Client > Select Global Client Settings > Then select Passthrough List
3. Click the “Add…” button on the right > Select “Network Address”
4. Enter the following settings (as shown):
    A. IP address:192.168.200.0 (the zero is correct, it's an IP address “range”) Subnet Mask: 255.255.255.0.
    B. Keep all other settings default (as shown) and click OK.
5. The MDC must then disconnect from NetMotion and reconnect again for the settings to be applied locally.

3.1.2 Cisco VPN Client:

Make sure Stateful Firewall is unchecked and "Allow Local LAN".

3.1.3 Microsoft .NET 3.5 Installation

The PAGIS Software requires Microsoft .NET Framework 3.5 specifically. If the MDC doesn’t have .NET, it can be downloaded from the Microsoft website.

3.1.4 Firewall Settings for Client-Server Installations

For client-server installations, the Windows Firewall needs to allow the SX Processor and the MDC to communicate. If the MDC is maintained by a Network Administrator, he or she should be contacted before making changes to the firewall.

Option 1: Allow Microsoft Windows Version 8 or newer to auto-detect the launch of the PAGIS.exe application and use the wizard to add the EXE to the exception list (making note of Public or Private Network settings as necessary).

Option 2: Add PAGIS to the exception list manually by browsing to the install path of PAGIS. The default is below for reference: “C:\Program Files (x86)\PIPS Technology, Inc\PAGIS2\PAGIS.exe”

Option 3: Add the communication ports manually:
TCP 8092
TCP 9000
TCP 9001
TCP 32023
TCP 32029
TCP 10000
TCP 10010
NOTE: XML Datastream uses TCP 10100 and TCP 7000

APPENDIX A: THE GLOSSARY

ALPR/ANPR	“Automatic License Plate Recognition/Automatic Number Plate Recognition”.
BOSS	“Back Office System Software”. This is the ALPR server.
GPS	“Global Positioning System”.
GUI	“Graphical User Interface”.
Hotlist	A database or list that contains vehicle license plates of interest (“alert list”).
IR	Infrared light.
License Plate	Also called a tag or number plate.
MDC	“Mobile Data Computer”. This is the tablet or laptop in the vehicle.
OCR	“Optical Character Recognition” (also referred to as a “cardet”).
OS	“Operating System”.
PAGIS	This is the License Plate Capture Software most commonly used in an ALPR vehicle.
Service	Operation mode of the PAGIS software. Service or “VPRelay” is used to refer to PAGIS instance that is running directly on the PIPS mobile processor without a GUI interface, this mode is intended to run in conjunction with MDC version of PAGIS installed on laptop connected via Ethernet.
Standalone	Operation mode of the PAGIS software. Standalone is used to refer to PAGIS instance that is running directly on the PIPS mobile processor with a GUI interface.
SX	SX is a short notation referencing PIPS’s mobile processor, commonly the SX is followed by the generation number of the processor, i.e. SX3, SX4 & SX4e.
UI	A “User Interface” is the means in which the user can access and navigate the software.
USB Flash Drive	Also called a thumb drive or memory stick.
VLP	“Vehicle License Plate”.
VPN	“Virtually Protected Network”.
VPRelay	Operation mode of the PAGIS software. VPRelay or “Service” is used to refer to PAGIS instance that is running directly on the PIPS mobile processor without a GUI interface, this mode is intended to run in conjunction with MDC versions of PAGIS installed on laptop connected via Ethernet.
Whitelist	Opposite of a standard BOSS Hotlist. This is a list of license plates that should not trigger an alert.

APPENDIX B: PAGIS SOFTWARE[4904] DATABASE FILE

This section is used to configure the PAGIS Software when it's not being used with the Back Office System Software (BOSS). Comma-separated value (CSV) format is the only format the PAGIS Software supports for importing data into the vehicles for the purpose of matching against the captured license plate data. PAGIS will support CSV files with any number of columns, called "fields", as long as the first field is the VLP (Vehicle License Plate). **NOTE**: The CSV format is standard ASCII.

Example CSV Files:

1. *ABC123, Red, Ford, Explorer, 1996, WANTED XYZ456, Blue, Audi, A4, 2001, MURDER*
2. *45ABC234, Vehicle wanted in associated with a kidnapping on 12/5/2005 995BD233, Vehicle reported stolen from Liz's Lounge at 6am on 12/1/2005*
3. *UIO223 ABC123*

General Function:

PAGIS calls/utilizes files in pairs. Each database in PAGIS is created using two files; a CSV file, and an INI configuration file. Without both of these files, the database will not load and PAGIS will not "see" it. Each CSV file/hotlist must have the exact same name as the INI configuration file. Example: Stolen.ini and Stolen.csv will work. Stolen.ini and Plates.csv will not.

Reading an INI Configuration File

Lines that appear in brackets [] are called "Headings". The labels that appear inside the headings, are called "values". Values will always contain an equal sign (=). If a line starts with a semicolon, it is considered to be a comment and is not read by the software. There is no limit to the number of comments in the INI file.

The [SETTINGS] Heading

The values in the Settings heading are: NumFiles, DbName, DbColor, Priority, Covert, Alarm, and NumFields.

- NumFiles: Determines how many database files the system should split the specified hotlist into. Generally, this value is set to 1. But for larger hotlists (200,000+ lines), a number of 2-5 may be more desirable.
- DbName: Tells the PAGIS Software what the displayed name of the hotlist should be.
- DbColor: Sets the display color of the hotlist. This is merely an esthetic setting and not a functional setting. The right-hand side of the equal sign is the HEX value representing the ARGB values for the color. If this value is unknown, the Admin should simply leave this line out of the file.
- Priority: Designates the priority of this hotlist in relation to other hotlists in the system. The highest priority database is 1 and the lowest is 999. **NOTE**: if a plate resides on multiple lists the higher priority will be alerted first.
- Covert: Determines whether standard PAGIS Software users are alerted when a hit is made from the database. Covert database can be used for hotlists that are included for information-gathering purposes rather than eliciting user intervention. The system can also be configured to notify via email or SMS message when a hit is made from a covert hotlist.
- Alarm: Sets the audible alert to be played in PAGIS when a hit is made from the hotlist. Values for Alarm are LOW, MED, HIGH
- NumFields: Indicates how many fields (columns) are in the CSV file. If this value is less than the actual number of fields in a file, then the additional fields are placed in the general information area. This value also determines the number of headings of the [Field x] present in the file. For example, if NumFields=2 then there will be two additional headings, [Field 0] and [Field 1]. **NOTE**: Adding "Creation =" will place the timestamp the hotlist was added to the Begin Shift file.

The [FIELD X] Heading

Under the Field heading, there are two configurable values, “Name” and “PAGIS”.

- Name: Tells the system what the name of this field is. If no name is specified, then no name given to the field. The format is Name = <field>
- PAGIS: Specifies how to display the field in the GUI/PAGIS Software.
    - If no value is defined, the field is placed as general information.
    - Values 1-5 represent special fields for the PAGIS Software that translate to the information being displayed in a box of its own when a hit is processed.
    - A value of 6 represents an ID number to cross reference the vehicle from the hotlist with a person from the wanted list.
    - A value of 7 is identical to leaving the value undefined.

Sample INI Configuration File

[Settings] NumFiles=1
DbName=Stolen Vehicles DbColor=ffffff00 Priority=5 Covert=False Alarm=MED NumFields=8
;PAGIS Values
;0 is VRM / VLP (Not User Definable, always Field 0)
;1 is Special Field 1
;2 is Special Field 2
;3 is Special Field 3
;4 is Special Field 4
;5 is Special Field 5
;6 is ID Number (PNC ID, Drivers License, Social Security Number, etc.)
;7 is General Info (Default for all undefined fields) [Field 0]
PAGIS=VRM

Sample INI Configuration File

[Field 0] Name=VRM
[Field 1] Name=Color
PAGIS=3 [Field 2]
Name=Make PAGIS=1
[Field 3] Name=Model
PAGIS=2 [Field 4]
Name=Action PAGIS=4
[Field 5] Name=Warning
PAGIS=5 [Field 6]
Name=PNCID PAGIS=6
[Field 7] Name=Intelligence PAGIS=7

APPENDIX C: FAQ

Q: **HOW DO I ENTER A SUPPORT CASE?**
A: We have a webform you can use here, you can email our Support Team at Support@PIPSTechnology.com, or you can call us on the phone Monday-Friday 8am to 4pm Central Time (9am-5pm Eastern) at (833) 747-7577 Option 2.

Q: **HOW DO WE CREATE USERS IN PAGIS?**
A: The agency BOSS Administrator creates all users, both for BOSS and for PAGIS. Once the user is created in BOSS, the Admin would click the user's name to select/edit the user. Then click the Advanced button and update the PAGIS specific password. Please note that the username and password fields are both case sensitive and the PAGIS users need to be added to a group with the Role that allows them to use PAGIS/LPCS.

If you have any further questions, please feel free to enter a request for support here.

Q: **WHERE DO USERS CHANGE THEIR LOGIN PASSWORD IN PAGIS?**
A: User passwords are created and updated in BOSS via the UI client software. For the majority of our customers using both the PAGIS Software and BOSS, any user accounts or passwords created in the PAGIS Software itself will be overwritten by the user information defined in BOSS during the next sync.

If you have any further questions, please feel free to enter a request for support here.

Q: **HOW DO WE REQUEST AN RMA REPAIR?**
A: To assist with this, please navigate here to review our RMA procedure as well as to download the request form. Please keep in mind that once submitted, all repairs are reviewed for age of equipment and warranty status before final processing takes place. Additionally, incomplete forms and those without much detail often result in processing delays.

If you have any further questions, please feel free to enter a request for support here.

Q: **WE HAVE NEW MDC LAPTOPS IN THE PATROL CARS, HOW DO WE ADD THOSE DEVICES TO BOSS?**
Q: **HOW DO WE EDIT THE DEVICE NAMES IN BOSS?**
A: The initial device template/skeleton is automatically created in BOSS the first time the device attempts to Sync from the field. Devices should NEVER be created manually. For PAGIS laptops, this is done after PAGIS is installed and configured and Begin Shift is launched. However, if the agency would like to organize the device list by updating the "Device Name" field, those steps are below:
1. Login to the BOSS UI with Admin rights
2. Navigate to Admin > Devices
3. Click on a device name to select it > Click Edit
4. Update the name of the device in the "Description" field (Name field cannot be altered)
5. Click Save > This will take you back to the Device Summary List. The "Device Name" field should show the new name

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **WE HAVE A NEW MOBILE COMPUTER/MDC THAT'S NOT SYNCING WITH BOSS.**
Q: **WE KEEP SEEING AN HTTP_STATUS_CODE ERROR WHEN RUNNING BEGIN SHIFT.**
A: This error most commonly means that a new device in the field (laptop/tablet) can "see" the BOSS server, but that it hasn't been enabled yet to "talk" with it. Follow the general steps below to address this issue:
1. The agency BOSS Administrator will need to login to the BOSS UI client and Select Admin
2. Then select Devices and from there, left click on the device/computer name of that MDC to edit it
3. Once in the Edit screen, Enable the device. This will take you back to the Device List.
4. Click the name to edit the device again. Now assign users/Owners and save.
NOTE: The Select button becomes a Save button when selecting which Groups/Users should have access to login to this device
5. Once that is done, navigate to Admin > Hotlists
6. From here, click on each hotlist one at a time to distribute them to the new device being sure to Save the changes next to the

Distribution field. Note again that the Select button becomes a Save button. And there's another Save button at the top left of the edit window.
7. After this is complete, perform Begin Shift from the field unit/MDC and confirm there are no further errors.

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **NEW PAGIS USER CAN'T LOGIN BUT OTHERS CAN.**
Q: **USERS CAN LOGIN TO PAGIS WITH NO CREDENTIALS AT ALL.**
A: Entry or login to the PAGIS software in the field is partially controlled by the Device settings in BOSS. The users themselves must also be properly setup with an LPCS/PAGIS password. To check the current device settings/ access, perform the following steps:
1. Login to BOSS UI (with Administrator rights)
2. Select the Admin Section
3. Select Devices and then Select the Device in question by PC name
4. Once selected click on the Edit button near the bottom
5. Locate and inspect the "Owners" Field (this is a list of users/groups that have access to login to the device)
NOTE: If this field is blank, the device is in an open configuration mode allowing admin level access simply by clicking login (any credentials would also be accepted).
6. To update the device owners, click the "Select" button next to the Owners field (notice it changes to a Save button)
7. Check which Users/Groups of Users should be able to login to PAGIS from this device
8. Click the Save button next to the field
9. And then click Save in the upper left portion of the Edit window
10. Have a previous user or Admin login to PAGIS and perform Begin Shift to sync the new data
11. A PAGIS Admin can confirm by navigating to Admin, Admin, and then Users to review the list
12. Another test would be to have the new user attempt to login

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **WHEN USERS LOGIN TO PAGIS, THEY ONLY SEE A GREY SCREEN.**
Q: **CAMERAS AREN'T SHOWING UP IN PAGIS ANYMORE.**
SEE ALSO: "THE LINK LIGHTS ON OUR ALPR COMPUTER/MDC WON'T TURN ON OR FLASH"
A: Below are some basic troubleshooting steps you'll want to follow before creating a support ticket.
1. Doublecheck the physical power switch on the black box/Processor is On. In many vehicles, there is also an in-line switch in the front of the vehicle that needs to be switched On. When the units are properly powered and on, you should see lights and hear fans running.
2. Confirm that the network adapter settings on the laptop match the proper Static IP scheme for the SX Processor in use. The older scheme is 192.200… and the newer scheme is 192.168…. NOTE: the adapter status in Windows should say "unidentified network". If it says "cable unplugged" the laptop can't "see" the SX.
3. If the power and Static IP settings are good and things still aren't working, test further by disabling the three main software related culprits. Turn off/bypass the local Windows firewall, antivirus, and VPN software one at a time.
4. If you're still not able to see the camera feed after that, you may want to use a different network cable as those can get damaged over time and then confirm that the cord is properly plugged into the ports.
5. If the network cord from the SX Processor is routed through a docking station, then it's possible the dock is preventing the traffic. You should contact the dock's manufacturer for the most recent firmware. To test for this, remove the laptop from the dock, directly connect the network cord to the laptop, and then reconfigure the network adapter settings (remove the static settings from the dock's adapter/ and assign the static IP to the laptop's NIC adapter).

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.
Q: **THE LEFT FRONT CAMERA ON OUR ALPR VEHICLE IS NO LONGER SHOWING IN PAGIS**?
Q: **HOW DO WE TROUBLESHOOT MOBILE CAMERAS**?
A: Below are the main troubleshooting steps to test the camera(s) and cable(s) on a system where only one or two cameras are no longer displaying images.
Step 1: Confirm MDC/SX communication - steps shown in section "Cameras aren't showing up in PAGIS anymore."

Step 2: Access the SX Processor – RDP or directly connect a monitor, keyboard, and mouse to the SX. Contact PIPS Support for help with RDP if the credentials are unknown to the agency.
Step 3: Confirm camera activity – Launch Tools. Then open P6Utility or Mobile Toolkit. Check the camera feeds/function by switching the Input menu to the camera(s) in question
Step 4: Unplug and Reattach the Camera Cables – Note, the cables DO NOT TWIST. The metal locking nut on the cable slides back about a millimeter and the cable comes straight out. Do this at the SX Processor and the Camera. You may need to remove the camera from the mount in order to unplug the cable successfully (most brackets use a #3.5 Hex/Allen Wrench)
Step 5: Swap Port on SX Processor – At the SX Processor, swap the camera cables from the non-working camera to a port with a working port (Take care to note the swap so the cables get back to their original ports). If the camera outage stays at the port site, the issue is most likely the capture card on the SX Processor and will require RMA (Example: working Left cam is swapped to port of non-working Right cam and no longer functions. AND the previous non-working Right cam starts working once it's plugged into the Left cam's port). If the fault/error stays with the camera regardless of SX port, continue to Step 6.
Step 6: Physically Swap Camera Locations – Once all other items are checked, move the camera itself to a working position in order to test the cable. (Example: physically move Left camera to the Right camera position on the top of the vehicle) Connect the cable at the new position and test feed in Tools > P6Utility/Mobile Toolkit. If the camera works at the new location, the issue is most likely a bad cable. If the camera still does not work, the issue is most likely a faulty camera in need of repair/RMA.

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **WE'RE NO LONGER GETTING GPS IN PAGIS.**
Q: **WE'RE NOT SEEING GPS DATA FROM SOME OF OUR FIELD UNITS IN BOSS.**
A: Below are the basic troubleshooting steps for checking the GPS of field units:
1. Login to PAGIS (as Admin)
2. Navigate to Admin section, then click the Admin button
3. Select "System" on the left pane
4. Confirm/Set the button at top to "Default"
5. Remove any value(s) stored in the GPS Connection String field. Leave '5' in the Computer String.
6. Click the Save button to retain changes made.
7. Close PAGIS fully and relaunch and log back in to test (Note: GPS will only show with test reads/hits)
8. For versions of PAGIS 2.9 and up, test with a GPS Connection String of 6 if the blank field doesn't work. Save the changes. Log out. Close the software and then relaunch to test.

Please be advised, that some GPS issues can be caused by local or domain firewall settings, antivirus software, or any other software package monitoring/transmitting network data. To test these, disable or bypass those software options on the MDC and retest.

If these initial troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **HOW DO I INSTALL THE PAGIS SOFTWARE?**
Q: **I JUST LOADED PAGIS ON A MACHINE AND IT CRASHES WITH A .DLL ERROR WHEN I TRY TO LAUNCH IT.**
A: The most common installation of PAGIS is Client/Server or "VPRelay Mode". The .dll error is caused by the installer not being run from the HDD and/or the wrong install option being selected (Example: SupeRex instead of MDC). The best practices for the installation are below. (Note, this does not cover MDC or PAGIS configuration, only the act of installation)
1. Always copy the installer over to the HDD/Desktop of the MDC. Never run it from a thumb-drive or network share
2. Regardless of how you're logged in to Windows, right click the installer and select "run as Admin" or "run with elevated privileges"
3. Continue through the message/error about OS compatibility
4. Click next on the wizard and then be sure to select the MDC option (to use with VPRelay)
5. After that, it's next, next, next, finish the reboot is not necessary

If these steps did not resolve the issue, please feel free to enter a request for support here.

Q: **USERS ARE GETTING HITS/ALERTS ON PREVIOUSLY RECOVERED STOLEN PLATES.**
Q: **USERS AREN'T GETTING HITS FROM KNOWN ACTIVE PLATES.**
Q: **THE HOTLISTS IN PAGIS DON'T SHOW TODAY'S DATE.**
Q: **THE HOTLISTS AREN'T SYNCING WITH BEGIN/END SHIFT.**
A: Whether it's from data latency or just use over time, the local file structure can get some minor corruption and will need to be refreshed. The steps below show the best practices:
1. Login to Windows with Admin rights (ability to uninstall/delete software)
2. Login to PAGIS and perform an End Shift
3. When complete without error, Logout of PAGIS and then Exit/Close the program
NOTE: If the End Shift fails or displays an error, contact Support for additional assistance.
4. If there were no errors, locate the PAGIS icon on the desktop.
5. Right click on the icon and select "Open File Location" (This should open a window where the program was installed)
6. Scroll up and locate the folder labeled "data". Double-click it to open it
7. Select and delete everything in here EXCEPT for "Attributes.db"
8. Once that's complete, Login to the PAGIS software again
9. Perform a Begin Shift. This will pull down fresh data from the server
NOTE: Once complete, the files in the data subfolder as well as the Databases section of PAGIS should be restored.

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **IS PAGIS COMPATIBLE WITH OUR NEW WINDOWS 10 LAPTOPS?**
A: Although there's a warning about compatibility during the install of PAGIS on any Windows OS after XP, it is compatible with all them. However, we have seen errors occur when agencies copy and paste folder structures from previous installations. This of course is not recommended.

Q: **THE LINK LIGHTS ON OUR ALPR COMPUTER/MDC WON'T TURN ON OR FLASH.**
Q: **OUR WINDOWS 10 MDC WAS WORKING BUT HAS STOPPED COMMUNICATING TO THE SX PROCESSOR.**
A: There are many variables with troubleshooting any network connection. And the connection from the ALPR computer to the SX Processor is no different. The following troubleshooting list highlights the most common:
1. The physical network cord is bad/damaged.
A: Test with a different cable and confirm that it is plugged in fully

2. The network adapters are not configured or have incorrect static IPs
A: Confirm the Static IP scheme in use and properly configure the network adapters

3. Local and/or Domain Firewall rules have prevented the flow of communication
A: Disable or bypass these and test again

4. VPN, Anti-Spyware, Antivirus, or other monitoring software has blocked communication
A: Disable or bypass these one at a time and test after each to find the culprit(s)

5. Docking Station Firmware can be incompatible with some newer computers or become corrupt
A: Test by running the network cord straight to the MDC and then configuring the network adapters (NOTE: It would also be a good idea to contact station manufacturer to see what the latest firmware version is and upgrade as necessary)

6. The NIC Drivers have become corrupt
A: Update the specific Networking drivers in use on the MDC through the Device Manager in Windows

7. Turn off all power saving settings of the Ethernet Adapter in the device manager
A: Uncheck "Allow the computer to turn off this device to save power"

8. Check for Windows 10 update 1709 and 1803 as this update will not allow the NIC and Cellular Aircard to run simultaneously
A: Settings > Update and Security > Windows Update > "Update History" link – if there, see the steps in the FAQ

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **AS SOON AS WE DOCK OUR MDC, WE LOSE CONNECTION TO THE WIRELESS.**
Q: **OUR WINDOWS 10 LAPTOP LOSES CONNECTION TO THE INTERNET WHEN THE NETWORK CABLE IS PLUGGED IN.**
Q: **OUR MDC HAS MICROSOFT VERSION 1709 OR 1803 AND CAN'T CONNECT TO WIFI WHEN DOCKED.**
A: Microsoft Updates (1709 and 1803) prevent the Wireless connection as soon as a Network cable is plugged into the device. This also occurs for MDCs/laptops that are docked (where the Network cable from the SX Processor is run through the docking station). As of January 2019, the steps to correct this are below.
WIN10 version 1803
1. Open Regedit
2. Expand HKEY_LOCAL_MACHINE
3. Navigate to Software > Policies > Microsoft > WcmSvc > Local
4. Right click on Local > Hover over New > Select "DWORD (32-bit)"
5. Name the new value "fMinimizeConnections"
6. Right click the on the new name > select Modify > Set value data to 1 (leave base Hex) > Click OK
7. Reboot Windows and test

WIN10 version 1709 - Microsoft fixed this with Update KB 4284822. But if you still have issues, the registry steps are below:
1. Open Regedit
2. Navigate to HKEY_LOCAL_MACHINE > Software > Policies > Microsoft > WcmSvc > Local
3. Right click on Local > Hover over New > Select "DWORD (32-bit)"
4. Name the new value "fMinimizeConnections"
5. Right click the on the new name > select Modify > Set value data to 0 (leave base Hex) > Click OK
6. Then Navigate to HKEY_LOCAL_MACHINE\Software\Microsoft\Wcmsvc
7. Right click on Wcmsvc > Hover over New > Select DWORD (32-bit)
8. Name the value "IgnoreNonRoutableEthernet"
9. Right click on the new value > Modify > Set value data to 1 (leave base in Hex) > OK
10. Reboot Win10 and test

If the steps above did not resolve the issue, you may need to address this with Microsoft. Their support site is here.

6 January 2020

PIPS Product Bulletin

With the start of the new year, we have a few announcements and reminders regarding PIPS Technology™ solutions. We are starting 2020 with revamped software and product solutions that have greater capabilities to help you in your daily mission! We dedicate a third of our staff to product and solution improvements and innovations to make your job easier, safer, and more efficient.

BOSS 4 Continued Roll Out

In 2019, we released an early version of our new BOSS 4 software. This new software is a leap forward in design and usability compared to our BOSS 3 product and provides additional features not currently in existing software. The new web-based design also offers the ability to rapidly add features and deploy the software to any number of users in your network. As before, the BOSS software gives you complete control over your data and allows you to dictate who you share data with and how much access to give them.



BOSS 4 provides the ability for you to host inside your own servers/data center as with previous generations of BOSS. However, in response to feedback from the customers, we are also now offering a Hosted Managed Service. Providing industry leading infrastructure and service management, including 99.999% infrastructure availability with the latest in security, this option provides the ability for your teams to focus on front-line duties rather than worrying about Databases, Servers and Infrastructure.

Give us a call at 833-PIPS-LPR (833-747-7577) and speak with our sales team to get a free online demonstration and test run.

New Mobile System Hardware and Software Continued Roll Out

Also, in 2019, we released a new version of our popular mobile system with the SX4e processor and P720 camera. The P720 uses the same form factor as the robust P634 camera, but provides better lenses, better sensors which provides higher quality images, and more lane coverage. The optical performance improvements this technology provides improves detection and recognition rates compared to previous generations of PIPS' products and those of our competitors.

The SX4e is the power-over-ethernet (PoE) version of the processor allowing more versatility in configuration and deployment of the mobile system. System configuration still allows between one to four cameras per processor, but the PoE cable can have 100 feet between processor and camera.

Questions / Concerns? Contact Technical Services (833) PIPS-LPR or (833) 747-7577

Along with the new hardware, we are making continuous improvements to our PAGIS in-car mobile software. This includes security enhancements, more firmware updating, and additional mapping tools. Our development team continues to roll out new changes and features which are available free of charge, during their warranty phase, to those customers who have already upgraded.



If you are interested in any of our new mobile products, please reach out to our sales team for a demonstration. You can also contact our support team to see if your existing system is on the latest software or firmware version. Contact us at 833-PIPS-LPR or at support@pipstechnology.com.

BOSS 3 End of Life Notice – December 31, 2020

At the end of 2020, we will no longer support our BOSS 3 software. This includes software updates and service/support inquires related to this product.

The migration from BOSS 3 to BOSS 4 is designed to be made as simple as possible for the customer, with specific migration tools developed by PIPS to aid the process. Please get in touch so we can discuss how you could migrate to BOSS 4 from BOSS 3. For any customers committing to upgrade before the end of March 2020 we will be crediting any pro-rata BOSS3 support fees against the BOSS 4 license as well as waiving the migration cost.

We will naturally continue to support those customers who have recently purchased software support for the BOSS 3 product until the end of the current obligation.

Questions / Concerns? Contact Technical Services (833) PIPS-LPR or (833) 747-7577

IRIS P500 Latest Software Build with feature enhancements and bug fixes
The IRIS P500 series camera was newly released in 2019 and received superb feedback from those customers who used it, including beating competitor products in numerous “head to head” performance evaluations by customers.

As with all new products we were providing software releases throughout the year in direct feedback from customers for enhancements as well as reported bug fixing highlighted to our Service / Support teams.



We formally released 4 updates during the year and one hot-fix in response to feedback, including the latest hot fix in December 2019. These releases resolved the reported issues, including one that can appear in some of the earlier IRIS cameras under certain circumstances which were not running on the latest released software standard. This manifest itself when the camera first booted, it may erroneously use GMT time instead of the configured time zone. This will cause the camera to record images with the time stamp of GMT instead of local, but not give an indication that the image is using an incorrect time zone. Once the camera is finished booting and synchronizing with its time source (typically within 1 minute), it will use the local time zone, but the images captured during the booting process will have an incorrect timestamp.

We have issued a firmware update to correct this issue. This ensures that the correct time zone is applied to all reads, even during boot up. Please call our support line, 833-PIPS-LPR, to receive the latest firmware and have it setup on your camera system.

NOTE – this only applies to the IRIS P500 series cameras and does not manifest itself in previous generations of our products.

Questions / Concerns? Contact Technical Services (833) PIPS-LPR or (833) 747-7577

New Termination Box (T-Box) Design
In 2020, we begin rolling out a new T-Box design. This design reduces the weight and size of the previous T-Box, while continuing to provide the same functionality. The new design also helps control costs, which in turn helps prevent price increases on the product.

Please call our support line at 833-PIPS-LPR or email us at support@pipstechnology.com to let us know how we can continue to improve this and our other products.

Update to Latest Versions of Software and Camera Firmware
Throughout the year, we have released updates to the firmware of our camera products (both mobile and fixed) along with software updates to PAGIS. We recommend that either your IT staff check to see if your cameras are on the latest patch or contact us to determine your camera status.

Our service staff would be happy to evaluate any of your PIPS products to determine if they are on the latest version. Give our support team a call at 833-PIPS-LPR.

Update Product Passwords
As a means of providing sound security, we recommend changing that the passwords on each camera system and software. In following CJIS policy (code 5.6.2.1.1), we recommend passwords should contain the following:

1. Be a minimum length of eight (8) characters on all systems.
2. Not be a dictionary word or proper name.
3. Not be the same as the User ID.
4. Changed regularly (ideally every 90 days)
5. Not be identical to the previous ten (10) passwords.
6. Not be transmitted in the clear outside the secure location.

Remember, every law enforcement agency that uses CJIS is audited at least once every three years. We are aware of customer being asked about their password policy in relation to their ALPR infrastructure and would urge the ALPR cameras to be considered as part your organizations' password policy.

Regards,



Peter Crary
Global R&D Director, ALPR/ANPR

Questions / Concerns? Contact Technical Services (833) PIPS-LPR or (833) 747-7577

Requirements and Specifications
Back Office Server Software (BOSS4)

On-Premise Applications Server

Below, there are the minimal recommended configurations for different capacity configurations for BOSS4 On-Premise infrastructure.

Application Servers Specifications				
Configuration	**Demo**	**Medium**	**Large**	**High Capacity**
ALPR Devices	1 to 3	3 to 50	50 to 150	Beyond 150
Average Daily Intake	Around 30,000 events	Around 500,000 events	Around 1,500,000 events	Beyond 1,500,000 events
Average of users querying data	3 users	15 users	25 users	Beyond 25 users
Alert list averaging	Around 1M records	Around 2M records	Around 2M records	Around 2M records
Operating System	Amazon Linux / Amazon Linux 2 x64 Linux x64 (RHEL/CentOS, Ubuntu, Debian, SUSE) macOS x64 Windows 10 Professional x64 Windows Server 2016 x64			
Memory	16GB	32GB	64GB	192GB
Processor	x64 2.0 GHz 8 cores o better	Server Processor x64 (Intel Xeon Gold) 2 GHz 4 cores, 8 threads, 4MB cache	Server Processor x64 (Intel Xeon Platinum) 2.4 GHz 16 cores, 32 threads, 8MB cache	Server Processor x64 (Intel Xeon Platinum) 2.4 GHz 24 cores, 48 threads, 24MB cache
Hard Drive	7200 RPM SATA3	SSD SATA3	SSD SATA3 or NVMe PCI Express	SSD SATA3 or NVMe PCI Express
Application Space	128 GB of available space	256GB of available space	320GB of available space	512GB of available space

On-Premise Database Server

BOSS4 uses the MongoDB Database Engine.

Specifications of the Database Server				
Configuration	**Demo**	**Medium**	**Large**	**High Capacity**
ALPR Devices	1 to 3	3 to 50	50 to 150	Beyond 150
Average Daily Intake	Around 30,000 events	Around 500,000 events	Around 1,500,000 events	Beyond 1,500,000 events
Average of users querying data	3 users	15 users	25 users	Beyond 25 users
Alert list averaging	Around 1M records	Around 2M records	Around 2M records	Around 2M records
Database Engine	Mongo DB Community	MongoDB Enterprise		
Operating System	Amazon Linux / Amazon Linux 2 x64 Linux x64 (RHEL/CentOS, Ubuntu, Debian, SUSE) macOS x64 Windows 10 Professional x64 Windows Server 2016 x64			
Processor	x64 2.0 GHz 8 cores o better	Server Processor x64 (Intel Xeon Gold) 2.5 GHz 4 cores, 8 threads, 4MB cache	Server Processor x64 (Intel Xeon Platinum) 2.4 GHz 16 cores, 32 threads, 16MB cache	Server Processor x64 (Intel Xeon Platinum) 2.4 GHz 24 cores, 48 threads, 24MB cache
Memory	N/A	32 GB	128GB	256GB
Hard Drive	7200 RPM SATA3 Not suitable for camera implantation with any kind of data retention expected	SSD SATA3 RAID level redundancy and scheduled DB backups recommended *See sizing chart for storage.*	SSD SATA3 or NVMe PCI Express RAID level redundancy and scheduled DB backups recommended *See sizing chart for storage.*	SSD SATA3 or NVMe PCI Express RAID level redundancy and scheduled DB backups recommended *See sizing chart for storage.*

This document and its contents are intended for the recipient only. Copying, redistributing, or discussing with any other party outside of the intended recipient and PIPS-Neology is prohibited.

Data Storage Requirements

The calculation of storage applies to Cloud and On-Premise configurations.

Approximant Sizing based on Hybrid data, Mobile & Fixed Camera data			
# of records	Database size Metadata and indexes	Repository Size Imagery	Total
1 Million	32GB	153GB	**185GB**
5 Million	64GB	763GB	**827GB**
10 Million	320GB	1.5TB	**1.82TB**
50 Million	1.6TB	7.5TB	**6.1TB**
100 Million	3.2TB	15TB	**18.2TB**

The calculations for storage are approximated based on an average sampling of around 192KB per event.

System Communication Ports

Ports	TCP / UDP	Description
80	TCP	HTTP Web access port for mapping.
443**	TCP	HTTPS Web access for client access, SW Updates, AWS Services.
8090	TCP	Legacy Pagis 268 data port, not required unless using older Pagis SW.
8092	TCP	REST API data port for PAGIS, supports TLS v1.0.
8093	TCP	REST API data port for PAGIS, supports TLS v1.3.
10000	TCP	VES Image port for fixed cameras.
10005	TCP	VES Heartbeat for fixed cameras.
10010	UDP	VES Ping port for fixed cameras.
27017	TCP	MongoDB data connection port.
**	Specific BOSS4 Micro Services require Internet access to AWS Services managed by Neology.	

Additional System Requirements

Application Server:

- Linux x64 (RHEL/CentOS, Ubuntu, Debian, SUSE).
- MacOS x64.
- Windows 10 Professional x64 or newer.
- Windows Server 2016 x64 or newer.

Database Server:

- MongoDB.

Client-Side:

- Chrome v72 and newer, we are currently working to validate more browsers.
- Standalone Alert application- Windows version 7 and up, x32/x64.

Remote Access:

- Scheduled or 24x7 remote access is required during installation and testing.

This document and its contents are intended for the recipient only. Copying, redistributing, or discussing with any other party outside of the intended recipient and PIPS-Neology is prohibited.

Frequently Asked Questions, FAQ's.

Q. Support for other Operating Systems?
A. Currently supported are Windows based x64 OS's, MacOS x64, Linux x64 (RHEL/CentOS, Ubuntu, Debian, SUSE). The preferred OS is Linux for BOSS application server.

Q. Can Boss work in virtual OS's?
A. Yes, supported are Windows based x64 OS's, MacOS x64, Linux x64 (RHEL/CentOS, Ubuntu, Debian, SUSE). The preferred OS is Linux for BOSS application server.

Q. How long does a typical BOSS4 installation take?
A. Boss4 installation and setup can vary depending on requirements, typical installations can take anywhere for 1-3 days to complete and possible longer depending on data migration.

Q. What Database programs are supported?
A. Currently MongoDB is supported, other databases will be supported in future releases.

Q. Can you migrate data from non-PIPS ALPR servers into BOSS4?
A. No. We can only migrate data from existing BOSS3 systems.

Q. Can existing BOSS3 database files be utilized when upgrading to BOSS4?
A. No. BOSS4 is a completely new database structure, however data can be migrated.

Q. How long can data migration take.
A. Data migration can vary depending on volume, anywhere from hours to days.

Q. What data is miraged from BOSS3?
A. Customizable among the following. Reads, Hits, Users, Groups, Roles, Devices, Sites, and Hotlist.

Q. Can BOSS4 reside on same OS as database application?
A. Yes. Only small demo or trial configurations can support same OS for both.
A. No. Production deployments it is not recommended.

Q. Can BOSS4 ports be customized?
A. No. Current BOSS4 version does not support customer port configurations.

Q. Can BOSS4 versions share data with older BOSS3 versions?
A. Yes. Data sharing is built into our latest versions to connect with other older versions of BOSS3.

Q. How are the database tables created?
A. BOSS4 application installation and start configures the required database structure needed.

This document and its contents are intended for the recipient only. Copying, redistributing, or discussing with any other party outside of the intended recipient and PIPS-Neology is prohibited.

PIPS Fixed ANPR Camera User Manual

PIPS Fixed ANPR Camera User Manual

Version 4.9.11308 created on 2020-12-04 13:14:46 ; with commands from versions: P492:version 4.9.11308 .
Copyright © 2007-2017 Neology

Table of Contents

1. Introduction 1
P382 1
P392+/P492 2
Assumptions 2
Conventions 2
2. Getting started 4
Connectivity 4
Discovery 4
Serial RS-232 5
Ethernet 5
Networking setup 5
Basic Configuration 6
Connecting 6
SSH 6
Restarting and Shutting Down 7
Restarting after changing settings 7
Switching off for planned maintenance 7
Power-cycling 7
3. PIPS ANPR Toolkit 8
Viewfinder 8
Vehicle Events 9
Review 9
Camera Software 9
Software Management 10
Software Installation 10
4. Camera technical overview 11
Interfaces: Output mechanisms 11
5. Configuration using Webmin 13
Camera control 13
Network 13
Mounting network disks 13
NFS 14
Windows shares 14
6. PIPS ANPR Shell 15
PIPS Shell Commands 15
ACS - Access Control System (acs) 15
ANPR Vehicle Analyser (anpr) 24
Asynchronous Payload Matching (asyncp) 27
BOF2 protocol (bof2) 28
IR Camera (cam1) 30
Overview Camera (cam2) 34
Client vehicle event reporter (client) 36
Contexts (contexts) 37
Plate Database Matcher (dbmatcher) 40
Diagnostics and Exceptions Manager (diagnostics) 42
File Logger (filelog) 43
Vehicle Fusion (fusion) 43
GPS Time Manager (gps) 46
Heartbeat (heartbeat) 46
Image File Outputter (ifo) 47
JPEG Service (jpegService) 48
JTMS - Journey Time Measurement System (jtms) 49
External Led Control (ledControl) 50
Metadata store (metadata) 50
OEM Modules (modules) 53

Network user interface manager (netuis) 54
NTP Monitor (ntpMonitor) 54
Licence options (options) 55
Patch Overlay Control (patchoverlay) 55
PCI Camera Source (pciSource) 56
PIXI Contexts (pixicontexts) 56
Power Manager (power) 56
Relay Out (relayOut) 56
SAP - Serial Application Port (sap) 57
Vehicle Image Selector (selector) 57
Hardware Monitoring sensors (sensors) 58
Console Logger (stdout) 58
System Details (system) 58
Trigger Control (trig) 60
Trigger Script (trigScript) 64
UTMC Delivery Module (utmc) 65
UTMC V1.2 Delivery Module (utmcv12) 67
VES - Violation Enforcement System (ves) 68
Vehicle Event Database (vfeDB) 78
Logging bits 79
Notifications 82
7. Format strings 84
Control Characters 84
Replacement specifier 85
Format 85
Format Detail 85
List of replacement values 86
Examples 96
8. PIXI Protocol 98
Protocol 98
Example documents 101
Root objects 102
Subobjects 103
Properties 104
Logging 105
Notifications 107
Issue Command 108
Event data 109
Event data with pull 110
PIXI Documents 111
commands.xsd 111
output.xsd 113
common.xsd 117
List of PIXI values 119
PIXI values image_* 119
PIXI values cam_* 119
PIXI values hazcam_* 120
PIXI values event_* 120
PIXI values file_* 120
PIXI values hazard_* 121
PIXI values heartbeat_* 121
PIXI values imglocaltime_* 122
PIXI values imgutctime_* 122
PIXI values jpeg_* 123
PIXI values location_* 123
PIXI values globalmeta_* 124
PIXI values timeoffset_* 125
PIXI values plate_* 126

PIXI values triglocaltime_* 127
PIXI values trigutctime_* 128
PIXI values site_* 128
PIXI values supplementary_* 129
PIXI values localtime_* 129
PIXI values utctime_* 130
A. Technical Details 131
Communication 131
Console Serial RS-232 131
Ethernet 131
Network details 132
Filesystem layout 133
Backup 135
B. Software installation and upgrades 136
C. Factory Defaults 137
D. File transfers 138
SFTP 138
SCP 138
FTP 138
NFS 140
CIFS/Samba (Windows shares) 140
Transfer troubleshooting 140
Network problems 140
Permissions 141
E. Software tools 142
PIPS ANPR Toolkit 142
Windows 7 142
PuTTY 142
Filezilla 142
WinSCP 142
NFS Server on Windows 142
F. Nano - text editor 143
Opening and creating files 143
Saving and exiting 143
Cutting and pasting 143
Searching for text 143
G. rc-update 144
Introduction 144
rc-update commands 144
runlevels 144
Examples 144
Other information 144
H. Viewfinder Protocol 145
Viewfinder commands 145
Viewfinder messages 146
Version 1 146
Version 2 146
Version 3 147
Version 4 148
I. Vehicle Event Viewer Protocol 149
Vehicle Event Viewer commands 149
Vehicle Event Viewer data 149
Header Format 149
J. Legal Notices 152
English 152
Copyright Notice 152
Warranty 152
Service 152

Technical Support 152
Design Changes 153
Trademarks 153
FCC Declaration 153
Français 153
Notification de Copyright 153
Garantie 153
Service 153
Support Technique 153
Changements de Conception 154
Marques Déposées 154
K. Contact information 155

List of Figures

4.1. Objects in the system and how they fit together. 11
8.1. Link with no heartbeat, camera will close when no command has been received for 5 minutes. 100
8.2. Link with heartbeat, client chooses when to end by closing the link. 101
8.3. Get Root Objects - a list of all configureable objects is collected, some may have subobjects 102
8.4. Get subobjects of an object - a list of all subobjects is collected, some may have subobjects. The list may be empty, as in the example 103
8.5. Get properties of an object - a list of all the properties of an object. The list may be empty. 104
8.6. Start some logging. Asynchronous messages will be sent back by the Camera containing the log messages 105
8.7. Start notification messages. Asynchronous messages will be sent back by the Camera containing the notification messages of the requested events 107
8.8. Issue a command and receive the responses. 108
8.9. Connect to the camera and get events as it reads vehicles. 109
8.10. Here we are collecting (pulling) certain vehicle details when a particular vehicle is found. 110

List of Tables

7.1. Format characters 85
8.1. PIXI Packet Format 99
A.1. TCP/IP and UDP/IP Port numbers 133
C.1. Default IP configuration 137
K.1. Contact Information 155

Chapter 1. Introduction

This manual is for the Neology ANPR cameras listed inside the front cover. These cameras are very similar so most of this manual covers them all. Where differences occur the manual will note them.

The P382, P392+ and P492 share many common features, the highlights of which are

- ANPR Camera, illuminator and processor in one package
- Provides savings in system cost, complexity and timescales
- Neology proven camera and processor technology

This manual is only as up to date as the software it ships with. The corresponding version number is listed in the Revision note. Trying to use this manual with the wrong version of the software will be frustrating where differences occur.

P382

P382 is a fully integrated number plate reading camera incorporating both the camera and the recogniser within a single sealed enclosure. It is designed for use in the highest performance applications where it is necessary to provide the ANPR function across a full 4metre carriageway (3.5m with 0.5m overlap). The unit comprises a high resolution monochrome CCD camera with high sensitivity in the infra-red, surrounded by two banks of IR LEDs. Patented filter / flash technique gives suppression of headlights and bright sunlight. Field-by-field control of camera parameters allows the use of the ‘triple flash’ technique to reduce problems of plate-to-plate variability.

An optional independent, integrated, synchronous, colour camera may be configured to the same focal length as the monochrome camera, or to a wider field of view, as required. Therefore an ANPR read will have a colour overview image associated with it.

The integrated number-plate recogniser incorporates the Neology ‘Autoplate’ ANPR engine, which has been proven in many countries worldwide. Patented real-time video triggering upon plate presence provides excellent plate detection. A vehicle presence trigger input is also provided for the most demanding applications, e.g. taking an overview picture of a vehicle with a missing plate.

P382 can be integrated into a wide variety of systems via relay output, RS232, TCP/IP Ethernet with socket and FTP protocols (100baseT). Wireless IP connectivity over GPRS, EDGE or 3G is provided by fitting an optional modem. Additionally IEE802.11b/g ‘WiFi’ may be fitted to give local wireless operation. IP connectivity, (wired or wireless), provides time-lock of distributed cameras to a central server via NTP. A GPS unit may be fitted giving very high accuracy time and position information.

Real-time JPEG hardware compression is provided for both IR and colour images and can be used to provide a real-time IP video stream of the traffic. This can be used to record the image stream for ground-truthing.

P382 is fully web-enabled and can be configured and monitored from a standard web-browser on a PC.

External devices such as DSRC, Radar, Weigh-in-Motion or ticketing systems can be integrated into the system via RS232 or TCP/IP. A flexible interface allows this data to trigger the camera or be added asynchronously to the data set which the camera provides for each vehicle.

The Vehicle Enforcement System (VES) application software offers socket based transfer of Summary and Evidential Records via either push or pull protocols with full key handling, authentication, encryption and local storage of up to 60,000 events. Pre and post event contextual images showing the direction of travel may also optionally be captured. The direction of travel may also be captured.

- 4 metre road width coverage, using 1392 x 512 pixel sensor
- Powerful processor
- Reading multiple number plates in a single field of view

- Embedded Linux operating system, offering standard Linux connectivity including encrypted links
- Multiple concurrent access to viewfinder and event viewer
- Hardware MJPEG streaming of the video streams (50fps, 1392 x 512) eliminating the need for a high performance frame-grabber on a PC for data acquisition

P392+/P492

P392+/P492 is a fully-integrated number plate recognition unit incorporating camera (s), illuminator and data and image processing within a single sealed enclosure. The unit comprises a monochrome camera surrounded by two sets of IR LEDs. Neology patented filter/flash technique provides suppression of headlights and bright sunlight. Field-by-field control of camera parameters allows the use of ‘triple flash’ technique to reduce any problems of plate to plate variability.

P392+/P492 can also include an optional independent, integrated, synchronous, colour camera. The colour camera can be configured to the same focal length as the monochrome camera, or to a wider field of view as required enabling ANPR (Automatic Number Plate Recognition) reads to have associated colour overview images.

The integrated number-plate recogniser incorporates the Neology ‘AutoPlate’ ANPR engine, proven in many countries worldwide. Patented real-time video triggering upon plate presence provides excellent plate detection. A vehicle presence trigger is also provided for the most demanding applications, for example taking an overview picture of a vehicle with a missing plate.

P392+/P492 can be integrated into a wide variety of systems. Wireless IP connectivity over GPRS, EDGE or 3G can be provided by fitting an optional internal modem.

IP connectivity (wired or wireless), provides a time-lock of distributed cameras to a central server via NTP.

Real-time JPEG hardware compression is provided for both IR and colour images and can be used to provide a real-time IP video stream of the traffic. This can be used to record the image stream for ANPR data verification.

P392+/P492 is fully web-enabled and can be configured and monitored from a standard web-browser. External devices such as DSRC, radar, weigh-in-motion or ticketing systems can be integrated into the system. A flexible interface allows this data to trigger the camera or be added, without synchronisation, to the data set which the camera generates for each vehicle.

- Reading multiple number plates in a single field of view.
- Embedded Linux operating system, offering standard Linux connectivity including encrypted links.
- Multiple concurrent access to viewfinder and Neology client monitor application.
- Hardware MJPEG streaming of the video streams (50fps, 752x480 - P392/P392+ or 2048x720 P492) eliminating the need for a high performance frame-grabber on a PC for data acquisition.

Assumptions

The P382, P392+ and P492 are networked cameras, and a course in networking is beyond the scope of this manual. You are expected to have a working understanding of TCP/IP networking, or be able to consult with someone who can help you with this.

Conventions

We use several typographic conventions in this manual to describe things including interaction with a computer terminal.

Commands to be typed in are described as follows:

- `command`

The name of the command.

- {required_argument}
  A required argument to the command.
- [optional_arument]
  An optional argument to the command.
- [*replace_me*]
  Text which should be replaced by you to indicate, for example, the file to be worked on

these can be combined, for example

`ls` [-l] [*directory*]
describes part of how to use the ls command in Linux.

Some text needs to be typed in exactly as given

```
type this in exactly
```

and sometimes we give some representative response from the system

```
and it will print this out,
or at least something similar
```

We will also provide links to other sections of the book, for example this section is the section called “Conventions”[2] or sometimes external references, like this one to our web homepage: http://solutions.Pips.co.uk/wps/portal/Neology/en_GB/TrafficSafety/Systems/-/AutomaticNumberPlateRecognition/. If the medium you are reading this on supports it, you may be able to click to go to the appropriate place. Obviously, this doesn't work on printed copies!

Chapter 2. Getting started

It is highly recommended that you get familiar with your P382, P392+ or P492 camera indoors prior to taking the camera to the roadside.

Connectivity

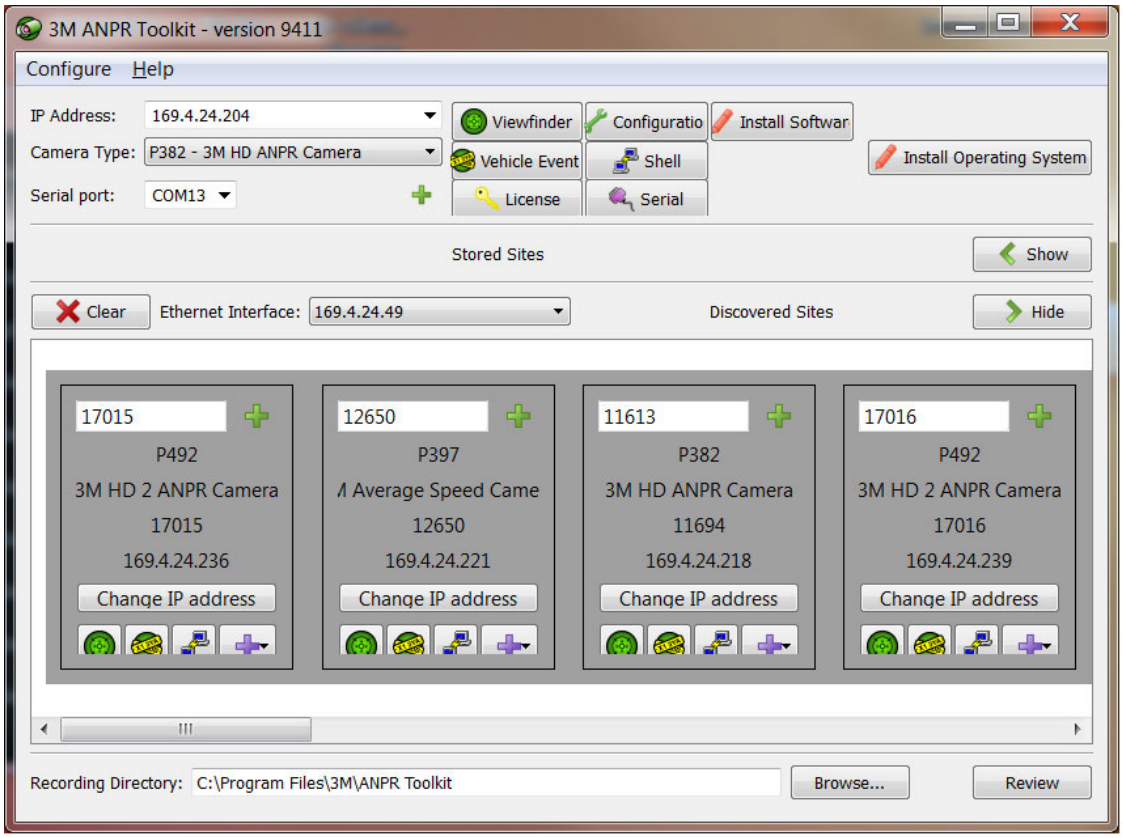
The PIPS ANPR Toolkit application should be installed on your PC, the camera connected to is often the easiest way to connect to the camera. If for some reason you cannot use this you will either need to connect via serial or via SSH and configure the network by hand the section called “Networking setup” [5].

Discovery

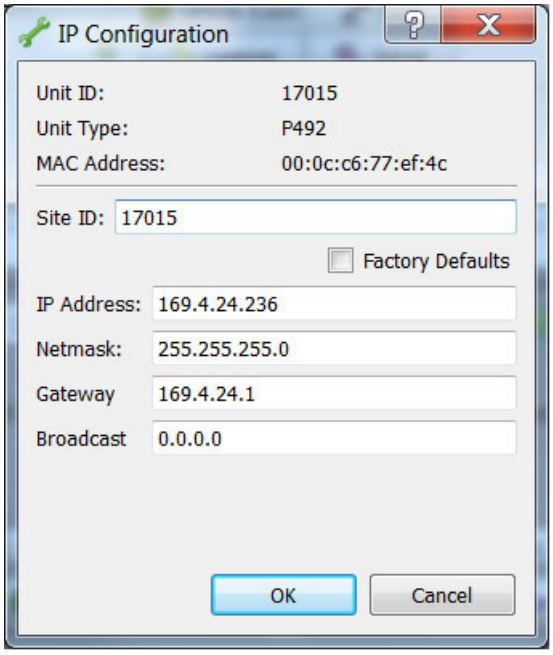
To use Discovery you will need to install the PIPS ANPR Toolkit (refer to Chapter 3, *PIPS ANPR Toolkit*[8]). If you connect the camera to the same ethernet as the PC on which you are running the toolkit and run the Toolkit you should be able to see the P382, P392+ or P492 in the list of discovered cameras.

Note

You can connect the camera to the same switch or hub, through multiple switches and hubs, or just use a cross over ethernet lead. However, the discovery protocol cannot traverse routers or gateways in your network.



If you start the application and select the network interface on your PC which matches the one to which the P382, P392+ or P492 is connected you should be able to see the camera. To identify the correct camera if you have multiple cameras on the network you should cross reference the serial number with that printed on the back of the camera. To configure the IP address of the camera click on `Change IP Address` edit the values displayed. Once you press OK, the camera will store the options and the address will change.



After around one minute you should be able to ping the camera and go on to configure the rest of the camera (see the section called “Connecting” [6]).

Serial RS-232

Full details on the console serial port are available in the hardware manual.

You will need a serial terminal, such as Kea! Term for Windows, PuTTY for Windows (see the section called “PuTTY” [142]), Minicom for Linux, or Hyperterminal for Windows (not recommended due to quirky behaviour). This should be connected at a line speed of 38,400 bits per second with 8 bits of data, no parity and 1 stop bit. This is often abbreviated to 38,400 8N1. No flow control is necessary. This should be connected to an appropriate serial port on the PC.

The system will boot into linux, eventually presenting you with the login prompt:

```
 * Starting portmap ...                                    [ ok ]
 * Mounting network filesystems ...                        [ ok ]
 * Starting sshd ...                                       [ ok ]
 * Starting vixie-cron ...                                 [ ok ]
 * Starting Webmin ...                                     [ ok ]
 * Starting local ...                                      [ ok ]


This is localhost.(none) (Linux i586 2.6.19.2) 01:42:51

localhost login:
```

If this is successful you can log in as root using by typing in **root** and then entering the root password (given in Appendix C, *Factory Defaults* [137].

Ethernet

As an alternative you can connect via ethernet. Knowledge of TCP/IP networking is assumed when reading this manual. The camera will be shipped from the factory with the settings specified in Appendix C, *Factory Defaults* [137]. If you can set up an SSH session to the camera then you do not need to use the serial port to configure the camera.

Networking setup

To use this section you are already logged into the camera via serial or SSH. You do not need to do this if you can use the IP discovery program (see the section called “Discovery”[4]). If you are not logged in, return to an earlier section to get a login prompt working. To set up networking we edit `/opt/config/current/netmon.xml`.

```
nano /opt/config/current/netmon.xml
```

Note

A guide to how to use nano is available in Appendix F, *Nano - text editor* [143]

Basic Configuration

In its basic form you can just edit the existing contents to change the IP address, netmask and gateway. The file should look like:

```
<?xml version="1.0"?>
<netmon>
  <main>
    <services>ethernet</services>
    <hostname>Camera</hostname>
  </main>
  <ethernet>
    <ip>aa.aa.aa.aa</ip>
    <netmask>bb.bb.bb.bb</netmask>
  </ethernet>
  <routes>
    <default>ethernet cc.cc.cc.cc</default>
  </routes>
</netmon>
```

Where `aa.aa.aa.aa` is the IP address you'd like to assign to the camera, `bb.bb.bb.bb` is the netmask, and `cc.cc.cc.cc` is the default gateway (remove this section if you don't want one). Under many circumstances this is acceptable.

Connecting

Although configuration is possible over the console serial port, the natural way to connect to the P382, P392+ or P492 is via the network, so we will get that working next. You may wish to skip this and move straight onto Chapter 5, *Configuration using Webmin* [13] to use the built in webserver to configure the camera.

SSH

Secure Shell or SSH is a secure networking protocol which can be used for many things, but here we will use it to provide a shell on the camera. It is running on the standard port, 22.

Many operating systems have an ssh client built in which can be invoked by typing ssh from the command line. Briefly:

`ssh` [*`user`*`@`] {*`hostname`*}
However Windows does not have one, we recommend PuTTY (see the section called “PuTTY” [142]). Any ssh client capable of SSH2 should work, feedback is welcomed on other implimentations. There is an SSH client available in Webmin under Others → SSH/Telnet Login which requires Java, but if you can see webmin I'd recommend you use that instead where possible as documented in Chapter 5, *Configuration using Webmin* [13]

Launch your ssh client to log into the camera, referring to Appendix C, *Factory Defaults* [137] for the root password. Once you have logged in you have the network working correctly and you can configure and use the camera.

You are logged into a Linux shell, and can use many normal Linux commands to navigate. A brief set of useful commands and arguments are given here.

- `ls` [-l] [*`directory`*]
  get a directory listing, similar to **dir** under DOS
- `pwd`
  display the current working directory
- `cd` {*`directory`*}

change directory to given directory. Use `..` to go up one directory

- `nano` {*`filename`*}
  edit a file. See Appendix F, *Nano - text editor* [143] for more details.
- `cat` {*`filename`*}
  quickly show a file.
- `less` {*`filename`*}
  display a file, so you can scroll up and down.
- `ftp` [*`ip_address`*]
  launch the FTP client to transfer files to or from a remote machine. TODO - xref

This is only a very brief list. A good list can be found online at http://www.ss64.com/bash/, and a comprehensive introduction which is worth reading at http://en.flossmanuals.net/command-line/. These links are not under our control and may expire with time.

Note

Manual pages are *not* installed on the camera so you cannot refer to them there. Sorry.

Restarting and Shutting Down

Due to the possibility of corrupting the filesystem, the following should as far as possible be adhered to for P382, P392+ and P492 cameras.

Restarting after changing settings

Some settings require that the camera is restarted before the change is applied. To do this, users must issue the reboot command via ssh or use the reboot button in webmin. Users must not switch off the power supply to the camera.

Switching off for planned maintenance

When wanting to switch off the camera, it is recommended that users do not simply remove the power from the camera or unplug the connector. Instead, best practice is to connect to the camera using ssh (eg. Putty) and issue the shutdown now command. After this, you should wait approximately 30 seconds for the camera to shut down, and then remove the power within a further 30 seconds.

Power-cycling

If you wish to power cycle the camera to attempt to recover from some error you should use the shutdown now command via ssh to cleanly shutdown the camera and remove power from the camera 30 seconds after issuing this command. Keep power off the camera for over 30 seconds before re-applying it.

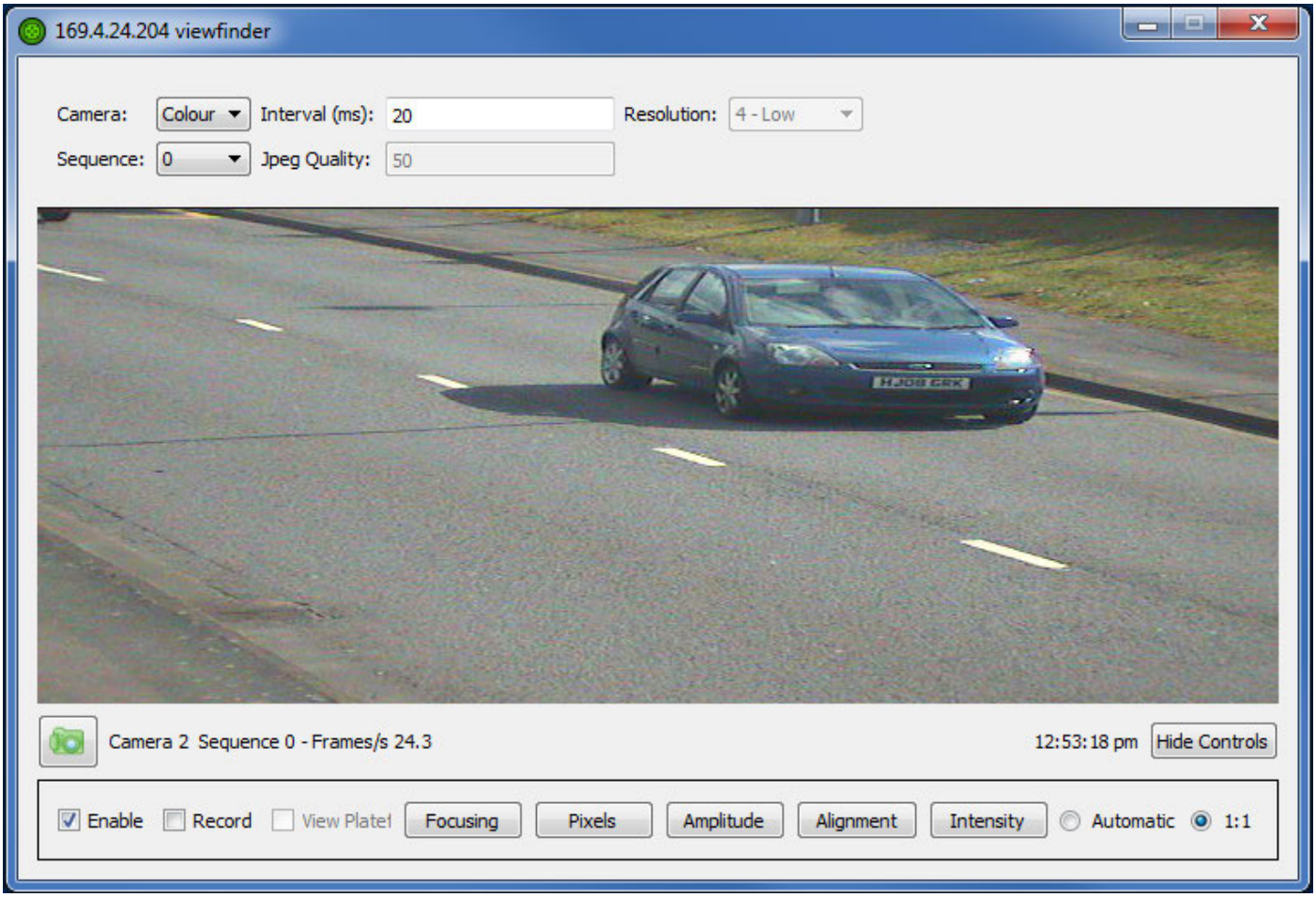
If you are unable to issue the shutdown command due to the problem you are trying to resolve, you must still observe the long delay between removing power and re-applying it – re-applying power to the camera too quickly can cause problems.

Chapter 3. PIPS ANPR Toolkit

PIPS ANPR Toolkit (see the section called “PIPS ANPR Toolkit”[142]) is a valuable tool in diagnosing, setting up and maintaining your camera. To use it, launch the viewer from the Start → PIPS → Toolkit on Windows. You can then enter the IP address of the camera you wish to view, or select it from the drop down list if you have viewed it before.

Viewfinder

By pressing the **`Viewfinder`** button, you can launch a "through the camera" viewer.



From this you can select to view either camera, and whichever sequence number of the camera you wish (which are valid is dependent on the `numentries` parameter of the camera you are viewing, by changing the drop down list. Camera 1 is the infra-red camera, 2 is the colour one.

You can speed up or slow down the image rate dependent on your PC loading and network bandwidth - if you select a low interval it will cause more loading. Quality and Resolution have no effect on a P382, P392+ or P492.

The Enable checkbox connects or disconnects the viewfinder from the camera. If the Record box is checked then the Toolkit will record the received images. The radio buttons can be used to select the size of the images as displayed by the viewfinder.

The buttons along the bottom of the window provide access to other tools. The Enable checkbox connects or disconnects the viewfinder from the camera.

Vehicle Events

By pressing the **`Vehicle Events`** button, you can launch an event viewer, which shows each vehicle that the camera detects separately.



The Enable checkbox connects or disconnects the event viewer from the camera. If the Record box is checked then the Toolkit will record the received data and images.

The radio buttons are used to select the protocol used to connect to the camera. If the PIXI protocol is selected then the Configure PIXI button can be used to select the event data and image to display. The Expand All Show More option can be used to show additional data received via PIXI.

The trigger button can be used to send a TCP trigger to the camera. The trigger message can be configured using the Trigger Config tab.

The Clear button clears the display.

Review

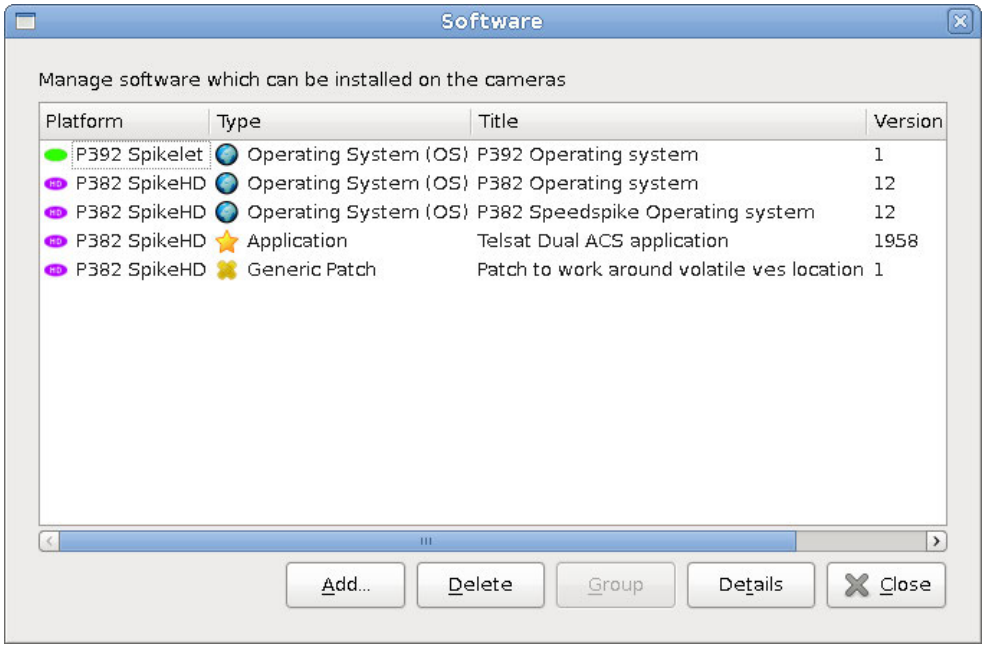
In the viewfinder and vehicle events view you can select to disable or enable updates, and also record the data using the tick boxes in the lower left hand corner. If you have recorded events you can view them by pressing the **`Review`** button. This is currently functional but not complete.

Camera Software

The toolkit allows you to maintain the software on your cameras. There are two parts to this.

Software Management

By selecting Configure → Software from the menus of the toolkit you can *locally* manage software which you can install on the camera.



- Add: You can add software distributed from PIPS to your pool of available software to install. Mostly these will be .tar.lzma files, but also the libcardet files which are number plate reading engines can be placed here. The files will be copied and stored by the application in it's own private repository..
- Delete: Delete items from your local pool of files. Any groups which depend on these files also get deleted.
- Group: Group a set of items together for ease of installation. Once grouped together a set of files will behave like a single unit and can all be installed together to ease installation. Example uses are grouping an ANPR library with an application to install the two together, or adding a patch to an os to install as one.
- Close: Close the dialogue box.

Software Installation

Software can be installed on the camera by clicking on the small orange pencil. Some basic options as to what type of installation to do, and it will ask you to enter details for the camera so that it can connect. To perform an operating system installation you must be connected via a serial port and via ethernet.

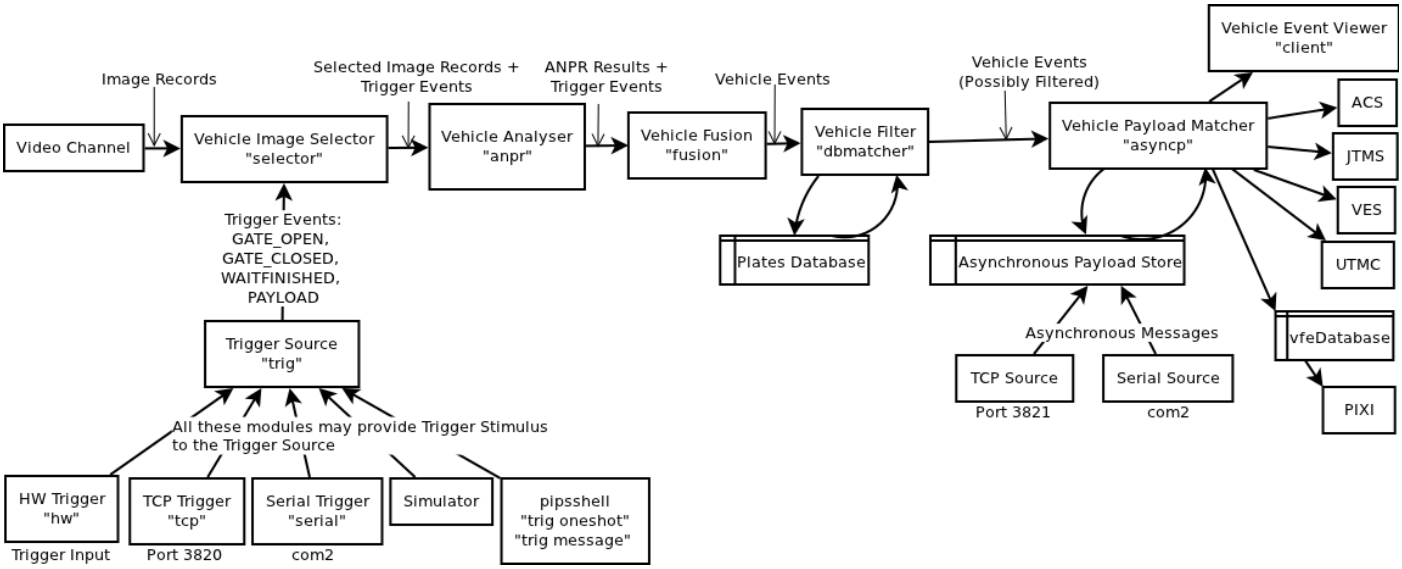
A critical concept is that some software contains a 'complete operating system' (OS) and some does not. To install a complete operating system there is quite a lot more work required, so these software packages are separated from the non-OS components

Chapter 4. Camera technical overview

The P382, P392+ and P492 are very configurable, and complex to understand. This chapter will hopefully help you to understand the internals and what they do so that you can make wise choices in setting up.

This diagram shows the objects in the system and how they fit together. Each of the individual objects is documented more completely in the section called “PIPS Shell Commands”[15], but this overview will help you put those pieces together.

Figure 4.1. Objects in the system and how they fit together.



Interfaces: Output mechanisms

The P382, P392+ and P492 have various mechanisms for outputting the resulting data from their operation and delivering it to another system for processing. This chapter describes them each in brief to allow you to understand and choose what to use. Most of these systems can be used at the same time as one another.

- *ACS* stands for Access Control System. It is a simple network delivery of image and text files via FTP or SFTP. It is designed for production use, and is recommended as a simple way to get started. This simplicity does not mean it is unsuitable for large scale deployments, but it does require a reasonable amount of bandwidth. It is very flexible in which images are available and what metadata is contained in the text file and the filenames. More detail on configuring the system is available in the section called “ACS - Access Control System (acs)”[15] and the available metadata list is Chapter 7, *Format strings* [84]. I would recommend developing with ACS unless you have a reason why you cannot use it. You can use this delivery mechanism alongside others, such as PIXI. There is a separate ACS interface document available which is for legacy systems, and not particularly relevant to the P382, P392+ and P492.

- *PIXI* is an XML based interface for collecting information and controlling all aspects of the camera. It can flexibly push and pull data from the camera, and requires no configuration on the camera. All configuration can be done via this protocol. For more complex requirements that cannot be met with ACS we would encourage the use of this protocol, which is fully documented in Chapter 8, *PIXI Protocol* [98].

- *JTMS* stands for Journey Time Measurement System. This is a relatively simple TCP/IP mechanism for delivering data suitable for measuring journey times. It uses very little bandwidth, and is not flexible for other uses. It does not provide any images. More detail on configuring this system is available in the section called “JTMS - Journey Time Measurement System (jtms)” [49]

- *VES* stands for Violation Enforcement System. This is a complex TCP/IP mechanism for delivering data suitable for many uses. It can provide images, encryption and push and pull of data. There is a separate interface document

available under an NDA (Non-Disclosure Agreement) from Neology describing this interface in detail. For new developments, unless you need encryption we'd encourage the use of PIXI instead of VES.

- *UTMC* stands for Urban Traffic Management and Control. This is a web-base mechanism for delivering data. A camera can be configured to deliver data to one or more UTMC servers. Protocol versions 1.0 and 1.2 are supported.
- *SAP* is the serial application port. This provides delivery of the plate or other metadata via the second serial port on the camera (COM2). It is flexible, but obviously cannot deliver images. More detail on configuring the system is available in the section called “SAP - Serial Application Port (sap)”[57] and the available metadata list is Chapter 7, *Format strings* [84]. You may (as with all the other output systems) use this in conjunction with other output mechanisms listed here. The serial port may only be used for one function at once.
- *Image File Output* is a debugging system, and should not be used for any production system. It places fixed filename images on the local /storage device. It may have a performance impact on the system if it is used.
- *Viewfinder* is a legacy TCP/IP protocol for viewing live images from the camera. It does not guarantee the delivery of any images. The protocol is defined in Appendix H, *Viewfinder Protocol* [145]. This is used by the Toolkit.
- *Vehicle Event Viewer* is a legacy TCP/IP protocol for viewing read images from the camera. It does not guarantee the delivery of any images and is therefore not suitable for production use. The protocol is defined in Appendix I, *Vehicle Event Viewer Protocol* [149]. This is used by the Toolkit.

Chapter 5. Configuration using Webmin

The camera provides a web administration utility called webmin. You can access this from your web browser on

`https://camera.ip.address/`

You will need to log in, referring to Appendix C, *Factory Defaults* [137] for the root password.

From here you can configure many aspects of the camera. This manual will take you through some of the more important ones. You can break the camera using some of these options, don't play unless you understand what you are doing.

Note

The web interface is only available over the https protocol, not the http protocol. Ensure you put the s in the URL

On the P392+ and P492 cameras (and only these models) should have the /backup.pl script run from the command line after any change - once that change is determined to be satisfactory. Changes include:

- New OS and application installations
- Application upgrades, Cardet upgrades
- Configuration changes

Running backup ensures that should a file system corruption be recoverable via this mechanism, the recovery will be to the last backed up state.

Camera control

Initially you will be presented with the camera application interface to configure the camera aspects of the system. This is accessible under Others → Camera Application if you need to get back to it. This manual is available from this page (indeed, you may be reading it there right now!). As well as this all the configuration options and commands are available with online help. This help is also printed for reference in Chapter 6, *PIPS ANPR Shell* [15] should you need it.

Webmin allows all of the shell parameters and commands to be accessed, as listed in Chapter 6, *PIPS ANPR Shell* [15].

You can also manage the anpr libraries from here and upload new ones by selecting Spike II (382) Application → ANPR Vehicle Analyser → Library Manager → Manage number plate libraries

Network

The network configuration is available under Networking → Networking Configuration and allows control of the IP address parameters and the hostname of the camera. It is important to set up the hostname of the camera to something useful and unique as several subsystems use it to identify the camera. The factory default is the serial number of the camera.

You can also set up an on camera firewall Networking → Linux Firewall.

Caution

Incorrectly configuring the firewall can make the camera *completely unresponsive* to network control, including webmin and SSH, requiring you to access it via the RS232 port or return it to Pips.

Mounting network disks

The P382, P392+ and P492 have the ability to save files to disk, which can be remotely mounted over NFS. Most operating systems come with an NFS server, so you can just use those. Windows users may wish to see the section

called “NFS Server on Windows”[142]. You can also mount CIFS and SMB "Windows shares" from windows servers or workstations.

NFS

Once you have a directory exported so that the camera can see it you can mount it via the System → Disk and Network Filesystems menu option. Use the drop down list to select **`Network Filesystem (nfs)`** and make sure you fill in the Mounted As, NFS Hostname and NFS Directory to be **`/storage/`*`pre-created-directory`***, the IP address of the server and the directory you have entered in `/etc/exports` respectively.

Windows shares

There are so many versions of Windows, and depending upon what you have installed it is hard to tell if you will need to use CIFS. In theory it is downwards compatible, but you definitly need it for Windows 2003 server shares. If it fails try **`Windows Networking Filesystem`** instead of **`Common Internet Filesystem`** in the instructions below.

You can mount a windows share via the System → Disk and Network Filesystems menu option. Use the drop down list to select **`Common Internet Filesystem (cifs)`** and make sure you fill in the Mounted As, Server Name and ShareName to be **`/storage/`*`pre-created-directory`***, the IP address of the server and the share name you have shared respectively. I would not attempt to use server names rather than IP addresses, although it may work for you, it may be unreliable. You will almost definitly have to fill in Login Name and Login Password details.

Chapter 6. PIPS ANPR Shell

The shell is an alternative way to access and control the camera's parameters. You can start it whilst at the linux command prompt (either via SSH or on the console serial port) by typing

```
/opt/PIPS/PIPSshell

 Welcome to the PIPS ANPR Camera shell - 127.0.0.1
 Shell Version Version 4.7.9540 built at 13:06:54 on Mar 17 2015
 (Using library version Version 9540 built at 15:02:53 on Mar 20 2015)

 Log: Mon Mar 23 11:39:24 2015 - NetUI.cpp:1179:Copyright (C) Neology UK Ltd., 2006-2013. All Rights Reserved. on 17015
 Log: Mon Mar 23 11:39:24 2015 - NetUI.cpp:1180:Serial number: 17015
 Log: Mon Mar 23 11:39:24 2015 - NetUI.cpp:1181:Version 4.7.9540 built at 15:03:29 on Mar 20 2015
 Log: Mon Mar 23 11:39:24 2015 - NetUI.cpp:1182:libPIPSLinux:Version 9540 built at 15:02:53 on Mar 20 2015
 Log: Mon Mar 23 11:39:24 2015 - NetUI.cpp:1183:Hardware: Version 647 (Cap 406), Internal JPEG Compressor, Square Platefinder, Dual JPEG, Mono flash table,
 Log: Mon Mar 23 11:39:24 2015 - NetUI.cpp:1211:Sensor 0CMV2000 (CMOS): Width: 2048, Height: 720 @ 50FPS as a Monochrome Processing sensor
 Log: Mon Mar 23 11:39:24 2015 - NetUI.cpp:1211:Sensor 1CMV2000 (CMOS): Width: 2048, Height: 720 @ 50FPS as a Colour Overview sensor
 Log: Mon Mar 23 11:39:24 2015 - NetUI.cpp:1226:uname: Linux 17015 2.6.36.2 #4 Mon Jan 27 09:49:07 Local time zone must be set--see zic manu armv5tel
 >>
```

The double chevrons are the prompt and you can type in commands here.

The model of commands is one of objects, which have properties and commands. Objects can be nested, and the sub-object's name is separated by a space from the parent. This may sound confusing, re-read it after you have read the list of commands.

- `help` [*`object`*]
  You can see a list of objects by typing **help** with no arguments, and see properties and commands of each object by giving the object name as an argument.
- `history`
  Display a list of old commands you have typed in. The command line supports full “GNU readline” command line editing and history. Basically the arrow keys work like you might hope.
- `quit`
  Leave the shell.

The complete list of objects with their properties and commands follows, but this may be out of date as with any printed material, and I suggest referring to the command line help.

The objects, properties and commands are not guaranteed to stay the same between software releases - although all functionality formally available will remain. Please consult with Neology of details on how to upgrade.

On the P392+ and P492 cameras (and only these models) should have the /backup.pl script run from the command line after any change - once that change is determined to be satisfactory.

PIPS Shell Commands

ACS - Access Control System (acs)

Available on platforms: All

The Access Control System is an output module which sends vehicle details to an external computer for processing. It will output a (configurable) number of jpeg images of the vehicle along with a text record describing the license plate event (LPR). This data may be sent as separate files, named according to the lpr_filename (with .lpr extension) and img_filename (with .jpg extension) properties. Alternatively, the data may be sent within a single packed file consisting of an XML header followed by the binary image data. In this case the filename will be the lpr_filename with a .axi extension and the LPR text record is contained withing the XML header. The XML header also contains data allowing the extraction of the image data.

Platforms	Name	Command	Default Value	Description
All	Append lpr text data	`acs set append_lpr {`*`value`*`}`	false	When using FTP/SFTP the LPR file can be appended onto an existing file if this option

Platforms	Name	Command	Default Value	Description
				is set to true. This can be used for example to create a single .csv file for all events delivered.
All	Buffer the transfer	`acs set buffer_transfers {value}`	true	Stores images in internal non-volatile storage to allow them to be transferred later should the file server be inaccssable for any reason.
All	Output Character Encoding for filenames	`acs set char_set {value}`	0	If in doubt, set this to 0. The character encoding used for strings for filepaths. 0 - ASCII-7bit 1 - ISO8859-1 2 - UTF-8 If using ASCII-7bit any special characters will be converted to nearest ASCII equivalents. If using anything other than ASCII-7, please ensure your server and other software is capable of handling the specific encoding
All	The Delivery Order	`acs set delivery_order {value}`	FIFO	The delivery order is a choise between First In First Out (FIFO) or Last In First Out (LIFO). (If switching between modes the data stored before switching will be lost). (If order is not FIFO or LIFO it will be treated as FIFO).
All	Enabled	`acs set enabled {value}`	false	Allows the ACS system to be enabled and disabled. Disable it unless you are using it.
All	Fast Ftp	`acs set fast_ftp {value}`	false	Accelerate FTP by ignoring what RFC1738 says and just transferring files directly into directories with STOR, rather than CWD first. Most off the shelf FTP servers will accept this happily, and it reduces latency.
All	Output Character Encoding For file Contents	`acs set file_char_set {value}`	0	If in doubt, set this to 0. The character encoding used for strings for LPR file contents. 0 - ASCII-7bit 1 - ISO8859-1 2 - UTF-8 If using ASCII-7bit any special characters will be converted to nearest ASCII equivalents. If using anything other than ASCII-7, please ensure your server and other software is capable of handling the specific encoding
All	Host	`acs set host {value}`		The IP address to which the files will be transferred. LPR files will be transferred last, after the jpeg files.

Platforms	Name	Command	Default Value	Description
All	Fallback Host	`acs set host2` {*value*}		Fallback IP address to which the files will be transferred if transfer to Host fails. LPR files will be transferred last, after the jpeg files.
All	Image filename	`acs set img_filename` {*value*}	%Jts%Id02u%Vm02u%Vd02u%Vh02u%Vn02u%Vs02u%Id02u,%Pps	A format string containing how to construct the image filename. You MUST put %Jtc in this string if you are outputting multiple images per event or else they WILL all have the same filename and overwrite each other. Note this property is only meaningful if transfer_packed is false
All	LPR contents	`acs set lpr_contents` {*value*}	%PNs\n%Pas\n%Pat%Jtn%Ets%Fmw	A format string containing how to construct the data you would like in the LPR file
All	LPR filename	`acs set lpr_filename` {*value*}	%Ei08X.lpr	A format string containing how to construct an LPR or AXI filename. If the transfer_packed property is set 1 (true) an AXI file is transferred. Otherwise an LPR file will sent with any required image files sent separately.
All	Maximum Disk Queue Length	`acs set nlog` {*value*}	100	The maximum number of ACS events which will be stored on the local filesystem before they are overwritten if it is not possible to contact the instation. Warning, arbitrarily setting this to a high value may fill up the device on which you are storing the files and then the system will lose the wrong data or may perform badly.
All	Password	`acs set pass` {*value*}		The password used to log in to the server or to unlock your private key, depending upon which method you're using to transfer.
All	Noread patch	`acs set patch_noread` {*value*}	false	When there is a no read there is also no patch. If you set this to true you'll get the full IR image output as a patch instead of no output.
All	Timeout	`acs set timeout` {*value*}	60	The timeout on operations over the file transfer link. NB: May not be what you expect from legacy systems.
All	Transfer overview context images	`acs set transfer_contexts` {*value*}	true	Transfer the overview context images (if any). The number and offsets of context images are configured under Contexts. Depending on the setting of transfer_packed this may be sent as a JPG file or within an AXI file
All	Transfer hazard IR images	`acs set transfer_hazard_ir` {*value*}	true	Transfer the full infra-red monochrome images. Depending on the setting of transfer_packed this may be sent as a JPG file or within an AXI file
All	Transfer hazard overview images	`acs set transfer_hazard_overview` {*value*}	true	Transfer the overview images (e.g. the colour images). Depending on the setting of transfer_packed this may be sent as a JPG file or within an AXI file
All	Transfer hazard patch images	`acs set transfer_hazard_patch` {*value*}	true	Transfer a small image of just the number plate patch. Depending on the setting of transfer_packed this may be sent as a JPG file or within an AXI file

Platforms	Name	Command	Default Value	Description
All	Transfer IR images	`acs set transfer_ir {value}`	true	Transfer the full infra-red monochrome images. Depending on the setting of transfer_packed this may be sent as a JPG file or within an AXI file
All	Transfer lpr text data	`acs set transfer_lpr {value}`	true	Transfer a text block containing metadata, called LPR data. Depending on the setting of transfer_packed this may be sent as an LPR file or within an AXI file
All	Transfer overview images	`acs set transfer_overview {value}`	true	Transfer the overview images (e.g. the colour images). Depending on the setting of transfer_packed this may be sent as a JPG file or within an AXI file
All	Transfer all data in a single AXI file	`acs set transfer_packed {value}`	false	Normally the data is transferred as separate LPR file and up to 3 image (JPG) files. Set this to true to transfer all required data in a single file (with file name lpr_filename.axi) consisting of an XML header followed by image data if required
All	Transfer patch images	`acs set transfer_patch {value}`	true	Transfer a small image of just the number plate patch. Depending on the setting of transfer_packed this may be sent as a JPG file or within an AXI file
All	Transfer path	`acs set transfer_path {value}`	%Shs/	A format string containing the path on theserver you'd like the files transferred to. This should contain / or \ as directory separators. It should end with a directory separator.
All	Transport	`acs set transport {value}`	sftp	The transport mechanism by which the system will transfer files. The options are sftp (recommended), scp, ftp, file. If you use scp the system is unable to create directories, so you must do that for it. File will deliver to the local filesystem under /storage.
All	Username	`acs set user {value}`		The username used to log in to the server

- `acs clearStats`

  Resets all Statistics. Platforms: All.

  Resets all Statistics

- `acs diskq_flush`

  Empty the Disk Queue. Platforms: All.

  All ACS events currently stored in the persistant Disk Queue will be deleted and will not be recoverable. Use this with care.

- `acs diskq_length`

  Length of Disk Queue. Platforms: All.

The number of ACS events stored in the persistant Disk Queue will be reported. Note this value may be non zero even if buffer_transfers is false. If buffer_transfers is false, the system still uses the disk queue, it just wont store items between reboots.

- `acs stats`

  Statistics. Platforms: All.

  Statistics for debugging

Specific Filenames (acs filenames)

Available on platforms: All

If you wish to have more control over the image filenames of the ACS output this section is for you, otherwise you can ignore it. You can specify filenames for each individual image that ACS outputs. If you leave the filenames blank then the standard ACS configuration will apply for that file. If you specify anything for a file, that file will be output with that filename. It will have the transfer_path prepended like with the standard naming scheme. If you want to output to different directories for each file, you can specify the path as part of the filename. If the transfer_path is blank you could output each file to a completely different directory. You cannot specify the lpr filename here as it is already available as a solo format string in the main ACS section.

Platforms	Name	Command	Default Value	Description
All	Hazard Full IR Filename	`acs filenames set haz_ir_filename {value}`		The format string used for the filename for the hazard full IR images.
All	Hazard Overview Filename	`acs filenames set haz_oview_filename {value}`		The format string used for the filename for the hazard overview images.
All	Hazard Patch Filename	`acs filenames set haz_patch_filename {value}`		The format string used for the filename for the hazard patch images.
All	Full IR Filename	`acs filenames set ir_filename {value}`		The format string used for the filename for the full IR images.
All	Overview Filename	`acs filenames set oview_filename {value}`		The format string used for the filename for the overview images.
All	Patch Filename	`acs filenames set patch_filename {value}`		The format string used for the filename for the patch images.

Context 1 (acs filenames context1)

Available on platforms: All

If you wish to have more control over the image filenames of the ACS output this section is for you, otherwise you can ignore it. You can specify filenames for each individual image that ACS outputs. If you leave the filenames blank then the standard ACS configuration will apply for that file. If you specify anything for a file, that file will be output with that filename. It will have the transfer_path prepended like with the standard naming scheme. If you want to output to different directories for each file, you can specify the path as part of the filename. If the transfer_path is blank you could output each file to a completely different directory. You cannot specify the lpr filename here as it is already available as a solo format string in the main ACS section.

Platforms	Name	Command	Default Value	Description
All	Contexts Filename			

Platforms	Name	Command	Default Value	Description
		`acs filenames context1 set filename {`*`value`*`}`		The format string used for the filename for this context images.

Context 2 (acs filenames context2)

Available on platforms: All

If you wish to have more control over the image filenames of the ACS output this section is for you, otherwise you can ignore it. You can specify filenames for each individual image that ACS outputs. If you leave the filenames blank then the standard ACS configuration will apply for that file. If you specify anything for a file, that file will be output with that filename. It will have the transfer_path prepended like with the standard naming scheme. If you want to output to different directories for each file, you can specify the path as part of the filename. If the transfer_path is blank you could output each file to a completely different directory. You cannot specify the lpr filename here as it is already available as a solo format string in the main ACS section.

Platforms	Name	Command	Default Value	Description
All	Contexts Filename	`acs filenames context2 set filename {`*`value`*`}`		The format string used for the filename for this context images.

Context 3 (acs filenames context3)

Available on platforms: All

If you wish to have more control over the image filenames of the ACS output this section is for you, otherwise you can ignore it. You can specify filenames for each individual image that ACS outputs. If you leave the filenames blank then the standard ACS configuration will apply for that file. If you specify anything for a file, that file will be output with that filename. It will have the transfer_path prepended like with the standard naming scheme. If you want to output to different directories for each file, you can specify the path as part of the filename. If the transfer_path is blank you could output each file to a completely different directory. You cannot specify the lpr filename here as it is already available as a solo format string in the main ACS section.

Platforms	Name	Command	Default Value	Description
All	Contexts Filename	`acs filenames context3 set filename {`*`value`*`}`		The format string used for the filename for this context images.

Context 4 (acs filenames context4)

Available on platforms: All

If you wish to have more control over the image filenames of the ACS output this section is for you, otherwise you can ignore it. You can specify filenames for each individual image that ACS outputs. If you leave the filenames blank then the standard ACS configuration will apply for that file. If you specify anything for a file, that file will be output with that filename. It will have the transfer_path prepended like with the standard naming scheme. If you want to output to different directories for each file, you can specify the path as part of the filename. If the transfer_path is blank you could output each file to a completely different directory. You cannot specify the lpr filename here as it is already available as a solo format string in the main ACS section.

Platforms	Name	Command	Default Value	Description
All	Contexts Filename			

Platforms	Name	Command	Default Value	Description
		`acs filenames context4 set filename {`*`value`*`}`		The format string used for the filename for this context images.

Context 5 (acs filenames context5)

Available on platforms: All

If you wish to have more control over the image filenames of the ACS output this section is for you, otherwise you can ignore it. You can specify filenames for each individual image that ACS outputs. If you leave the filenames blank then the standard ACS configuration will apply for that file. If you specify anything for a file, that file will be output with that filename. It will have the transfer_path prepended like with the standard naming scheme. If you want to output to different directories for each file, you can specify the path as part of the filename. If the transfer_path is blank you could output each file to a completely different directory. You cannot specify the lpr filename here as it is already available as a solo format string in the main ACS section.

Platforms	Name	Command	Default Value	Description
All	Contexts Filename	`acs filenames context5 set filename {`*`value`*`}`		The format string used for the filename for this context images.

Context 6 (acs filenames context6)

Available on platforms: All

If you wish to have more control over the image filenames of the ACS output this section is for you, otherwise you can ignore it. You can specify filenames for each individual image that ACS outputs. If you leave the filenames blank then the standard ACS configuration will apply for that file. If you specify anything for a file, that file will be output with that filename. It will have the transfer_path prepended like with the standard naming scheme. If you want to output to different directories for each file, you can specify the path as part of the filename. If the transfer_path is blank you could output each file to a completely different directory. You cannot specify the lpr filename here as it is already available as a solo format string in the main ACS section.

Platforms	Name	Command	Default Value	Description
All	Contexts Filename	`acs filenames context6 set filename {`*`value`*`}`		The format string used for the filename for this context images.

Context 7 (acs filenames context7)

Available on platforms: All

If you wish to have more control over the image filenames of the ACS output this section is for you, otherwise you can ignore it. You can specify filenames for each individual image that ACS outputs. If you leave the filenames blank then the standard ACS configuration will apply for that file. If you specify anything for a file, that file will be output with that filename. It will have the transfer_path prepended like with the standard naming scheme. If you want to output to different directories for each file, you can specify the path as part of the filename. If the transfer_path is blank you could output each file to a completely different directory. You cannot specify the lpr filename here as it is already available as a solo format string in the main ACS section.

Platforms	Name	Command	Default Value	Description
All	Contexts Filename			

Platforms	Name	Command	Default Value	Description
		`acs filenames context7 set filename {`*`value`*`}`		The format string used for the filename for this context images.

Context 8 (acs filenames context8)

Available on platforms: All

If you wish to have more control over the image filenames of the ACS output this section is for you, otherwise you can ignore it. You can specify filenames for each individual image that ACS outputs. If you leave the filenames blank then the standard ACS configuration will apply for that file. If you specify anything for a file, that file will be output with that filename. It will have the transfer_path prepended like with the standard naming scheme. If you want to output to different directories for each file, you can specify the path as part of the filename. If the transfer_path is blank you could output each file to a completely different directory. You cannot specify the lpr filename here as it is already available as a solo format string in the main ACS section.

Platforms	Name	Command	Default Value	Description
All	Contexts Filename	`acs filenames context8 set filename {`*`value`*`}`		The format string used for the filename for this context images.

Event Filter (acs filter)

Available on platforms: All

Platforms	Name	Command	Default Value	Description
All	Tag Regex	`acs filter set tag_regex {`*`value`*`}`	.*	

Using ACS

ACS uses various different file transfer protocols. It is recommended that you use SFTP as it is secure, can create directories, and has less network overhead than the FTP protocol. Historically ACS used the FTP protocol and that is also still possible. A suitable FTP server is required (FileZilla server is recommended for MS Windows platforms). SCP is also supported, but most platforms which work with SCP also work with SFTP which is able to create directories, wheras SCP is not.

Based on a number plate read event, ACS can transfer the following information:

- LPR data which consists of text metadata regarding the plate read event. LPR data will be transferred if **`transfer_lpr`** is set. The exact content of LPR text may be specified with the **`lpr_contents`** format string.
- A plate patch image in jpeg format. A patch image will be transferred if **`transfer_patch`** is set.
- A complete Infrared (IR) image in jpeg format. An IR image will be transferred if **`transfer_ir`** is set.
- A colour overview image in jpeg format. An overview image will be transferred if **`transfer_overview`** is set.

This ACS event data data may be transferred as separate files (up to 3 jpeg image files and an LPR textfile). These files are named according to the **`lpr_filename`** and **`image_filename`** properties.

Alternatively, if the **`transfer_packed`** property is set, all the required data is packed into a single AXI file. An AXI file consists of an XML header section followed by binary image data for whichever of the images are required. The advantage of using a packed AXI file is that there is less transfer overhead (a particular problem with normal FTP, a single transfer vs. up to four separate transfers) and may simplify processing at the receiver (no need to correlate the multiple files that relate to a single plate read event). One disadvantage with the packed format is that the file needs to be unpacked. However, the format is very simple (see the section called “ACS Event XML Schema”[23]) and should be easy to decode.

Older ACS systems only ever transferred separate files. Thus, for compatibility reasons, it may be necessary to disable the **`transfer_packed`** property.

Authentication

If you are using SFTP or SCP you can authenticate with your server in two ways.

- Conventional username and password, in a similar way to keyboard authentication. This is generally accepted as less secure, but is trivial to setup and may be good enough. To do this just set the **`user`** and **`pass`** properties and log in with those. This is the only option with conventional FTP.
- Using an SSH public key. You will need to create a public/private key pairing and install both of these onto your camera as `/opt/config/current/key_acs` and `/opt/config/current/key_acs.pub`. You can do this on the camera using **`ssh-keygen -t rsa`**. You must also give the public key to the server to allow it to authenticate - on a conventional openssh system this would be done by appending the public key into `~/.ssh/authorized_keys2` for the user you're going to transfer as. Once this is done you set up the user in the **`user`** field and if your private key has a passphrase enter that into the **`pass`** property.

ACS Event XML Schema

The packed AXI file format consists of an XML header followed by binary data for whatever images are required. The XML header part is a NULL terminated string. Binary data starts immediately after the NULL character. This XML header data contains the LPR text (if required) and, for each required image, the offset from the start of the binary data to the start of the image and the image length. This information is sufficient to extract the individual jpeg images.

The XML schema for the header is as follows:

axi.xsd

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
  <xs:element name="acs_event_header">
    <xs:complexType>
      <xs:sequence>
        <xs:element minOccurs="0" maxOccurs="1" ref="lpr"/>
        <xs:element minOccurs="0" maxOccurs="1" ref="patch"/>
        <xs:element minOccurs="0" maxOccurs="1" ref="full"/>
        <xs:element minOccurs="0" maxOccurs="1" ref="overview"/>
        <xs:element minOccurs="0" maxOccurs="1" ref="hazardPatch"/>
        <xs:element minOccurs="0" maxOccurs="1" ref="hazardFull"/>
        <xs:element minOccurs="0" maxOccurs="1" ref="hazardOverview"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="lpr" type="xs:string"/>
  <xs:element name="patch">
    <xs:complexType>
      <xs:attribute name="length" use="required" type="xs:integer"/>
      <xs:attribute name="offset" use="required" type="xs:integer"/>
    </xs:complexType>
  </xs:element>
  <xs:element name="full">
    <xs:complexType>
      <xs:attribute name="length" use="required" type="xs:integer"/>
      <xs:attribute name="offset" use="required" type="xs:integer"/>
    </xs:complexType>
  </xs:element>
  <xs:element name="overview">
    <xs:complexType>
      <xs:attribute name="length" use="required" type="xs:integer"/>
      <xs:attribute name="offset" use="required" type="xs:integer"/>
    </xs:complexType>
  </xs:element>
  <xs:element name="hazardPatch">
    <xs:complexType>
      <xs:attribute name="length" use="required" type="xs:integer"/>
      <xs:attribute name="offset" use="required" type="xs:integer"/>
    </xs:complexType>
  </xs:element>
  <xs:element name="hazardFull">
    <xs:complexType>
      <xs:attribute name="length" use="required" type="xs:integer"/>
      <xs:attribute name="offset" use="required" type="xs:integer"/>
    </xs:complexType>
  </xs:element>
  <xs:element name="hazardOverview">
    <xs:complexType>
      <xs:attribute name="length" use="required" type="xs:integer"/>
      <xs:attribute name="offset" use="required" type="xs:integer"/>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

ANPR Vehicle Analyser (anpr)

Available on platforms: All

This module processes images to read the number plates in them.

Platforms	Name	Command	Default Value	Description
All	Cardet Debugging	`anpr set debugging {value}`	false	Make the engine output debugging files to dlldeb
All	Prioritse Hazard	`anpr set hazard_priority {value}`	false	Only relevant if hazard plate reading engine is loaded. If set true, will try harder to read hazard plates and may therefore improve hazard reading performance. However setting true may cause overall performance to deteriorate slightly.
All	Maximum mean character height	`anpr set max_char {value}`	32	Maximum mean character height above which an exception will be generated
All	Maximum mean horizontal plate angle	`anpr set max_mhpa {value}`	5	Maximum mean horizontal plate angle above which an exception will be generated
All	Maximum mean vertical plate angle	`anpr set max_mvpa {value}`	10	Maximum mean vertical plate angle above which an exception will be generated
All	Maximum Syntax Error Ratio	`anpr set max_ser {value}`	40	The maximum syntax error ratio (as percentage) above which an exception will be generated
All	Minimum mean character height	`anpr set min_char {value}`	16	Minimum mean character height below which an exception will be generated
All	Minimum Mean Plate Quality	`anpr set min_mpq {value}`	2000	The minimum mean plate quality below which an exception will be generated
All	Minimum mean tag confidence	`anpr set min_mtc {value}`	90	Minimum mean tag confidence below which an exception will be generated.
All	Square Plates	`anpr set square {value}`	false	Tell the engine that you have a high number of square plates and to try harder to read these. If you have only a small number of these plates this may degrade overall performance. The system will still read long plates.
All	Threshold of Confidence	`anpr set threshold {value}`	60	The minimum read confidence that the system will pass on to further modules. Set this to zero to pass through images from triggers (in an externally triggered system) when the trigger fires even if we didn't manage to read any number plate.
All	Trigger Passthrough	`anpr set trigger_pass {value}`	true	If selected the system will always pass through an image during a trigger, guaranteeing that you see a picture of a vehicle from which we couldn't read anything when you trigger. This overrides the threshold for triggers only.

Platforms	Name	Command	Default Value	Description
All	White On Black	`anpr set whiteonblack {value}`	false	Tell the engine that you have a high number of white on black plates and to try harder to read these. If you have only a small number of these plates this may degrade overall performance. The system will still read black on white plates.

- `anpr clearstats`

  Clears Cumulative statistics. Platforms: All.

  Resets all statistics collection variables to initial values

- `anpr stats`

  Cumulative statistics. Platforms: All.

  Provides cumulative statistics of longterm vehicle processing

Lane Identification Control (anpr laneId)

Available on platforms: All

This control is for determining what lane a number plate is travelling in. There is a maximum of four lanes which is designated by the lanes property. There are a lines which is used to differentiate between different lanes. The user will need to ensure that the lines do not cross, if they do no lane information will be provided within the region, a programatic method to prevent crossing has not been provided to enhance the users ability to setup the lane id system.

Platforms	Name	Command	Default Value	Description
All	Lane 1 name	`anpr laneId set Lane1Name {value}`	1	This is the lane which is the left of line 1
All	Lane 2 name	`anpr laneId set Lane2Name {value}`	2	This is the lane which is the left of line 2 and right of line 1
All	Lane 3 name	`anpr laneId set Lane3Name {value}`	3	This is the lane which is the left of line 3 and right of line 2
All	Lane 4 name	`anpr laneId set Lane4Name {value}`	4	This is the lane which is the right of line 3
All	Bottom X position of line 1	`anpr laneId set Line1bottomX {value}`	2048	This is the position of line 1 at the bottom of the image.
All	Top X position of line 1	`anpr laneId set Line1topX {value}`	2048	This is the position of line 1 at the top of the image
All	Bottom X position of line 2	`anpr laneId set Line2bottomX {value}`	2048	This is the position of line 2 at the bottom of the image.
All	Top X position of line 2	`anpr laneId set Line2topX {value}`	2048	This is the position of line 2 at the top of the image
All	Bottom X position of line 3	`anpr laneId set Line3bottomX {value}`	2048	This is the position of line 3 at the bottom of the image.
All	Top X position of line 3	`anpr laneId set Line3topX {value}`	2048	This is the position of line 3 at the top of the image
All	Enables the lane identification system	`anpr laneId set enabled {value}`	false	Enables the lane identification system.

Platforms	Name	Command	Default Value	Description
All	Sets the number of lanes	`anpr laneId set lanes` {*value*}	1	Set the number of lanes the system will recognise

Library Manager (anpr library)

Available on platforms: All

Management of which library you are using for plate recognition. Different libraries are tuned for different regions of the world to enhance recognition of local plates correctly. Using the correct engine for the location and type of plates you are likely to see is important to ensure good read rates. The libraries live in /opt/pips/

Platforms	Name	Command	Default Value	Description
All	Colour Plate Reading Engine	`anpr library set colour` {*value*}	none	The filename of the libcardet colour plate reading engine in use
All	Plate Reading Engine	`anpr library set engine` {*value*}	none	The filename of the libcardet plate reading engine in use
All	Hazard Plate Reading Engine	`anpr library set hazard` {*value*}	none	The filename of the libcardet Hazard plate reading engine in use

- `anpr library list`

  List. Platforms: All.

  List all available engines on this camera

Overview Crop Control (anpr overviewCrop)

Available on platforms: All

Control the overview crop

Platforms	Name	Command	Default Value	Description
All	Overlay Overlay Crop	`anpr overviewCrop set enabled` {*value*}	false	Enables the overlay crop. This creates smaller, cropped, overview images. Ensure that the FocalLength values for cam1 and cam2 are correct if this feature is enabled.
All	Image Height	`anpr overviewCrop set height` {*value*}	480	The height in pixels of the area cropped from the overview image. A value of 0 will cause the images to be cropped to the height of the plate.
All	Horizontal Offset	`anpr overviewCrop set horizontalOffset` {*value*}	-240	The offset in pixels from left edge of the plate to the left edge of the cropped overview image. A negative value indicates that the left edge of the image is to the left of the plate. A positive value indicates that the left edge of the image is to the right of the plate.
All	Horizontal Scale	`anpr overviewCrop set horizontalScale` {*value*}	0	Reduces the width of the cropped image: 0, No scaling; 1, Half Scale; 2, Quarter Scale.
All	Vertical Offset	`anpr overviewCrop set verticalOffset` {*value*}	-400	The offset in pixels from top edge of the plate to the top edge of the cropped overview

Platforms	Name	Command	Default Value	Description
				image. A negative value indicates that the top edge of the image is above the plate. A positive value indicates that the top edge of the image is below the plate.
All	Vertical Scale	`anpr overviewCrop set verticalScale {value}`	0	Reduces the height of the cropped image: 0, No scaling; 1, Half Scale; 2, Quarter Scale.
All	Image Width	`anpr overviewCrop set width {value}`	752	The width in pixels of the area cropped from the overview image. A value of 0 will cause the images to be cropped to the width of the plate.

Asynchronous Payload Matching (asyncp)

Available on platforms: All

The payload matching system allows the system to match up Vehicle Events with asynchronously provided payloads (user supplied data).

This data may then be included with the final event sent to the user.

See also the %PA format specifier.

Platforms	Name	Command	Default Value	Description
All	Acknowledge	`asyncp set ack_enabled {value}`	false	To enable/disable the generation of acks. If enabled the whole message, exactly as sent, will be echoed back to you.
All	Serial Baud Rate	`asyncp set baud {value}`	115200	The serial port baud rate. For changes to take effect, disable then re-enable. Valid values 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400
All	Binary	`asyncp set binary {value}`	false	If set true, will allow binary data. Otherwise data must be XML legal ASCII
All	Drop unmatched	`asyncp set drop_unmatched {value}`	false	Allows the vehicle events to be surpressed if no matching payload is found.
All	Enabled	`asyncp set enabled {value}`	false	Allows the Filter system to be enabled and disabled. Disable it unless you are using it.
All	Event Match Regex	`asyncp set eventmatch_regex {value}`		A regular expression (matching the Perl Regular Expression Syntax). If set to anything other than an empty string, it will be used to select an appropriate matching payload for the read event. If set it will be used instead of time proximity. (Selecting by time proximity within the time window is the default behaviour). Unlike the above regex in that this one can use format specifiers to extract information from the vehicle read event - to match to the async payloads.

Platforms	Name	Command	Default Value	Description
All	Match Window in milliseconds	`asyncp set matchwindow {value}`	1000	The maximum period that the times of the async payload and vehicle event may differ and still be considered for matching
All	Maximum age	`asyncp set max_age {value}`	20000	The maximum time in milliseconds that payloads are kept in memory.
All	Payload Regular Expression	`asyncp set payload_regex {value}`	(.*)\n	A regular expression (matching the Perl Regular Expression Syntax) that the incoming string must match in order for a payload to be recognised and stored. The actual payload will be the concatination of those parts of the incoming string that match any subexpressions in the regex, as specified by ()'s. If no ()'s are present in the payload_regex, then the entire incoming string, that matches the regex, will be used as the actual stored payload. Note: If the binary flag is set to false then a payload may only contain XML legal ASCII. If it contains any illegal characters, the entire string will be discarded.
All	TCP Port	`asyncp set port {value}`	3821	The TCP port to be used to accept incoming connections.
All	Message Source	`asyncp set source {value}`	tcp	The source of the messages. Set to either tcp or serial

- `asyncp statistics`

  Cumulative statistics. Platforms: All.

  Provides cumulative statistics of longterm vehicle filter processing

BOF2 protocol (bof2)

Available on platforms: All

The module implements the BOF 2.2 Protocol

Platforms	Name	Command	Default Value	Description
All	Authenticate using username and password	`bof2 set authenticate {value}`	false	Authenticate using username and password
All	Camera Identifier	`bof2 set cameraId {value}`	1	Specified through the use of the a format string, if the value of the format string does not evaluate between -32768 and 32767 it will be 0.
All	Delivery Order	`bof2 set delivery_order {value}`	FIFO	The order in which events can be delivered, First in First Out (FIFO) or Last In First Out (LIFO). NB: Switching between modes deletes all data queued for delivery.

Platforms	Name	Command	Default Value	Description
All	Enabled	`bof2 set enabled {value}`	false	Allows the BOF2 system to be enabled and disabled. Disable it unless you are using it.
All	Feed Identifier	`bof2 set feedId {value}`	1	Also known as Force ID. Specified through the use of the a format string, if the value of the format string does not evaluate between -32768 and 32767 it will be 0.
All	Host	`bof2 set host {value}`	192.168.1.1:8080	IP address and port of the instation which will receive the BOF2.2 data.
All	Event Queue Size	`bof2 set nlog {value}`	100	The maximum number of events which will be enqueued for delivery. This delivery module uses the VFE Database, so events will get deleted based upon the rules set within the VFE database. If an event has been deleted we will continue on to the next in the queue
All	Camera Pan	`bof2 set pan {value}`	0	For CCTV cameras.
All	Password	`bof2 set password {value}`		Password for BOF transport user
All	Path	`bof2 set path {value}`	/bof2/services/InputCaptureWebService	The path on the http url.
All	Camera Preset Position	`bof2 set position {value}`	0	Used to indicate direction of travel on multi-use CCTV cameras
All	Send overview	`bof2 set send_overview {value}`	true	Allows sending of overview image to the BOF2 system to be enabled and disabled.
All	Send Patch	`bof2 set send_patch {value}`	true	Allows sending of patch image to the BOF2 system to be enabled and disabled.
All	Public Signature Of Sender	`bof2 set signature {value}`		Format not specified in BOF 2.2 spec, left as std::string for users
All	Source Identifier	`bof2 set sourceId {value}`	1	Specified through the use of the a format string, if the value of the format string does not evaluate between -32768 and 32767 it will be 0.
All	Camera Tilt	`bof2 set tilt {value}`	0	For CCTV cameras.
All	BOF2.2 transport	`bof2 set transport {value}`	HTTPS	HTTP or HTTPS
All	username	`bof2 set username {value}`	Unattended	Username for BOF user
All	Verify Peer	`bof2 set verifyPeer {value}`	true	Allows the verification of the BOF2 server certificate to be disabled when set to false.
All	Camera Zoom	`bof2 set zoom {value}`	0	For CCTV cameras.

- `bof2 clearStats`

  Resets all Statistics. Platforms: All.

  Resets all Statistics

- `bof2 diskq_flush`

  Empty the Disk Queue. Platforms: All.

All BOF events currently stored in the persistant Disk Queue will be deleted and will not be recoverable. Use this with care.

- `bof2 diskq_length`

  Length of Disk Queue. Platforms: All.

  The number of BOF events stored in the persistant Disk Queue will be reported.

- `bof2 stats`

  Statistics. Platforms: All.

  Statistics for debugging

IR Camera (cam1)

Available on platforms: All

Controls for managing the camera and images that it takes

Platforms	Name	Command	Default Value	Description
All	Sensor ADC gain	`cam1 set ADCgain {value}`	52	This sets the adc gain for the Overview sensor Warning don't alter this value. When finished commit will need to be run.
All	Lens Focal Length	`cam1 set FocalLength {value}`	35	The focal length of the lens in front of the IR sensor. This value must be set correctly if overview cropping is in use
All	Platefinder Regions of Interest Coordinates	`cam1 set ROICoordinates {value}`	(0,0),(2048,0),(2048,720),(0,720)	Region polygon(s) co-ordinates clockwise from Top Left. Region polygons are separated by a semi-colon.
All	Platefinder Regions of Interest	`cam1 set ROIEnabled {value}`	false	Sets whether Region of Interest polygon(s) is used or not.
All	Sensor Vramp	`cam1 set Vramp {value}`	109	This sets the Vramp value for the Overview sensor Warning don't alter this value. When finished commit will need to be run.
All	Points at front of vehicles	`cam1 set front_facing {value}`	true	Sets whether the camera is reading from the front of the vehicle. If you have bi-directional traffic set this false.
All	Horizontal Scale	`cam1 set horizontalScale {value}`	0	This will control the scale the channel (but not the plate patch), 0 = no scaling, 1 = half scaling, 2 = quarter scaling
All	Number of Exposure entries cycled in a sequence	`cam1 set numentries {value}`	0	Number of exposure entries cycled through. Set to 1 to disable exposure sequencing, just using the first entry. Otherwise each exposure will be taken with a different entry from the table.
All	Platefinder bottom plate width	`cam1 set platewidth_b {value}`	180	Sets the plate width for this channel in pixels at the bottom of the image. Try to get your plates to be between 180 and 220 pixels wide (for UK style plates), or 140-180 pixels (for US style plates). Getting this right will improve plate recognition.

Platforms	Name	Command	Default Value	Description
All	Platefinder top plate width	`cam1 set platewidth_t {value}`	180	Sets the plate width for this channel in pixels at the top of the image. Try to get your plates to be between 180 and 220 pixels wide (for UK style plates), or 140-180 pixels (for US style plates). Getting this right will improve plate recognition.
All	Fields of Retard	`cam1 set retard {value}`	0	Sets the number of fields of retard for this video channel. The video will be delayed by this number of fields .This feature is only useful in triggered systems. It adds flexibility by allowing compensation for a chronically late trigger. It is suggested that this feature only be used as a last resort.
All	Sharpening mode	`cam1 set sharpening {value}`	1	ENGINEERING USE ONLY:Then enables image sharpening - mode 0 off, mode 1 old sharpening mode, mode 2 a new sharpening mode
All	Vertical Scale	`cam1 set verticalScale {value}`	0	This will control the scale the channel (but not the plate patch), 0 = no scaling, 1 = half scaling, 2 = quarter scaling

- `cam1 commit`

  Commit the new ADC gain and V Ramp settings. Platforms: All.

  Commits the ADC gain and V Ramp to nand flash

Exposure Controller (cam1 exposure)

Available on platforms: All

An automated controller for the exposures on the camera. It will run with our triple flash system and adjust the sequence entries for shutter and gain appropriatly to optimise the image for plate reading.

Platforms	Name	Command	Default Value	Description
All	Brightness cutoff	`cam1 exposure set bright_cutoff {value}`	5	This value determines the percentage of pixels in the plate which differentiate between an underexposed and a correctly exposed plate .If brightness control is making your plates too bright lower this value or vice-versa. Also see the Brightness overexposure setting and set the two in parallel.
All	Exposure control enabled	`cam1 exposure set enabled {value}`	true	Allows you to switch the exposure controller on or off. It is recommended to use this system, if you disable it you should manually set up the exposure sequence.
All	Good DB Value	`cam1 exposure set good_db_value {value}`	2000	Not normally set by user except for testing purposes (it is automatically updated). This

Platforms	Name	Command	Default Value	Description
				determines at what brightness the system starts after a reboot. This value will be used to adjust the brightness when there is not enough traffic.
All	Maximum gain	`cam1 exposure set max_gain {value}`	11	Maximum gain value that is used by the exposure controller.
All	Maximum shutter length	`cam1 exposure set max_shutter {value}`	1000	Maximum shutter length in microseconds that the exposure controller will use. For most uses leave this at 1000, but if you are trying to read very high speed (>160kph) traffic all the time you can shorten this at the expense of all other traffic reads. This is not recommended.
All	Single Sequence Outside Trigger	`cam1 exposure set single_seq_outside_trig {value}`	false	

- `cam1 exposure info`

  Information. Platforms: All.

  Get detailed information of the status of the exposure controller. For debugging purposes.

- `cam1 exposure setBrightDBValue {dbValue}`

  Set absolute brightness DB value. Platforms: All.

  Instantly, manually set the brightness to a DB value. Mostly used for testing, if the exposure controller is on it will adapt the image again after you do this.

#	Name	Parameter	Description
1	Brightness to set to	dbValue	Brightness DB value.

- `cam1 exposure setbrightness {brightness}`

  Set Brightness. Platforms: All.

  Instantly, manually set the brightness to a value. Mostly used for testing, if the exposure controller is on it will adapt the image again after you do this.

#	Name	Parameter	Description
1	Brightness to set to	brightness	Brightness value.

Overlay Control (cam1 overlay)

Available on platforms: All

One overlay control per chanel

Platforms	Name	Command	Default Value	Description
All	Image Below	`cam1 overlay set below {value}`	false	Enables overlayed text on the Image. If not set the text will be above the image.

Platforms	Name	Command	Default Value	Description
All	Overlay Text Enable	`cam1 overlay set enabled {value}`	false	Enables additional text on the Image
All	Expand	`cam1 overlay set expand {value}`	true	Makes the image larger when the text is added. If not set the text will eat into the visible image area.
All	Text	`cam1 overlay set text {value}`	%Shs %Iy04u/ %Io02d/ %Id02u %Ih02u:%Im02u:%Is02u.%Ii03u	The format string for the overlayed text. This has limitations

Platewidth Control (cam1 platewidth)

Available on platforms: All

Automatically calculate and setup plate widths

Platforms	Name	Command	Default Value	Description
All	Plate width Control Enable	`cam1 platewidth set enabled {value}`	false	Enables Automatic Platewidth Control

- `cam1 platewidth info`

  Information. Platforms: All.

  Get detailed information of the status of the platewidth controller. For debugging purposes.

Sequence 1 (cam1 seq1)

Available on platforms: All

One exposure in the sequence for camera

Platforms	Name	Command	Default Value	Description
All	Gain	`cam1 seq1 set gain {value}`	48	Gain in the camera, which increases brightness (and noise) in the image. An aribrary but linear value.
All	Shutter length	`cam1 seq1 set shutter {value}`	16	Length of time that the shutter is open for, and the flash is fired for. This is 0 for 10 microseconds and 31 for 1 millisecond, linearly running between those values.

Sequence 2 (cam1 seq2)

Available on platforms: All

One exposure in the sequence for camera

Platforms	Name	Command	Default Value	Description
All	Gain	`cam1 seq2 set gain {value}`	48	Gain in the camera, which increases brightness (and noise) in the image. An aribrary but linear value.

Platforms	Name	Command	Default Value	Description
All	Shutter length	`cam1 seq2 set shutter {value}`	16	Length of time that the shutter is open for, and the flash is fired for. This is 0 for 10 microseconds and 31 for 1 millisecond, linearly running between those values.

Sequence 3 (cam1 seq3)

Available on platforms: All

One exposure in the sequence for camera

Platforms	Name	Command	Default Value	Description
All	Gain	`cam1 seq3 set gain {value}`	48	Gain in the camera, which increases brightness (and noise) in the image. An aribrary but linear value.
All	Shutter length	`cam1 seq3 set shutter {value}`	16	Length of time that the shutter is open for, and the flash is fired for. This is 0 for 10 microseconds and 31 for 1 millisecond, linearly running between those values.

Sequence 4 (cam1 seq4)

Available on platforms: All

One exposure in the sequence for camera

Platforms	Name	Command	Default Value	Description
All	Gain	`cam1 seq4 set gain {value}`	48	Gain in the camera, which increases brightness (and noise) in the image. An aribrary but linear value.
All	Shutter length	`cam1 seq4 set shutter {value}`	16	Length of time that the shutter is open for, and the flash is fired for. This is 0 for 10 microseconds and 31 for 1 millisecond, linearly running between those values.

Overview Camera (cam2)

Available on platforms: All

Controls for managing the camera and images that it takes

Platforms	Name	Command	Default Value	Description
All	Sensor ADC gain	`cam2 set ADCgain {value}`	52	This sets the adc gain for the Overview sensor Warning don't alter this value. When finished commit will need to be run.
All	Lens Focal Length	`cam2 set FocalLength {value}`	25	The focal length of the lens in front of the overview sensor. This value must be set correctly if overview cropping is in use
All	Sensor Vramp	`cam2 set Vramp {value}`	109	This sets the Vramp value for the Overview sensor Warning don't alter this value. When finished commit will need to be run.

Platforms	Name	Command	Default Value	Description
All	Automatic White Balance	`cam2 set autoWhiteBalance {value}`	true	Enables automatic white balance.
All	Exposure mode	`cam2 set auto_mode {value}`	true	The exposure mode settings, true - auto mode, false - manual mode.
All	Bayer Pattern	`cam2 set bayerOrder {value}`	1	0, 1, 2 or 3. For PIPS engineering use only.
All	Bypass the Bayer Filter	`cam2 set bypassBayer {value}`	false	For PIPS engineering use only.
All	Chroma Order	`cam2 set chromaOrder {value}`	1	0 = YCbCr, 1 = YCrCb, For PIPS engineering use only.
All	FPN removal enabled	`cam2 set fpnRemovalEnabled {value}`	false	Enables and disables FPN removal. Requires the camera to have had the removal image calibrated using calibrateFPN
All	Gain	`cam2 set gain {value}`	0	The gain value(0-15). This only can be set when in manual mode. Mainly for debug use.
All	Gamma Value	`cam2 set gammaCurve {value}`	2	Specifies the gamma correction value. 0 = 1.00, 1 = 0.45, 2 = 0.50 (recommended), 3 = 0.55.
All	Horizontal Scale	`cam2 set horizontalScale {value}`	0	This will control the scale of the whole channel (but not the overview crop), 0 = no scaling, 1 = half scaling, 2 = quarter scaling
All	Maximum Gain	`cam2 set max_gain {value}`	15	The maximum gain value. This camera will automatically set gain and shutter. Setting this higher will result in less blurring, but may cause more noise
All	Maximum shutter length	`cam2 set max_shutter {value}`	4	The maximum shutter length. This camera will automatically set gain and shutter. Setting this lower will give less blurring in the picture, but in low light you may not be able to see anything in the picture if you set it too low as it will not get enough light. Your hardware description must mention that you have a Overview Shutter Limiter for this to work. Values 1-8 are interpreted as milli-seconds. Other values are interpreted as micro-seconds
All	Colour Saturation	`cam2 set saturation {value}`	256	Sets the image saturation level. The recommended value is 256.
All	Sharpening Mode	`cam2 set sharpening {value}`	0	Selects the image sharpening algorithm. 0 = off (for PIPS engineering use only), 1 = the algorithm used in earlier releases, 2 = the improved algorithm (recommended).
All	Shutter length	`cam2 set shutter {value}`	5000	The shutter length in microseconds(16-7500). This only can be set when in manual mode. Mainly for debug use.
All	Target Brightness	`cam2 set target {value}`	110	The target brightness is value that the brightness controller will try and adjust the average pixel value to reach

Platforms	Name	Command	Default Value	Description
All	Vertical Scale	`cam2 set verticalScale {value}`	0	This will control the scale of the whole channel (but not the overview crop), 0 = no scaling, 1 = half scaling, 2 = quarter scaling
All	White Balance Blue Coefficient	`cam2 set whiteBalanceCoeffBlue {value}`	0	The blue coefficient for the white balance operation. This is a read-only value showing the output of auto white balance.
All	White Balance Red Coefficient	`cam2 set whiteBalanceCoeffRed {value}`	0	The red coefficient for the white balance operation. This is a read-only value showing the output of auto white balance.

- `cam2 calibrateFPN`

  Calibrate the Fixed Pattern Noise reference image. Platforms: All.

  Automatically builds a reference image of the Fixed Pattern Noise on the sensor, to allow this to be removed from the images.

- `cam2 ccm`

  Dump Colour Correction Matrix. Platforms: All.

  Dump Colour Correction Matrix

- `cam2 commit`

  Commit the new ADC gain and V Ramp settings. Platforms: All.

  Commits the ADC gain and V Ramp to nand flash

Overlay Control (cam2 overlay)

Available on platforms: All

One overlay control per chanel

Platforms	Name	Command	Default Value	Description
All	Image Below	`cam2 overlay set below {value}`	false	Enables overlayed text on the Image. If not set the text will be above the image.
All	Overlay Text Enable	`cam2 overlay set enabled {value}`	false	Enables additional text on the Image
All	Expand	`cam2 overlay set expand {value}`	true	Makes the image larger when the text is added. If not set the text will eat into the visible image area.
All	Text	`cam2 overlay set text {value}`	%Shs %Iy04u/ %Io02d/ %Id02u %Ih02u:%Im02u:%Is02u.%Ii03u	The format string for the overlayed text. This has limitations

Client vehicle event reporter (client)

Available on platforms: All

Reports individual vehicle events over the network to a client for live monitoring and diagnostics. Using the ClientView application you can see these images.

Platforms	Name	Command	Default Value	Description
All	Platefinder position instead	`client set platefinder {value}`	false	Show the plate patches from the hardware platefinder rather than the ANPR engine. This is for debugging purposes.

Contexts (contexts)

Available on platforms: All

Control for managing context images associated with an event

Platforms	Name	Command	Default Value	Description
All	Number of Context Images	`contexts set number {value}`	0	Number of context images associated with a vehicle event

Context 1 (contexts ctx1)

Available on platforms: All

An entry defining the offset of a single context image.

Platforms	Name	Command	Default Value	Description
All	Offset	`contexts ctx1 set offset {value}`	250	The offset in milliseconds from the actual read event time. Negative offset will give images prior to the read. Positive offset will give images after the read. Note, the images returned may not have the exact timestamps as specified by the offsets. They will however be the nearest time matching images available. Image timestamp best resolution is affected by the frame rate (for example 50fps implies images are 20ms apart). Images older than a certain period may also be subject to decimation due to limited RAM storage.

Context 2 (contexts ctx2)

Available on platforms: All

An entry defining the offset of a single context image.

Platforms	Name	Command	Default Value	Description
All	Offset	`contexts ctx2 set offset {value}`	250	The offset in milliseconds from the actual read event time. Negative offset will give

Platforms	Name	Command	Default Value	Description
				images prior to the read. Positive offset will give images after the read. Note, the images returned may not have the exact timestamps as specified by the offsets. They will however be the nearest time matching images available. Image timestamp best resolution is affected by the frame rate (for example 50fps implies images are 20ms apart). Images older than a certain period may also be subject to decimation due to limited RAM storage.

Context 3 (contexts ctx3)

Available on platforms: All

An entry defining the offset of a single context image.

Platforms	Name	Command	Default Value	Description
All	Offset	`contexts ctx3 set offset {`*`value`*`}`	250	The offset in milliseconds from the actual read event time. Negative offset will give images prior to the read. Positive offset will give images after the read. Note, the images returned may not have the exact timestamps as specified by the offsets. They will however be the nearest time matching images available. Image timestamp best resolution is affected by the frame rate (for example 50fps implies images are 20ms apart). Images older than a certain period may also be subject to decimation due to limited RAM storage.

Context 4 (contexts ctx4)

Available on platforms: All

An entry defining the offset of a single context image.

Platforms	Name	Command	Default Value	Description
All	Offset	`contexts ctx4 set offset {`*`value`*`}`	250	The offset in milliseconds from the actual read event time. Negative offset will give images prior to the read. Positive offset will give images after the read. Note, the images returned may not have the exact timestamps as specified by the offsets. They will however be the nearest time matching images available. Image timestamp best resolution is affected by the frame rate

Platforms	Name	Command	Default Value	Description
				(for example 50fps implies images are 20ms apart). Images older than a certain period may also be subject to decimation due to limited RAM storage.

Context 5 (contexts ctx5)

Available on platforms: All

An entry defining the offset of a single context image.

Platforms	Name	Command	Default Value	Description
All	Offset	`contexts ctx5 set offset {value}`	250	The offset in milliseconds from the actual read event time. Negative offset will give images prior to the read. Positive offset will give images after the read. Note, the images returned may not have the exact timestamps as specified by the offsets. They will however be the nearest time matching images available. Image timestamp best resolution is affected by the frame rate (for example 50fps implies images are 20ms apart). Images older than a certain period may also be subject to decimation due to limited RAM storage.

Context 6 (contexts ctx6)

Available on platforms: All

An entry defining the offset of a single context image.

Platforms	Name	Command	Default Value	Description
All	Offset	`contexts ctx6 set offset {value}`	250	The offset in milliseconds from the actual read event time. Negative offset will give images prior to the read. Positive offset will give images after the read. Note, the images returned may not have the exact timestamps as specified by the offsets. They will however be the nearest time matching images available. Image timestamp best resolution is affected by the frame rate (for example 50fps implies images are 20ms apart). Images older than a certain period may also be subject to decimation due to limited RAM storage.

Context 7 (contexts ctx7)

Available on platforms: All

An entry defining the offset of a single context image.

Platforms	Name	Command	Default Value	Description
All	Offset	`contexts ctx7 set offset {value}`	250	The offset in milliseconds from the actual read event time. Negative offset will give images prior to the read. Positive offset will give images after the read. Note, the images returned may not have the exact timestamps as specified by the offsets. They will however be the nearest time matching images available. Image timestamp best resolution is affected by the frame rate (for example 50fps implies images are 20ms apart). Images older than a certain period may also be subject to decimation due to limited RAM storage.

Context 8 (contexts ctx8)

Available on platforms: All

An entry defining the offset of a single context image.

Platforms	Name	Command	Default Value	Description
All	Offset	`contexts ctx8 set offset {value}`	250	The offset in milliseconds from the actual read event time. Negative offset will give images prior to the read. Positive offset will give images after the read. Note, the images returned may not have the exact timestamps as specified by the offsets. They will however be the nearest time matching images available. Image timestamp best resolution is affected by the frame rate (for example 50fps implies images are 20ms apart). Images older than a certain period may also be subject to decimation due to limited RAM storage.

Plate Database Matcher (dbmatcher)

Available on platforms: All

The database matching system allows the system to look up number plates in a database.

It is possible to filter out plates based on whether they are found or not.

It is also possible to collect a tag string for plates which are found which can be output by the delivery system.

No spaces or commas are allowed in the plate or tag string.

INSTALLING NEW DATABASE FILES:

Copy a file named [YourPlatesDatabaseName].install into the camera /storage/db/ directory.

For example, for the default plates.db name, you would copy a file named plates.db.install into the /storage/db/ directory.

The system should automatically detect this and install the new file. To confirm this, do a directory listing of the /storage/db/ directory and confirm:

1)That the plates.db.install you just copied in has disappeared (GUI Tool may need refreshing)

2)That the plates.db file md5sum matches the file you installed.

If for some reason this does not work, then copy your plates.db.install into /storage/

and then, using the linux command prompt, move this file into /storage/db/

mv /storage/plates.db.install /storage/db/.

and then verify as above.

Platforms	Name	Command	Default Value	Description
All	Enabled	`dbmatcher set enabled {value}`	false	Allows the Filter system to be enabled and disabled. Disable it unless you are using it.
All	Forward Event on match	`dbmatcher set forward_on_match {value}`	false	Will forward the plate read event only if a match is found in the database. May be enabled simultaneously with forward_on_nomatch. This will have the effect of all plates being forwarded but matching plates will carry their corresponding tags.
All	Forward Event on no match	`dbmatcher set forward_on_nomatch {value}`	false	Will forward the plate read event if no match is found in the database. May be enabled simultaneously with forward_on_match. This will have the effect of all plates being forwarded but matching plates will carry their corresponding tags.
All	Plate Database File Name	`dbmatcher set plates_filename {value}`	plates.db	Specify the filename of the plates SQLite database. This file may be pre-created and placed in the /storage/db/ directory. The SQL to create a compatible database is: CREATE TABLE plateDB(plate TEXT PRIMARY KEY ASC, tag TEXT);

- `dbmatcher insert {plate} {tag}`

  Insert a plate+tag. Platforms: All.

  Adds a plate+tag combination to the plates database.

#	Name	Parameter	Description
1		plate	The plate you wish to insert

#	Name	Parameter	Description
	Plate Entry to insert		
2	Plate Tag	tag	The tag associated with the plate you wish to insert

- `dbmatcher lookup` {*`plate`*}

  Lookup a plate. Platforms: All.

  Determines if a plate exists in the current database. Will confirm if the plate is found and print its tag value

#	Name	Parameter	Description
1	Plate Entry to lookup	plate	The plate you wish to find in the database

- `dbmatcher reload`

  Load the database file. Platforms: All.

  Load the file named by plates_filename. Use this command to reload the plates database file if it has been changed or replaced, or if you have changed the name.

- `dbmatcher remove` {*`plate`*}

  Remove a plate. Platforms: All.

  If the plate exists in the current database it (and its associated tag) will be removed.

#	Name	Parameter	Description
1	Plate Entry to remove	plate	The plate you wish to remove from the database

- `dbmatcher statistics`

  Cumulative statistics. Platforms: All.

  Provides cumulative statistics of longterm vehicle filter processing

Diagnostics and Exceptions Manager (diagnostics)

Available on platforms: All

Diagnostics and Exceptions

Platforms	Name	Command	Default Value	Description
All	Acknowledgents Enabled	`diagnostics set ack_enabled` {*`value`*}	true	If true, the delivery system will await acknowledgement
All	Diagnostic/ Exception ack wait timeout	`diagnostics set ack_timeout` {*`value`*}	30	Period in seconds to wait for an acknowledgement of a diagnostic or exception message
All	Minimum Samples for Diagnostics	`diagnostics set min_samples` {*`value`*}	10	Certain types of diagnostics (e.g. mean values or ratios) are only considered valid after a certain number of samples.

Platforms	Name	Command	Default Value	Description
All	Diagnostic period	`diagnostics set diagnostic_period {value}`	20	Period in minutes between diagnostic updates
All	Diagnostic Delivery Port	`diagnostics set diagnostic_port {value}`	5001	The TCP port that diagnostic messages will be delivered on. Set to
All	Disk Queue Length	`diagnostics set disk_queue_length {value}`	5	The number of diagnostic and exception events that are maintained in a persistent disk queue while the in station receiver is offline. Diagnostics are kept in a seperate queue to exceptions. This value applies to all queues
All	Diagnostics enabled	`diagnostics set enabled {value}`	false	Allows diagnostic and exception reporting to be enabled/disabled
All	Minimum Samples for Exceptions	`diagnostics set exception_min_samples {value}`	20	Certain types of exceptions (e.g. mean values or ratios) are only considered valid after a certain number of samples.
All	Exception Period	`diagnostics set exception_period {value}`	5	Period in minutes between (non-realtime) exception updates
All	Exception Delivery Port	`diagnostics set exception_port {value}`	5002	The TCP port that exception messages will be delivered on
All	Delivery Host	`diagnostics set host {value}`	10.1.1.1	The IP address to which the diagnsotic and exception messages will be transferred.
All	JTMS Compatible	`diagnostics set jtms {value}`	false	Generate JTMS compatible diagnostics instead of VES compatible diagnostics. The differences are small but significant.

File Logger (filelog)

Available on platforms: All

The logger which reports information to specified file. NB: A log file can grow to fill the disk. Use logrotate to manage log files.

Platforms	Name	Command	Default Value	Description
All	Enable file logging	`filelog set enabled {value}`	false	Enable logging to a file. NB, the camera does not manage the file size or archiving. Please use logrotate
All	Log File Name	`filelog set filename {value}`	/var/log/start382.log	Specify the filename to receive log output. NB: To avoid this file growing too large, please use logrotate
All	Print line/file	`filelog set lineFilePrint {value}`	true	Print Linenumber and Filename for logging messages
All	Print time	`filelog set timePrint {value}`	true	Print time for logging messages

Vehicle Fusion (fusion)

Available on platforms: All

The system may read multiple images of any given vehicle, and this subsystem merges those multiple vehicle reads into a single coherant result for output.

Platforms	Name	Command	Default Value	Description
All	Combine hazard and normal plates	`fusion set combine_hazard {value}`	false	If this is set true, an attempt will be made to match the hazard plate with the normal plate of the same vehicle. If successful, a combined event will be forwarded. If a hazard plate is read, it will normally be forwarded as an independant plate read.
All	Distance from edge	`fusion set distance {value}`	256	Distance from the edge specified in the selector parameter to the centre of the plate which will be used to try to select an appropriate plate for you (measured in pixels). May not be used if no distance selector in use.
All	Duplicate Level	`fusion set duplicate_level {value}`	60	Percentage match level at which the numberplates will be considered as duplicates for matching multiple reads of a vehicle together. 100 means they must be identical, and 0 means anything will match anything else (which makes the camera pretty useless).
All	Early result	`fusion set early {value}`	false	Output the first event from a vehicle even if it may well be wrong. Useful if the time between a vehicle being seen and the camera reporting it is critical, otherwise don't choose this
All	Maximum gap	`fusion set gap {value}`	700	Length of time after seeing a vehicle when we pass on the vehicle when we haven't seen it again for this long. Given in milliseconds.
All	Maximum age of vehicle	`fusion set max_age {value}`	2000	Maximum time the vehicle can be in the field of view before we pass it on anyway. Given in milliseconds.
All	No Event Timeout	`fusion set noevent_timeout {value}`	4294967295	If no vehicle event has been delivered within this timeout period (in seconds) a Vehicle Detect Timeout exception will be generated. This is a boolean exception and will be cleared as soon as a vehicle event is forwarded. This cannot be set below 10 seconds
All	Allow out of trigger images	`fusion set outoftrigger {value}`	false	If a vehicle arrives during a trigger we will only deliver images from within the trigger period unless you tick this box. This allows us to deliver better images from earlier.
All	Persistant event id	`fusion set persistantEventId {value}`	true	Set this value to true to keep the next event id in a separate file. Setting this value to false causes the camera to calculate the next event id using the data stored on the VFE database. It takes some time to update the VFE database and

Platforms	Name	Command	Default Value	Description
				the event id sequence may not be updated correctly if the camera app is restarted. If the VFE database is disabled then the event id sequence is reset to 0 when the camera app is restarted. Set this value to true if the uniqueness of event ids is important. Set the value to false if performance is important.
All	Repeating vehicles	`fusion set repeat {value}`	true	If a vehicle stays in the field of view we will pass it on every max_age milliseconds if this is set true, otherwise just once. In the presence of triggers, all vehicles are flushed when the trigger gate closes. Repeats may then still be experienced. In order to prevent repeats in the presence of triggers, set the repeat_on_trigger to false.
All	Repeating vehicles per trigger	`fusion set repeat_on_trigger {value}`	true	If true, a vehicle staying in the field of view we will be forwarded on every trigger (default). Otherwise the vehicle will only be forwarded the first time it is detected within a trigger period.
All	Plate Selector	`fusion set selector {value}`	0	This parameter will allow the system to select an appropriate plate for you. Sometimes we may not be able to select a plate which matches your criteria very well, but we will do what we can. 0=Best plate read. 1=Distance from top edge. 2=Distance from left edge. 3=Plate exposure quality, for better visibility of the non plate text details
All	Set reads forwarded from a trigger to 1	`fusion set single_read_on_trigger {value}`	false	Only applies to triggered systems. Will limit the maximum number of read events delivered per trigger to 1. The vehicle chosen for delivery will be decided according to read confidence. Beware of setting this as vehicles (such as adjacent vehicles) may be missed. Also, if set, a parked vehicle may prevent any other vehicles being read.
All	Supplementary IR Images	`fusion set supplementary_images {value}`	false	Only works for images within a trigger gate open period.

Platforms	Name	Command	Default Value	Description
				If true, up to two additional full IR image will be available for delivery. These will be alternatively exposed IR images (if alternative exposure sequence images are available). If no other sequence images are available the best exposed of the remaining IR images (if any) will be available. In the case where only one image was analysed for the vehicle, no additional image will be available.

- `fusion clearstats`

  Clears Cumulative statistics. Platforms: All.

  Resets all statistics collection variables to initial values

- `fusion stats`

  Cumulative statistics. Platforms: All.

  Provides cumulative statistics of longterm vehicle processing

- `fusion status`

  Current status. Platforms: All.

  Gets the current status of the vehicles being processed by the module

GPS Time Manager (gps)

Available on platforms: All

Manages GPS Time Sync

Platforms	Name	Command	Default Value	Description
All	Enabled	`gps set enabled` {*value*}	false	Enables gps time manager

- `gps status`

  Current status of GPS/PPS. Platforms: All.

  Gets the current status of the GPS and PPS time management

Heartbeat (heartbeat)

Available on platforms: All

Platforms	Name	Command	Default Value	Description
All	Heartbeat Content	`heartbeat set content` {*value*}	%Shs,%hsx,%lcm,%hfm	A format string specifying the content of the heartbeat message.

Platforms	Name	Command	Default Value	Description
All	Enabled	`heartbeat set enabled {value}`	false	Allows the Heartbeat system to be enabled and disabled. Disable it unless you are using it.
All	Delivery Host	`heartbeat set host {value}`	10.1.1.1	The IP address to which the heartbeat messages will be transferred.
All	Heartbeat period	`heartbeat set period {value}`	60	Period in seconds between heartbeats
All	Heartbeat Delivery Port	`heartbeat set port {value}`	10005	The TCP port that heartbeat messages will be delivered on.

Image File Outputter (ifo)

Available on platforms: All

Stores the images from the camera onto disk. These are just periodic images from the selected camera, like a video stream, not ones of particular interest, and they may or may not contain plates. If you have network mounted a disk this would be most useful, as otherwise you'll quickly fill up the internal storage of the camera. Look at mounting a disk in /storage to use this. This module is designed purely for testing and debugging, not for production systems. There is no guarantee that images will come out at all if the rest of the system is too busy. Image metadata is stored in the filename. The filename format may change without notice.

Platforms	Name	Command	Default Value	Description
All	Anpr Patches	`ifo set anprpatch {value}`	true	When looking at plates, output an extra file for the anpr patch. This file will have the prefix A
All	Bitmap	`ifo set bitmap {value}`	false	Enable this to output bitmap files, otherwise the output is jpeg format. Only works for monochrome images, colour ones are always jpeg format.
All	Colour	`ifo set colour {value}`	false	Enable this to store video images from the colour camera, otherwise look at the monochrome camera. Has no effect on plate images which are always monochrome.
All	Output Directory	`ifo set directory {value}`	/tmp	Directory to receive the files relative to the /storage directory. It is recommended you mount an external network disk here to collect the images.
All	Enabled	`ifo set enabled {value}`	false	Enable or disable the output of raw image files (e.g. this whole module). Should be turned off on production systems.
All	Minimum interval	`ifo set interval {value}`	1000	Minimum number of milliseconds between files, with a busy camera, filesystem or network this may not be adhered to.
All	Hardware Platefinder Patches	`ifo set pfpatch {value}`	false	When looking at plates, output an extra file for the platefinder patch. This file will have the prefix H
All	Plates	`ifo set plates {value}`	true	Enable or disable the output of plate images. These are images where we have read a plate. May be used simultaneously with video if you want. These files will have the prefix P

Platforms	Name	Command	Default Value	Description
All	PreFusion	`ifo set prefusion {value}`	false	When looking at plates, enable or disable looking at the plates prior to processing by the vehicle fusion, instead of after. These plates may be rubbish. If you have no idea what this means you will want it off, it is mainly for debugging.
All	Video	`ifo set video {value}`	false	Enable or disable the output of the video stream. This does not contain every field, just a periodic selection. Enabling this produces a LOT of data. These files will have the prefix V.

- `ifo burst`

  Burst Video. Platforms: All.

  Output a burst of consecutive video fields from the selected camera in the selected format. Will burst for a short while based upon the data rate we can write at. May upset the rest of the camera during the burst, so never do this on a production system. This will work even if the rest of this subsystem is disabled.

JPEG Service (jpegService)

Available on platforms: All

Controls the generation of JPEG images

Platforms	Name	Command	Default Value	Description
All	NASP compliant jpeg patch of 120x60	`jpegService set fixedPatch {value}`	false	Forces the size of the patch to match the requirement in the UK Govenments NASP specification of 120x60 pixels
All	Enable Histogram Stretching	`jpegService set histogramEnable {value}`	true	Set true to enable histogram stretching to improve contrast (recommended).
All	Lower Ignore	`jpegService set lowIgnoreAmount {value}`	300	100 times the percentage of dark pixels excluded from histogram stretching (e.g. 300 = 3%). Only change this value if you are familiar with image processing algorithms or under instruction from PIPS engineers.
All	Maximum Stretch Percentage	`jpegService set maxStretchPercent {value}`	80	Maximum amount to stretch the histogram (1-100%). Only change this value if you are familiar with image processing algorithms or under instruction from PIPS engineers.
All	Minimum Stretch Percentage	`jpegService set minStretchPercent {value}`	40	Minimum amount to stretch the histogram (1-100%). Only change this value if you are familiar with image processing algorithms or under instruction from PIPS engineers.
All	JPEG Target Size	`jpegService set size {value}`	192	Varies the target size of the jpegs, in KB, Patches will be 1/4 of the size
All		`jpegService set targetQuality {value}`	0	
All	Upper Ignore	`jpegService set upIgnoreAmount {value}`	200	100 times the percentage of bright pixels excluded from histogram stretching (e.g. 200 = 2%). Only change this value if you are

Platforms	Name	Command	Default Value	Description
				familiar with image processing algorithms or under instruction from PIPS engineers.

- `jpegService qualities`

  Display qualities. Platforms: All.

  Display the controller selected quality for each channel (or each exposure sequence of each channel) and for patches.

JTMS - Journey Time Measurement System (jtms)

Available on platforms: All

A system for delivering numberplates using very low bandwidth specifically for journey time measurement. Only minimal information is transmitted by the system. To use JTMS you must give your camera a 4 digit numerical hostname, which will be its site ID. This module only supplies tags, you should look at the diagnostics module to enable diagnostics and exceptions in jtms compatible format.

Platforms	Name	Command	Default Value	Description
All	Tag format	`jtms set binary` {*value*}	1	The format of the tag messages. 0 - human readable text messages. 1 - binary messages (more compact). 2 - Extended binary format with state/country, classification, confidence and 24 bit hashed tags.
All	Enabled	`jtms set enabled` {*value*}	false	Allows the JTMS system to be enabled and disabled. Disable it unless you are using it.
All	Host	`jtms set host` {*value*}	192.168.1.1	The IP address of the instation which will receive the JTMS data.
All	Merge Characters	`jtms set mergechars` {*value*}	true	Enable merging of possible ambiguous characters such as 8 and B prior to transmission
All	Maximum Files	`jtms set nlog` {*value*}	6	The maximum number of files which will be stored on the local filesystem before they are overwritten if it is not possible to contact the instation. Warning, arbitrarily setting this to a high value may fill up the device on which you are storing the files and then the system will lose the wrong data or may perform badly.
All	Tag Period	`jtms set period` {*value*}	5	The number of minutes between sending tag messages
All	Time Slot	`jtms set time_slot` {*value*}	0	Time slot which is used by this system for transmission. Use this to spread the network load of your outstations. This is a percentage value and is used as an offset from the beginning of the time which could be used for transmission verses the end of that transmission slot - e.g. 0 it will transmit at the very beginning of the slot, at 100 at the very end.
All	ACK Timeout	`jtms set timeout` {*value*}	60	Number of seconds to wait for an ACK (if ACKs are enabled). Set to zero to disable

- `jtms reset`

Reset statistics. Platforms: All.

Reset the statistics for this module

- `jtms statistics`

  Statistics. Platforms: All.

  Display statistics from this module

External Led Control (ledControl)

Available on platforms: All

Setting to Control the pips illuminator

Platforms	Name	Command	Default Value	Description
All	Length of flash in microseconds	`ledControl set flashTime` {*value*}	1000	Sets the length of the flash in microseconds
All	Enable internal Led's	`ledControl set internalEnable` {*value*}	true	Set this to false to disable the internal LED's
All	Set mode of external Led's	`ledControl set mode` {*value*}	0	Mode 0 = Off, Mode 1 = Synced to Cam1(triple sequence), Mode 2 = Synced to Cam2, Mode 3 = Fixed Length

Metadata store (metadata)

Available on platforms: All

This is an object for storing site metadata as string values. The information stored in here is NOT used by the system, and is just for you to use when creating format strings. The data will be output in the format strings unchanged, and allows you to put per-site data in here, keeping the format strings the same on all sites. You might wish to store lane IDs, zones, site direction or anything else similar in here. We would recommend setting the hostname as the unique site identifer which may be accessed though %Sh. It also provides a way of mapping from long event metadata into short codes for output with the %E* variables. You enter into map_a the long name of the variable you'd like available as %Ea. This part is probably not useful to you at the moment unless you understand this without further explanation.

Platforms	Name	Command	Default Value	Description
All	Mapping a	`metadata set map_a` {*value*}		Name of an event metadata string you'd like visible in %Ea.
All	Mapping b	`metadata set map_b` {*value*}		Name of an event metadata string you'd like visible in %Eb.
All	Mapping c	`metadata set map_c` {*value*}		Name of an event metadata string you'd like visible in %Ec.
All	Mapping d	`metadata set map_d` {*value*}		Name of an event metadata string you'd like visible in %Ed.
All	Mapping e	`metadata set map_e` {*value*}		Name of an event metadata string you'd like visible in %Ee.
All	Mapping f	`metadata set map_f` {*value*}		Name of an event metadata string you'd like visible in %Ef.
All	Mapping g	`metadata set map_g` {*value*}		Name of an event metadata string you'd like visible in %Eg.

Platforms	Name	Command	Default Value	Description
All	Mapping h	`metadata set map_h {value}`		Name of an event metadata string you'd like visible in %Eh.
All	Mapping i	`metadata set map_i {value}`		Name of an event metadata string you'd like visible in %Ei.
All	Mapping j	`metadata set map_j {value}`		Name of an event metadata string you'd like visible in %Ej.
All	Mapping k	`metadata set map_k {value}`		Name of an event metadata string you'd like visible in %Ek.
All	Mapping l	`metadata set map_l {value}`		Name of an event metadata string you'd like visible in %El.
All	Mapping m	`metadata set map_m {value}`		Name of an event metadata string you'd like visible in %Em.
All	Mapping n	`metadata set map_n {value}`		Name of an event metadata string you'd like visible in %En.
All	Mapping o	`metadata set map_o {value}`		Name of an event metadata string you'd like visible in %Eo.
All	Mapping p	`metadata set map_p {value}`		Name of an event metadata string you'd like visible in %Ep.
All	Mapping q	`metadata set map_q {value}`		Name of an event metadata string you'd like visible in %Eq.
All	Mapping r	`metadata set map_r {value}`		Name of an event metadata string you'd like visible in %Er.
All	Mapping s	`metadata set map_s {value}`		Name of an event metadata string you'd like visible in %Es.
All	Mapping t	`metadata set map_t {value}`		Name of an event metadata string you'd like visible in %Et.
All	Mapping u	`metadata set map_u {value}`		Name of an event metadata string you'd like visible in %Eu.
All	Mapping v	`metadata set map_v {value}`		Name of an event metadata string you'd like visible in %Ev.
All	Mapping w	`metadata set map_w {value}`		Name of an event metadata string you'd like visible in %Ew.
All	Mapping x	`metadata set map_x {value}`		Name of an event metadata string you'd like visible in %Ex.
All	Mapping y	`metadata set map_y {value}`		Name of an event metadata string you'd like visible in %Ey.
All	Mapping z	`metadata set map_z {value}`		Name of an event metadata string you'd like visible in %Ez.
All	String a	`metadata set string_a {value}`		A string, access in format strings as %Ma.
All	String b	`metadata set string_b {value}`		A string, access in format strings as %Mb.
All	String c	`metadata set string_c {value}`		A string, access in format strings as %Mc.
All	String d	`metadata set string_d {value}`		A string, access in format strings as %Md.

Platforms	Name	Command	Default Value	Description
All	String e	`metadata set string_e {value}`		A string, access in format strings as %Me.
All	String f	`metadata set string_f {value}`		A string, access in format strings as %Mf.
All	String g	`metadata set string_g {value}`		A string, access in format strings as %Mg.
All	String h	`metadata set string_h {value}`		A string, access in format strings as %Mh.
All	String i	`metadata set string_i {value}`		A string, access in format strings as %Mi.
All	String j	`metadata set string_j {value}`		A string, access in format strings as %Mj.
All	String k	`metadata set string_k {value}`		A string, access in format strings as %Mk.
All	String l	`metadata set string_l {value}`		A string, access in format strings as %Ml.
All	String m	`metadata set string_m {value}`		A string, access in format strings as %Mm.
All	String n	`metadata set string_n {value}`		A string, access in format strings as %Mn.
All	String o	`metadata set string_o {value}`		A string, access in format strings as %Mo.
All	String p	`metadata set string_p {value}`		A string, access in format strings as %Mp.
All	String q	`metadata set string_q {value}`		A string, access in format strings as %Mq.
All	String r	`metadata set string_r {value}`		A string, access in format strings as %Mr.
All	String s	`metadata set string_s {value}`		A string, access in format strings as %Ms.
All	String t	`metadata set string_t {value}`		A string, access in format strings as %Mt.
All	String u	`metadata set string_u {value}`		A string, access in format strings as %Mu.
All	String v	`metadata set string_v {value}`		A string, access in format strings as %Mv.
All	String w	`metadata set string_w {value}`		A string, access in format strings as %Mw.
All	String x	`metadata set string_x {value}`		A string, access in format strings as %Mx.
All	String y	`metadata set string_y {value}`		A string, access in format strings as %My.

Platforms	Name	Command	Default Value	Description
All	String z	`metadata set string_z {value}`		A string, access in format strings as %Mz.

OEM Modules (modules)

Available on platforms: All

Allows the specification of the supported OEM module types

Platforms	Name	Command	Default Value	Description
All	Number of ACS	`modules set num_acs {value}`	1	Number of ACS modules. Any change will require a restart to take effect. Set to 0 if you dont need ACS. If set to 1, will be called simply acs. If>1 will be called acs1, acs2 etc.
All	Number of BOF 2	`modules set num_bof2 {value}`	0	Number of BOF 2.2 Delivery modules. Any change will require a restart to take effect. Set to 0 if you dont need the Relay Output. Otherwise set to 1. Only a single Relay Output module is allowed.
All	Number of JTMS	`modules set num_jtms {value}`	1	Number of JTMS modules. Any change will require a restart to take effect. Set to 0 if you dont need JTMS. Otherwise set to 1. Only a single JTMS module allowed. .
All	Number of Relay Output	`modules set num_relayOut {value}`	0	Number of Relay Output modules. Any change will require a restart to take effect. Set to 0 if you dont need the Relay Output. Otherwise set to 1. Only a single Relay Output module is allowed.
All	Number of SAP	`modules set num_sap {value}`	0	Number of SAP modules. Any change will require a restart to take effect. Set to 0 if you dont need SAP. Otherwise set to 1. Only a single sap module allowed.
All	Number of UTMC	`modules set num_utmc {value}`	0	Number of UTMC modules. Any change will require a restart to take effect. Set to 0 if you dont need UTMC.

Platforms	Name	Command	Default Value	Description
				Otherwise set to 1. Only a single UTMC module allowed.
All	Number of UTMCV12	`modules set num_utmcv12 {value}`	0	Number of UTMC Version 1.2 modules. Any change will require a restart to take effect. Set to 0 if you dont need UTMC Version 1.2. Otherwise set to 1. Only a single UTMC Version 1.2 module allowed.
All	Number of VES	`modules set num_ves {value}`	1	Number of VES modules. Any change will require a restart to take effect. Set to 0 if you dont need VES. Otherwise set to 1. Only a single ves module allowed.

Network user interface manager (netuis)

Available on platforms: All

The manager for the network user interfaces. These are the interfaces which the web and shell connect to.

Platforms	Name	Command	Default Value	Description
All	To enable/disable the generation of exceptions	`netuis set exceptions {value}`	false	If true, will transmit an exception when a control connection is made. Will only count the first control connection and will only clear the condition when there have been no connections for 5 minutes

- `netuis status`

  Current status. Platforms: All.

  Display the status of the NetUI servers, how many are in use.

Network user interface (netuis netui1)

Available on platforms: All

Network user interface instance which communicates with users

Platforms	Name	Command	Default Value	Description
All	Print line/file	`netuis netui1 set lineFilePrint {value}`	true	Print Linenumber and Filename for logging messages
All	Print time	`netuis netui1 set timePrint {value}`	true	Print time for logging messages
All	Disconnect timeout	`netuis netui1 set timeout {value}`	300	Disconnect timeout in seconds, for when the interface is inactive

NTP Monitor (ntpMonitor)

Available on platforms: All

Monitors NTP status and generates exceptions if any issues detected.

Platforms	Name	Command	Default Value	Description
All	Allowed missed polls	`ntpMonitor set allowed_missed_polls {value}`	8	Number of allowed consecutive missed polls of NTP server before an exception is flagged. The NTP daemon itself flags after 8 missed polls, so that will always generate an exception. However, 8 polls may take quite some time to complete (hours). While system time should be stable and accurate during this period, some might prefer to know sooner if the NTP server has not been reached. This value is also for consecutive missed polls. Set this to between 0 and 8.

Licence options (options)

Available on platforms: All

Management of the licence file

- `options display`

  Display Licence. Platforms: All.

  Display current licence information

- `options load`

  Read Licence file. Platforms: All.

  Load a new licence file from /storage/options.txt, and install's to system licence information

- `options test` {*on_off*}

  Set System in test mode. Platforms: All.

  Enable test mode, allows 100 Reads before marking number plate unreadable

#	Name	Parameter	Description
1	Test Mode	on_off	Test mode enable / disable

Patch Overlay Control (patchoverlay)

Available on platforms: All

Specify whether the plateread patch has an overlay, and what its contents should be.

Platforms	Name	Command	Default Value	Description
All	Overlay Text Enable	`patchoverlay set enabled` {*value*}	false	Enables additional text on the Image
All	Text	`patchoverlay set text` {*value*}		The format string for the overlayed text. This has limitations

Platforms	Name	Command	Default Value	Description
			%Iy04d/%Io02d/%Id02d_%Ih02d:%Im02d:%Is02d\n%Shs_%Pps_%Pc02d	

PCI Camera Source (pciSource)

Available on platforms: All

The internal camera subsystem, connected via PCI to the processor. These controls are mostly for diagnostics.

- `pciSource clear`

  Reset interrupt latency statistics. Platforms: All.

  Reset counts of interrupts from the PCI camera.

- `pciSource irbufs`

  Dump IR Bufs in use. Platforms: All.

  Dump IR Bufs in use

- `pciSource latency`

  Display interrupt latency statistics. Platforms: All.

  Display details and counts of interrupts from the PCI camera.

PIXI Contexts (pixicontexts)

Available on platforms: All

Manages PIXI contexts

- `pixicontexts list`

  List PIXI Contexts. Platforms: All.

  List existing PIXI persistent LIFOS as well as their lengths.

Power Manager (power)

Available on platforms: All

Power Management subsystem, monitoring the power coming into the system and dealing with power down when the power is cut.

Relay Out (relayOut)

Available on platforms: All

Controls the relay according to plate read events

Platforms	Name	Command	Default Value	Description
All	Relay Action	`relayOut set action {value}`	close	

Platforms	Name	Command	Default Value	Description
All	Enabled	`relayOut set enabled` {*value*}	false	
All	Relay Pulse Period	`relayOut set period` {*value*}	250	
All	Tag Match Regular Expression	`relayOut set tag_regex` {*value*}	.*	

SAP - Serial Application Port (sap)

Available on platforms: All

Simple serial port output

Platforms	Name	Command	Default Value	Description
All	Serial Baud Rate	`sap set baud` {*value*}	9600	The serial port baud rate. For changes to take effect, disable then re-enable. Valid values 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400
All	Enabled	`sap set enabled` {*value*}	false	Allows the SAP system to be enabled and disabled. Disable it unless you are using it.
All	Message contents	`sap set msg_contents` {*value*}	%Pps\n	A format string specifying the message content. The default gives you the plate-read text followed by newline.

Vehicle Image Selector (selector)

Available on platforms: All

Selects images from the hardware platefinder for further analysis and ANPR by the rest of the software.

Platforms	Name	Command	Default Value	Description
All	Previous trigger frame	`selector set pre_trigger_frame` {*value*}	true	Allow the camera to select the frame before the trigger was recieved if it has a lower time proximity to the trigger than the event after
All	Selector queue length	`selector set queueLength` {*value*}	5	Do not chnge this without good reason. By Changing the length of the queue it may change the latency to delivery, but is very likely to affect the read rate
All	Trigger Overview	`selector set triggerOview` {*value*}	false	If this is set *when triggered* the overview will be coincident with the trigger start. If this is not set or the vehicle was not triggered then the overview image will be taken at the same time as the IR image.
All	Triggers Only	`selector set triggersOnly` {*value*}	false	If this is set we will only detect vehicles during the trigger period, otherwise we'll auto detect

Platforms	Name	Command	Default Value	Description
				vehicles all the time but explicitly pass them on when triggered

- `selector statistics`

  Cumulative statistics. Platforms: All.

  Provides cumulative statistics of longterm vehicle processing

Hardware Monitoring sensors (sensors)

Available on platforms: All

This module periodically polls the sensor values

- `sensors dump`

  Dump Current readings. Platforms: All.

  Displays the current readings of the sensors

Console Logger (stdout)

Available on platforms: All

The logger which reports information to the standard out (stdout) device (usually the console). This is probably of no use to you as you probably aren't looking at it.

Platforms	Name	Command	Default Value	Description
All	Print line/file	`stdout set lineFilePrint {`*`value`*`}`	true	Print Linenumber and Filename for logging messages
All	Print time	`stdout set timePrint {`*`value`*`}`	true	Print time for logging messages

System Details (system)

Available on platforms: All

An object for collecting lists of system details and objects.

Platforms	Name	Command	Default Value	Description
All	P392 Bracket Location	`system set bracketBottom {`*`value`*`}`	true	P392 mounted with bracket at the bottom is true otherwise the variable should be false
All	COM2 serial use	`system set com2 {`*`value`*`}`	disabled	This settings determines what the com2 second user available serial port is used for. Options are: 'trig_serial' - generic serial triggering with regex matching and variable baud rate. 'sap' - Serial text output of vehicle plateread events. 'vestrigger' - 19.2k STX delimited trigger messages for VES.

Platforms	Name	Command	Default Value	Description
				'gps' - GPS unit talking NMEA at 4.8k. 'disabled' - not in use.
All	Coordinates Valid	`system set coord_valid {value}`	false	A flag indicating whether these coordinates are valid or not
All	East (not West)	`system set east {value}`	true	Flag indicating whether the longitude value is East or West. 1->East, 0->West
All	North Degrees	`system set latitude {value}`	0	This is the latitude coordinate of this camera, and this is the degree portion of the coordinate. If you have a GPS system attached and working this will be automatically updated everytime we have a lock, otherwise it is manually enterable.
All	North Microdegrees	`system set latitude_micro {value}`	0	This is the latitude coordinate of this camera, and this is the microdegree portion of the coordinate. If you have a GPS system attached and working this will be automatically updated everytime we have a lock, otherwise it is manually enterable.
All	East Degrees	`system set longitude {value}`	0	This is the longitude coordinate of this camera, and this is the degree portion of the coordinate. If you have a GPS system attached and working this will be automatically updated everytime we have a lock, otherwise it is manually enterable.
All	East Microdegrees	`system set longitude_micro {value}`	0	This is the longitude coordinate of this camera, and this is the microdegree portion of the coordinate. If you have a GPS system attached and working this will be automatically updated everytime we have a lock, otherwise it is manually enterable.
All	North (not south)	`system set north {value}`	true	Flag indicating whether the latitude value is North or South. 1->North, 0->South
All	Relay output use	`system set relay {value}`	disabled	This setting determines what the relay input is used for. Options are: 'gpspower' - for use in switching on and off a gps unit (only usable with the serial port com2 also connected to the gps). 'disabled' - not in use.
All	Trigger input use	`system set trigger {value}`	disabled	This setting determines what the trigger input is used for. Options are: 'hwtrigger' - for a triggering vehicles detection. 'gpspps' - for the pulse per second signal from a gps unit (only useable with the serial port com2 also connected to the gps). 'exception' - generate exceptions when the line changes state. 'script' - run a user script on line state change. 'anpr_enable' - only perform anpr when trigger input circiut is completed. 'disabled' - not in use.

- `system crc`

  Display CRCs. Platforms: All.

Display CRCs of the system and configuration

- `system info`

  Display information. Platforms: All.

  Display general information about this camera. Always useful as a debugging aid.

- `system queues`

  Queues. Platforms: All.

  List all queues and their state

- `system reboot`

  Reboot camera. Platforms: All.

  Reboot the camera now unconditionally.

- `system relay`

  Toggle Relay. Platforms: All.

  Change the state of the relay

- `system relay_close`

  Close Relay. Platforms: All.

  Set the state of the relay to closed

- `system relay_open`

  Open Relay. Platforms: All.

  Set the state of the relay to open.

- `system relay_pulse` {*`closed`*} {*`period`*}

  Pulse Relay. Platforms: All.

  Set the relay to a specified state for a period

#	Name	Parameter	Description
1	Pulse Closed	closed	true to set relay closed, then, after period, open. Otherwise relay will open and, after period, close
2	Pulse Period	period	The relay pulse period in milliseconds

- `system restart`

  Restart application. Platforms: All.

  Attempt to restart the application without rebooting. May reboot camera under some circumstances.

Trigger Control (trig)

Available on platforms: All

External trigger control, for when you have wired an external vehicle detector into the camera. To use this you must set the Vehicle Image Selector filter to triggered rather than auto.

Platforms	Name	Command	Default Value	Description
All	Forward All Payloads	`trig set forward_all_payloads {value}`	false	For an already open gate, subsequent trigger stimuli will be processed for payload (while the gate is open). This will for example allow the hardware trigger to cause the gate to open and a TCP trigger (while the gate is open) could provide the payload. Please note that timing is important. If the payload-providing-trigger is late (arrives after the gate has closed) it will generate a new trigger rather than a payload to a current open trigger. See also the trigger payload format specifiers.
All	Trigger Latency	`trig set latency {value}`	0	Sets configurable delay from electrical signal edge to when we regard the trigger to have occurred.
All	Gate open period	`trig set open_period {value}`	250	Sets period during which we enable image processing for the triggering vehicle.
All	Appends the trigger id to all trigger acknowledgement messages	`trig set reply_with_trigger_id {value}`	false	
All	Simulated trigger period	`trig set simulated_period {value}`	1000	Sets the period between simulated triggers. Not for use in a production system.
All	Simulation Mode	`trig set simulation_mode {value}`	false	Enabling simulation mode causes software triggers to be generated at the rate determined by the simulated period
All	Variable Gate Open Period	`trig set variable_period {value}`	false	For an already open gate, the open period will be extended if further stimulus received (e.g. motion detection, physical trigger, TCP trigger). Under this mechanism the gate will always stay open for a minimum of the configured Gate Open Period and for no longer than 2 seconds.
All	Wait period	`trig set wait_period {value}`	700	Sets period after latency expires before we will accept another trigger. Can be used to prevent noisy triggers causing problems.

- `trig message {msg}`

  Single Simulated Trigger with content. Platforms: All.

Generates a single simulated trigger. Note, this will be generated regardless of whether simulation mode is enabled. It takes an argument which will populate the OEM trigger data field for the vehicle. How you next see this information is dependant upon your output mechanism.

#	Name	Parameter	Description
1	Message Content	msg	The OEM trigger data field.

- `trig oneshot`

  Single Simulated Trigger. Platforms: All.

  Generates a single simulated trigger. Note, this will be generated regardless of whether simulation mode is enabled.

- `trig statistics`

  Cumulative statistics. Platforms: All.

  Provides cumulative statistics of longterm trigger processing

Hardware Trigger (trig hw)

Available on platforms: All

This module manages the external trigger input on the rear of the camera. You must connect this up to a 12V external trigger input such as a loop or other vehicle detector for this to be of any use. To use this you must assign the trigger to be 'hwtrigger' in the system parameters.

Platforms	Name	Command	Default Value	Description
All	Debounce time	`trig hw set debounce {value}`	1	Number of milliseconds for which a trigger has to be stable before it is accepted by the system. Increasing this will remove false short triggers from the system at the expense of the same amount of latency in the trigger. It could also miss triggers if your trigger system produces very short pulses and you set it too high. This debounce parameter is applied for all uses of the trigger input, including scripts and exceptions.
All	Falling Edge	`trig hw set falling_edge {value}`	false	This chooses which edge of the signal will be used to trigger on, if unselected you will trigger on the rising edge of the signal. You will need to refer to the manual for your trigger source to determine which it produces when a vehicle enters the field of view.

- `trig hw clearcount`

  Clear Hardware trigger count. Platforms: All.

  Resets the count of number of hardware triggers recorded to 0

- `trig hw count`

  Hardware trigger count. Platforms: All.

Provides a count of number of hardware triggers recorded

- `trig hw status`

  Current trigger status. Platforms: All.

  Gets the current status of the trigger input signal

Serial Trigger (trig serial)

Available on platforms: All

This module manages Serial Triggers. These may be sent into com2.

Platforms	Name	Command	Default Value	Description
All	Acknowledge	`trig serial set ack_enabled` {*value*}	true	To enable/disable the generation of acks. If enabled the whole message as sent will be echoed back to you.
All	Serial Baud Rate	`trig serial set baud` {*value*}	115200	The serial port baud rate. For changes to take effect, disable then re-enable. Valid values 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400
All	Serial triggers enabled	`trig serial set enabled` {*value*}	false	If true, will detect and propogate triggers from com2.
All	Heartbeat Regular Expression	`trig serial set heartbeat_regex` {*value*}	disabled	If the string arriving on the trigger port matches this regex, it will NOT generate a trigger, it will simply echo the pattern back exactly as received. Notes: To disable it, set it to the string disabled. Heartbeat will work regardless of the ack_enabled setting
All	Trigger Regular Expression	`trig serial set trig_regex` {*value*}	(.*)\n	A regular expression (matching the Perl Regular Expression Syntax) that the incoming string must match in order for a trigger to be generated. The trigger payload will be the concatination of those parts of the incoming string that match any subexpressions in the regex, as specified by ()'s. If no ()'s are present in the trig_regex, then the entire incoming string, that matches the regex, will be used as the trigger payload. Note: A trigger payload may only contain XML legal ASCII. If it contains any illegal characters, no trigger will be generated.

TCP Trigger (trig tcp)

Available on platforms: All

This module manages TCP Triggers. These are sent in to a server socket on port 3820.

Platforms	Name	Command	Default Value	Description
All	Acknowledge	`trig tcp set ack_enabled {value}`	true	To enable/disable the generation of acks. If enabled the whole message, exactly as sent, will be echoed back to you.
All	TCP triggers enabled	`trig tcp set enabled {value}`	true	If true, will detect and propogate TCP Socket triggers.
All	Heartbeat Regular Expression	`trig tcp set heartbeat_regex {value}`	disabled	If the string arriving on the trigger port matches this regex, it will NOT generate a trigger, it will simply echo the pattern back exactly as received. Notes: To disable it, set it to the string disabled. Heartbeat will work regardless of the ack_enabled setting
All	Trigger Regular Expression	`trig tcp set trig_regex {value}`	(.*)\n	A regular expression (matching the Perl Regular Expression Syntax) that the incoming string must match in order for a trigger to be generated. The trigger payload will be the concatination of those parts of the incoming string that match any subexpressions in the regex, as specified by ()'s. If no ()'s are present in the trig_regex, then the entire incoming string, that matches the regex, will be used as the trigger payload. Note: A trigger payload may only contain XML legal ASCII. If it contains any illegal characters, no trigger will be generated.

Trigger Script (trigScript)

Available on platforms: All

This module will run a unix binary when the trigger input changes state. You must connect this up to an external trigger input for this to be of any use. To use this modules you must assign the trigger to 'script' in the system parameters. Note, each script must finish running before we will run the next script if the scripts take time to execute and the trigger makes fast transitions. The use of this feature is obviously unsupportable as you can cause anything to run which could cause the system to become unstable. It is suggested you get your script verified by PIPS if you do require support. These scripts will run a maximum of once every 5 seconds.

Platforms	Name	Command	Default Value	Description
All	Falling Edge	`trigScript set falling {value}`		This is the full path to a binary (usually a unix shell script) will be run on the falling edge of the trigger. If this is left blank or an invalid binary nothing will happen. This script will be run at bootup if the trigger input is low at bootup.

Platforms	Name	Command	Default Value	Description
All	Rising Edge	`trigScript set rising {value}`		This is the full path to a binary (usually a unix shell script) will be run on the rising edge of the trigger. If this is left blank or an invalid binary nothing will happen. This script will be run at bootup if the trigger input is high at bootup.

UTMC Delivery Module (utmc)

Available on platforms: All

The UTMC module is a delivery module which sends vehicle event data to an external computer (instation) using the UTMC protocol.

Platforms	Name	Command	Default Value	Description
All	Authenticate using username and password	`utmc set authenticate {value}`	false	authenticate
All	UTMC Camera ID	`utmc set cameraID {value}`	0	The UTMC camera ID
All	Minimum Samples for Diagnostics	`utmc set diagnostic_min_samples {value}`	10	Certain types of diagnostics (e.g. mean values or ratios) are only considered valid after a certain number of samples.
All	Diagnostic period	`utmc set diagnostic_period {value}`	20	Period in minutes between diagnostic updates
All	Diagnostics and Exceptions Enabled	`utmc set diagnostics_exceptions_enabled {value}`	false	Send diagnostics and exceptions.
All	Timeout (in seconds) for DNS caching	`utmc set dnsCacheTimeout {value}`	60	Selectable option to change the timeout used by the DNS cache within libCURL. 60 to maintain backwards compatability, or 0 to completely disable DNS caching.
All	Enabled	`utmc set enabled {value}`	false	Allows the UTMC system to be enabled and disabled. Disable it unless you are using it.
All	Minimum Samples for Exceptions	`utmc set exception_min_samples {value}`	20	Certain types of exceptions (e.g. mean values or ratios) are only considered valid after a certain number of samples.
All	Exception Period	`utmc set exception_period {value}`	5	Period in minutes between (non-realtime) exception updates
All	Host	`utmc set host {value}`	192.168.1.1:8080	IP address and port of the instation which will receive the UTMC data.
All	Maximum number of vehicles in a batch	`utmc set maxBatchSize {value}`	100	The Maximum number of vehicles that can be in a batch, if the number of vehicles becomes larger than this number we will send out a batch
All	Merge Characters	`utmc set mergechars {value}`	true	

Platforms	Name	Command	Default Value	Description
				Enable merging of possible ambiguous characters such as 8 and B prior to transmission (for tags only)
All	Maximum Files	`utmc set nlog {value}`	100	The maximum number of files which will be stored on the local drive if it is not possible to contact the instation. Once this number has been stored, the oldest will be overwritten. Warning, arbitrarily setting this to a high value may fill up the device on which you are storing the files and then the system will lose the wrong data or perform badly (or not at all).
All	Password for transport	`utmc set password {value}`		Password
All	Path	`utmc set path {value}`	utmc	The path on the http url.
All	Tag Period	`utmc set period {value}`	5	The number of minutes between sending tag messages
All	Send Tag	`utmc set sendTag {value}`	true	Send hashed plates
All	Send VRN	`utmc set sendVRN {value}`	false	Send raw plates (VRNs)
All	Time Slot	`utmc set time_slot {value}`	0	Time slot which is used by this system for transmission. Use this to spread the network load of your outstations. This is a percentage value and is used as an offset from the beginning of the time which could be used for transmission verses the end of that transmission slot - e.g. 0 it will transmit at the very beginning of the slot, at 100 at the very end.
All	ACK Timeout	`utmc set timeout {value}`	60	Number of seconds to wait for an ACK (if ACKs are enabled). Set to zero to disable
All	UTMC transport	`utmc set transport {value}`	HTTP	HTTP or HTTPS
All	Use Gzip	`utmc set useGzip {value}`	true	Encode with gzip to save bandwidth
All	Use SOAP	`utmc set useSOAP {value}`	true	Wrap with SOAP envelope
All	Username for transport	`utmc set username {value}`		Username

- `utmc clearstats`

  Clear statistics. Platforms: All.

  Reset the statistics for this module

- `utmc stats`

  Statistics. Platforms: All.

Display statistics from this module

UTMC V1.2 Delivery Module (utmcv12)

Available on platforms: All

The UTMC module is a delivery module which sends vehicle event data to an external computer (instation) using version 1.2 of the UTMC protocol.

Platforms	Name	Command	Default Value	Description
All	Authenticate using username and password	`utmcv12 set authenticate {value}`	false	authenticate
All	UTMCV1_2 Camera ID	`utmcv12 set cameraID {value}`	0	The UTMCV1_2 camera ID
All	Timeout (in seconds) for DNS caching	`utmcv12 set dnsCacheTimeout {value}`	60	Selectable option to change the timeout used by the DNS cache within libCURL. 60 to maintain backwards compatability, or 0 to completely disable DNS caching.
All	Enabled	`utmcv12 set enabled {value}`	false	Allows the UTMCV1_2 system to be enabled and disabled. Disable it unless you are using it.
All	Host	`utmcv12 set host {value}`	192.168.1.1:8080	The IP address and port of the instation which will receive the UTMCV1_2 data.
All	Merge Characters	`utmcv12 set mergechars {value}`	true	Enable merging of possible ambiguous characters such as 8 and B prior to transmission (for tags only)
All	Maximum Files	`utmcv12 set nlog {value}`	100	The maximum number of files which will be stored on the local drive if it is not possible to contact the instation. Once this number has been stored, the oldest will be overwritten. Warning, arbitrarily setting this to a high value may fill up the device on which you are storing the files and then the system will lose the wrong data or perform badly (or not at all).
All	Password for transport	`utmcv12 set password {value}`		Password
All	Path	`utmcv12 set path {value}`	utmc	The path on the http url.
All	Send ANPR Image	`utmcv12 set sendANPRImage {value}`	true	Send the ANPR Image (the image used for the ANPR.)
All	Send Asynchronous Payload	`utmcv12 set sendAsyncPayload {value}`	false	Manufacturer Specific. Will send the asynchrounous payload within the UTMC ManufacturerSpecific area.
All	Send Overview Image	`utmcv12 set sendOverviewImage {value}`	true	Send the overview image
All	Send Plate Patch Image	`utmcv12 set sendPlatePatch {value}`	true	Send patch Image

Platforms	Name	Command	Default Value	Description
All	Send Tag	`utmcv12 set sendTag {value}`	false	Send hashed plates
All	Send VRN	`utmcv12 set sendVRN {value}`	true	Send raw plates (VRNs)
All	ACK Timeout	`utmcv12 set timeout {value}`	60	Number of seconds to wait for an ACK (if ACKs are enabled). Set to zero to disable
All	UTMCV1_2 transport	`utmcv12 set transport {value}`	HTTP	HTTP or HTTPS
All	Use Gzip	`utmcv12 set useGzip {value}`	true	Encode with gzip to save bandwidth
All	Use SOAP	`utmcv12 set useSOAP {value}`	true	Wrap with SOAP envelope
All	Username for transport	`utmcv12 set username {value}`		Username
All	Async. Payload is XML	`utmcv12 set xmlPayload {value}`	false	Manufacturer Specific. The async payload contains further XML tags within the ManufacturerSpecific area.

- `utmcv12 clearstats`

  Clear statistics. Platforms: All.

  Reset the statistics for this module

- `utmcv12 stats`

  Statistics. Platforms: All.

  Display statistics from this module

VES - Violation Enforcement System (ves)

Available on platforms: All

Highly configurable system with many options. Please refer to VES Software Interface Specification

Platforms	Name	Command	Default Value	Description
All	Enable Ack	`ves set ack_enable {value}`	0	When set require ack from instation on summary and/or evidential records. Retry on ack failure. 0x01 - ack required on evidential records (ERs) 0x02 - ack required on individual summary records (SRs) 0x04 - ack required on diagnostics 0x08 - ack required on exceptions 0x10 - ack required when transferring a record from spikestore to instation

Platforms	Name	Command	Default Value	Description
				0x20 - ack required on batched summary records (BSRs)
All	Retry attempts	`ves set ack_retry {value}`	3	Retry transfers this many times before giving up
All	ack timeout	`ves set ack_timeout {value}`	500	Time to wait for an ack (mS). This timeout is used for longg transfer events. Specifically full ERs. On a system connected by hi speed links, system overhead may dominate so this and the short timeout may be identical. Where comms is slow, a separate timeout is beneficial.
All	Alternate Host	`ves set alt_host {value}`	10.1.1.1	Sets the IP address of the alternate instation.
All	Enforcement area	`ves set area {value}`	WEZ	The name of the enforcement zone. This is expected to be a three character field. However up to seven characters are accepted.
All	batched SR interval	`ves set bsr_interval {value}`	300	Interval (seconds) over which SRs are accumulated to build a batch. If no data is collected during the interval, then no batch is generated. The current batch is skipped.
All	batched SR max batches	`ves set bsr_nlog {value}`	12	Maximum number of historic SR batches which may be stored on the camera. When this number is exceeded the oldest batch will be overwritten.
All	batched SR port	`ves set bsr_port {value}`	10007	Port for transfer of batched SRs. This may be the same port as used by standard SRs.
All	Cabinet controller	`ves set cabinet {value}`		Sets the IP address the cabinet controller if present. Used to monitor the cabling and link to detect intrusions or failures.
All	cf age limit	`ves set cf_age_limit {value}`	48	Maximum time (hours) an evidential record may be retained on camera. Records older than this will be deleted.
All	No. of context images	`ves set context_count {value}`	2	Specify the number of supporting context images which must be captured. The permissable range is 0-8. The number must be even. If an odd number is entered, it will be interpreted as the next lower even number.
All	Context image offset	`ves set context_offset {value}`	250	Specify the approximate interval (mS) between context images.
All	Context image order	`ves set context_order {value}`	0	Specify whether context images are split equally before/after the event, all before the event or all after the event.
All	Country Code standard	`ves set country_code {value}`	0	Determines the standard used for country codes. 0 - PIPS ANPR Standard

Platforms	Name	Command	Default Value	Description
				2 - ISO 3166-1 Alpha 2 3 - ISO 3166-1 Alpha 3
All	D&E debug	`ves set de_debug {value}`	0	set debug flags for diagnostic and exceptions module
All	D&E Ping wait time	`ves set de_ping_wait {value}`	15000	Applicable to diagnistics & exceptions only. Amount of time the system should wait for a ping acknowledge message before giving up. The system usually pings the instation before connecting to it. Set to zero to disable these pre-transmission pings.
All	VES Debug	`ves set debug {value}`	0	Bit field specifying which code modules genetate debug information 0x00000001 - main VES process 0x00000002 - summary record transmission 0x00000004 - image (blob) record transmission 0x00000008 - session & initial key exchange 0x00000010 - message port 0x00000020 - heartbeat system 0x00000040 - DSRC trigger system 0x00000080 - NVT control port 0x00000100 - PING events 0x00000200 - show ping replies 0x00000400 - transmission of records from file buffer 0x00000800 - local file index management 0x00001000 - blob generation 0x00002000 - system timing 0x00004000 - match slots 0x00008000 - data cleanup 0x00010000 - encryption 0x00020000 - key exchange 0x00040000 - diagnostics

Platforms	Name	Command	Default Value	Description
				0x00080000 - oem specific 0x00100000 - oem specific 0x00200000 - context capture 0x00400000 - pull archtecture 0x00800000 - image synchronisation 0x01000000 - radar interface 0x02000000 - trajectory computations 0x04000000 - spikestore interface 0x08000000 - batch summary records 0x10000000 - clock drifts 0x20000000 - audit trail 0x40000000 - oem data record
All	Local Directory	`ves set directory {value}`	/ves	Directory where diagnostic and exception files will be created and stored locally on the system before transfer to the host.
All	VES Enabled	`ves set enabled {value}`	false	Enables/Disables VES. If enabled is false on camera startup, VES will not load. To get VES to load, set enabled to true and restart the camera. Once VES is loaded the enable flag has the effect of enabling/disabling the flow of events into VES.
All	Max ER file size	`ves set file_size {value}`	256	Size in kbytes to be preallocated for storage of ERs. Also sets the storage allocation on the Compact Flash device. ERs larger than this size will be discarded.
All	Heartbeat Port	`ves set hb_port {value}`	10005	The TCP/IP port number used for heartbeat messages.
All	Heartbeat period	`ves set heart_beat {value}`	0	The period in seconds between heart beat (hb) messages. If set to 0, no heart beat messages will be sent.
All	Host	`ves set host {value}`	10.1.1.1	Sets the IP address of the instation.
All	Image port	`ves set image_port {value}`	10000	port on host server expecting image data
All	Image port (background)	`ves set image_port_b {value}`	10000	port on host server expecting image data from background process. This may - and usually will - be exactly the same port as the foreground process.
All	Image Timeout	`ves set image_timeout {value}`	5	Timeout in seconds after which a camera as marked as having a possible problem
All	Switch overview to monochrome	`ves set jpeg_mono {value}`	0	Set to force overview image to monochrome

Platforms	Name	Command	Default Value	Description
All	Colour image scale factor	`ves set jpeg_scale {value}`	0	Set Colour image jpeg scale factor. Only applies to systems equiped with hardware jpeg accelerator. 0 - not scaled 1 - 360x288 2 - 180x144
All	Colour image file size	`ves set jpeg_size {value}`	22	Set Colour image jpeg file size (kbytes). Default is 22k. Only applies to systems equiped with hardware jpeg accelerator
All	Key Exchange port	`ves set key_port {value}`	10003	port on camera listening for session start and key exchange requests
All	Lane Name	`ves set lane {value}`	1	short machine name for this ANPR system. Format TBD.
All	Link Timeout	`ves set link_timeout {value}`	20	Timeout in seconds after which image or summary ports will be closed when inactive.
All	VES Site Location	`ves set location {value}`	test site description	A site specific location string. If using pipsshell and the string contains spaces, then quote the whole string with "".
All	Event match window	`ves set match_window {value}`	700	Only applicable to externally triggered systems. This window (mS) specifies the maximum time window between a trigger event and the matching image set. Alternatively, this window may be used when other events must be matched to an image event.
All	Enable trigger match	`ves set matched_trig {value}`	0	Set this parameter to configure the system to use lane controller messages 0-subsystem disabled 1-A message triggers the camera. The message is not retained. 2-A message must be assocciated with a plate event. Any plate event without an assocciated message is disgarded 3-A message triggers the camera and is subsequently associated with the plate event

Platforms	Name	Command	Default Value	Description
				Messages may arrive on either designated tcp/ip connection or on the serial port. However note that trigger events received via tcp/ip are subject to latencies beyond the control of the system and may be unusable in many circumstances
All	batched SR max count	`ves set max_batch_size {value}`	100	Maximum number of records in a SR batch. When this number is reached, the batch will be queued for transmission even if the interval has not expired.
All	Message Port	`ves set msg_port {value}`	10004	The TCP/IP port number used for messages.
All	Message Timeout	`ves set msg_timeout {value}`	60	Timeout in seconds after which the message port will be closed when inactive.
All	Camera Name	`ves set name {value}`	lane	short machine name for this ANPR system. Format TBD.
All	Number of Files	`ves set nlog {value}`	200	Number of image files to store on local disk.
All	Not Alive Counter	`ves set not_alive {value}`	10	If the heart beat process is running (heartbeat period>0) then if the heart beat fails to send its message (i.e. unable to establish a connection for this many attempts), then the system will attempt recovery action.
All	NVT control mode	`ves set nvt_mode {value}`	0	set nvt control channel mode
All	NVT port	`ves set nvt_port {value}`	10002	port on camera listening for NVT control connection
All	NVT channel timeout	`ves set nvt_timeout {value}`	5	Timeout in seconds after which the NVT port will be closed when inactive.
All	OEM contents	`ves set oem_contents {value}`	%PTs	A format string specifying how to construct the data you would like in the OEM field. NB: The OEM field is limited to 64 bytes. Excess data will be truncated.
All	Camera Direction	`ves set orientation {value}`	0	Set camera orientation according to cardinal compass point ie N, NW, W etc.
All	Ping Interval	`ves set ping_interval {value}`	300	Number of seconds interval between ping requests. These ping requests are used to establish whether and which server is online.
All	Ping Port	`ves set ping_port {value}`	10010	Selects the port on which UDP pings will be sent.
All	Ping Wait Time	`ves set ping_wait {value}`	100	Number of milliseconds to wait for a response to a ping request. Ping requests are sent before opening a connection to the host system.

Platforms	Name	Command	Default Value	Description
All	Reference image file	`ves set ref_file {value}`	mem:/ dummy.bin	The name of a file containing a set of reference jpeg images used to prepare dummy records.
All	Remote Network Router	`ves set router {value}`		Sets the IP address of the remote network router. May be used to monitor the cabling and link to detect failures.
All	Session control rules	`ves set rules {value}`	0xffff	Set the rules which specify which items will be checked before a session may be started. This may be hard coded in shipping systems but can be set to facilitate testing. Not all rules may apply to all system builds. 0x001 - check time sync 0x002 - check config crc 0x004 - check tamper switch 0x008 - check equipment 0x010 - only set secret from serial port 0x020 - terminate on network hack 0x040 - terminate on multiple password fail 0x080 - terminate on restart 0x100 - terminate on network tamper.
All	Disk Buffer scan interval	`ves set scan_interval {value}`	30	Interval in seconds between scans of disk buffer system to check for any oustanding files to transfer to host
All	ER transfer throttle	`ves set scan_throttle {value}`	500	throttle background transfer of ERs to approximately one record per this many mS. Set to 0 to disable the throttle
All	security level	`ves set security {value}`	3	This setting defines the security level used by the system 0x00 - no security 0x01 - HMAC - ERs will have an HMAC applied but are sent in clear text 0x02 - ERs are encrypted (AES256 with CBC) 0x04 - ERs are transferred with rolling keys 0x80 - Diagnostics and exceptions are encrypted NB: Batched SRs are always encryypted

Platforms	Name	Command	Default Value	Description
All	SER transfer throttle	`ves set ser_throttle {value}`	500	throttle background transfer of SERs to approximately one record per this many mS. Set to 0 to disable the throttle
All	Enable serial trigger	`ves set serial_trig {value}`	0	Set to enable serial trigger input. This will of course only be meaningfull if the hardware has a serial input available.
All	session options	`ves set session_opts {value}`	0	Set the session security level in use 0x00 - No sessions - no session security 0x01 - Sessions enabled, session control must pass CHAP 0x02 - Sessions enabled, session control is encrypted
All	short ack timeout	`ves set short_ack_timeout {value}`	500	Time to wait for an ack (mS) This timeout is used for short events. Specifically SRs SERs. On systems with slows comms benefit is gained by setting this to a more appropriate value.
All	Slot age limit	`ves set slot_age_limit {value}`	30	Maximum time (seconds) an event (summary and/or evidential record) will spend in ram before being transferred to Compact Flash store (or deleted if no CF store in use)
All	Media Source	`ves set source {value}`	NULL	The name of the media source type. This is expected to be a four character field. However up to seven characters are accepted.
All	SPIKEstore Account	`ves set store_account {value}`	vesstore	Username used for transfer of ERs to SPIKEstore.
All	SPIKEstore enable	`ves set store_enable {value}`	0	When a record is deleted from Compact Flash or ram buffers either through a specific delete request or through age expiry, an option exists to transfer the record to SPIKEstore. This store can provide very long term historical storage of records. Set this option to enable transfer to this store. NB: No facility exists to transfer these records to the host system. It is expected that this and any other housekeeping required will be the direct responsibility of the host system.
All	SPIKEstore Host IP	`ves set store_host {value}`	10.1.1.1	Sets the IP address of the SPIKEstore module.

Platforms	Name	Command	Default Value	Description
All	SPIKEstore Password	`ves set store_password {value}`	vesstore	Password used for transfer of ERs to SPIKEstore.
All	SPIKEstore Path	`ves set store_path {value}`		sub path in which files will be created on SPIKEstore server. NB: This path is NOT created on the host system by the camera software. It is assumed to exist. Transfers will fail if this path does not exist. The path, if set, should terminate in / or \ as appropriate for the SPIKEstore system. This path is used as a prefix to directories and files when they are created on the host.
All	Summary port	`ves set summary_port {value}`	10001	port on host server expecting summary data
All	Summary port (background)	`ves set summary_port_b {value}`	10001	port on host server expecting summary data from background process. This may - and usually will - be exactly the same port as the foreground process.
All	summary rate threshold	`ves set summary_rate {value}`	0	Set a control on transfer of summary records based on the outstanding count of evidential records. Set to zero to disable this control. Minimum active value:10 When set, if there are more outstanding ERs than this count, then transfer of summary records from backing store will be suspended. A hysteresis of 10% is applied.
All	Conf threshold	`ves set threshold {value}`	35	When transfer on threshold set, only ANPR reads with a threshold higher than this will be transferred to the host system.
All	Time slot	`ves set time_slot {value}`	0	Time slot which is used by this system for transmission of diagnostics & exceptions. Use this to spread the network load of your outstations. This is a percentage value and is used as an offset from the beginning of the time which could be used for transmission verses the end of that transmission slot - e.g. 0 it will transmit at the very beginning of the slot, at 100 at the very end.
All	Timeout	`ves set timeout {value}`	300	If no plate image is received on a camera for this many seconds, then a bit will be set in the status register. This may indicate a possible system failure e.g. camera fault or may indicate that a lane is closed.
All	Transfer	`ves set transfer {value}`	0x09f7	Bit field specifying which data must be transferred 0x00001 - transfer patch

Platforms	Name	Command	Default Value	Description
				0x00002 - transfer full IR 0x00004 - transfer scene 0x00008 - transfer context images 0x00010 - explicit delete required on PULL protocol 0x00020 - add text to patch & IR images 0x00040 - discard events below threshold 0x00080 - transfer ERs only on request (PULL protocol) 0x00100 - on tx failure buffer data to local disk 0x00200 - send M001 message 0x00400 - send M002 message 0x00800 - send WARNing messages 0x01000 - send ERRor messages 0x02000 - transfer Hearbeat as H001 messag 0x04000 - transfer session state messages 0x08000 - transfer summary records 0x10000 - create short evidential record 0x20000 - transfer batched summary records 0x40000 - Always transfer ERs via CF and background channel
All	TCPIP trigger port	`ves set trig_port {value}`	10006	TCP/IP Port on camera listening trigger messages. The protocol accepted on this port may be OEM specific.

- `ves aes`

  . Platforms: All.

- `ves clear`

  . Platforms: All.

- `ves delete`

  . Platforms: All.

- `ves init`

. Platforms: All.

- `ves list`

  . Platforms: All.

- `ves ping`

  . Platforms: All.

- `ves rebuild`

  . Platforms: All.

- `ves remove`

  . Platforms: All.

- `ves secret`

  . Platforms: All.

- `ves send`

  . Platforms: All.

- `ves statistics`

  VES Statistics. Platforms: All.

- `ves test`

  . Platforms: All.

- `ves trigger`

  . Platforms: All.

Vehicle Event Database (vfeDB)

Available on platforms: All

Platforms	Name	Command	Default Value	Description
All	Enabled	`vfeDB set enabled` {*value*}	false	Enables the storage capability within the vfeDB
All	Maximum Age	`vfeDB set max_age` {*value*}	0	The Maximum age records are allowed to be specified in minutes. Set to 0 for no time restriction
All	Store Analysis Images	`vfeDB set store_analysis_images` {*value*}	true	This parameter is used to control if analysis images are stored
All	Store Context Images	`vfeDB set store_context_images` {*value*}	true	This parameter is used to control if context images are stored
All	Store Overview Images	`vfeDB set store_overview_images` {*value*}	true	This parameter is used to control if overview images are stored

Platforms	Name	Command	Default Value	Description
All	Store Patch Images	`vfeDB set store_patch_images {value}`	true	This parameter is used to control if patch images are stored
All	Store Supplementary Images	`vfeDB set store_supplementary_images {value}`	true	This parameter is used to control if supplementary images are stored

- `vfeDB statistics`

  Cumulative statistics. Platforms: All.

  Provides cumulative statistics

Logging bits

These commands can be used to turn on and off real time messages from the camera about its status. These are implemented for debugging purposes in the main, and may not be meaningful at all. Turning too many of these on may adversely impact the performance of the camera. It is recommended that you use a pipsshell over SSH to watch logging, rather than serial, as the serial port can become overloaded if you turn too many messages on.

Platforms	Command	Description
All	`log acs bufferdisk_append {on/off}`	Appends to buffer disk queue
All	`log acs bufferdisk_remove {on/off}`	Removals from buffer disk queue
All	`log acs disk {on/off}`	Disk interactions
All	`log acs events {on/off}`	ACS events
All	`log acs filenames {on/off}`	Filename details
All	`log acs images {on/off}`	Image aquisition status
All	`log acs inevents {on/off}`	Incoming events
All	`log acs overviews {on/off}`	Overview aquisition status
All	`log acs transfer {on/off}`	Transfer messages
All	`log anpr allreads {on/off}`	Reports all vehicle read events, may be very noisy
All	`log anpr colour {on/off}`	Reports on colour full screen retries
All	`log anpr laneId {on/off}`	Reports information for debugging and varifiying the lane identification system - Only works on supported platforms
All	`log anpr latency {on/off}`	Reports age of departing ImageRecords associated with events
All	`log anpr noreads {on/off}`	Reports vehicle noread events
All	`log anpr patches {on/off}`	Reports on patches and full screen retries
All	`log anpr performance {on/off}`	Reports time taken by AnprLib_run
All	`log anpr reads {on/off}`	Reports vehicle read events
All	`log asyncp incoming {on/off}`	Incoming vehicle events
All	`log asyncp matches {on/off}`	Reports on Matches made between the async payloads and vehicle events. Also reports failures to match
All	`log asyncpStore payloads {on/off}`	Reports payloads added to store
All	`log bof2 incoming {on/off}`	Incoming Events

Platforms	Command	Description
All	`log bof2 messages` {*on/off*}	BOF2.2 Message Log
All	`log bof2 verbose` {*on/off*}	Display error message from the BOF2.2 instation
All	`log cam2exposure brightness` {*on/off*}	Exposure process debugging
All	`log cam2exposure settings` {*on/off*}	Shutter and gain settings debugging
All	`log client connections` {*on/off*}	Connection events
All	`log client latency` {*on/off*}	Reports age of departing ImageRecords associated with events
All	`log client overviews` {*on/off*}	Overview aquisition status
All	`log client vehicles` {*on/off*}	Vehicle events
All	`log dbmatcher incoming` {*on/off*}	Incoming vehicle events
All	`log dbmatcher matches` {*on/off*}	Matches made by the duplicate matcher
All	`log dbmatcher notification` {*on/off*}	Reasons for passing on this image
All	`log diskDB deletes` {*on/off*}	log when an entity is deleted
All	`log exposure brightness` {*on/off*}	Brightness controller actions
All	`log exposure processing` {*on/off*}	Exposure process debugging
All	`log exposure statistics` {*on/off*}	Collect some data for analysis.
All	`log exposure vehicles` {*on/off*}	Number of vehicles checks
All	`log exposure voting` {*on/off*}	Voting by the exposure subsystem on getting brighter or dimmer
All	`log fusion best` {*on/off*}	Choices made by the best plate chooser
All	`log fusion hazard` {*on/off*}	Hazard Processing
All	`log fusion incoming` {*on/off*}	Incoming vehicle events
All	`log fusion latency` {*on/off*}	Latency of events through the system
All	`log fusion matches` {*on/off*}	Matches made by the duplicate matcher
All	`log fusion noread` {*on/off*}	Noread Processing
All	`log fusion notify` {*on/off*}	Reasons for passing on this image
All	`log fusion resetting` {*on/off*}	Resetting a vehicle
All	`log fusion supplementary` {*on/off*}	Supplementary Image Processing
All	`log fusion timers` {*on/off*}	Event timer details
All	`log fusion traj` {*on/off*}	Trajectory of vehicle
All	`log gps controller` {*on/off*}	GPS Controller status reported at poll interval
All	`log gps sentences` {*on/off*}	Echo GPS sentences
All	`log gps time` {*on/off*}	Time Management status reported at poll interval
All	`log heartbeat incoming` {*on/off*}	Incoming vehicle events
All	`log hwtrigger latency` {*on/off*}	Latency of triggers through the system
All	`log ifo outputName` {*on/off*}	Filenames of output
All	`log jpegService performance` {*on/off*}	Performance measurements on the JPEG system
All	`log jpegService retries` {*on/off*}	Report whether we are having to retry JPEG compressions to fit into the buffers
All	`log jpegService type` {*on/off*}	Reports whether JPEG processing is performed in hardware, or software and what type
All	`log jtms connection` {*on/off*}	Connection issues

Platforms	Command	Description
All	`log jtms incoming` {*on/off*}	Incoming events
All	`log jtms messages` {*on/off*}	See outgoing messages, (Text format only)
All	`log jtms outgoing` {*on/off*}	Outgoing events
All	`log jtms timing` {*on/off*}	Timing information
All	`log ntp peers` {*on/off*}	Logs extracted Peers values as stored internally.
All	`log ntp raw` {*on/off*}	Logs raw unparsed data as received from the ntpq script.
All	`log ntp reach` {*on/off*}	Logs NTP reach processing.
All	`log ntp values` {*on/off*}	Logs extracted NTP values.
All	`log pciSource capIR` {*on/off*}	Outputs periodic updates of IR capture count
All	`log pciSource capOview` {*on/off*}	Outputs periodic updates of overview capture count
All	`log pciSource initialisation` {*on/off*}	Initialisation of the cameras
All	`log platefinder groups` {*on/off*}	Groups process debugging
All	`log platefinder hwoutput` {*on/off*}	FPGA output debugging
All	`log platefinder plates` {*on/off*}	Found plates debugging
All	`log platefinder searchgroups` {*on/off*}	Search group debugging
All	`log platewidth processing` {*on/off*}	PlateWidth process debugging
All	`log platewidth samples` {*on/off*}	PlateWidth collected samples debugging
All	`log platewidth shape` {*on/off*}	PlateWidth plate shape debugging
All	`log power state` {*on/off*}	Power state changes
All	`log relayOut incoming` {*on/off*}	Incoming events
All	`log relayOut outgoing` {*on/off*}	Outgoing events
All	`log sap incoming` {*on/off*}	Incoming events
All	`log sap outgoing` {*on/off*}	Outgoing events
All	`log selector detects` {*on/off*}	Reports generated vehicle detect events
All	`log selector indrops` {*on/off*}	Drops on the input queue
All	`log selector latency` {*on/off*}	Reports generated vehicle detect events associated ImageRecord age
All	`log selector multi` {*on/off*}	Show how many vehicles were detected in each image
All	`log selector notify` {*on/off*}	Notification from selector
All	`log selector performance` {*on/off*}	Reports the time taken to do the software portion of platefinding, the tracking algorithm and disposal algorithm
All	`log selector platefinder` {*on/off*}	Platefinder output
All	`log selector queue` {*on/off*}	Show the internal queue adds and deletes
All	`log selector score` {*on/off*}	Show how vehicles are scored and dropped from the internal queue
All	`log selector score_detail` {*on/off*}	Show details on scoring
All	`log selector tracking` {*on/off*}	Show details of the vehicle tracking
All	`log sensors changes` {*on/off*}	Reports changes in sensor values - currently just voltage, but may be extended to temperature etc. in the future

Platforms	Command	Description
All	`log system crcs` {*on/off*}	Reports changes in CRCs
All	`log transport_2acs failure` {*on/off*}	Brief failure details
All	`log transport_2acs items` {*on/off*}	Items being transferred
All	`log transport_2acs verbose` {*on/off*}	Verbose transfer details
All	`log transport_acs failure` {*on/off*}	Brief failure details
All	`log transport_acs items` {*on/off*}	Items being transferred
All	`log transport_acs verbose` {*on/off*}	Verbose transfer details
All	`log transport_bof2 failure` {*on/off*}	Brief failure details
All	`log transport_bof2 items` {*on/off*}	Items being transferred
All	`log transport_bof2 verbose` {*on/off*}	Verbose transfer details
All	`log transport_utmc failure` {*on/off*}	Brief failure details
All	`log transport_utmc items` {*on/off*}	Items being transferred
All	`log transport_utmc verbose` {*on/off*}	Verbose transfer details
All	`log transport_utmcv12 failure` {*on/off*}	Brief failure details
All	`log transport_utmcv12 items` {*on/off*}	Items being transferred
All	`log transport_utmcv12 verbose` {*on/off*}	Verbose transfer details
All	`log trig events` {*on/off*}	Instruments the triggers events
All	`log trig timers` {*on/off*}	Instruments the trigger timers, probably not of much interest
All	`log trigScript script` {*on/off*}	Show the running of scripts.
All	`log utmc connection` {*on/off*}	Connection issues
All	`log utmc incoming` {*on/off*}	Incoming events
All	`log utmc messages` {*on/off*}	See outgoing messages, (Text format only)
All	`log utmc outgoing` {*on/off*}	Outgoing events
All	`log utmc timing` {*on/off*}	Timing information
All	`log vfeDB deletes` {*on/off*}	Log when database records are deleted
All	`log vfeDB incoming` {*on/off*}	Incoming vehicle events
All	`log vfeDB notification` {*on/off*}	Reasons for passing on this image
All	`log vfeDB overviews` {*on/off*}	Log Overview information
All	`log vfeDB retrievals` {*on/off*}	Log when database objects are retrieved
All	`log videoStore fails` {*on/off*}	Retrieval failures
All	`log videoStore requests` {*on/off*}	Retrieval requests
All	`log viewfinder connections` {*on/off*}	Connection events
All	`log viewfinder sessions` {*on/off*}	Session events

Notifications

These commands can be used to turn on and off real time notifications from the camera. These notifications may be seen via pipsshell or via file logging, but the most useful way to use these notifications is via PIXI. To turn the notifications on/off via pipshell, use the command 'notification <source> <type> [on/off]'.

Platforms	Source	Type	Description
All	acs	datasetComplete	Provides notification of the successful transfer of an entire data-set via ACS. This notification has an

Platforms	Source	Type	Description
			additional property of 'eventId' which identifies the event the data transferred relates to.
All	acs	fileComplete	Provides notification of the successful completion of the transfer of an individual file via ACS. The notification will have an additional 'eventId' property which indicates the event that the file relates to. The property 'destpath' includes the full destination URL of the file which has now been transferred.

Chapter 7. Format strings

Format strings are a powerful tool for configuring the output from the camera. Spend some time studying this chapter to understand how they work if you want to change them. They can be used to configure file names and the format of outputted data in many places. Familiarity with the C (or other languages which have copied it) *printf* command will help in understanding what is going on here.

Only configuration parameters which specify that they are a format string may use this syntax. Please notify us if you think we should make a string into a format string.

Caution

Beware, you can configure the system incorrectly so that you get bad filenames which then cannot transfer. Be especially careful of the characters : / \ and . in your filename strings. Also, most systems won't accept filenames with control characters in them.

A format string consists of any number of parts, but essentially there are three different types of data you can put in it.

- Ordinary characters: which will just be output as is. This is the simplest type of entry. For example: if you want your filename to end in .txt, then just put .txt in the format string at the end. Note, you cannot put a \ or % in the string this way, you need to use a control character to do this.
- Control characters: which are used for unprintable characters which you can't simply enter into your string, such as **\n** for end of line. There is more detail on these in the section called “Control Characters” [84].
- Replacement specifiers: these are completely replaced by other text or numbers which are dependant upon the current item the string is working with. For example **%Pps** would be replaced by the read number plate. This is where the real power of the format strings lies. There is more detail on these in the section called “Replacement specifier” [85].

Control Characters

Each one of these will be replaced by a single control character in the output. These do *not* make sense for filenames, and are likely to cause problems with filesystems and FTP if you try to use them. They are of most use in file contents where you may want to add carriage returns or tabs.

- **\a** Alert (bell) (not often used)
- **\b** Backspace (not often used)
- **\f** Form feed, or new page (not often used)
- **\r** Carriage return. Combined with \n this is the DOS style end of line marker (e.g. **\r\n**.
- **\n** New line. This is the unix style end of line marker.
- **\t** Tab (horizontal)
- **\v** Vertical Tab (not often used)
- **** Gives a single \. Remember to put in two of these when you only want one in the output
- _ Gives a single space. You can use space directly on the P382, P392+ and P492 but this is for compatiblilty with the P357/P372. You cannot currently enter spaces in the shell, only on the web pages, so you'll need to use this from pipsshell.
- **\%** Gives a single %. Otherwise we think the % is the start of a replacement specifier

This paragraph can be skipped if you do not understand it. The escape character is ****, and can be followed by a character to cause various outputs, see above. **\octal-number** as in **\077** and **\hex-number** as in **\x3f** are also supported to output other ascii values - both of those will give a question mark character in ASCII.

Replacement specifier

The real power of format strings is in these. They all start with a % sign and there are a multitude of options for formatting the value. You then specify what the value is you want, and then how you want it presented.

Note

The format differs from printf, in that we must say what we are trying to display in the % as well as how to display it. The minimum length for a replacement specifier is 4 characters, including the % sign

The format goes as follows:

%{*replacement value*}[*format detail*]{*format*}

- *%* indicates the start of a replacement specifier
- *replacement value* is a two character string indicating what it is we wish to display here
- *format detail* is an optional string indicating more detail on how we wish to display it
- *format* is a single character indicating how we wish to display the value, e.g. as a decimal or hexadecimal number. Some values only make sense when displayed with a certain format

Format

The following characters are valid as the format in the replacement specifiers. Not all printf formats are valid.

Table 7.1. Format characters

Character	Desrciption
c	A single character
d	A signed decimal integer
i	A signed decimal integer (the same as d)
o	An octal integer
s	A string
u	An unsigned decimal integer
x	A hexadecimal integer with lower case letters
X	A hexadecimal integer with upper case letters
t	Treat the entry as numeric, and convert it to a string using the asctime() call to give something like 'Wed Jun 30 21:49:08 1993'. Trailing carriage return will be stripped.

Format Detail

An integer value placed here will ensure that the output is at least that many characters long. It will be padded with spaces. If you precede the integer with a 0 then it will pad with zeros instead. This is totally optional.

For example **`The plate is %Pp8s\n`** Will pad the plate string with spaces so outputting for a plate N7CTR

```
The plate is    N7CTR
```

with 4 spaces between the s and the N.

List of replacement values

Format value C

The camera detail of the plate the vehicle was read on

Platforms	Detail	Data Type	Description
All	Ce	Number	The shutter setting used for this image
All	Cg	Number	The gain setting used for this image
All	Cn	Number	The camera number (starting at zero)
All	CN	Number	The camera number (starting at one)
All	Cs	Number	The sequence setting (starting at zero)
All	CS	Number	The sequence setting (starting at one)

Format value D

The camera detail of the hazard plate the vehicle was read on

Platforms	Detail	Data Type	Description
All	De	Number	The shutter setting used for this image
All	Dg	Number	The gain setting used for this image
All	Dn	Number	The camera number (starting at zero)
All	DN	Number	The camera number (starting at one)
All	Ds	Number	The sequence setting (starting at zero)
All	DS	Number	The sequence setting (starting at one)

Format value E

Unique information about delivery event, Not usable under all circumstances

Platforms	Detail	Data Type	Description
All	Ei	Number	The Event id, which uniquly identifies the event

Format value F

Associated file. Not useable under all circumstances. Primarily for use in ACS's LPR files.

Platforms	Detail	Data Type	Description
All	F1	String	The filename of context image 1
All	F2	String	The filename of context image 2
All	F3	String	The filename of context image 3
All	F4	String	The filename of context image 4
All	F5	String	The filename of context image 5
All	F6	String	The filename of context image 6
All	F7	String	The filename of context image 7
All	F8	String	The filename of context image 8
All	Fl	String	The lpr text filename
All	Fn	String	The IR image filename

Platforms	Detail	Data Type	Description
All	FN	String	The hazard IR image filename
All	Fp	String	The patch image filename
All	FP	String	The hazard patch image filename
All	Ft	String	The transfer path (which is not prepended to the other filenames)
All	Fw	String	The wide angle, overview image filename
All	FW	String	The hazard wide angle, overview image filename

Format value H

The read hazard plate from the vehicle

Platforms	Detail	Data Type	Description
All	Ha	Number	The anpr classification (not useful with many ANPR engines)
All	HA	String	The OEM asynchronous payload. Asynchronous messages injected via serial (or TCP) will be associated with messages based on a closest match within a window. Otherwise an empty string.
All	Hc	Number	The confidence of the hazard plate read
All	HC	Number	The confidence category of the hazard plate read
All	Hf	Number	The confidence of the hardware platefinder
All	HF	Number	The field number
All	Hn	Number	The nationality code (not generally useful, see HN which is)
All	HN	String	The nationality (country and state) of origin of this plate if known
All	Ho	Number	The time offset between the trigger time and the image associated with this read (milliseconds). If not triggered, will be 0
All	Hp	String	The text of the hazard plate
All	Hr	Number	The total number of reads associated with the trigger that caused this plateread (A single trigger can lead to >1 plateread event). For a NOREAD the value will still be 1.
All	Hs	Number	The syntax confidence of the hazard plate read. This is a measure of how confident we are that the hazard plate matched the syntax of the reported country or state.
All	Ht	String	The plate tag, as extracted from the vehicle filter database. Will be blank if no tag entered, the plate is not matched, or the filter is off
All	HT	String	The OEM trigger payload. If you are using serial (or TCP/IP) triggers, this will be the OEM content of those, otherwise it will be boring. Text 'auto' will be returned if not triggered
All	Hx	Number	The x position of the plate's left edge in pixels
All	HX	Number	The width of the plate in pixels
All	Hy	Number	The y position of the plate's top edge in pixels
All	HY	Number	The height of the plate in pixels

Format value h

The camera heartbeat delivery

Platforms	Detail	Data Type	Description
All	hc	Number	The count of heartbeat delivery attempts.

Platforms	Detail	Data Type	Description
All	hf	Number	The count of heartbeat delivery failures.
All	hs	Number	A camera status bitfield (legacy).

Format value l

The image timestamp, the moment the image for the vehicle was captured.

This is a local time and accounts for timezone and daylight saving

Platforms	Detail	Data Type	Description
All	la	String	The string am for the morning, pm for the afternoon
All	lc	Number	Seconds since midnight 1st of January 1970 (commonly known as C time). This is UTC always, included for completeness.
All	ld	Number	The day of the month
All	lD	Number	The day of the year, with January the 1st as zero
All	lh	Number	The hour, 24 hour clock
All	lH	Number	The hour, 12 hour clock
All	li	Number	Milliseconds
All	ll	Number	Indicates if time is locked via NTP
All	lL	String	Indicates if time is locked via NTP as a string
All	lm	Number	Minutes past the hour
All	lM	Number	Tens of minutes past the hour
All	lo	Number	Month of the year (January as one)
All	lO	String	Month of the year as a word, in English
All	lP	String	Month of the year as three letter shortened word, in English
All	ls	Number	Seconds past the minute
All	lt	Number	Tenths of seconds
All	lu	Number	Hundredths of seconds
All	lv	Number	One if daylight saving is in effect, zero otherwise
All	lw	Number	The day of the week as a number, with zero being Sunday
All	lW	String	The day of the week as a word, in English
All	lX	String	The day of the week as a three letter shortened word, in English
All	ly	Number	The year
All	lY	Number	The last two digits of the year

Format value i

The image timestamp, the moment the image for the vehicle was captured.

This is UTC time (like GMT)

Platforms	Detail	Data Type	Description
All	ia	String	The string am for the morning, pm for the afternoon
All	ic	Number	Seconds since midnight 1st of January 1970 (commonly known as C time)
All	id	Number	The day of the month

Platforms	Detail	Data Type	Description
All	iD	Number	The day of the year, with January the 1st as zero
All	ih	Number	The hour, 24 hour clock
All	iH	Number	The hour, 12 hour clock
All	ii	Number	Milliseconds
All	il	Number	Indicates if time is locked via NTP
All	iL	String	Indicates if time is locked via NTP as a string
All	im	Number	Minutes past the hour
All	iM	Number	Tens of minutes past the hour
All	io	Number	Month of the year (January as one)
All	iO	String	Month of the year as a word, in English
All	iP	String	Month of the year as three letter shortened word, in English
All	is	Number	Seconds past the minute
All	it	Number	Tenths of seconds
All	iu	Number	Hundredths of seconds
All	iv	Number	One if daylight saving is in effect, zero otherwise
All	iw	Number	The day of the week as a number, with zero being Sunday
All	iW	String	The day of the week as a word, in English
All	iX	String	The day of the week as a three letter shortened word, in English
All	iy	Number	The year
All	iY	Number	The last two digits of the year

Format value J

JPEG data. Not useable under all circumstances. Primarily for use in output filenames to distinguish between them.

Platforms	Detail	Data Type	Description
All	Jt	Character	The file type. Will be p for a patch, n for an IR image, and w for an overview wide angle image. Context images will be 1 (for context 1), 2 (for context 2). Currently up to 8 context images are supported.

Format value L

The location of the camera

Platforms	Detail	Data Type	Description
All	Ld	Number	The whole number of degrees of latitude (north or south). Will always be positive.
All	LD	Number	The whole number of degrees of longitude (east or west). Will always be positive.
All	Le	Number	The whole number of degrees north we are. Will be negative if we are south.
All	LE	Number	The whole number of degrees east we are. Will be negative if we are west.
All	Lf	Number	The number of millidegrees of latitude we are away from the nearest degree.
All	LF	Number	The number of millidegrees of longitude we are away from the nearest degree.
All	Lg	Number	The number of microdegrees of latitude we are away from the nearest degree.

Platforms	Detail	Data Type	Description
All	LG	Number	The number of microdegrees of longitude we are away from the nearest degree.
All	Ll	Character	A character for latitude, N (north) or S (south) depending upon which hemisphere the location represents.
All	LL	Character	A character for longitude, E (east) or W (west) depending upon which side of the meridian the location represents.
All	Lm	Number	The number of minutes of latitude (north or south) that we are away from the nearest whole degree. Will always be positive.
All	LM	Number	The number of minutes of longitude (east or west) that we are away from the nearest whole degree. Will always be positive.
All	Ln	Number	The number of minutes of latitude (north or south) that we are away from the equator. Will always be positive.
All	LN	Number	The number of minutes of longitude (east or west) that we are away from the equator. Will always be positive.
All	Lo	Number	The number of minutes north that we are away from the equator. Will be negative if we are south.
All	LO	Number	The number of minutes east that we are away from the equator. Will be negative if we are south.
All	Lp	Number	The number of milliminutes of latitude we are away from the nearest minute.
All	LP	Number	The number of milliminutes of longitude we are away from the nearest minute.
All	Lq	Number	The number of microminutes of latitude we are away from the nearest minute.
All	LQ	Number	The number of microminutes of longitude we are away from the nearest minute.
All	LV	String	The string Valid or Invalid depending upon whether the location is deemed good.

Format value M

Metadata strings from the Metadata object. This is purely here so you can have the same format strings on all sites, and just change the metadata in this store

Platforms	Detail	Data Type	Description
All	Ma	String	Metadata string a
All	Mb	String	Metadata string b
All	Mc	String	Metadata string c
All	Md	String	Metadata string d
All	Me	String	Metadata string e
All	Mf	String	Metadata string f
All	Mg	String	Metadata string g
All	Mh	String	Metadata string h
All	Mi	String	Metadata string i
All	Mj	String	Metadata string j
All	Mk	String	Metadata string k
All	Ml	String	Metadata string l
All	Mm	String	Metadata string m
All	Mn	String	Metadata string n
All	Mo	String	Metadata string o

Platforms	Detail	Data Type	Description
All	Mp	String	Metadata string p
All	Mq	String	Metadata string q
All	Mr	String	Metadata string r
All	Ms	String	Metadata string s
All	Mt	String	Metadata string t
All	Mu	String	Metadata string u
All	Mv	String	Metadata string v
All	Mw	String	Metadata string w
All	Mx	String	Metadata string x
All	My	String	Metadata string y
All	Mz	String	Metadata string z

Format value o

The time offsets of overview context images

Platforms	Detail	Data Type	Description
All	o1	Number	The offset (in milliseconds) of context image 1 measured from the vehicle event timestamp
All	o2	Number	The offset (in milliseconds) of context image 2 measured from the vehicle event timestamp
All	o3	Number	The offset (in milliseconds) of context image 3 measured from the vehicle event timestamp
All	o4	Number	The offset (in milliseconds) of context image 4 measured from the vehicle event timestamp
All	o5	Number	The offset (in milliseconds) of context image 5 measured from the vehicle event timestamp
All	o6	Number	The offset (in milliseconds) of context image 6 measured from the vehicle event timestamp
All	o7	Number	The offset (in milliseconds) of context image 7 measured from the vehicle event timestamp
All	o8	Number	The offset (in milliseconds) of context image 8 measured from the vehicle event timestamp

Format value P

The read number plate from the vehicle

Platforms	Detail	Data Type	Description
All	P2	String	The 2-character nationality of origin of this plate if known, as defined by ISO 3166-1
All	P3	String	The 3-character nationality of origin of this plate if known, as defined by ISO 3166-1
All	Pa	Number	The anpr classification (not useful with many ANPR engines)
All	PA	String	The OEM asynchronous payload. Asynchronous messages injected via serial (or TCP) will be associated with messages based on a closest match within a window. Otherwise an empty string.

Platforms	Detail	Data Type	Description
All	Pc	Number	The confidence of the plate read
All	PC	Number	The confidence category of the plate read
All	Pd	String	The direction of travel of the plate read. This will be one of the following strings: AWAY, TOWARD, NOTSET. If NOTSET it indicates the direction could not be determined.
All	PD	String	The subdivision of origin of this plate if known, as defined by ISO 3166-2
All	Pf	Number	The confidence of the hardware platefinder
All	PF	Number	The field number
All	Pg	String	The source of OEM trigger
All	Pi	String	The OEM trigger payload from the first TCP/IP trigger
All	PI	Number	The trigger identifier.
All	PL	String	The lane in which the plate is located.
All	Pn	Number	The nationality code (not generally useful, see PN which is)
All	PN	String	The nationality (country and state) of origin of this plate if known
All	Po	Number	The time offset between the trigger time and the image associated with this read (milliseconds). If not triggered, will be 0
All	Pp	String	The text of the plate
All	Pr	Number	The total number of reads associated with the trigger that caused this plateread (A single trigger can lead to >1 plateread event). For a NOREAD the value will still be 1.
All	Ps	Number	The syntax confidence of the plate read. This is a measure of how confident we are that the plate matched the syntax of the reported country or state.
All	PS	String	The OEM trigger payload from the first Serial trigger
All	Pt	String	The plate tag, as extracted from the vehicle filter database. Will be blank if no tag entered, the plate is not matched, or the filter is off
All	PT	String	The OEM trigger payload. If you are using serial (or TCP/IP) triggers, this will be the OEM content of those, otherwise it will be boring. Text 'auto' will be returned if not triggered
All	Px	Number	The x position of the plate's left edge in pixels
All	PX	Number	The width of the plate in pixels
All	Py	Number	The y position of the plate's top edge in pixels
All	PY	Number	The height of the plate in pixels

Format value R

The trigger timestamp, the moment the trigger started. You should probably be using T instead of this, as if the event was not a triggered one you will not get anything in the string with R.

This is a local time and accounts for timezone and daylight saving

Platforms	Detail	Data Type	Description
All	Ra	String	The string am for the morning, pm for the afternoon
All	Rc	Number	Seconds since midnight 1st of January 1970 (commonly known as C time). This is UTC always, included for completeness.
All	Rd	Number	The day of the month
All	RD	Number	The day of the year, with January the 1st as zero

Platforms	Detail	Data Type	Description
All	Rh	Number	The hour, 24 hour clock
All	RH	Number	The hour, 12 hour clock
All	Ri	Number	Milliseconds
All	Rm	Number	Minutes past the hour
All	RM	Number	Tens of minutes past the hour
All	Ro	Number	Month of the year (January as one)
All	RO	String	Month of the year as a word, in English
All	RP	String	Month of the year as three letter shortened word, in English
All	Rs	Number	Seconds past the minute
All	Rt	Number	Tenths of seconds
All	Ru	Number	Hundredths of seconds
All	Rv	Number	One if daylight saving is in effect, zero otherwise
All	Rw	Number	The day of the week as a number, with zero being Sunday
All	RW	String	The day of the week as a word, in English
All	RX	String	The day of the week as a three letter shortened word, in English
All	Ry	Number	The year
All	RY	Number	The last two digits of the year

Format value r

The trigger timestamp, the moment the trigger started. You should probably be using t instead of this, as if the event was not a triggered one you will not get anything in the string with r.

This is UTC time (like GMT)

Platforms	Detail	Data Type	Description
All	ra	String	The string am for the morning, pm for the afternoon
All	rc	Number	Seconds since midnight 1st of January 1970 (commonly known as C time)
All	rd	Number	The day of the month
All	rD	Number	The day of the year, with January the 1st as zero
All	rh	Number	The hour, 24 hour clock
All	rH	Number	The hour, 12 hour clock
All	ri	Number	Milliseconds
All	rm	Number	Minutes past the hour
All	rM	Number	Tens of minutes past the hour
All	ro	Number	Month of the year (January as one)
All	rO	String	Month of the year as a word, in English
All	rP	String	Month of the year as three letter shortened word, in English
All	rs	Number	Seconds past the minute
All	rt	Number	Tenths of seconds
All	ru	Number	Hundredths of seconds
All	rv	Number	One if daylight saving is in effect, zero otherwise
All	rw	Number	The day of the week as a number, with zero being Sunday

Platforms	Detail	Data Type	Description
All	rW	String	The day of the week as a word, in English
All	rX	String	The day of the week as a three letter shortened word, in English
All	ry	Number	The year
All	rY	Number	The last two digits of the year

Format value S

The site details for this unit

Platforms	Detail	Data Type	Description
All	Sh	String	The site's hostname, the recommended way of identifying a site
All	Sl	Number	The system's library version number
All	Sn	Number	The system's serial number
All	Sv	Number	The system's application version number

Format value s

The supplementary images details

Platforms	Detail	Data Type	Description
All	s1	Number	The offset (in milliseconds) of supplementary image 1 measured from the vehicle event timestamp
All	s2	Number	The offset (in milliseconds) of supplementary image 2 measured from the vehicle event timestamp
All	s3	Number	Supplementary image 1 sequence setting (starting at one)
All	s4	Number	Supplementary image 2 sequence setting (starting at one)
All	s5	Number	Supplementary image 1 shutter setting
All	s6	Number	Supplementary image 2 shutter setting
All	s7	Number	Supplementary image 1 gain setting
All	s8	Number	Supplementary image 2 gain setting

Format value T

The timestamp for the vehicle, which is the trigger timestamp if the vehicle was triggered (see R), or the image timestamp if it was not (see I).

This is a local time and accounts for timezone and daylight saving

Platforms	Detail	Data Type	Description
All	Ta	String	The string am for the morning, pm for the afternoon
All	Tc	Number	Seconds since midnight 1st of January 1970 (commonly known as C time). This is UTC always, included for completeness.
All	Td	Number	The day of the month
All	TD	Number	The day of the year, with January the 1st as zero
All	Th	Number	The hour, 24 hour clock
All	TH	Number	The hour, 12 hour clock

Platforms	Detail	Data Type	Description
All	Ti	Number	Milliseconds
All	Tm	Number	Minutes past the hour
All	TM	Number	Tens of minutes past the hour
All	To	Number	Month of the year (January as one)
All	TO	String	Month of the year as a word, in English
All	TP	String	Month of the year as three letter shortened word, in English
All	Ts	Number	Seconds past the minute
All	Tt	Number	Tenths of seconds
All	Tu	Number	Hundredths of seconds
All	Tv	Number	One if daylight saving is in effect, zero otherwise
All	Tw	Number	The day of the week as a number, with zero being Sunday
All	TW	String	The day of the week as a word, in English
All	TX	String	The day of the week as a three letter shortened word, in English
All	Ty	Number	The year
All	TY	Number	The last two digits of the year

Format value t

The timestamp for the vehicle, which is the trigger timestamp if the vehicle was triggered (see r), or the image timestamp if it was not (see i).

This is UTC time (like GMT)

Platforms	Detail	Data Type	Description
All	ta	String	The string am for the morning, pm for the afternoon
All	tc	Number	Seconds since midnight 1st of January 1970 (commonly known as C time)
All	td	Number	The day of the month
All	tD	Number	The day of the year, with January the 1st as zero
All	th	Number	The hour, 24 hour clock
All	tH	Number	The hour, 12 hour clock
All	ti	Number	Milliseconds
All	tm	Number	Minutes past the hour
All	tM	Number	Tens of minutes past the hour
All	to	Number	Month of the year (January as one)
All	tO	String	Month of the year as a word, in English
All	tP	String	Month of the year as three letter shortened word, in English
All	ts	Number	Seconds past the minute
All	tt	Number	Tenths of seconds
All	tu	Number	Hundredths of seconds
All	tv	Number	One if daylight saving is in effect, zero otherwise
All	tw	Number	The day of the week as a number, with zero being Sunday
All	tW	String	The day of the week as a word, in English
All	tX	String	The day of the week as a three letter shortened word, in English
All	ty	Number	The year

Platforms	Detail	Data Type	Description
All	tY	Number	The last two digits of the year

Examples

Here are a few example format specifiers which might help you concoct your own. All the example output assumes a plate of RG51BTV has been read with confidence 96, on shutter 50/gain 9 at 15:34:30.2234 on 2008/03/27 in the eastern european timezone (GMT+2) on hostname "testsite" and that we're looking at the IR image, and the system is not triggered.

%Shs/

Input	%Shs	/
Output	testsite	/

(example result `testsite/`) This is the default ACS transfer path, just putting the hostname into the path.

acs/%Shs/

Input	acs/	%Shs	/
Output	acs/	testsite	/

(example result `acs/testsite/`) Now we have shifted to putting it into an acs subdirectory, followed by a site dependant hostname.

acs\\%Shs

Input	acs\\	%Shs	\\
Output	acs\	testsite	\

(example result `acs\testsite\`) And this version uses windows style directory separators, which is necessary for some broken windows FTP servers. Note we need to escape the \ by putting \\ in the path.

%Shs/%Iy04d%Io02d%Id02d/%Ih02d%IMd0/

Input	%Shs	/	%Iy04d	%Io02d	%Id02d	/	%Ih02d	%Idm	0/
Output	testsite	/	2008	03	27	/	12	3	0/

(example result `acs/20080327/1230/`) And now we are storing the files in time and date subdirectories, with 10 minutes worth of files per directory. Note the use of %IMd0 at the end which gives us the digit for each of the ten minutes, followed by a 0 which is copied through unchanged.

%Jtc%Id02u%Io02u%Iy04u,%Ih02u%Im02u%Is02u%Iu02u,%Pps,%Pc02u.jpg

Input	%Jtc	%Id02u	%Io02u	%Iy04u	,	%Ih02u	%Im02u	%Is02u	%Iu02u
Output	n	27	03	2008	,	12	34	30	22

Input	,	%Pps	,	%Pc02u	.jpg
Output	,	RG51BTV	,	96	.jpg

(example result `n27032008,12343022,RG51BTV,96.jpg`) This is the default image filename for ACS images. It produces a string starting with a character to identify which type of image it is. Followed by the date in DDMMYYYY format, followed by the time with hundredths of seconds, follwed by the plate and then the confidence. All of these are separated by commas.

%Jtc%Iy04u%Io02u%Id02u_%Ih02u%Im02u%Is02u%Iu02u_%Pps_%Pc02u.jpg

Input	%Jtc	%Iy04u	%Io02u	%Id02u	_	%Ih02u	%Im02u	%Is02u	%Iu02u
Output	n	2008	03	27	_	12	34	30	22

Input	_	%Pps	_	%Pc02u	.jpg
Output	_	RG51BTV	_	96	.jpg

(example result `n20080327_12343022_RG51BTV_96.jpg`) Now we have changed the commas to underscores, and swapped the date around to be YYYYMMDD.

%Jtc%ty04u%to02u%td02u%th02u%tm02u%ts02u%tu02u,%Pps,%Pc02u,%Ced,%Cgd.jpg

Input	%Jtc	%td02u	%to02u	%ty04u	%th02u	%tm02u	%ts02u	%tu02u
Output	n	27	03	2008	10	34	30	22

Input	,	%Pps	,	%Pc02u	,	%Ced	,	%Cgd	.jpg
Output	,	RG51BTV	,	96	,	50	,	9	.jpg

(example result `n2703200810343022,RG51BTV,96,50,9.jpg`) This time we are using GMT trigger time if the system is triggered, instead of local time of the image. We're also putting the shutter and gain settings for the read into the plate. We have also gone back to commas, loosing the separator between the date and time.

Chapter 8. PIXI Protocol

Note

PIXI was formerly known as NetUI, but has been renamed as it has been extended and the old name became inappropriate for the functions delivered.

This is a highly technical appendix describing the raw protocol you can use to communicate with and control the camera. This is of no interest unless you want to do that.

Using this protocol you can implement anything that the pipsshell, web interface to the camera application or manual generation tools can do. It is able to query application parameters, set them, issue commands, watch logging parameters and find out other details from the camera application. You can also get the camera to push images and event data to you, and collect image and event data (pull) from the camera.

Protocol

This protocol is run over TCP/IP to the camera, on port 3382. On OS release version 8 or later this port is firewalled off from the outside world, you will have to add a firewall rule to allow your remote application to access the camera. The protocol is a simple encapsulation of XML documents within a couple of boundaries. The XML must be correctly formed, if it is not then nothing in the message will be processed. The messages are not compressed, nor are they encrypted in any way.

Warning

Opening this port up may be a security risk to the camera.

The suggested way of working is to set up an ssh tunnel into the camera which will provide a way around the firewall without compromising it, and requires zero setup. This will also encrypt the data on the wire.

The XML may refer to some extra binary data which will follow the XML data.

The basic packet format is

Table 8.1. PIXI Packet Format

Name	Bytes	Content
Head	2	1. 0x0000 if there are no binary blobs in this data 2. 0x0001 if there are one or more binary blobs in the data
Length	2	XML Document length in bytes, as 2 byte, big endian value. Maximum length that the camera will accept is 16k. This is only the XML document portion.
Data	as required	Fully formed XML document adhering to schema below
Binary Length	0 or 4	Length of the binary blob if marked as present by the header.
Binary Data	0 or as required	Zero or more binary blobs. The position and size of the individual may be determined from the XML content.
End	4	0xffffffff

The link observes the following:

1. Multiple documents can be passed down the same link.

2. The link will stay open for a period of time, the camera will close it after 5 minutes of inactivity. To prevent this happening you can send heartbeat message which will be echoed back to you to show the camera is alive.

3. Either end can send a message unsolicited.

4. The camera responds to messages in the order in which the messages were received. This is on a per-connection basis, each connection can execute in parallel with others.

5. The camera will allow a maximum of 5 links at once.

Figure 8.1. Link with no heartbeat, camera will close when no command has been received for 5 minutes.

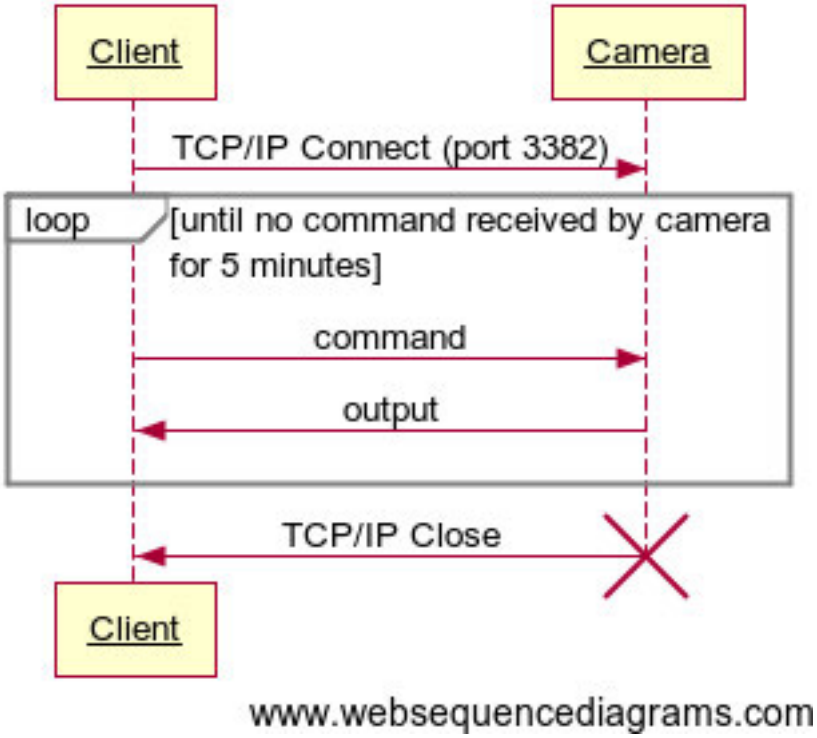
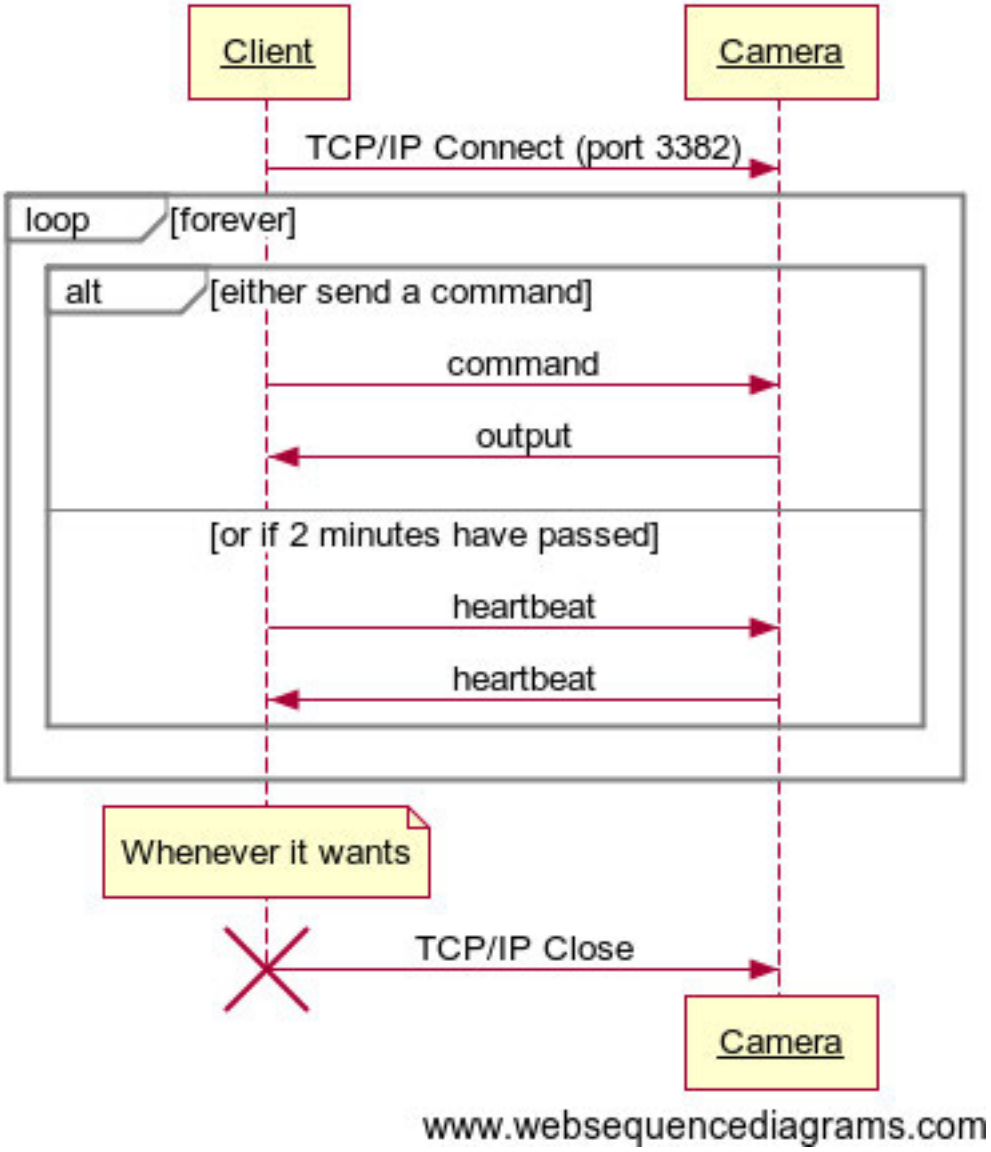


Figure 8.2. Link with heartbeat, client chooses when to end by closing the link.



Example documents

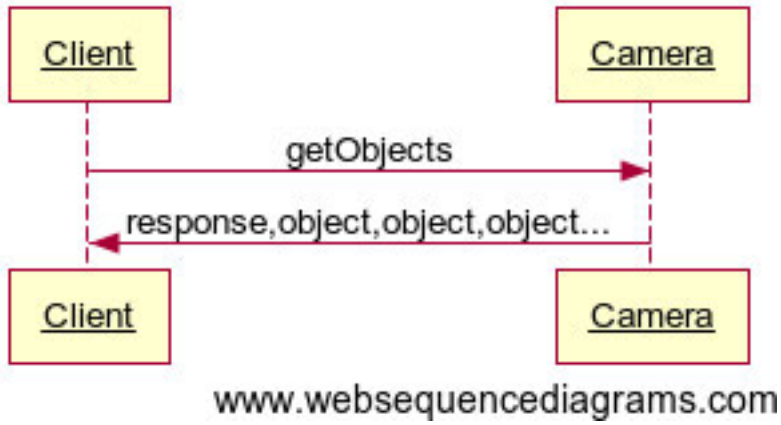
Here are few example documents to help you with composing your own messages and developing an application. In each case the PC/Instation/Handheld/other device is referred to as the Client, and the end that is implemented in the P382, P392+ and P492 is the Camera.

Note

All examples are "pretty printed" with space and formatting to make them easier to read. The camera will actually respond with documents without formatting, and for efficiency reasons I would suggest also sending unformatted documents.

Root objects

Figure 8.3. Get Root Objects - a list of all configureable objects is collected, some may have subobjects



This command to gets the root objects from the camera:

```
<?xml version="1.0"?>
<commands>
  <getObjects name=""/>
</commands>
```

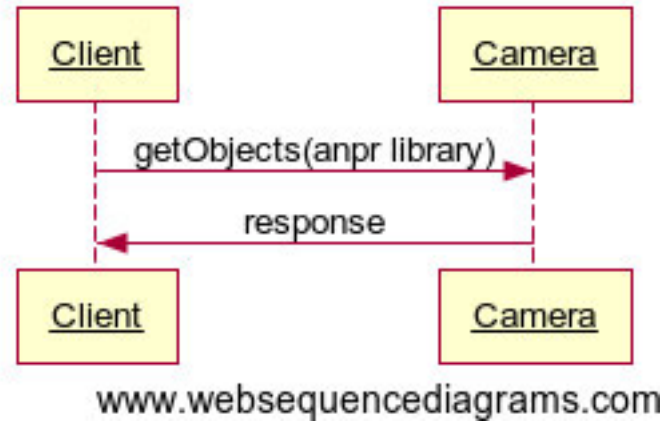
And the reply with the root objects

```
<?xml version="1.0"?>
<output>
  <response name="getObjects">
    <object/>
    <success>true</success>
  </response>
  <object name="acs">
    <longName>ACS - Access Control System</longName>
    <help>The Access Control System is an output module which sends vehicle details to an external computer for processing via the FTP protocol. It will ou
    <typeName/>
  </object>
  <object name="anpr">
    <longName>ANPR Vehicle Analyser</longName>
    <help>This module processes images to read the number plates in them.</help>
    <typeName/>
  </object>
  <object name="cam1">
    <longName>IR Camera</longName>
    <help>Controls for managing the camera and images that it takes</help>
    <typeName/>
  </object>
  <object name="cam2">
    <longName>Colour Camera</longName>
    <help>Controls for managing the camera and images that it takes</help>
    <typeName/>
  </object>
  <object name="client">
    <longName>Client vehicle event reporter</longName>
    <help>Reports individual vehicle events over the network to a client for live monitoring and diagnostics. Using the PIPS ClientView application you can
    <typeName/>
  </object>
  <object name="filter">
    <longName>Vehicle Filter</longName>
    <help>The filter system allows the system to look up number plates in a database. It is possible to filter out plates based on whether they are found o
    <typeName/>
  </object>
  <object name="fusion">
    <longName>Vehicle Fusion</longName>
    <help>The system may read multiple images of any given vehicle, and this subsystem merges those multiple vehicle reads into a single coherant result fo
    <typeName/>
  </object>
  <object name="imageFileOutput">
    <longName>Image File Outputter</longName>
    <help>Stores the images from the camera onto disk. These are just periodic images from the selected camera, like a video stream, not ones of particular
    <typeName/>
  </object>
  <object name="jpegService">
    <longName>JPEG Service</longName>
    <help>Controls the generation of JPEG images</help>
    <typeName/>
  </object>
  <object name="jtms">
    <longName>JTMS - Journey Time Measurement System</longName>
```

```
    <help>A system for delivering numberplates using very low bandwidth specifically for journey time measurement. Only minimal information is transmitted
    <typeName/>
  </object>
  <object name="metadata">
    <longName>Metadata store</longName>
    <help>This is purely an object for storing site metadata. The information stored in here is NOT used by the system, and is just for you to use when crea
    <typeName/>
  </object>
  <object name="netuis">
    <longName>Network user interface manager</longName>
    <help>The manager for the network user interfaces. These are the interfaces which the web and shell connect to.</help>
    <typeName/>
  </object>
  <object name="pci">
    <longName>PCI Interface to the cameras</longName>
    <help>Low level controls for the PCI interface talking to the cameras. This is for debugging and testing only, you can break your camera by playing.</he
    <typeName/>
  </object>
  <object name="pciSource">
    <longName>PCI Camera Source</longName>
    <help>The internal camera subsystem, connected via PCI to the processor. These controls are mostly for diagnostics.</help>
    <typeName/>
  </object>
  <object name="power">
    <longName>Power Manager</longName>
    <help>Power Management subsystem, monitoring the power coming into the system and dealing with power down when the power is cut.</help>
    <typeName/>
  </object>
  <object name="selector">
    <longName>Vehicle Image Selector</longName>
    <help>Selects images from the hardware platefinder for further analysis and ANPR by the rest of the software.</help>
    <typeName/>
  </object>
  <object name="sensors">
    <longName>Hardware Monitoring sensors</longName>
    <help>This module periodically polls the sensor values</help>
    <typeName/>
  </object>
  <object name="stdout">
    <longName>Console Logger</longName>
    <help>The logger which reports information to the standard out (stdout) device (usually the console). This is probably of no use to you as you probably
    <typeName/>
  </object>
  <object name="system">
    <longName>System Lists</longName>
    <help>A debugging object for collecting lists of objects and finding out their details</help>
    <typeName/>
  </object>
  <object name="trig">
    <longName>Trigger Control</longName>
    <help>External trigger control, for when you have wired an external vehicle detector into the camera.</help>
    <typeName/>
  </object>
  <object name="ves">
    <longName>VES - Violation Enforcement System</longName>
    <help>Highly configurable system with many options. Please refer to VES Software Interface Specification</help>
    <typeName/>
  </object>
</output>
```

Subobjects

Figure 8.4. Get subobjects of an object - a list of all subobjects is collected, some may have subobjects. The list may be empty, as in the example



A command to get a subobject's objects

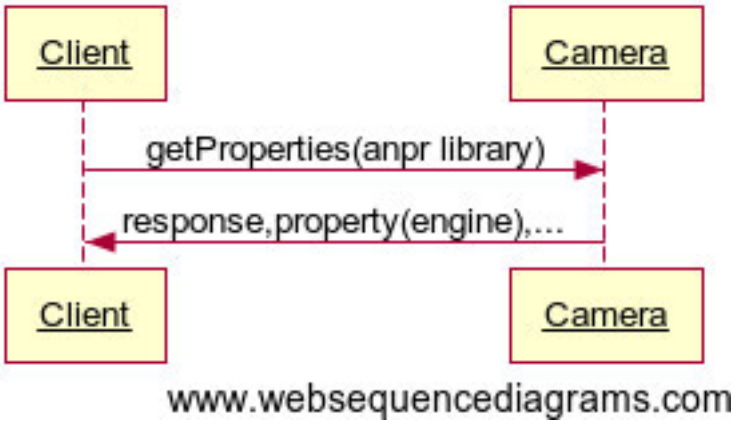
```
<?xml version="1.0"?>
<commands>
  <getObjects name="anpr library"/>
</commands>
```

And the reply, with no subobjects

```
<?xml version="1.0"?>
<output>
  <response name="getObjects">
    <object>anpr library</object>
    <success>false</success>
  </response>
</output>
```

Properties

Figure 8.5. Get properties of an object - a list of all the properties of an object. The list may be empty.



And now getting the properties of an object

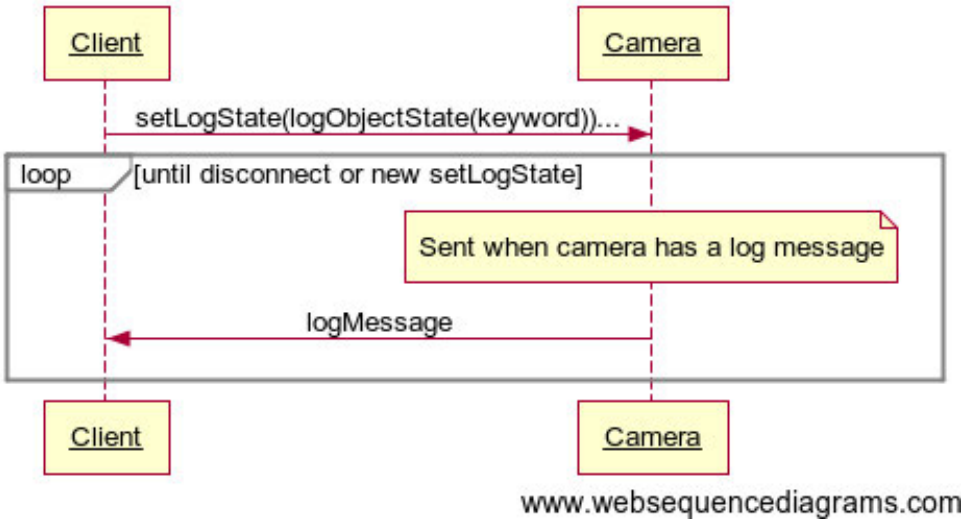
```
<?xml version="1.0"?>
<commands>
  <getProperties name="anpr library"/>
</commands>
```

And the reply, with just one property

```
<?xml version="1.0"?>
<output>
  <response name="getProperties">
    <object>anpr library</object>
    <success>true</success>
  </response>
  <property name="engine">
    <longName>Plate Reading Engine</longName>
    <default>none</default>
    <type>6</type>
    <current>libcardet.p382.so.1.2212.UK_IE</current>
    <help>The filename of the libcardet plate reading engine in use</help>
    <qualifier/>
  </property>
</output>
```

Logging

Figure 8.6. Start some logging. Asynchronous messages will be sent back by the Camera containing the log messages



Now setting up logging (note, no immediate reply)

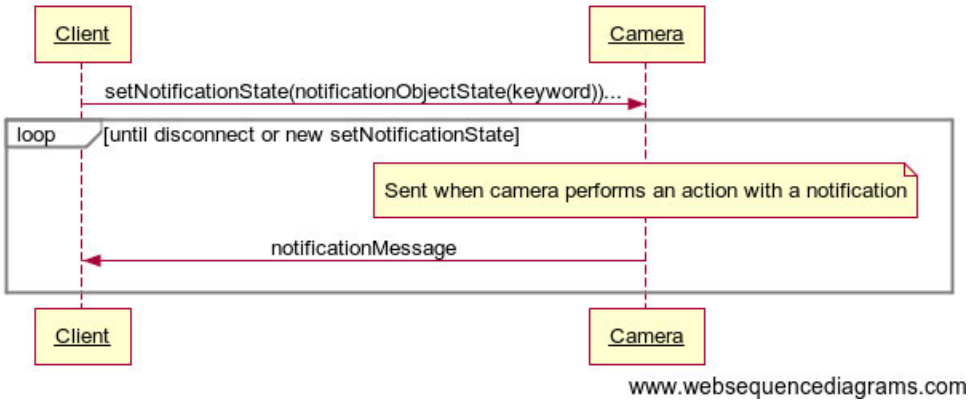
```
<?xml version="1.0"?>
<commands>
  <setLogState name="stdout">
    <logObjectState name="acs">
      <keywordState name="disk">
        <onoff>on</onoff>
      </keywordState>
      <keywordState name="events">
        <onoff>off</onoff>
      </keywordState>
      <keywordState name="filenames">
        <onoff>off</onoff>
      </keywordState>
      <keywordState name="ftp">
        <onoff>off</onoff>
      </keywordState>
      <keywordState name="inevents">
        <onoff>off</onoff>
      </keywordState>
      <keywordState name="overviews">
        <onoff>off</onoff>
      </keywordState>
    </logObjectState>
    <logObjectState name="anpr">
      <keywordState name="latency">
        <onoff>off</onoff>
      </keywordState>
      <keywordState name="noreads">
        <onoff>off</onoff>
      </keywordState>
      <keywordState name="patches">
        <onoff>off</onoff>
      </keywordState>
      <keywordState name="performance">
        <onoff>on</onoff>
      </keywordState>
      <keywordState name="reads">
        <onoff>on</onoff>
      </keywordState>
    </logObjectState>
    <logObjectState name="cam1exposure">
      <keywordState name="averages">
        <onoff>off</onoff>
      </keywordState>
      <keywordState name="brightness">
        <onoff>off</onoff>
      </keywordState>
      <keywordState name="processing">
        <onoff>off</onoff>
      </keywordState>
      <keywordState name="vehicles">
        <onoff>off</onoff>
      </keywordState>
      <keywordState name="voting">
        <onoff>off</onoff>
      </keywordState>
```

```
</logObjectState>
<logObjectState name="client">
  <keywordState name="connections">
    <onoff>off</onoff>
  </keywordState>
  <keywordState name="latency">
    <onoff>off</onoff>
  </keywordState>
  <keywordState name="overviews">
    <onoff>off</onoff>
  </keywordState>
  <keywordState name="vehicles">
    <onoff>off</onoff>
  </keywordState>
</logObjectState>
<logObjectState name="filter">
  <keywordState name="incoming">
    <onoff>off</onoff>
  </keywordState>
  <keywordState name="matches">
    <onoff>off</onoff>
  </keywordState>
  <keywordState name="notification">
    <onoff>off</onoff>
  </keywordState>
</logObjectState>
<logObjectState name="fusion">
  <keywordState name="best">
    <onoff>off</onoff>
  </keywordState>
  <keywordState name="incoming">
    <onoff>off</onoff>
  </keywordState>
  <keywordState name="latency">
    <onoff>off</onoff>
  </keywordState>
  <keywordState name="matches">
    <onoff>off</onoff>
  </keywordState>
  <keywordState name="notification">
    <onoff>off</onoff>
  </keywordState>
  <keywordState name="resetting">
    <onoff>off</onoff>
  </keywordState>
  <keywordState name="timers">
    <onoff>off</onoff>
  </keywordState>
</logObjectState>
<logObjectState name="hwtrigger">
  <keywordState name="latency">
    <onoff>off</onoff>
  </keywordState>
</logObjectState>
<logObjectState name="imageFileOutput">
  <keywordState name="outputName">
    <onoff>off</onoff>
  </keywordState>
</logObjectState>
<logObjectState name="jpegService">
  <keywordState name="HWorSW">
    <onoff>off</onoff>
  </keywordState>
</logObjectState>
<logObjectState name="jtms">
  <keywordState name="connection">
    <onoff>off</onoff>
  </keywordState>
  <keywordState name="disk">
    <onoff>off</onoff>
  </keywordState>
  <keywordState name="incoming">
    <onoff>off</onoff>
  </keywordState>
  <keywordState name="timing">
    <onoff>off</onoff>
  </keywordState>
</logObjectState>
<logObjectState name="pciInterface">
  <keywordState name="setup">
    <onoff>off</onoff>
  </keywordState>
</logObjectState>
<logObjectState name="pciSource">
  <keywordState name="capColour">
    <onoff>off</onoff>
  </keywordState>
  <keywordState name="capIR">
    <onoff>on</onoff>
  </keywordState>
  <keywordState name="initialisation">
    <onoff>off</onoff>
  </keywordState>
</logObjectState>
<logObjectState name="power">
  <keywordState name="state">
```

```
        <onoff>off</onoff>
      </keywordState>
    </logObjectState>
    <logObjectState name="selector">
      <keywordState name="detects">
        <onoff>off</onoff>
      </keywordState>
      <keywordState name="latency">
        <onoff>off</onoff>
      </keywordState>
      <keywordState name="multi">
        <onoff>off</onoff>
      </keywordState>
    </logObjectState>
    <logObjectState name="videoStore">
      <keywordState name="fails">
        <onoff>off</onoff>
      </keywordState>
    </logObjectState>
    <logObjectState name="viewfinder">
      <keywordState name="connections">
        <onoff>off</onoff>
      </keywordState>
      <keywordState name="sessions">
        <onoff>off</onoff>
      </keywordState>
    </logObjectState>
  </setLogState>
</commands>
```

Notifications

Figure 8.7. Start notification messages. Asynchronous messages will be sent back by the Camera containing the notification messages of the requested events



To enable notifications, send a setNotificationState message listing the notifications that you wish to enable. Note that there will not be an immediate reply from this message.

```
<?xml version="1.0"?>
<commands>
 <setNotificationState name="self">
  <notificationObjectState name="acs">
   <keywordState name="fileComplete">
    <onoff>on</onoff>
   </keywordState>
   <keywordState name="datasetComplete">
    <onoff>on</onoff>
   </keywordState>
  </notificationObjectState>
 </setNotificationState>
</commands>
```

When an event for which you have registered a notification occurs, you will now receive an unsolicited notificationMessage

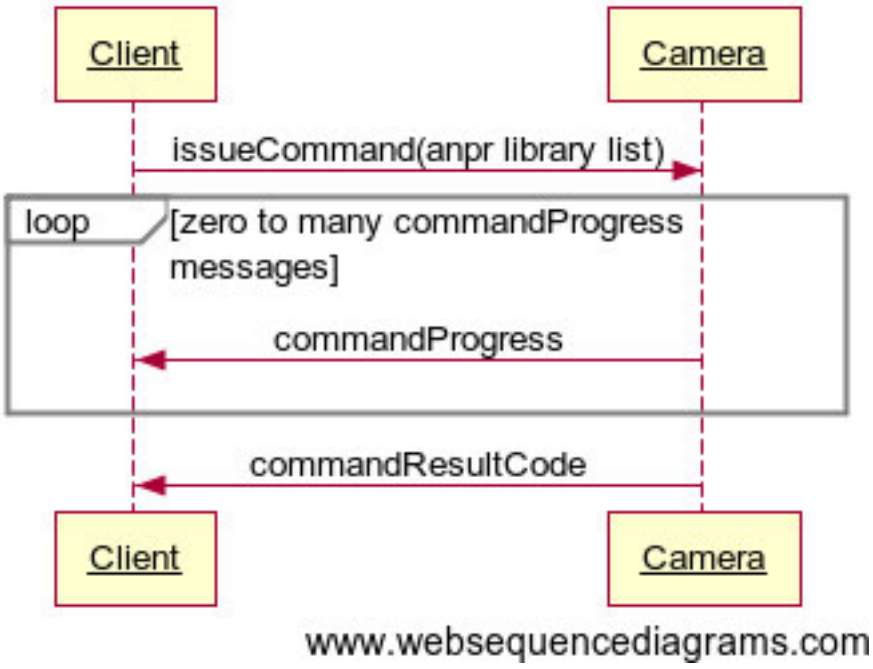
```
<?xml version="1.0"?>
<output>
 <notificationMessage>
  <source>acs</source>
  <type>fileComplete</type>
  <timeDate>2013-03-11T13:36:51.989154</timeDate>
  <destpath>ftp://10.20.13.120/11662/0008764A.lpr</destpath>
  <eventId>513dddf20008764a</eventId>
 </notificationMessage>
</output>
```

All notifications will have the source, type, and timeDate values, indicating when the notification was triggered, and what triggered it. Each notification type may have additional properties that are specific to that notification type. The available notifications are:

Platforms	Source	Type	Description
All	acs	datasetComplete	Provides notification of the successful transfer of an entire data-set via ACS. This notification has an additional property of 'eventId' which identifies the event the data transferred relates to.
All	acs	fileComplete	Provides notification of the successful completion of the transfer of an individual file via ACS. The notification will have an additional 'eventId' property which indicates the event that the file relates to. The property 'destpath' includes the full destination URL of the file which has now been transferred.

Issue Command

Figure 8.8. Issue a command and receive the responses.



A command, which has 3 replies. Note: issueCommand will probably be deprecated in the future

```
<?xml version="1.0"?>
<commands>
  <issueCommand>anpr library list</issueCommand>
</commands>
```

The output, as the command is processed

```
<?xml version="1.0"?>
<output>
  <commandProgress>Available cardet libraries</commandProgress>
</output>

<?xml version="1.0"?>
<output>
  <commandProgress>UK, Ireland, France (version 2212) - libcardet.p382.so.1.2212.UK_IE</commandProgress>
</output>
```

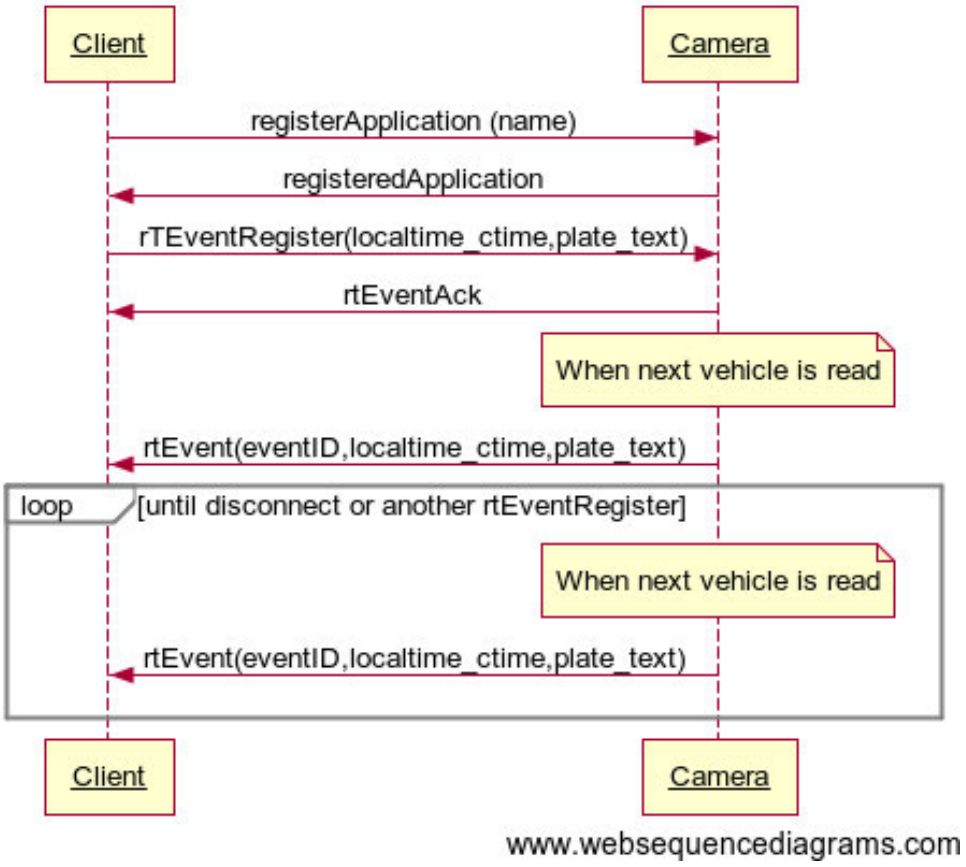
Then the result, one (and only one) of which is guaranteed to arrive

```
<?xml version="1.0"?>
<output>
  <commandResultCode>OK</commandResultCode>
```

```
</output>
```

Event data

Figure 8.9. Connect to the camera and get events as it reads vehicles.



Here we need to register the application, prior to setting up and receiving events as they occur. We are receiving minimal information, just what would be required for say a journey time measurement system. You can request as much data as you like in the rtEventRegister, and it will all be sent on every event.

First we register the application.

```
<?xml version="1.0"?>
<commands>
  <registerApplication name="test">
    <description>A test application</description>
  </registerApplication>
</commands>
```

and receive a success response

```
<?xml version="1.0"?>
<output>
  <response name="registerApplication">
    <object>test</object>
    <success>true</success>
  </response>
  <registeredApplication/>
</output>
```

And then we request real time events

```
<?xml version="1.0"?>
<commands>
  <rtEventRegister>
    <eventDetail>localtime_ctime</eventDetail>
    <eventDetail>plate_text</eventDetail>
  </rtEventRegister>
</commands>
```

Which come back like follows when they occur. Note the details *are not* in the same order as when they were requested.

```
<?xml version="1.0"?>
```

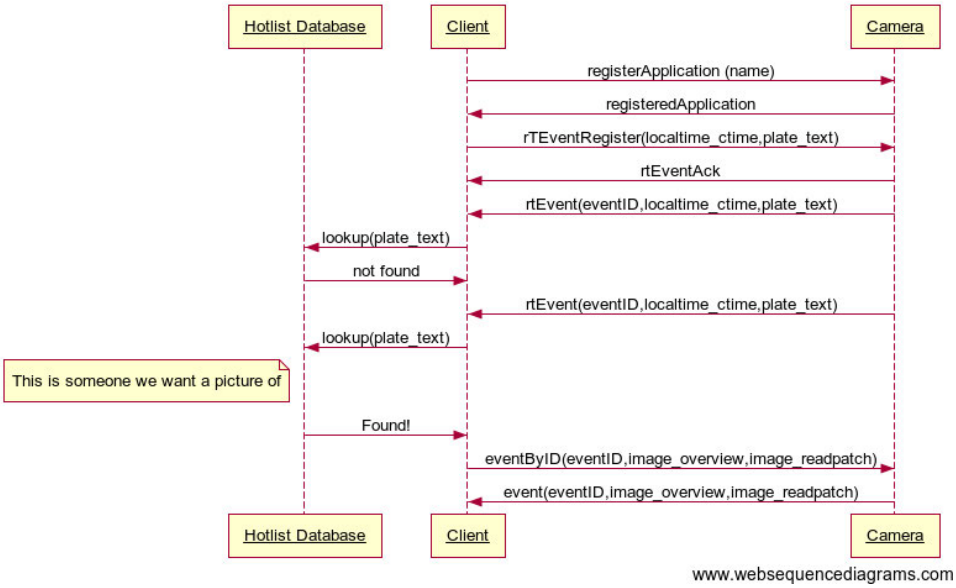
```
<output>
  <rtEvent>
    <eventID>4df5ee07000d6ae9</eventID>
    <eventData name="plate_text">
      <data>FJ05PKV</data>
    </eventData>
    <eventData name="localtime_ctime">
      <data>1308219250</data>
    </eventData>
  </rtEvent>
</output>
```

Alternatively, when registering to receive events you can specify an nlog parameter. This specifies a maximum number of events to buffer on the camera if the client application is not currently connected. This can be used to prevent data-loss should client applications disconnect.

```
<xi:include></xi:include>
```

Event data with pull

Figure 8.10. Here we are collecting (pulling) certain vehicle details when a particular vehicle is found.



As an extension to the section called “Event data” [109], here we have a database of vehicles we are particularly interested in and are requesting images for just particular vehicles. This will save bandwidth over pulling data for all vehicles.

The new message is an event request

```
<?xml version="1.0"?>
<commands>
  <eventByID>
    <eventID>4df5ee07000d6ae9</eventID>
    <eventDetail>image_overview</eventDetail>
    <eventDetail>image_readpatch</eventDetail>
  </eventByID>
</commands>
```

which gets a response indicating two binary data blobs are following the XML which can be extracted into JPEG files (JFIF).

```
<?xml version="1.0"?>
<output>
  <rtEvent>
    <eventID>4df5ee07000d6ae9</eventID>
    <eventData name="image_overview">
      <length>30412</length>
      <offset>0</offset>
    </eventData>
    <eventData name="image_readpatch">
      <length>4972</length>
      <offset>30412</offset>
    </eventData>
  </rtEvent>
</output>
```

PIXI Documents

The documents you can send across the link are in XML, as defined by the following schemas. You can send documents from the command.xsd schema, and expect to receive documents from the output.xsd schema. The definitive versions of the schemas are found on the camera under the following URLs:

1. `https://camera.ip.address/spikeapp/commands.xsd` - for commands to send to the camera

2. `https://camera.ip.address/spikeapp/output.xsd` - for output from the camera

3. `https://camera.ip.address/spikeapp/common.xsd` - a common file, included by both the other files

These are the definitive versions of these files, and should always be used, not any other versions. They are not generated on the fly, and will only change when software on the camera is changed.

The schemas *will* change between releases of the camera software and are not currently written as extensible. Adding the necessary text into the xsds to make them extensible also makes them confusing, so we have left it out, but consider that they will always be extended in logical ways - for example new parameters, result fields or command. We will maintain backwards compatibility, but rigid checks against historic schemas will fail.

There are a lot of correctly formed documents according to the schemas that are error conditions. For example asking for a non-existant object... for example it is required that you ask the camera for it's objects to verify that the object you want to talk about does exist.

commands.xsd

```
<?xml vers
<xsd:schem
  <xsd:inc
  <xsd:ele
  <xsd:com
    <xsd:s
      <xsd
 <xsd:elem
 <xsd:elem
 <xsd:elem
 <xsd:elem
 <xsd:elem
 <xsd:elem
 <xsd:elem
 <xsd:elem
 <xsd:elem
 <xsd:elem
 <xsd:elem
 <xsd:elem
 <xsd:elem
 <xsd:elem
 <xsd:elem
 <xsd:elem
 <xsd:elem
 <xsd:elem
 <xsd:elem
 <xsd:elem
 <xsd:elem
 <xsd:elem
 <xsd:elem
 <xsd:elem
 <xsd:elem
 <xsd:elem
 <xsd:elem
      </xs
    </xsd:
  </xsd:co

  <!-- **

  <xsd:com
  <!-- Res

  <xsd:com
    <!-- G
    <!-- R
    <xsd:a
  </xsd:co

  <xsd:com
    <!-- O
    <!-- R
    <xsd:a
    <xsd:a
  </xsd:co

  <xsd:com
    <!-- O
    <!-- R
```

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

```
objects -->
```

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

```
    <xsd:a
  </xsd:co

  <xsd:com
    <!-- O
    <!-- R
    <xsd:s
      <xsd
    </xsd:
    <xsd:a
  </xsd:co
  <xsd:com
    <xsd:s
      <xsd
<xsd:attr
      </xs
    </xsd:
  </xsd:co

  <xsd:com
    <!-- T                                                          made available -->
    <!-- R
    <xsd:s
      <xsd
      <!--
    </xsd:
  </xsd:co

  <xsd:com
  <!-- Get
  <!-- Res

  <xsd:com
  <!-- Get
  <!-- Res

  <xsd:com
    <!-- G
    <xsd:a
  </xsd:co

  <xsd:com
  <!-- Get                                                          objects. Also no nesting here -->
  <!-- Res

  <xsd:com
    <!-- G
    <!-- R
    <xsd:a
  </xsd:co

  <xsd:com
    <!-- G
    <!-- R
    <xsd:a
  </xsd:co

  <xsd:com
  <!-- Get
  <!-- Res

  <xsd:com
    <!-- G
    <!-- R
    <xsd:a
  </xsd:co

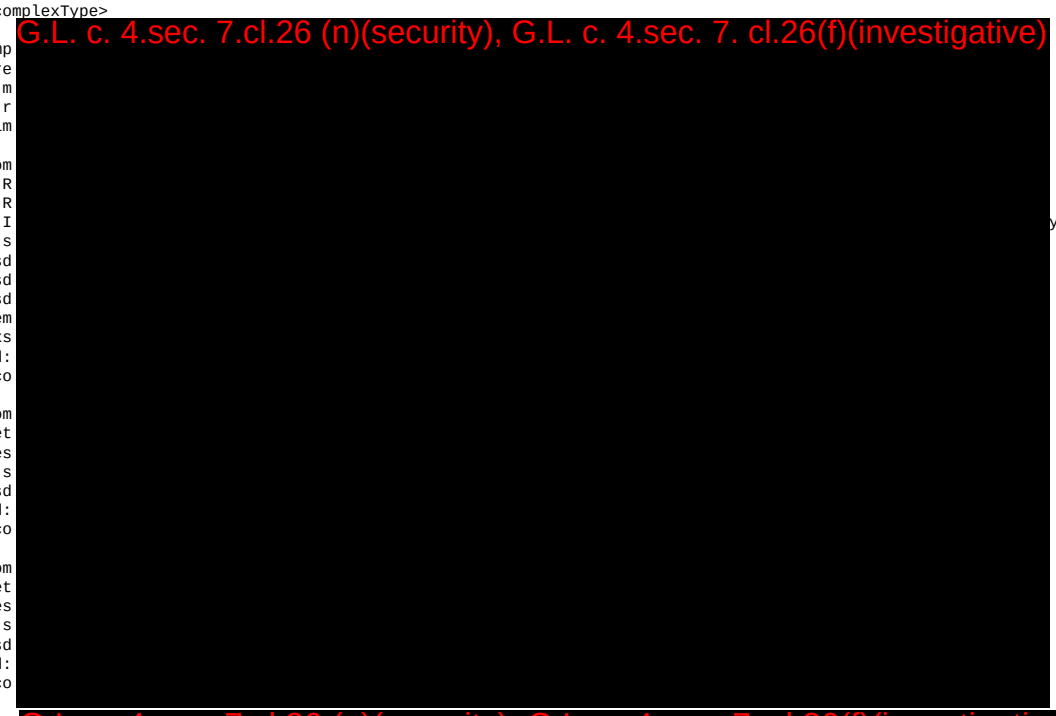
  <xsd:com
    <!-- G
    <!-- R
    <xsd:a
  </xsd:co

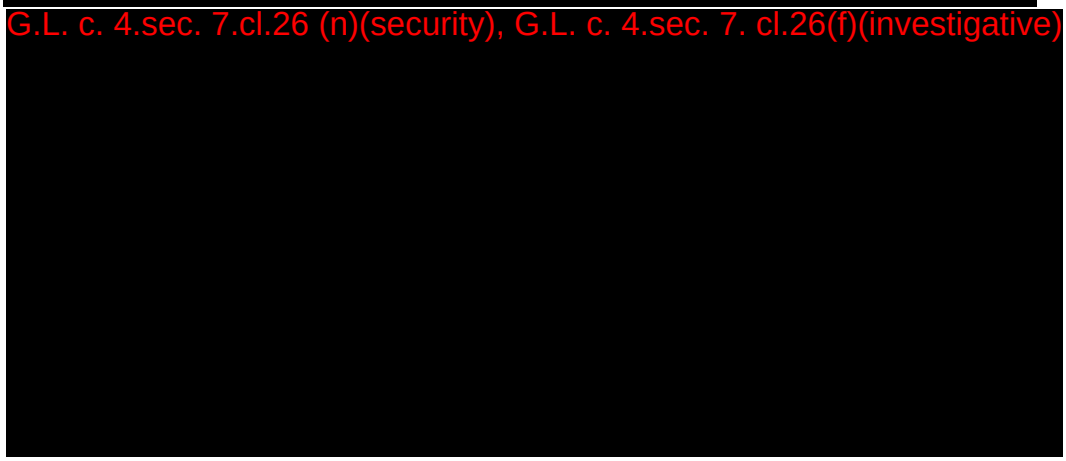
  <xsd:com
    <!-- S
    <!-- T
    <xsd:s
      <xsd
<xsd:elem
      </xs
    </xsd:
    <xsd:a
  </xsd:co

  <xsd:com
    <!-- S
    <!-- T
    <xsd:s
      <xsd
<xsd:elem
      </xs
    </xsd:
    <xsd:a
  </xsd:co

  <xsd:com
```

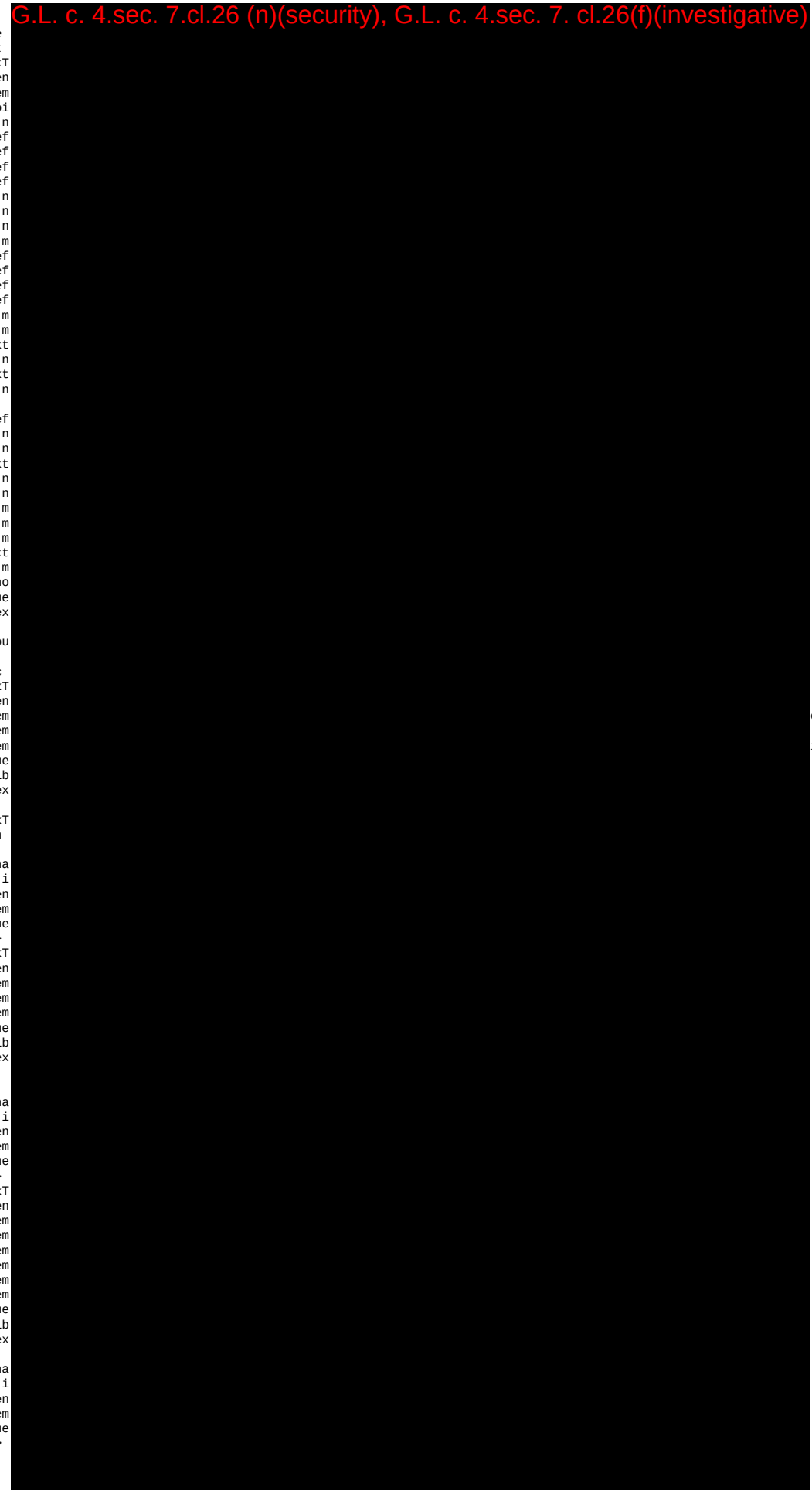






output.xsd

```
<?xml version="1.0" encoding="UTF-8" ?>
<xsd:schema  xmlns:xsd="http://www.w3.org/2001/XMLSchema">
```




```
 <xsd:include
 <xsd:element
 <xsd:complexT
   <xsd:sequen
     <xsd:elem
     <xsd:choi
<xsd:element n
<xsd:group ref
<xsd:group ref
<xsd:group ref
<xsd:group ref
<xsd:element n
<xsd:element n
<xsd:element n
<xsd:element m
<xsd:group ref
<xsd:group ref
<xsd:group ref
<xsd:group ref
<xsd:element m
<xsd:element m
<!-- This next
<xsd:element n
<!-- This next
<xsd:element n

<xsd:group ref
<xsd:element n
<xsd:element n
<!-- This next
<xsd:element n
<xsd:element n
<xsd:element m
<xsd:element m
<xsd:element m
<!-- This next
<xsd:element m
     </xsd:cho
   </xsd:seque
 </xsd:complex

 <!-- ** Outpu

 <!-- Generic
 <xsd:complexT
   <xsd:sequen
     <xsd:elem                                                    obvious -->
     <xsd:elem
     <xsd:elem                                                    ish text describing failure -->
   </xsd:seque
   <xsd:attrib                                                    -->
 </xsd:complex

 <xsd:complexT
 <!-- Sent in

 <xsd:group na
   <!-- Sent i
   <xsd:sequen
     <xsd:elem
   </xsd:seque
 </xsd:group>
 <xsd:complexT
   <xsd:sequen
     <xsd:elem
     <xsd:elem
     <xsd:elem
   </xsd:seque
   <xsd:attrib
 </xsd:complex


 <xsd:group na
   <!-- Sent i
   <xsd:sequen
     <xsd:elem
   </xsd:seque
 </xsd:group>
 <xsd:complexT
   <xsd:sequen
     <xsd:elem
     <xsd:elem
     <xsd:elem
     <xsd:elem
     <xsd:elem
     <xsd:elem
   </xsd:seque
   <xsd:attrib
 </xsd:complex

 <xsd:group na
   <!-- Sent i
   <xsd:sequen
     <xsd:elem
   </xsd:seque
 </xsd:group>
```

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

```
<xsd:complexType
  <xsd:sequence>
    <xsd:element
    <xsd:element
    <xsd:element
  </xsd:sequence
  <xsd:attribute
</xsd:complexTyp
<xsd:complexType
  <xsd:sequence>
    <xsd:element
    <xsd:element
    <xsd:element
    <xsd:element
    <xsd:element
  </xsd:sequence
  <xsd:attribute
</xsd:complexTyp

<xsd:group name=
  <!-- Sent in r
  <!-- Only vali
  <xsd:sequence>
    <xsd:element
  </xsd:sequence
</xsd:group>
<xsd:complexType
  <xsd:sequence>
    <xsd:element
    <xsd:element
    <xsd:element
  </xsd:sequence
  <xsd:attribute
</xsd:complexTyp

<xsd:complexType
  <!-- Zero or m
  <xsd:simpleCon
    <xsd:extensi
  </xsd:simpleCo
</xsd:complexTyp

<xsd:complexType
  <!-- One of th
  <xsd:simpleCon
    <xsd:extensi
  </xsd:simpleCo
</xsd:complexTyp


<xsd:complexType
  <!-- Sent in r
  <xsd:sequence
    <xsd:element
  </xsd:sequence
</xsd:complexTyp
<xsd:complexType
  <xsd:simpleCon
    <xsd:extensi
<xsd:attribute na
    </xsd:extens
  </xsd:simpleCo
</xsd:complexTyp

<xsd:complexType
  <!-- Sent in r
  <xsd:sequence>
    <xsd:element
    <xsd:element
  </xsd:sequence
  <xsd:attribute
</xsd:complexTyp

<xsd:group name=
  <!-- Sent in r
  <xsd:sequence>
    <xsd:element
  </xsd:sequence
</xsd:group>
<xsd:complexType
  <xsd:sequence>
    <xsd:element
    <xsd:element
    <xsd:element
  </xsd:sequence
  <xsd:attribute
</xsd:complexTyp

<xsd:group name=
  <!-- Sent in r
  <xsd:sequence>
    <xsd:element
  </xsd:sequence
</xsd:group>
<xsd:complexType
  <!-- NOT the s
```

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

```
    <xsd:attri
  </xsd:comple

  <xsd:group n
    <xsd:seque
      <xsd:ele
    </xsd:sequ
  </xsd:group>
  <xsd:complex
    <xsd:seque
      <xsd:ele
    </xsd:sequ
    <xsd:attri
  </xsd:comple

  <xsd:group n
    <xsd:seque
      <xsd:ele
    </xsd:sequ
  </xsd:group>
  <xsd:complex
    <xsd:seque
      <xsd:ele
    </xsd:sequ
    <xsd:attri
  </xsd:comple

  <xsd:complex
    <xsd:simpl
      <xsd:ext
    </xsd:simp
  </xsd:comple

  <xsd:complex
    <xsd:attri
  </xsd:comple

  <xsd:complex
    <!-- An un
    <xsd:seque
      <xsd:ele
      <xsd:ele
      <xsd:ele
      <xsd:ele
    </xsd:sequ
  </xsd:comple

  <xsd:complex                                                
```

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

```
      <xsd:element
      <xsd:element
      <xsd:element
      <xsd:element
      <xsd:element
      <xsd:element
      <xsd:element
    </xsd:sequence
    <xsd:attribute
  </xsd:complexTyp

  <xsd:complexType
    <xsd:sequence>
      <xsd:element
      <xsd:element                                                    w current state -->
      <xsd:element
    </xsd:sequence
    <xsd:attribute
  </xsd:complexTyp

  <xsd:complexType

  <xsd:complexType
    <xsd:sequence>
      <xsd:element
    </xsd:sequence
    <xsd:attribute
  </xsd:complexTyp

  <xsd:complexType
    <xsd:sequence>
      <xsd:element                                                    >
    </xsd:sequence
    <xsd:attribute
  </xsd:complexTyp
</xsd:schema>
```

commo

```
<?xml version="1.0
<xsd:schema  xmlns
  <!-- Descriptive
  <xsd:simpleType
    <xsd:restricti
  </xsd:simpleType
  <xsd:simpleType
    <xsd:restricti
  </xsd:simpleType
  <xsd:simpleType
    <xsd:restricti
  </xsd:simpleType
  <xsd:simpleType
    <xsd:restricti
  </xsd:simpleType
  <xsd:simpleType
    <xsd:restricti
  </xsd:simpleType
  <xsd:simpleType
    <xsd:restricti
  </xsd:simpleType
  <xsd:simpleType
    <xsd:restricti
  </xsd:simpleType
  <xsd:simpleType
    <xsd:restricti
  </xsd:simpleType
  <xsd:simpleType
    <xsd:restricti
  </xsd:simpleType
  <xsd:simpleType
    <xsd:restricti
  </xsd:simpleType
  <xsd:simpleType
    <xsd:restricti
  </xsd:simpleType
  <xsd:simpleType
    <xsd:restricti
  </xsd:simpleType
  <xsd:simpleType
    <xsd:restricti
  </xsd:simpleType
  <xsd:simpleType
    <xsd:restricti
  </xsd:simpleType
  <xsd:simpleType
    <xsd:restricti
  </xsd:simpleType
  <xsd:simpleType
    <xsd:restricti
  </xsd:simpleType
  <xsd:simpleType
    <xsd:restricti
  </xsd:simpleType
  <xsd:simpleType
    <xsd:restricti
  </xsd:simpleType
  <xsd:simpleType
    <!-- A list of
    <xsd:restricti
  </xsd:simpleType

  <!-- Types -->
  <xsd:simpleType
    <xsd:restricti
      <xsd:pattern
    </xsd:restrict
  </xsd:simpleType

  <xsd:simpleType
    <xsd:restricti
```

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

```
    <xsd:patter
  </xsd:restric
</xsd:simpleTyp

<xsd:simpleType
  <xsd:restrict
    <xsd:patter
  </xsd:restric
</xsd:simpleTyp

<xsd:simpleType
  <xsd:restrict
    <xsd:patter
  </xsd:restric
</xsd:simpleTyp

<xsd:simpleType
  <xsd:restrict
    <xsd:patter
  </xsd:restric
</xsd:simpleTyp

<xsd:simpleType
  <xsd:restrict
    <xsd:enumer
    <xsd:enumer
    <xsd:enumer
    <xsd:enumer                                                    te the save anyway -->
    <xsd:enumer
    <xsd:enumer
  </xsd:restric
</xsd:simpleTyp

<xsd:simpleType
  <xsd:restrict
    <xsd:enumer
    <xsd:enumer
  </xsd:restric
</xsd:simpleTyp

<xsd:simpleType
  <xsd:restrict
    <xsd:enumer
    <xsd:enumer
    <xsd:enumer
    <xsd:enumer
    <xsd:enumer
    <xsd:enumer
    <xsd:enumer
    <xsd:enumer
    <xsd:enumer
    <xsd:enumer
    <xsd:enumer
    <xsd:enumer
    <xsd:enumer
    <xsd:enumer
    <xsd:enumer
    <xsd:enumer
    <xsd:enumer
    <xsd:enumer
  </xsd:restric
</xsd:simpleTyp

<xsd:simpleType
  <xsd:restrict
    <xsd:enumer
    <xsd:enumer
    <xsd:enumer
    <xsd:enumer
    <xsd:enumer
  </xsd:restric
</xsd:simpleTyp

<xsd:simpleType
  <xsd:restrict
    <xsd:enumer
    <xsd:enumer
    <xsd:enumer
  </xsd:restric
</xsd:simpleTyp

<xsd:simpleType
  <xsd:restrict
    <xsd:enumer
    <xsd:enumer
  </xsd:restric
</xsd:simpleTyp

<xsd:simpleType
  <xsd:restrict
    <xsd:enumer
    <xsd:enumer
  </xsd:restric
</xsd:simpleTyp

<!-- Complex st
<xsd:complexTyp
  <xsd:sequence
```

```
      <xsd:elemen
    </xsd:sequenc
    <xsd:attribut
  </xsd:complexTy
  <xsd:complexTyp
    <xsd:sequence
      <xsd:elemen
    </xsd:sequenc
    <xsd:attribut
  </xsd:complexTy

  <xsd:complexTyp
    <xsd:sequence
      <xsd:elemen
    </xsd:sequenc
    <xsd:attribut
  </xsd:complexTy

  <xsd:simpleType
    <xsd:restrict
      <xsd:enumer
      <xsd:enumer
    </xsd:restric
  </xsd:simpleTyp
</xsd:schema>
```

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

List of

This is a list of all the eventDetails available on the camera and a description of them. The "image" types will return a length and offset, whereas the other types return data.

PIXI values image_*

The images from the cameras. Not all images are always available in all circumstances.

Platforms	Name	Type	Description
All	image_overview	image	The image from the overview taken at the same time as the plate was read, or at the same time as the trigger depending upon settings.
All	image_analysis	image	The full image from the camera from which the number plate was read. Usually this will be an infrared image.
All	image_readpatch	image	The image of the number plate, cropped so that the number plate is all that is visible.
All	image_hazoverview	image	The image from the overview taken at the same time as the hazard plate was read, or at the same time as the trigger depending upon settings.
All	image_hazanalysis	image	The full image from the camera from which the hazard plate was read. Usually this will be an infrared image.
All	image_hazreadpatch	image	The image of the hazard plate, cropped so that the hazard plate is all that is visible.

PIXI values cam_*

The camera detail of the plate the vehicle was read on

Platforms	Name	Type	Description
All	cam_shutter	xsd:integer	The shutter setting used for this image
All	cam_gain	xsd:integer	The gain setting used for this image
All	cam_cam0	xsd:integer	The camera number (starting at zero)

Platforms	Name	Type	Description
All	cam_cam1	xsd:integer	The camera number (starting at one)
All	cam_seq0	xsd:integer	The sequence setting (starting at zero)
All	cam_seq1	xsd:integer	The sequence setting (starting at one)

PIXI values hazcam_*

The camera detail of the hazard plate the vehicle was read on

Platforms	Name	Type	Description
All	hazcam_shutter	xsd:integer	The shutter setting used for this image
All	hazcam_gain	xsd:integer	The gain setting used for this image
All	hazcam_cam0	xsd:integer	The camera number (starting at zero)
All	hazcam_cam1	xsd:integer	The camera number (starting at one)
All	hazcam_seq0	xsd:integer	The sequence setting (starting at zero)
All	hazcam_seq1	xsd:integer	The sequence setting (starting at one)

PIXI values event_*

Unique information about delivery event, Not usable under all circumstances

Platforms	Name	Type	Description
All	event_id	xsd:integer	The Event id, which uniquly identifies the event

PIXI values file_*

Associated file. Not useable under all circumstances. Primarily for use in ACS's LPR files.

Platforms	Name	Type	Description
All	file_context1_file	xsd:string	The filename of context image 1
All	file_context2_file	xsd:string	The filename of context image 2
All	file_context3_file	xsd:string	The filename of context image 3
All	file_context4_file	xsd:string	The filename of context image 4
All	file_context5_file	xsd:string	The filename of context image 5
All	file_context6_file	xsd:string	The filename of context image 6
All	file_context7_file	xsd:string	The filename of context image 7
All	file_context8_file	xsd:string	The filename of context image 8
All	file_lpr	xsd:string	The lpr text filename
All	file_ir	xsd:string	The IR image filename
All	file_hazir	xsd:string	The hazard IR image filename
All	file_patch	xsd:string	The patch image filename
All	file_hazpatch	xsd:string	The hazard patch image filename
All	file_path	xsd:string	The transfer path (which is not prepended to the other filenames)
All	file_overview	xsd:string	The wide angle, overview image filename

Platforms	Name	Type	Description
All	file_hazoverview	xsd:string	The hazard wide angle, overview image filename

PIXI values hazard_*

The read hazard plate from the vehicle

Platforms	Name	Type	Description
All	hazard_classification	xsd:integer	The anpr classification (not useful with many ANPR engines)
All	hazard_asyncpayload	xsd:string	The OEM asynchronous payload. Asynchronous messages injected via serial (or TCP) will be associated with messages based on a closest match within a window. Otherwise an empty string.
All	hazard_readconfidence	xsd:integer	The confidence of the hazard plate read
All	hazard_readconfidencecat	xsd:integer	The confidence category of the hazard plate read
All	hazard_platefinderconfidence	xsd:integer	The confidence of the hardware platefinder
All	hazard_fieldnum	xsd:integer	The field number
All	hazard_natcode	xsd:integer	The nationality code (not generally useful, see HN which is)
All	hazard_nationality	xsd:string	The nationality (country and state) of origin of this plate if known
All	hazard_tiggeroffset	xsd:integer	The time offset between the trigger time and the image associated with this read (milliseconds). If not triggered, will be 0
All	hazard_text	xsd:string	The text of the hazard plate
All	hazard_numreads	xsd:integer	The total number of reads associated with the trigger that caused this plateread (A single trigger can lead to >1 plateread event). For a NOREAD the value will still be 1.
All	hazard_syntaxconfidence	xsd:integer	The syntax confidence of the hazard plate read. This is a measure of how confident we are that the hazard plate matched the syntax of the reported country or state.
All	hazard_tag	xsd:string	The plate tag, as extracted from the vehicle filter database. Will be blank if no tag entered, the plate is not matched, or the filter is off
All	hazard_triggerpayload	xsd:string	The OEM trigger payload. If you are using serial (or TCP/IP) triggers, this will be the OEM content of those, otherwise it will be boring. Text 'auto' will be returned if not triggered
All	hazard_xpos	xsd:integer	The x position of the plate's left edge in pixels
All	hazard_width	xsd:integer	The width of the plate in pixels
All	hazard_ypos	xsd:integer	The y position of the plate's top edge in pixels
All	hazard_height	xsd:integer	The height of the plate in pixels

PIXI values heartbeat_*

The camera heartbeat delivery

Platforms	Name	Type	Description
All	heartbeat_attemptcount	xsd:integer	The count of heartbeat delivery attempts.
All	heartbeat_failurecount	xsd:integer	The count of heartbeat delivery failures.
All	heartbeat_statusbits	xsd:integer	A camera status bitfield (legacy).

PIXI values imglocaltime_*

The image timestamp, the moment the image for the vehicle was captured.

This is a local time and accounts for timezone and daylight saving

Platforms	Name	Type	Description
All	imglocaltime_ampm	xsd:string	The string am for the morning, pm for the afternoon
All	imglocaltime_ctime	xsd:integer	Seconds since midnight 1st of January 1970 (commonly known as C time). This is UTC always, included for completeness.
All	imglocaltime_day	xsd:integer	The day of the month
All	imglocaltime_dayyear	xsd:integer	The day of the year, with January the 1st as zero
All	imglocaltime_hour	xsd:integer	The hour, 24 hour clock
All	imglocaltime_hour12	xsd:integer	The hour, 12 hour clock
All	imglocaltime_millisecond	xsd:integer	Milliseconds
All	imglocaltime_locked	xsd:integer	Indicates if time is locked via NTP
All	imglocaltime_locked_text	xsd:string	Indicates if time is locked via NTP as a string
All	imglocaltime_minute	xsd:integer	Minutes past the hour
All	imglocaltime_tenmin	xsd:integer	Tens of minutes past the hour
All	imglocaltime_month	xsd:integer	Month of the year (January as one)
All	imglocaltime_monthname	xsd:string	Month of the year as a word, in English
All	imglocaltime_monthnamesh	xsd:string	Month of the year as three letter shortened word, in English
All	imglocaltime_second	xsd:integer	Seconds past the minute
All	imglocaltime_tenthsecond	xsd:integer	Tenths of seconds
All	imglocaltime_hundredthsecond	xsd:integer	Hundredths of seconds
All	imglocaltime_daylight	xsd:integer	One if daylight saving is in effect, zero otherwise
All	imglocaltime_dayweek	xsd:integer	The day of the week as a number, with zero being Sunday
All	imglocaltime_dayweekname	xsd:string	The day of the week as a word, in English
All	imglocaltime_dayweeknamesh	xsd:string	The day of the week as a three letter shortened word, in English
All	imglocaltime_year	xsd:integer	The year
All	imglocaltime_year2	xsd:integer	The last two digits of the year

PIXI values imgutctime_*

The image timestamp, the moment the image for the vehicle was captured.

This is UTC time (like GMT)

Platforms	Name	Type	Description
All	imgutctime_ampm	xsd:string	The string am for the morning, pm for the afternoon
All	imgutctime_ctime	xsd:integer	Seconds since midnight 1st of January 1970 (commonly known as C time)
All	imgutctime_day	xsd:integer	The day of the month
All	imgutctime_dayyear	xsd:integer	The day of the year, with January the 1st as zero
All	imgutctime_hour	xsd:integer	The hour, 24 hour clock
All	imgutctime_hour12	xsd:integer	The hour, 12 hour clock
All	imgutctime_millisecond	xsd:integer	Milliseconds
All	imgutctime_locked	xsd:integer	Indicates if time is locked via NTP
All	imgutctime_locked_text	xsd:string	Indicates if time is locked via NTP as a string
All	imgutctime_minute	xsd:integer	Minutes past the hour
All	imgutctime_tenmin	xsd:integer	Tens of minutes past the hour
All	imgutctime_month	xsd:integer	Month of the year (January as one)
All	imgutctime_monthname	xsd:string	Month of the year as a word, in English
All	imgutctime_monthnamesh	xsd:string	Month of the year as three letter shortened word, in English
All	imgutctime_second	xsd:integer	Seconds past the minute
All	imgutctime_tenthsecond	xsd:integer	Tenths of seconds
All	imgutctime_hundredthsecond	xsd:integer	Hundredths of seconds
All	imgutctime_daylight	xsd:integer	One if daylight saving is in effect, zero otherwise
All	imgutctime_dayweek	xsd:integer	The day of the week as a number, with zero being Sunday
All	imgutctime_dayweekname	xsd:string	The day of the week as a word, in English
All	imgutctime_dayweeknamesh	xsd:string	The day of the week as a three letter shortened word, in English
All	imgutctime_year	xsd:integer	The year
All	imgutctime_year2	xsd:integer	The last two digits of the year

PIXI values jpeg_*

JPEG data. Not useable under all circumstances. Primarily for use in output filenames to distinguish between them.

Platforms	Name	Type	Description
All	jpeg_type	xsd:string length='1'	The file type. Will be p for a patch, n for an IR image, and w for an overview wide angle image. Context images will be 1 (for context 1), 2 (for context 2). Currently up to 8 context images are supported.

PIXI values location_*

The location of the camera

Platforms	Name	Type	Description
All	location_latitude	xsd:integer	The whole number of degrees of latitude (north or south). Will always be positive.

Platforms	Name	Type	Description
All	location_longitude	xsd:integer	The whole number of degrees of longitude (east or west). Will always be positive.
All	location_north	xsd:integer	The whole number of degrees north we are. Will be negative if we are south.
All	location_east	xsd:integer	The whole number of degrees east we are. Will be negative if we are west.
All	location_millideglat	xsd:integer	The number of millidegrees of latitude we are away from the nearest degree.
All	location_millideglong	xsd:integer	The number of millidegrees of longitude we are away from the nearest degree.
All	location_microdeglat	xsd:integer	The number of microdegrees of latitude we are away from the nearest degree.
All	location_microdeglong	xsd:integer	The number of microdegrees of longitude we are away from the nearest degree.
All	location_ns	xsd:string length='1'	A character for latitude, N (north) or S (south) depending upon which hemisphere the location represents.
All	location_ew	xsd:string length='1'	A character for longitude, E (east) or W (west) depending upon which side of the meridian the location represents.
All	location_minlatitude	xsd:integer	The number of minutes of latitude (north or south) that we are away from the nearest whole degree. Will always be positive.
All	location_minlongitude	xsd:integer	The number of minutes of longitude (east or west) that we are away from the nearest whole degree. Will always be positive.
All	location_minlatitudetotal	xsd:integer	The number of minutes of latitude (north or south) that we are away from the equator. Will always be positive.
All	location_minlongitudetotal	xsd:integer	The number of minutes of longitude (east or west) that we are away from the equator. Will always be positive.
All	location_minnorthtotal	xsd:integer	The number of minutes north that we are away from the equator. Will be negative if we are south.
All	location_mineasttotal	xsd:integer	The number of minutes east that we are away from the equator. Will be negative if we are south.
All	location_milliminuteslat	xsd:integer	The number of milliminutes of latitude we are away from the nearest minute.
All	location_milliminuteslong	xsd:integer	The number of milliminutes of longitude we are away from the nearest minute.
All	location_microminuteslat	xsd:integer	The number of microminutes of latitude we are away from the nearest minute.
All	location_microminuteslong	xsd:integer	The number of microminutes of longitude we are away from the nearest minute.
All	location_validity	xsd:string	The string Valid or Invalid depending upon whether the location is deemed good.

PIXI values globalmeta_*

Metadata strings from the Metadata object. This is purely here so you can have the same format strings on all sites, and just change the metadata in this store

Platforms	Name	Type	Description
All	globalmeta_a	xsd:string	Metadata string a
All	globalmeta_b	xsd:string	Metadata string b
All	globalmeta_c	xsd:string	Metadata string c
All	globalmeta_d	xsd:string	Metadata string d
All	globalmeta_e	xsd:string	Metadata string e
All	globalmeta_f	xsd:string	Metadata string f
All	globalmeta_g	xsd:string	Metadata string g
All	globalmeta_h	xsd:string	Metadata string h
All	globalmeta_i	xsd:string	Metadata string i
All	globalmeta_j	xsd:string	Metadata string j
All	globalmeta_k	xsd:string	Metadata string k
All	globalmeta_l	xsd:string	Metadata string l
All	globalmeta_m	xsd:string	Metadata string m
All	globalmeta_n	xsd:string	Metadata string n
All	globalmeta_o	xsd:string	Metadata string o
All	globalmeta_p	xsd:string	Metadata string p
All	globalmeta_q	xsd:string	Metadata string q
All	globalmeta_r	xsd:string	Metadata string r
All	globalmeta_s	xsd:string	Metadata string s
All	globalmeta_t	xsd:string	Metadata string t
All	globalmeta_u	xsd:string	Metadata string u
All	globalmeta_v	xsd:string	Metadata string v
All	globalmeta_w	xsd:string	Metadata string w
All	globalmeta_x	xsd:string	Metadata string x
All	globalmeta_y	xsd:string	Metadata string y
All	globalmeta_z	xsd:string	Metadata string z

PIXI values timeoffset_*

The time offsets of overview context images

Platforms	Name	Type	Description
All	timeoffset_context1	xsd:integer	The offset (in milliseconds) of context image 1 measured from the vehicle event timestamp
All	timeoffset_context2	xsd:integer	The offset (in milliseconds) of context image 2 measured from the vehicle event timestamp
All	timeoffset_context3	xsd:integer	The offset (in milliseconds) of context image 3 measured from the vehicle event timestamp
All	timeoffset_context4	xsd:integer	The offset (in milliseconds) of context image 4 measured from the vehicle event timestamp
All	timeoffset_context5	xsd:integer	The offset (in milliseconds) of context image 5 measured from the vehicle event timestamp
All	timeoffset_context6	xsd:integer	The offset (in milliseconds) of context image 6 measured from the vehicle event timestamp

Platforms	Name	Type	Description
All	timeoffset_context7	xsd:integer	The offset (in milliseconds) of context image 7 measured from the vehicle event timestamp
All	timeoffset_context8	xsd:integer	The offset (in milliseconds) of context image 8 measured from the vehicle event timestamp

PIXI values plate_*

The read number plate from the vehicle

Platforms	Name	Type	Description
All	plate_isoalpha2	xsd:string	The 2-character nationality of origin of this plate if known, as defined by ISO 3166-1
All	plate_isoalpha3	xsd:string	The 3-character nationality of origin of this plate if known, as defined by ISO 3166-1
All	plate_classification	xsd:integer	The anpr classification (not useful with many ANPR engines)
All	plate_asyncpayload	xsd:string	The OEM asynchronous payload. Asynchronous messages injected via serial (or TCP) will be associated with messages based on a closest match within a window. Otherwise an empty string.
All	plate_readconfidence	xsd:integer	The confidence of the plate read
All	plate_readconfidencecat	xsd:integer	The confidence category of the plate read
All	plate_direction	xsd:string	The direction of travel of the plate read. This will be one of the following strings: AWAY, TOWARD, NOTSET. If NOTSET it indicates the direction could not be determined.
All	plate_isosubdivision	xsd:string	The subdivision of origin of this plate if known, as defined by ISO 3166-2
All	plate_platefinderconfidence	xsd:integer	The confidence of the hardware platefinder
All	plate_fieldnum	xsd:integer	The field number
All	plate_trigsource	xsd:string	The source of OEM trigger
All	plate_tcppayload	xsd:string	The OEM trigger payload from the first TCP/IP trigger
All	plate_triggerId	xsd:integer	The trigger identifier.
All	plate_laneId	xsd:string	The lane in which the plate is located.
All	plate_natcode	xsd:integer	The nationality code (not generally useful, see PN which is)
All	plate_nationality	xsd:string	The nationality (country and state) of origin of this plate if known
All	plate_triggeroffset	xsd:integer	The time offset between the trigger time and the image associated with this read (milliseconds). If not triggered, will be 0
All	plate_text	xsd:string	The text of the plate
All	plate_numreads	xsd:integer	The total number of reads associated with the trigger that caused this plateread (A single trigger can lead to >1 plateread event). For a NOREAD the value will still be 1.
All	plate_syntaxconfidence	xsd:integer	

Platforms	Name	Type	Description
			The syntax confidence of the plate read. This is a measure of how confident we are that the plate matched the syntax of the reported country or state.
All	plate_serialpayload	xsd:string	The OEM trigger payload from the first Serial trigger
All	plate_tag	xsd:string	The plate tag, as extracted from the vehicle filter database. Will be blank if no tag entered, the plate is not matched, or the filter is off
All	plate_triggerpayload	xsd:string	The OEM trigger payload. If you are using serial (or TCP/IP) triggers, this will be the OEM content of those, otherwise it will be boring. Text 'auto' will be returned if not triggered
All	plate_xpos	xsd:integer	The x position of the plate's left edge in pixels
All	plate_width	xsd:integer	The width of the plate in pixels
All	plate_ypos	xsd:integer	The y position of the plate's top edge in pixels
All	plate_height	xsd:integer	The height of the plate in pixels

PIXI values triglocaltime_*

The trigger timestamp, the moment the trigger started. You should probably be using T instead of this, as if the event was not a triggered one you will not get anything in the string with R.

This is a local time and accounts for timezone and daylight saving

Platforms	Name	Type	Description
All	triglocaltime_ampm	xsd:string	The string am for the morning, pm for the afternoon
All	triglocaltime_ctime	xsd:integer	Seconds since midnight 1st of January 1970 (commonly known as C time). This is UTC always, included for completeness.
All	triglocaltime_day	xsd:integer	The day of the month
All	triglocaltime_dayyear	xsd:integer	The day of the year, with January the 1st as zero
All	triglocaltime_hour	xsd:integer	The hour, 24 hour clock
All	triglocaltime_hour12	xsd:integer	The hour, 12 hour clock
All	triglocaltime_millisecond	xsd:integer	Milliseconds
All	triglocaltime_minute	xsd:integer	Minutes past the hour
All	triglocaltime_tenmin	xsd:integer	Tens of minutes past the hour
All	triglocaltime_month	xsd:integer	Month of the year (January as one)
All	triglocaltime_monthname	xsd:string	Month of the year as a word, in English
All	triglocaltime_monthnamesh	xsd:string	Month of the year as three letter shortened word, in English
All	triglocaltime_second	xsd:integer	Seconds past the minute
All	triglocaltime_tenthsecond	xsd:integer	Tenths of seconds
All	triglocaltime_hundredthsecond	xsd:integer	Hundredths of seconds
All	triglocaltime_daylight	xsd:integer	One if daylight saving is in effect, zero otherwise
All	triglocaltime_dayweek	xsd:integer	The day of the week as a number, with zero being Sunday
All	triglocaltime_dayweekname	xsd:string	The day of the week as a word, in English

Platforms	Name	Type	Description
All	triglocaltime_dayweeknamesh	xsd:string	The day of the week as a three letter shortened word, in English
All	triglocaltime_year	xsd:integer	The year
All	triglocaltime_year2	xsd:integer	The last two digits of the year

PIXI values trigutctime_*

The trigger timestamp, the moment the trigger started. You should probably be using t instead of this, as if the event was not a triggered one you will not get anything in the string with r.

This is UTC time (like GMT)

Platforms	Name	Type	Description
All	trigutctime_ampm	xsd:string	The string am for the morning, pm for the afternoon
All	trigutctime_ctime	xsd:integer	Seconds since midnight 1st of January 1970 (commonly known as C time)
All	trigutctime_day	xsd:integer	The day of the month
All	trigutctime_dayyear	xsd:integer	The day of the year, with January the 1st as zero
All	trigutctime_hour	xsd:integer	The hour, 24 hour clock
All	trigutctime_hour12	xsd:integer	The hour, 12 hour clock
All	trigutctime_millisecond	xsd:integer	Milliseconds
All	trigutctime_minute	xsd:integer	Minutes past the hour
All	trigutctime_tenmin	xsd:integer	Tens of minutes past the hour
All	trigutctime_month	xsd:integer	Month of the year (January as one)
All	trigutctime_monthname	xsd:string	Month of the year as a word, in English
All	trigutctime_monthnamesh	xsd:string	Month of the year as three letter shortened word, in English
All	trigutctime_second	xsd:integer	Seconds past the minute
All	trigutctime_tenthsecond	xsd:integer	Tenths of seconds
All	trigutctime_hundredthsecond	xsd:integer	Hundredths of seconds
All	trigutctime_daylight	xsd:integer	One if daylight saving is in effect, zero otherwise
All	trigutctime_dayweek	xsd:integer	The day of the week as a number, with zero being Sunday
All	trigutctime_dayweekname	xsd:string	The day of the week as a word, in English
All	trigutctime_dayweeknamesh	xsd:string	The day of the week as a three letter shortened word, in English
All	trigutctime_year	xsd:integer	The year
All	trigutctime_year2	xsd:integer	The last two digits of the year

PIXI values site_*

The site details for this unit

Platforms	Name	Type	Description
All	site_hostname	xsd:string	The site's hostname, the recommended way of identifying a site

Platforms	Name	Type	Description
All	site_libver	xsd:integer	The system's library version number
All	site_serialnumber	xsd:integer	The system's serial number
All	site_appver	xsd:integer	The system's application version number

PIXI values supplementary_*

The supplementary images details

Platforms	Name	Type	Description
All	supplementary_1_offset	xsd:integer	The offset (in milliseconds) of supplementary image 1 measured from the vehicle event timestamp
All	supplementary_2_offset	xsd:integer	The offset (in milliseconds) of supplementary image 2 measured from the vehicle event timestamp
All	supplementary_1_seq1	xsd:integer	Supplementary image 1 sequence setting (starting at one)
All	supplementary_2_seq1	xsd:integer	Supplementary image 2 sequence setting (starting at one)
All	supplementary_1_shutter	xsd:integer	Supplementary image 1 shutter setting
All	supplementary_2_shutter	xsd:integer	Supplementary image 2 shutter setting
All	supplementary_1_gain	xsd:integer	Supplementary image 1 gain setting
All	supplementary_2_gain	xsd:integer	Supplementary image 2 gain setting

PIXI values localtime_*

The timestamp for the vehicle, which is the trigger timestamp if the vehicle was triggered (see R), or the image timestamp if it was not (see I).

This is a local time and accounts for timezone and daylight saving

Platforms	Name	Type	Description
All	localtime_ampm	xsd:string	The string am for the morning, pm for the afternoon
All	localtime_ctime	xsd:integer	Seconds since midnight 1st of January 1970 (commonly known as C time). This is UTC always, included for completeness.
All	localtime_day	xsd:integer	The day of the month
All	localtime_dayyear	xsd:integer	The day of the year, with January the 1st as zero
All	localtime_hour	xsd:integer	The hour, 24 hour clock
All	localtime_hour12	xsd:integer	The hour, 12 hour clock
All	localtime_millisecond	xsd:integer	Milliseconds
All	localtime_minute	xsd:integer	Minutes past the hour
All	localtime_tenmin	xsd:integer	Tens of minutes past the hour
All	localtime_month	xsd:integer	Month of the year (January as one)
All	localtime_monthname	xsd:string	Month of the year as a word, in English
All	localtime_monthnamesh	xsd:string	Month of the year as three letter shortened word, in English
All	localtime_second	xsd:integer	Seconds past the minute

Platforms	Name	Type	Description
All	localtime_tenthsecond	xsd:integer	Tenths of seconds
All	localtime_hundredthsecond	xsd:integer	Hundredths of seconds
All	localtime_daylight	xsd:integer	One if daylight saving is in effect, zero otherwise
All	localtime_dayweek	xsd:integer	The day of the week as a number, with zero being Sunday
All	localtime_dayweekname	xsd:string	The day of the week as a word, in English
All	localtime_dayweeknamesh	xsd:string	The day of the week as a three letter shortened word, in English
All	localtime_year	xsd:integer	The year
All	localtime_year2	xsd:integer	The last two digits of the year

PIXI values utctime_*

The timestamp for the vehicle, which is the trigger timestamp if the vehicle was triggered (see r), or the image timestamp if it was not (see i).

This is UTC time (like GMT)

Platforms	Name	Type	Description
All	utctime_ampm	xsd:string	The string am for the morning, pm for the afternoon
All	utctime_ctime	xsd:integer	Seconds since midnight 1st of January 1970 (commonly known as C time)
All	utctime_day	xsd:integer	The day of the month
All	utctime_dayyear	xsd:integer	The day of the year, with January the 1st as zero
All	utctime_hour	xsd:integer	The hour, 24 hour clock
All	utctime_hour12	xsd:integer	The hour, 12 hour clock
All	utctime_millisecond	xsd:integer	Milliseconds
All	utctime_minute	xsd:integer	Minutes past the hour
All	utctime_tenmin	xsd:integer	Tens of minutes past the hour
All	utctime_month	xsd:integer	Month of the year (January as one)
All	utctime_monthname	xsd:string	Month of the year as a word, in English
All	utctime_monthnamesh	xsd:string	Month of the year as three letter shortened word, in English
All	utctime_second	xsd:integer	Seconds past the minute
All	utctime_tenthsecond	xsd:integer	Tenths of seconds
All	utctime_hundredthsecond	xsd:integer	Hundredths of seconds
All	utctime_daylight	xsd:integer	One if daylight saving is in effect, zero otherwise
All	utctime_dayweek	xsd:integer	The day of the week as a number, with zero being Sunday
All	utctime_dayweekname	xsd:string	The day of the week as a word, in English
All	utctime_dayweeknamesh	xsd:string	The day of the week as a three letter shortened word, in English
All	utctime_year	xsd:integer	The year
All	utctime_year2	xsd:integer	The last two digits of the year

Appendix A. Technical Details

Communication

Console Serial RS-232

The console runs at a fixed line speed of 38,400 bits per second with 8 bits of data, no parity and 1 stop bit. This is often abbreviated to 38,400 8N1. Hardware flow control is not supported, Xon/Xoff can be used, but no flow control also works.

Ethernet

The ethernet port is wired to the four Ethernet wires.

The ethernet port is 100BASE-TX autosensing 10/100 Mbit/s and full/half duplex over twisted pair. You must use Category 5e cable to make full use of the bandwidth of the connection, and are limited to 100metres total cable length from the camera to the receiver. If you are having problems with the ethernet link being intermittent or unreliable do ensure your cable meets full Cat 5e specification. The camera will work with a hub or switch with a "straight through" cable (pin 1 to 1, pin 2 to 2) or with a "cross-over" cable directly into the back of a PC. The camera will *not* autosense the RX and TX pairs so you must use the correct cable type for the far end unless that will autosense.

Although the camera is capable of 100Base-TX Full Duplex and will often negotiate to that given an appropriate other end point, sometimes the cable in between is not up to Cat 5e standards and running over long distances will drop packets. It is possible to force the camera to slow down or change to half duplex using a linux command called mii-tool.

`mii-tool` {-F} {*`10baseT-HD`*}
will force set it to 10 Mbit/s and half duplex. mii-tool has many other options, which are detailed below in the manual page for it.

If you need to make a permanent change to the speed of the camera's ethernet link you can put the command into `/etc/conf.d/local.start`, either using nano or by going to the System → Bootup and Shutdown page of webmin where you can edit the same file.

mii-tool

view, manipulate media-independent interface status

`mii-tool` [-v, --verbose] [-V, --version] [-R, --reset] [-r, --restart] [-w, --watch] [-l, --log] [-A, --advertise=*`media,`* ...] [-F, --force=*`media`*] [*`interface`*...]

This utility checks or sets the status of a network interface's Media Independent Interface (MII) unit. Most fast ethernet adapters use an MII to autonegotiate link speed and duplex setting.

Most intelligent network devices use an autonegotiation protocol to communicate what media technologies they support, and then select the fastest mutually supported media technology. The `-A` or `--advertise` options can be used to tell the MII to only advertise a subset of its capabilities. Some passive devices, such as single-speed hubs, are unable to autonegotiate. To handle such devices, the MII protocol also allows for establishing a link by simply detecting either a 10baseT or 100baseT link beat. The `-F` or `--force` options can be used to force the MII to operate in one mode, instead of autonegotiating. The `-A` and `-F` options are mutually exclusive.

The default short output reports the negotiated link speed and link status for each interface. If an interface or interfaces are not specified on the command line, then **mii-tool** will check any available interfaces from *eth0* through *eth7*.

`-v`, `--verbose`	Display more detailed MII status information. If used twice, also display raw MII register contents.

`-V`, `--version`	Display program version information.
`-R`, `--reset`	Reset the MII to its default configuration.
`-r`, `--restart`	Restart autonegotiation.
`-w`, `--watch`	Watch interface(s) and report changes in link status. The MII interfaces are polled at one second intervals.
`-l`, `--log`	Used with `-w`, records link status changes in the system log instead of printing on standard output.
`-F` *media*, `--force=`*media*	Disable autonegotiation, and force the MII to either *100baseTx-FD*, *100baseTx-HD*, *10baseT-FD*, or *10baseT-HD* operation.
`-A` *media,...*, `--advertise=`*media,...*	Enable and restart autonegotiation, and advertise only the specified media technologies. Multiple technologies should be separated by commas. Valid media are *100baseT4*, *100baseTx-FD*, *100baseTx-HD*, *10baseT-FD*, and *10baseT-HD*.

Diagnostics

SIOCGMIIPHY on 'eth?' failed: Invalid argument	If the interface is not running (up), kernel will refuse to report its link state.
SIOCGMIIPHY on 'eth?' failed: Operation not permitted	Most kernels restrict access to root.
SIOCGMIIPHY on 'eth?' failed: No such device	This error is shown, if the kernel does not know about the named device.
SIOCGMIIPHY on 'eth?' failed: Operation not supported	The interface in question does not support MII queries. Most likely, it does not have MII transceivers, at all.

Network details

The P382, P392+ and P492 are network capable cameras which make extensive use of TCP/IP and UDP/IP. They also use raw ethernet packets with type 0xAC01 for local configuration of the IP address details (sometimes known as IP Discovery or Remote IP Configuration). In case you need to pass TCP/IP or UDP/IP through a firewall or network translation device this table lists the appropriate ports.

Table A.1. TCP/IP and UDP/IP Port numbers

Port used for	Port type	Port number
SSH Shell	TCP/IP Server	22
Webmin secure HTTP	TCP/IP Server	443
Viewfinder	TCP/IP Server	9000
Client	TCP/IP Server	3570
PIXI (Unsecured, recommend an SSH tunnel to access). Usually firewalled on camera.	TCP/IP Server	3382
ACS	when FTP Client	21 plus ephemeral data ports
ACS	when SCP/SSH Client	22
NTP (where used)	UDP Client	123
Portmapper (where used for NFS)	UDP and TCP Server	111
NFS (where used)	UDP and TCP	2049
VES	TCP Server	Configurable, defaults [redacted] through [redacted] inclusive)
UDP Ping (may be used by VES)	UDP	10010
Ping	ICMP	No port for ICMP
TCP Trigger	TCP	3820
UTMC	TCP Server	Configurable

Filesystem layout

As you may well discover, the camera's root filesystem is mounted read-only to prevent accidental corruption. This section of the manual documents how the file system is layed out, and what goes where. A base knowledge of linux filesystems, disks, partitions and nomeclature for these is expected to be able to read this section.

There are flash devices within the camera, the internal flash, and the compact flash/SD card (not user removable). The internal flash is no longer used. The other flash card may vary in size, but only any space over 512Mb is available for user storage. It is a build to order option to have storage space in the camera.

On the P382 The flash is `/dev/hda` and on the P392+/P492 is `/dev/mmcblk0` and is partitioned into 5 sections as follows:

- 1 - This is the boot device. On the P382 it contains GRUB, the bootloader and the kernels. On the P392+/P492 it doesn't contain very much - all the boot data is held in NOR flash which is not accessible from linux. It is vital for booting, and there is no alternative. It is not usually mounted, so should be safe from damage. When mounted it exists as `/boot`
- 2 - This is the root filesystem. It is normally mounted as `/` *read only*.
- 5 - It is mounted as `/var` and is used for storing logging information and other run time data.
- 6 - It is mounted as `/opt` and is used for storing the PIPS application, libraries and configuration information. `/opt/pips` contains the ANPR reading engine, the application, the shell and other application files. `/opt/config/current` is a symbolic link to the current configuration of the camera including the usual `/etc`. You should back up `/opt/config/current` to preserve the state of a camera.
- 7 - It is mounted as `/storage` and is used for storing PIPS application data. All output from the camera application goes into this directory. If you have not purchased a larger than 512Mb compact flash this area will be small and should not be used for storage. You can (and should if you want to do this) mount a network filesystem under this directory to store files off camera.

Partition 1 on disk hda is known as `/dev/hda1` and on disk mmcblk0 it is known as `/dev/mmcblk0p1`.

Most of the filesystem is “normal linux” and adheres to the Linux Filesystem Standard (see http://tldp.org/LDP/Linux-Filesystem-Hierarchy/html/). Here are a few highlights and P382, P392+ and P492 specifics:

- `/etc` contains system specific configuration.
  - `fstab` mounted filesystems, included those mounted at boot. You can manipulate this in webmin, see the section called “Mounting network disks” [13]
  - `init.d/` several startup scripts, including those used to start the application and network
- `/opt/pips` contains the PIPS specific code including the applications.
  - `camera_app` the camera application which does ANPR and runs all the output modules
  - `libpipslinux.so.*` the shared library written by PIPS, used by all our applications on the camera
  - `libcardet*` are the ANPR libraries for reading plates. See the section called “Camera control” [13] to manipluate these.
  - `s2driver*` the kernel module (think of it like a windows device driver) for the PCI interface to the cameras and platefinder.
  - `ipconfigd` the IPDiscovery responder, this is what you're using when you use IP Discovery. This is started from `/etc/conf.d/local.start`
  - `modempulse` simple application which assists in turning the modem (where fitted) on and off.
  - `*.msc, *.isc, xcf08p_vo_48_1532.bsd, prog_prom*, jdrive, instfpga.pl` Files for setting up the FPGA. `instfpga.pl` uses the other files appropriately to reprogram the FPGA. Once the FPGA is programmed the camera will need rebooting.
  - `pipsshell` is the camera application's shell, see Chapter 6, *PIPS ANPR Shell* [15].
  - `uid.pl` generates a unique ID for this camera for use in VES.
  - `netmon.pl` manages the network and NTP on the camera.
- `/opt/config` contains all local configuration.
  - `current` is a symbolic link to the current configuration. You can use this to quickly switch configurations if you understand how to maniplate symbolic links.
  - `current/state.xml` is the camera script, containing all the configuration used by the camera application. This is XML, and must be correct or we will discard it. Hand edits are possible, but do take care. You can check it with **`xmllint`**
  - `current/netmon.xml` is the network configuration script. This is XML, and must be correct or we will discard it. Hand edits are possible, but do take care. You can check it with **`xmllint`**
  - `current/etc` is the actual `/etc` which is linked to here
- `/var` writable area used by linux. In particular contains linux's log files, see `log/messages` in particular. Equivalent of the event log on the P372.
- `/storage` writable area used by our application. This is user storage and all paths you enter in the application are relative to this directory, so entering `foo` as a directory will store the files in `/storage/foo`. This will contain the compact flash storage size minus 500Mb.

Backup

On the P392+ and P492 cameras (and only these models) should have the /backup.pl script run from the command line after any change - once that change is determined to be satisfactory. Changes include:

- New OS and application installations
- Application upgrades, Cardet upgrades
- Configuration changes

Appendix B. Software installation and upgrades

This appendix covers software maintenance of the camera which you may need to do, including upgrading or changing the software installed on the camera.

The camera software has a version numbering scheme to help you decide what action to take when new versions become available. The format of a version number is *major.minor.revision*. The "revision" will be an increasing "revision" number, always larger for later releases. For bug fixes, "revision" will increase. For minor enhancements, "minor" will increase. For major new features, or architectural changes, "major" will increase.

Optionally we may append the characters 'a', 'b' or "rc" to indicate alpha, beta or release candidate.

If only the revision number is increased, backward compatibility is guaranteed without any config changes.

If the minor number is increased, backward compatibility *may* be affected if deemed absolutely necessary. This will be clearly highlighted in the release note.

If the major number is increased, backward compatibility *may* be affected if deemed necessary or desirable. This will be clearly highlighted in the release note.

In general we will always try to maintain backward compatibility where it makes sense. Always refer to the release notes for more details on the changes that have occurred.

The old mechanisms of manual installation and web based installation are no longer possible nor supported. All software installation is managed via the PIPS ANPR Toolkit which is documented in Chapter 3, *PIPS ANPR Toolkit* [8].

Appendix C. Factory Defaults

On the P382 the password for the root user is *382*

On the P392+/P492 the password for the root user is *392*

The default network configuration stored in(`/opt/config/current/netmon.xml`) is

Table C.1. Default IP configuration

IP address	`10.20.xxx.yy`
Network mask	`255.255.0.0`
Default gateway	`10.20.100.1`

where `xxx` are the first three digits of the serial number of the camera, and `yy` are the last two. The serial number is printed on a sticker on the rear of the P382, P392+ and P492

Caution

It is important to note any changes which you make to these parameters. Without these details it may be impossible to maintain the camera and it may have to be returned to Neology for servicing

Appendix D. File transfers

This section describes how to transfer files to or from the camera by various means. You can pick which of these you want to try, although not all are suitable for all situations.

SFTP

SFTP stands for Secure File Transfer Protocol. It is an encrypted protocol, and is a partner to SSH. Like you can log onto a system using SSH, you can use SFTP to transfer files in both directions. It is simple to use if you are familiar with the ubiquitous FTP, and plenty of front ends make it's use trivial. It is the recommended way of transferring files, requiring little setup to use.

Multiplatform — The filezilla program (see the section called “Filezilla” [142]) provides a two window commander style interface for accessing the camera via sftp.

Windows — The WinSCP program (see the section called “WinSCP” [142]) provides an explorer or commander style interface for accessing the camera via scp and sftp.

To use SFTP I recommend a graphical browser unless you're happy to train yourself in the use of a command line version.

SCP

SCP stands for Secure CoPy. It is an encrypted protocol, and is also a partner to SSH. Like you can log onto a system using SSH, you can use SCP to transfer files in both directions. It is simple to use, but does not provide directory listings or any other features you might expect - you will need to use SSH for directory listings as a partner to SCP. As SCP is available on most operating systems as a built in, and is also available on the camera for camera-to-camera copies it is useful to understand.

Windows — The WinSCP program (see the section called “WinSCP” [142]) provides an explorer style interface for accessing the camera via scp and sftp.

Windows — The PuTTY project (see the section called “PuTTY” [142]) also provides PSCP for Windows. If you want to use it, put it on your path, or current directory, and use **pscp** instead of **scp** in the command examples.

Mac OS X — scp is a built in command.

Linux — scp is provided if you have ssh installed, which you most likely will do.

SCP is used like the standard DOS or Unix copy commands. You specify a source and target file to transfer, just one of them happens to be on a remote computer.

- `scp {`*`SourceFile`*`} {`*`user@host:directory/TargetFile`*`}`
  to copy a file to the remote computer
- `scp {`*`user@host:directory/SourceFile`*`} {`*`TargetFile`*`}`
  to copy a file from the remote computer

Note

SCP can be used from on the camera too; if you have a computer with an SSH server you can scp out from the camera, or from one camera to another.

FTP

FTP stands for File Transfer Protocol. It is a simple open protocol, and is purely for transferring files. To use it you will need an FTP server installed on a PC accessible via the network from the camera. There are various options available

for each operating system. FTP is not recommended, but included here as people familiar with our older cameras will be familiar with FTP. This is a quick introduction to FTP, not a complete guide. There are books available on the subject, or guides on the internet.

Windows	For Windows we recommend the free FileZilla server, which is a download from http://filezilla-project.org/. This is simple to setup and enable users without requiring rights to add users to the PC.
Windows (alternative)	For Windows you can also use the FTP server which comes with the OS as part of IIS. You can install this from Start → Settings → Control Panel+Add/Remove Programs. It is tricky to set up correctly, and requires that you create a Windows user, and assign them correct permissions to work right. I do not recommend it as FileZilla is easier to use.
Mac OS X	MacOS X comes with an FTP server which can be enabled using the Sharing Pane.
Linux	Different distributions of Linux come with different FTP servers which are probably not installed or enabled by default. I recommend the ProFTPd software, but any FTP server should work correctly.

If you now connect to the camera's shell you should be able to ftp from the camera and transfer files. A typical session is shown below.

Note

The use of the bin command to enable all binary transfers may be necessary otherwise binary files may get corrupted, and does no harm so always do it.

```
pole ~ # ftp 80.177.196.175
Connected to 80.177.196.175 (80.177.196.175).
220 ProFTPD 1.3.1rc3 Server (Alan's ProFTPD) [::ffff:80.177.196.175]
Name (80.177.196.175:root): ftp_boot
500 AUTH not understood
SSL not available
331 Password required for ftp_boot
Password:
230 User ftp_boot logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> bin
200 Type set to I
ftp> lcd /opt/config/current
Local directory now /opt/config/released
ftp> put state.xml
local: state.xml remote: state.xml
200 PORT command successful
150 Opening BINARY mode data connection for state.xml
226 Transfer complete
8089 bytes sent in 0.000208 secs (3.8e+04 Kbytes/sec)
ftp> cd 382
250 CWD command successful
ftp> lcd /storage
Local directory now /storage
ftp> get instapp.pl
local: instapp.pl remote: instapp.pl
200 PORT command successful
150 Opening BINARY mode data connection for instapp.pl (3132 bytes)
226 Transfer complete
3132 bytes received in 0.00201 secs (1.5e+03 Kbytes/sec)
ftp> cd app
250 CWD command successful
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
drwxr-xr-x   2 alan     alan         4096 Jul 23 23:00 254
drwxr-xr-x   2 alan     alan         4096 Sep 10 13:33 384
drwxr-xr-x   2 alan     alan         4096 Sep 25 11:39 435
drwxr-xr-x   2 alan     alan         4096 Oct 24 16:04 540
226 Transfer complete
ftp> cd 540
250 CWD command successful
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
-rw-r--r--   1 alan     alan      4553379 Oct 24 16:04 distrib.tbz2
226 Transfer complete
ftp> get distrib.tbz2
local: distrib.tbz2 remote: distrib.tbz2
200 PORT command successful
150 Opening BINARY mode data connection for distrib.tbz2 (4553379 bytes)
226 Transfer complete
```

```
4553379 bytes received in 0.741 secs (6e+03 Kbytes/sec)
ftp> quit
221 Goodbye.
pole ~ #
```

The **put** and **get** commands actually transfer files. **lcd** changes *local* directory, **cd** changes remote directory. **ls** will list files

Note

You cannot FTP from a remote computer into the P382, P392+ and P492

NFS

NFS stands for Network File System. This is an open protocol for sharing filesystems between computers. Unlike FTP and SCP this allows the camera to see remote files as if they were local files, rather than actually needing room to store them on its local storage. NFS is quite paranoid and must have all permissions correct before it will work. When it fails it doesn't usually give a helpful error message.

Windows see the section called “NFS Server on Windows” [142] to install nfs.

Mac OS X nfs is built in, but needs enabling.

Linux an nfs server is available for linux, see your distribution documentation to find out how to install it.

Setting up NFS involves editing /etc/exports and restarting the nfs server to pick up those changes. Once this is done you should be able to mount the exported filesystem from Webmin, as described in the section called “Mounting network disks” [13]. I'd suggest mounting the file system under /storage. Once this is done you should be able to list and access files on the remote PC as if they were local, using the standard **cd**, **ls** and **cp** commands.

CIFS/Samba (Windows shares)

CIFS is the latest version of Windows networking. It is available as samba for Linux and MacOS X, but it doesn't make as much sense as using NFS for those OSes.

Once you have a windows share set up you can mount the directories using webmin.

Transfer troubleshooting

A complete troubleshooting guide is beyond the scope of this manual, but I hope to give some hints and tips. Most problems boil down to one of two things, networking or permissions.

Network problems

- Can you ping the camera from the PC? If not then check your ethernet is correctly connected, networking settings are correct, and there is no firewall?
- Can you ping the PC from the camera? Both directions should work.
- Can you access the service on the PC from itself (not appropriate for all transfer types)? e.g. Can you FTP to the PC from itself?
- Is there a firewall running on the PC?
- Is there a second or third firewall running?
- Is there a firewall on the network in between?
- Or how about a NAT (network address translation) device?

- What happens if you telnet from either end to the service's port number? You should at least connect...

Permissions

- Do you have permissions to access the file you are trying to access? Can you read it locally on that machine?
- Do you have permissions to write to the file you are trying to write to?
- How about the directory that it is in?
- Do you have write permissions granted by the transport (e.g. FTP write permissions)? Or read permissions? *These permissions are separate from the permissions on the files... this often catches people out*
- Does the particular pairing of camera and PC allowed, lots of these services can restrict by IP address?

Appendix E. Software tools

This appendix lists some useful software tools you may wish to use with your camera

PIPS ANPR Toolkit

The PIPS ANPR Toolkit (P374) is available from PIPS. It consists of various software applications to install, diagnose and maintain PIPS cameras, including the P382, P392+ and P492. It is available as a package for Microsoft Windows 7.

Windows 7

To install the applications just double click on the installer executable and select the options you require.

PuTTY

PuTTY is a free terminal client. It can connect to the P382, P392+ and P492 via both the serial port and via SSH. It also provides the pscp SCP program. It is available from http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html and is highly recommended. A version of PuTTY is installed with the PIPS ANPR Toolkit.

Filezilla

Filezilla is a commander like file transfer program for many platforms suitable for using with the camera. It is available from http://filezilla-project.org/.

WinSCP

WinSCP is an explorer like file transfer program for Windows suitable for using with the camera. It is available from http://winscp.net/.

NFS Server on Windows

Windows does not come with an NFS server, however one is available for free as part of the cygwin project, and it is compatible with the P382, P392+ and P492. To install it

1. Download setup.exe from http://www.cygwin.com.
2. You should run this and select the **`nfs-server`** and **`cygrunsrv`** components.
3. Start the shell that is installed to Start → Cygwin → Cygwin Bash Shell and run **`nfs-server-config`**.
4. Now edit *`CYGWIN_DIR`*`/etc/exports` to add a directory to export. Full documentation of the exports file format is available online, but an example would be

   ```
   /cygdrive/d/workspace      80.177.196.176(rw,async,no_root_squash,insecure,no_subtree_check)
   /cygdrive/c/workdir/fish   80.177.196.0/24(ro,async,no_root_squash,insecure,no_subtree_check)
   ```

   which will export `d:\workspace` and the camera at 80.177.196.176 and `c:\workdir\fish` to all 80.177.196.* read-only.
5. Now start the **`Cygwin nfsd`** and **`Cygwin mountd`** services from Start → Settings → Control Panel+Administrative Tools → Services. You will need to restart them if you change the `exports` file.

Appendix F. Nano - text editor

This is a short guide to using the recommended text editor on the P382, P392+ and P492 *nano*. More detailed documentation is available on the web at http://www.nano-editor.org/docs.php

Opening and creating files

Opening and creating files is simple in nano, simply type:

nano {*filename*}
You can start typing immediately to insert text, and move around with the cursor keys.

Saving and exiting

If you want to save the changes you've made, press **Ctrl**+**O**. To exit nano, type **Ctrl**+**C**. If you ask nano to exit from a modified file, it will ask you if you want to save it. Just press **N** in case you don't, or **Y** in case you do. It will then ask you for a filename. Just type it in and press **Enter**.

If you accidentally confirmed that you want to save the file but you actually don't, you can always cancel by pressing **Ctrl**+**C** when you're prompted for a filename.

Cutting and pasting

To cut a single line, you use **Ctrl**+**K**. The line disappears. To paste it, you simply move the cursor to where you want to paste it and punch **Ctrl**+**U**. The line reappears. To move multiple lines, simply cut them with several **Ctrl**+**K**s in a row, then paste them with a single **Ctrl**+**U**. The whole paragraph appears wherever you want it.

If you need a little more fine-grained control, then you have to mark the text. Move the cursor to the beginning of the text you want to cut. Hit **Ctrl**+**6** (or **Alt**+**A**). Now move your cursor to the end of the text you want to cut: the marked text gets highlighted. If you need to cancel your text marking, simply hit **Ctrl**+**6** again. Press **Ctrl**+**K** to cut the marked text. Use **Ctrl**+**U** to paste it.

Searching for text

Searching for a string is easy as long as you think "WhereIs" instead of "Search". Simply hit **Ctrl**+**W**, type in your search string, and press Enter. To search for the same string again, hit **Alt**+**W**.

Note

Note: In nano's help texts the **Ctrl**-key is represented by a caret (^), so **Ctrl**+**W** is shown as ^W, and so on. The Alt-key is represented by an M (from "Meta"), so **Alt**+**W** is shown as M-W.

Appendix G. rc-update

This is a short guide on how to use *rc-update*

Introduction

rc-update is a script for adding/removing/listing available scripts to the boot, default and nonetwork run levels of your computer. these scripts allow you to run programs at your computers boot time.

rc-update is very useful and can be used to start anything from your network card to your login manager.

rc-update commands

adding a script to a runlevel

rc-update add script runlevel

will add a script to that runlevel of your computer.

removing a script from a runlevel

rc-update del script runlevel

will remove a script from the runlevel.

list available scripts and their current runlevel

rc-update show

will show all available scripts and their currently set runlevel(s) if any.

runlevels

boot

default

nonetwork

more runlevels may be added to /etc/runlevels/

Examples

rc-update add pips_app default

This will start the camera application at the default runlevel

rc-update del pips_app default

This will remove the camera application at the default runlevel

Other information

rc update uses scripts in the /etc/init.d/ directory exclusively

Appendix H. Viewfinder Protocol

The Viewfinder Protocol is a method for accessing the camera's video stream. The Viewfinder can be accessed via TCP port 9000.

There are several protocol versions available on the cameras, versions 1, 2, 3 and 4. By default the Viewfinder will be configured to use version 1

To initiate a Viewfinder session, you need to connect to the viewfinder port, to end the session just disconnect.

The viewfinder protocol constantly sends images, but when a session is first opened the camera needs to be set before any data will be sent, this is done by using the VF run command. Data will only stop being sent once the session is closed. The VF run command can be used to change the data that is sent, there may also be a small amount of lag before the changeover happens.

Viewfinder commands

Command	Description
VF set version *`version`*\n	Sets the version specified by *`version`* The viewfinder protocol does not respond
VF get channels\n	Gets information on the channels. See example below for output. (Viewfinder Protocol Version 2 or above must be used) The Viewfinder protocol responds with an xml type response
VF run camera *`camera`* seq *`sequence`* interval *`interval`* quality *`quality`* scale *`scale`*	Initiates the video stream. camera: The camera which is used to stream video from, required sequence: The sequence which is to be viewed, must be 0 for colour camera, default = 0, optional interval: The time between each frame, specified in ms, default = 2000, optional quality: Not used, optional scale: Not used, optional Viewfinder protocol responds with an image type response

Note

Camera 0 = cam1 in user interface = IR Camera

Camera 1 = cam2 in user interface = Colour Camera

Note

sequence 0 = seq1 in user interface

sequence 1 = seq2 in user interface

sequence 2 = seq3 in user interface

sequence 3 = seq4 in user interface

sequence 4 = seq5 in user interface

sequence 5 = seq6 in user interface

sequence 6 = seq7 in user interface

sequence 7 = seq8 in user interface

Viewfinder messages

This section contains information about the responses from the Viewfinder server

Version 1

In version 1 VF run is the only command that can be used. The following example I will configure the run command to the the IR camera and sequence 0 with 2 frames per second

`VF run camera 0 sequence 0 interval 500\n`

The response from the camera will be the following:

```
VF 1 0 0 11000\n[binary-jpeg-data]
```

Note

The [binary_jpeg_data] is a standalone JFIF (JPEG file interchange format), the specification can be found here, http://www.w3.org/Graphics/JPEG/jfif3.pdf

Note

This will be repeated every 500ms

VF *`version camera sequence jpeg_length`*

Version 2

In version 2 VF run and VF get can be used.

The response from version 2 is as follows

VF *`version type data`*

`VF set version 2`

`VF run camera 0 sequence 0 interval 500\n`

```
VF 2 image 0 0 5265846397017522284 11008\n[binary_jpeg_data]
```

Note

The [binary_jpeg_data] is a standalone JFIF (JPEG file interchange format), the specification can be found here, http://www.w3.org/Graphics/JPEG/jfif3.pdf

The above example gives a type of image which can be decoded as follows

VF *`version`* image *`camera sequence 64Bit_TimeStamp jpeg_length\n[binary_jpeg_data]`*

The 64bit Time Stamp can be decoded as follows, [Upper 32 bit Time stamp].[Lower 32 bit Time stamp].

The upper 32 bit Time stamp is a normal UTC time stamp indicating the number of seconds since 00:00:00 1st January 1970

The lower 32 bit Time stamp is the number milliseconds since the start of the current second

The second example

VF set version 2

VF get channels

```
VF 2 xml 367
<?xml version="1.0"?>
<channels model="P382" count="2">
 <channel0 num_sequence_entries="1">
  <format raw_type="mono" rate="50" quality="fixed" resolution="fixed" pixel_width="1" pixel_height="1"/>
 </channel0>
 <channel1 num_sequence_entries="1">
  <format raw_type="colour" rate="50" quality="fixed" resolution="fixed" pixel_width="2" pixel_height="1"/>
 </channel1>
</channels>
```

Note

The above example has been formatted for readability

The above example give an xml type which can be decoded as follows

VF *version* xml *xml_length*\n[xml_file]

<channels model="P382" count="2">indicates that the camera we are using is a P382 and that there are two possible image sources.

<channel0 num_sequence_entries="1"> indicates on the first channel has only one sequence available

<format raw_type="colour" rate="50" quality="fixed" resolution="fixed" pixel_width="2" pixel_height="1"/>

raw_type indicates that this channel is in colour, this can also be mono, or unknown

rate is not used, and is fixed at 50

quality is fixed so this cannot be changed, if it could this would be a number between 1 and 99

resolution is fixed which means it cannot be changed otherwise it would be a number such as 1, 2 or 4 which would be a defined resolution

pixel_width and pixel_height if pixel_width and pixel_height are the same then no adjustment of the image needs to take place, if they are different i.e. pixel_width = 2 and pixel_height = 1 means that each pixel needs to be made half the width, to view the image correctly.

Version 3

In version 3 VF run and VF get can be used.

The response from version 3 is as follows

VF *version type data*

VF set version 3

VF run camera 0 sequence 0 interval 500\n

```
VF 3 image 0 2 6129809915063042098 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1107 201 252 72 895 602 252 72 1023 92 252 72 93504\n[binary_jpeg_data]
```

Note

The [binary_jpeg_data] is a standalone JFIF (JPEG file interchange format), the specification can be found here, http://www.w3.org/Graphics/JPEG/jfif3.pdf

The above example gives a type of image which can be decoded as follows

VF *version* image *camera sequence 64Bit_TimeStamp PlateFindData jpeg_length\n[binary_jpeg_data]*

The 64bit Time Stamp can be decoded as follows, [Upper 32 bit Time stamp].[Lower 32 bit Time stamp].

The upper 32 bit Time stamp is a normal UTC time stamp indicating the number of seconds since 00:00:00 1st January 1970

The lower 32 bit Time stamp is the number milliseconds since the start of the current second

16 zeroes for future enhancement.

The plate find data describes up to 4 number plates found in the image. For each plate the x and y co-ordinates, width and height are displayed. This gives 16 data items in total.

Version 4

In version 4 VF run and VF get can be used.

The response from version 2 is as follows

VF *version type data*

VF set version 4

VF run camera 0 sequence 0 interval 500\n

```
VF 4 image 0 2 6129809915063042098 0 0 0 0 0 0 0 1107 201 252 72 5352 0 0 895 602 252 72 6737 0 0 1023 92 252 72 8941 0 0 93504\n[binary_jpeg_data]
```

Note

The [binary_jpeg_data] is a standalone JFIF (JPEG file interchange format), the specification can be found here, http://www.w3.org/Graphics/JPEG/jfif3.pdf

The above example gives a type of image which can be decoded as follows

VF *version* image *camera sequence 64Bit_TimeStamp PlateFindData jpeg_length\n[binary_jpeg_data]*

The 64bit Time Stamp can be decoded as follows, [Upper 32 bit Time stamp].[Lower 32 bit Time stamp].

The upper 32 bit Time stamp is a normal UTC time stamp indicating the number of seconds since 00:00:00 1st January 1970

The lower 32 bit Time stamp is the number milliseconds since the start of the current second

The plate find data describes up to 4 number plates found in the image. For each plate the x and y co-ordinates, width and height, plate find confidence, shape and clipped flag are displayed. This gives 28 data items in total.

The shape parameters indicate whether the plate is a number plate (0), a square number plate (1), a hazard plate (2) or a blank hazard plate (3).

The clipped flag indicates that the number plate may be partly obscured.

Appendix I. Vehicle Event Viewer Protocol

This section describes the PIPS Vehicle Event Viewer (aka "Client") protocol. It describes version 3 of the protocol as implemented by the cameras. The Vehicle Events can be accessed via TCP port 3570.

The Vehicle Event Viewer service runs on the camera and will be referred to as the "service". The service provides a stream of Vehicle Plate Read records (containing image and other data) for each vehicle plate read event created by the camera.

To initiate a Viewfinder session, you need to connect to the viewfinder port, to end the session just disconnect.

Entities may use TCP to connect to the camera and monitor this data stream. Any entity connecting to the "service" will be referred to as a "client".

Vehicle Event Viewer commands

Commands are sent to the service in ASCII text delimited by a Carriage Return character ('\r').

Currently, only a single command is recognised and this would normally only be issued once. The command (to select the version) is a string:

"vers[v]\r"

where v is the version "number", a single character in the ranges '1' to '9' or 'a' to 'z'.

The latest version supported on the cameras is 4 although it defaults to 2. If you connect to the service and issue no command, you will receive version 2 data. To switch to version 4, immediately on connection completion, the client should send the following string to the service: "vers4\r"

Vehicle Event Viewer data

The service starts streaming binary data to the client immediately on connection. It does not wait for anything from the client.

The data streamed from the service is binary. The binary data is streamed as a BLOB as follows:

1. Firstly a header structure which begins with a "start of block" pattern followed by information about the event, such as the plate string. It also contains information (lengths in bytes) allowing the end of the header and the start/endings of the subsequent jpeg images to be computed.

2. The header is immediately followed by the patch jpeg image - the length of which is contained in the header. The jpeg data is in JFIF format.

3. The patch jpeg is immediately followed by the colour overview jpeg image - the length of which is contained in the header. The jpeg data is in JFIF format.

Header Format

The header is a packed structure. Currently the cameras default to version 2, so the client must be able to recognise version 2 headers too. Since there is actually little difference between the versions, it is not difficult to support both.

Even if the client switches to version 3 immediately on connection, it is possible that one or more version 2 headers will be received first. Version 2 data may be used or ignored.

The difference between the version 2 and version 3 headers is that the version 3 header has two extra fields appended on the end - namely: utc_timestamp_s and utc_timestamp_ms.

The difference between the version 3 and version 4 headers is that the version 4 header has one extra field appended on the end - namely: m_plate.

The jpeg fields, if present, follow immediately after the header. Their location may be determined by the respective size fields in the header. The jpeg data is in JFIF format.

The version 3 header is shown below:

Note

Entries commented

```
//Not Used
```

are not currently used on the P382. It is possible that at some time in the future they may be used without causing a version number change. It will always be safe to ignore them).

```
struct PTFMPlateHeaderV3
{
 unsigned start; // start of message block indicator
 unsigned header_size; // size of header
 unsigned patch_size; // patch length
 unsigned overview_size; // overview length
 unsigned sum; //Not Used
 unsigned camera; //Not Used
 unsigned flash; //Not Used
 unsigned gain;
 unsigned shutter;
 unsigned seq; // exposure sequence number 0 - 2
 unsigned threshold; //Not Used
 unsigned platefinder_confidence;
 unsigned plateread_confidence;
 unsigned id; //Not Used
 unsigned ticks; // system tick counter at exposure time (ms)
 unsigned location; //Not Used
 unsigned mseq; //Not Used
 unsigned exp[3]; //Not Used
 unsigned event_count[4]; //Not Used
 char  plate_str[16];
 unsigned  utc_timestamp_s;
 unsigned  utc_timestamp_ms;
 char   m_plate[40];
};
```

Each field will be described below:

Note

All integer fields are transmitted in network byte order and will need to be converted back to host byte order before interpretation.

- *start:* A 4 byte pattern which identifies the start of the header. This will be 0x50544632 for version 2, 0x50544633 for version 3 and 0x50544634 for version 4.
- *header_size:* The size of the header (and only the header) in bytes. This will be different between versions. This value may be used to determine where the jpeg data begins.
- *patch_size:* The size in bytes of the patch jpeg. If this is non-zero, then this data begins immediately after the last header byte. (The patch jpeg is in jfif format).
- *overview_size:* The size in bytes of the overview jpeg. If this is non zero, this data begins immediately after the last byte of patch data. (The overview jpeg is in jfif format)
- *sum:*Currently unused
- *camera:* Currently unused
- *flash:* Currently unused. The flash period is equal to the shutter period.
- *gain:* The gain setting for this plate read event

- *shutter:* The shutter setting for this plate read event. A reported value of 0 indicates a shutter period 10us. The maximum value is 31 and indicates a shutter period of 1ms. In order to deduce in-between shutter period's note that there is a linear relationship between these reported values and actual shutter period.
- *seq:*The exposure sequence number, typically a number from 0 to 2 indicating which in a sequence of exposures was used to give this plate read event.
- *threshold:*Currently unused
- *platefinder_confidence:* The platefinder confidence value. This is not normally of much interest to an end user.
- *plateread_confidence:* The confidence of the plate read expressed as a number less than a 100 (where 100 would indicate absolute confidence).
- *id:*Currently unused
- *ticks:* A system monotonic tick count in milliseconds indicating the time of exposure. Has no meaning as an absolute time, but can be useful in relative terms - for example to measure elapsed time between two consecutive events. The tick value is strictly monotonic and therefore is unaffected by changes to the system time.
- *location:*Currently unused
- *mseq:* Currently unused
- *exp:* Currently unused
- *event_count:* Currently unused
- *plate_str:* Number plate string. Null terminated character string.
- *utc_timestamp_s:* (Version 3 and 4 only) UTC Timestamp of plate read image set (seconds). May be used together with utc_timestamp_ms (see below) to provide accurate UTC time.
- *utc_timestamp_ms:* (Version 3 and 4 only) UTC Timestamp of plate read image set (milliseconds)
- *m_plate:* (Version 4 only) The text read from the plate

Appendix J. Legal Notices

English

Copyright Notice

The information within this handbook is authorised for distribution to customers, authorised service centre personnel, and distributors of Neology. Every effort has been made to supply information within this handbook that is correct. However, Neology assumes neither responsibility for its use, nor any infringements of patents or other rights of third parties which would result. No licence is granted by the manufacturer under any patent or patent rights. The manufacturer reserves the right to modify and update the equipment at any time without prior notice.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means to a third party without the prior consent of the copyright holder.

The manufacturer's warranty will be invalidated if untrained personnel operate the equipment or if any attempt is made to service the equipment by untrained personnel.

Warranty

Neology warrants products and spare parts of its own manufacture against faulty materials and workmanship for a period of 12 months, or as modified by the contract, from the date of purchase or on site acceptance, if installed by Neology authorised personnel.

The warranty excludes consumable materials and parts with an inherently limited life and excludes faults arising from misuse, neglect or vandalism.

Neology will replace or repair at its option and at no cost to the purchaser any faulty items reported to it within the warranty period.

Service

Service of this equipment by replacement of parts, on site repair or routine maintenance inspections is available. Please contact Neology for a quotation. There are no user serviceable parts inside the camera.

Technical Support

Should you require technical support, please contact Neology.

Users finding errors or omissions in this document are requested to advise Neology.

Write or telephone:

Neology United Kingdom plc
17 Bartley Wood Business Park
Hook
Hampshire
RG27 9XA
United Kingdom
Telephone: +44 (0)
Email: <anprsupportous@uk.neology.net>

If you telephone please have the following information available:

product name and version number
operating system and version number

Design Changes

Neology reserves the right to change the design of any product from time to time without notice and with no obligation to make corresponding changes in products previously manufactured.

Trademarks

Windows and Windows XP are registered trademarks of Microsoft Corporation.

FCC Declaration

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Français

Notification de Copyright

L'information dans ce manuel est autorisée pour la distribution aux clients, au personnel des services de maintenance autorisés, et aux distributeurs de Neology (ci-après dénommée "La compagnie") Tout effort a été fait pour que l'information dans ce manuel soit correcte. Cependant, "La compagnie" n'assume ni la responsabilité pour son usage, ni aucune infraction à des brevets ou à d'autres droites des tiers qui résulteraient de son utilisation. "La compagnie" n'accorde aucune licence sous aucun brevet ou propriété industrielle. "La compagnie" se réserve le droit de modifier et mettre à jour le matériel à tout moment sans préavis.

Aucune partie de cette publication ne peut être reprise, reproduite ou enregistrée sous quelque forme que ce soit sans l'accord écrit préalable de "La compagnie".

La garantie de "La compagnie" sera infirmée si le matériel est utilisé ou si n'importe quelle tentative est faite de le réparer par un personnel non formé par "La compagnie".

Garantie

Cette garantie s'étend aux produits et pièces de rechange fabriquées par "La compagnie" contre les matériaux défectueux et l'exécution défectueuses pendant une période de 12 mois ou comme modifiée par le contrat, de la date de l'achat ou sur l'acceptation de site, si le matériel est installé par "La compagnie" ou un personnel autorisé.

La garantie exclut les matériaux consommables et les parties avec une durée de vie limitée et exclut des défauts redevant de l'abus, de la négligence ou du vandalisme.

"La compagnie" substituera ou réparera, à son option, et à aucun coût à l'acheteur tous les éléments défectueux reportés au cours de la période de garantie.

Service

Le service de ce matériel par le remplacement des parties, par des inspections de maintenance ou de réparation sur de site est disponible. Prière de contacter "La compagnie" pour la liste des coûts.

Support Technique

Pour tout support technique, prière de contacter "La compagnie" au Royaume-Uni.

Si vous trouvez des erreurs ou des omissions dans ce document prière d'informer "La compagnie"

Écrivez ou téléphonez:

Neology United Kingdom plc
17 Bartley Wood Business Park
Hook
Hampshire
RG27 9XA
United Kingdom
Telephone: +44 (0)
Email: <anprsupportous@uk.neology.net>

Si vous téléphonez, prière d’avoir l'information suivante disponible:

nom de produit et nombre de version
système d'exploitation et nombre de version

Changements de Conception

"La compagnie" se réserve le droit de changer la conception de n'importe quel produit de temps # autre sans communication préalable et sans l'obligation de faire les changements correspondants des produits construits antérieurement.

Marques Déposées

Windows et Windows XP sont des marques déposées de Microsoft Corporation.

Appendix K. Contact information

Table K.1. Contact Information

United Kingdom	USA
Neology United Kingdom plc 17 Bartley Wood Business Park Hook Hampshire RG27 9XA United Kingdom Telephone: +44 (0) Email: <anprsupportous@uk.neology.net>	Neology 12760 Danielson Ct., Suite A Poway CA USA Telephone: +1 (0) 858-391-0260 Fax:+1 (0) 858-391-0264
Web site:http://www.neology.net/	

COMFORT SYSTEMS USA
BCM Controls Corporation

Sierra Wireless Components

Quote #Q001602-BCM v1



Prepared For:

Massachusetts State Police

Brian Egnitz
470 Worcester Rd.
Framingham, MA 01702

P: (508) 410-1188
E: brian.egnitz@MassMail.State.MA.US

Prepared by:

BCM Controls

Bob Fecteau
30 Commerce Way
Woburn, MA 01801

P: 781-897-5151
E: fecteaur@bcmcontrols.com

Date Issued:

03.10.2020

Expires:

06.30.2020

Introduction

Dear Brian,

In accordance with your recent request, outlined as follows is the pricing that you requested for six (6) Sierra Wireless power adapters and twelve (12) cellular paddle antennas.

Thank you for allowing us this opportunity, and please do not hesitate to contact me with any questions.

Sincerely,

Bob Fecteau

COMFORT SYSTEMS USA
BCM Controls Corporation

Scope of Work



1. Scope Details
2. Scope Details
3. Scope Details

Equipment

Qty	Product Details	MSRP	Discount %	Price	Ext. Price
6	**Sierra 12VDC AC Adapter**	$20.00	5	$19.00	$114.00
12	**Sierra Cellular Paddle Antenna**	$14.00	5	$13.30	$159.60
				Subtotal:	**$273.60**

COMFORT SYSTEMS USA
BCM Controls Corporation

Assumptions & Clarifications

General:

- Pricing proposed is FOB: Delivered
- Pricing and warranty provided in accordance with MA State Contract: ITC71
- Pricing excludes any/all technical services labor

Privileged Information Statement

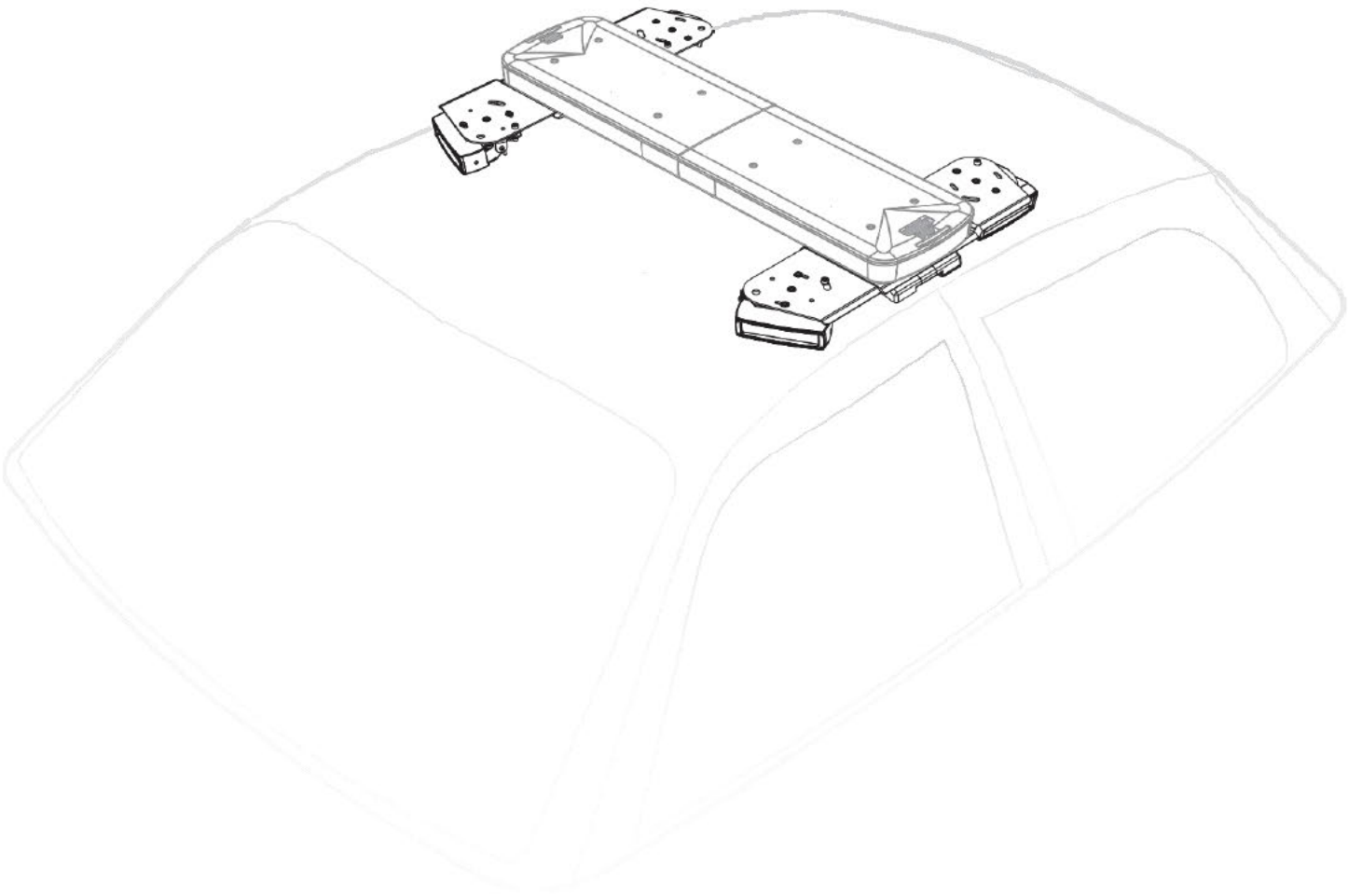
“The information contained in this document and the solution proposed by BCM Controls (BCM) is proprietary and confidential to BCM. These materials can be used solely for the purpose of evaluating a possible transaction between BCM and its existing and prospective customers. No recipient of these materials may use them for their own commercial advantage. The recipient of these materials must hold them in confidence and shall not distribute them, in whole or in part, to any other individual or entity in any form without the prior written consent of BCM.

Quote Summary	Amount
Equipment	$273.60
Total:	**$273.60**

Taxes, shipping, handling and other fees may apply. We reserve the right to cancel orders arising from pricing or other errors.

Acceptance

BCM Controls	**Massachusetts State Police**
Bob Fecteau	Brian Egnitz
Signature / Name	Signature / Name Initials
03/10/2020	
Date	Date



PIPS MOBILE ALPR SOLUTION

Installation Guide

Revised: Nov 2019

SAFETY INFORMATION ____ *4*
Intended System Use ____ 4
RISK REDUCTION ____ *4*
Safety Prerequisites ____ 4
Component Installation ____ 4
Vehicle/Component Safety ____ 5
Maintenance ____ 5
General Safety Precautions ____ 5
PRODUCT OVERVIEW ____ *6*
Applications ____ 6
System Configurations ____ 6
ALPR System Vehicle Power Draw ____ 6
Inventory Lists ____ 7
PHYSICAL INSTALLATION ____ *8*
Unpacking the ALPR System ____ 8
Damaged or Missing Item ____ 8
Planning the ALPR System Installation ____ 8
Assess Existing On-Board Systems ____ 9
Assess Power Source ____ 9
Unpacking the Mobile Cameras ____ 10
Record Each Serial and Model Number ____ 10
Identify Each Camera ____ 10
General Camera Layout ____ 10
Preparing the Zero-Clearance Bracket ____ 11
Changing the Orientation of the Zero-Clearance Bracket ____ 12
Attaching the Zero-Clearance Bracket to the Camera ____ 13
Mobile ALPR Mounting Solutions ____ 14
Mounting the Camera Assembly to the Vehicle ____ 15
Attaching a Camera to Non-Lightbar Mounts ____ 16
Mounting the Mobile Processor ____ 17
WIRING AND CONNECTIONS ____ *18*
The Power Wiring ____ 18
The GPS Antenna ____ 19
The Mobile Camera Cables ____ 19
Connecting Camera Cables to the Processor ____ 19
Connecting the GPS Antenna to the Processor ____ 20

Connecting the Networking Elements to the Processor ____ **20**
Connecting the Power Cable to the Processor ____ **21**
Confirming the Power Status ____ **21**
ALIGNMENT ____ ***22***
ALIGNMENT PROCEDURE ____ ***22***
Alignment Requirements ____ **22**
Tools Required ____ **22**
Distance Marker Diagram ____ **22**
Aligning the Front Left Camera ____ **23**
Aligning the Front Right Camera ____ **23**
Aligning the Right Rear Parking Camera ____ **24**
Aligning the Left Rear Camera ____ **24**
CALIBRATING EXPOSURE TABLES ____ ***25***
Exposure Table Best Practices ____ **25**
Setting the Exposure Table/Plate Illumination ____ **25**
MAINTENANCE AND SERVICE ____ ***26***
Qualifications ____ **26**
Servicing Mobile ALPR Cameras ____ **26**
Cleaning Mobile ALPR Cameras ____ **26**
Servicing the Mobile ALPR Processor ____ **26**
Servicing the 10.4 inch Touchscreen Monitor ____ **26**
Cleaning the Vehicle ____ **26**
APPENDIX A – ALPR COMPONENTS ____ ***27***
APPENDIX B – WIRING DIAGRAM ____ ***28***
APPENDIX C – WIRING DIAGRAM ____ ***29***

SAFETY INFORMATION

Please read, understand, and follow all safety information contained in this guide prior to any attempts to Install or use the Mobile ALPR System. Retain these instructions for future reference.

Intended System Use

The Mobile ALPR System is intended to provide Automatic License Plate Recognition (ALPR) to users by automatically “reading” number plate or license plate characters. It is expected that all users be fully trained in the safe operation of this Mobile ALPR System. Use in any other application is not condoned, may immediately void all warranties, and may lead to an unsafe condition.

RISK REDUCTION

This section lists the recommended best practices to take prior to the installation, during installation, and during operation or maintenance of the Mobile Platform. Failure to adhere to these recommendations may result in hazardous voltages, fire, property damage, and equipment failure due to impact as well as potential injury to installers and users.

Safety Prerequisites

- Refer to the vehicle's service manuals when performing vehicle equipment installation and follow accepted automotive mechanical and electrical installation procedures.
- Review the manufacturer's vehicle wiring diagram prior to the Mobile ALPR System installation to ensure the installation does not affect vehicle operation or mandated safety functions or circuits.
- Installation to be performed only by authorized personnel or certified and/or trained installers.
- Service to be performed only by authorized personnel in compliance with all local, regional, and national applicable motor vehicle codes.

Component Installation

- Do not interact with ALPR system while driving or in hazardous conditions.
- Use only the Mobile ALPR Processor, brackets, and cabling provided.
- Ensure all external electrical connections are protected from the environment.
- Do not kink or pinch cables when routing through the vehicle as this could damage the cable/system.
- Do not get metal shavings inside the Processor. Use an ESD-approved cover if drilling near unit cannot be avoided. After mounting, inspect area and remove any metal shavings.
- Do not co-locate the SX Processor within 18 inches (45.7 cm) of a radio antenna or transmitter.
- Clear both sides of vehicle structure when drilling. Remove burrs from drilled holes and use grommets for wiring. Use care when installing mounting screws.
- Do not mount cameras or components in unapproved locations or mounting brackets. Doing so may immediately void warranty and/or service contract.
- After installation of a component, ensure it is securely attached to the vehicle.
- Avoid placing a magnetic mounting bracket or other magnetic component next to an electronic device.
- Verify all component mounts, power connections and wiring are properly connected prior to powering On the system after installation, maintenance, and/or service.

Vehicle/Component Safety

- After installation, test all vehicle functions, including horn operation, vehicle safety functions, and vehicle lighting systems, to ensure proper operation.
- Ensure the installation has not affected the vehicle operation or changed any vehicle safety function or circuit.
- Locate any ALPR system controls so the vehicle can be operated safely under all driving conditions.
- Do not install equipment or route wiring in the deployment path of an air bag.
- After deployment, inspect ALPR System periodically to ensure proper operation and attachment to vehicle.

Maintenance

- Replace Mobile ALPR System fuses with same size, type, and rating specified in installation guide.
- Always keep the Mobile ALPR Processor vent areas clear.
- Keep the Mobile ALPR Processer in a dry location.
- Do not use cleaning solutions such as strong detergents, solvents, or petroleum-, alcohol-, or ammonia-based products. Use only a soft cloth and a mild soap and water solution.
- The Agency is required to open the Mobile ALPR Processor case in order to remove the battery prior to disposal.

NOTE: Opening the case of the Mobile ALPR Processor will void the warranty. Opening the case may adversely affect any future operation of the processor. Never open the case of the Mobile ALPR Processor unless authorized by PIPS Support or when removing the battery for disposal. All disposal operations must be performed within local guidelines and laws. It is the responsibility of the processer owner to ensure all local and regional regulations are followed for proper disposal.

General Safety Precautions

- Follow safe workplace practices during installation and maintenance.
- The ALPR cameras are Class 1M LED products and emit LED radiation. Do not view directly with the eye or optical instruments.
- Dispose of all system components in accordance with applicable local and government regulations.
- Dispose of lithium-ion batteries and electronic components according to all applicable recycling or waste regulations.
- Ensure to keep all fingers and items clear when mounting magnetic camera brackets.

PRODUCT OVERVIEW

This section discusses the general application, configuration, and ALPR system information.

Applications

- Law Enforcement
- Parking Enforcement
- Community Service Vehicles
- Private Security Vehicles

System Configurations

The PIPS ALPR Mobile SX Processor can be configured in two distinct ways; Client/Server or Stand Alone.

Client/Server (VPRelay) Mode:
The Client/Server configuration consists of a Mobile ALPR Processor, up to four ALPR cameras with mounting brackets, and a network connection to a Mobile Data Computer (MDC)/laptop in the front of the vehicle. The ALPR processor collects images and data for license plate recognition and relays it to the MDC over a static network connection. The primary advantage of the Client/Server configuration is that it allows a user to be notified of "alerts" while operating the vehicle. This is done through mobile ALPR software called "PAGIS" running on the laptop/MDC and displaying the ALPR data inside the vehicle.

Stand-Alone Mode:
The Stand-Alone configuration consists of a Mobile ALPR Processor, up to four mounted ALPR cameras, and a touchscreen monitor. The self-contained system performs all plate recognition and runs its own copy of the PAGIS software. The primary advantage of the Stand-Alone configuration is its deployment flexibility as it does not require the agency to own and maintain MDCs/laptops. Some utilization examples are speed trailers, parked covert vehicles, or in manned patrol units (when equipped with touchscreen monitors and a hotspot/cellular data network).

ALPR System Vehicle Power Draw

When off, the ALPR system should draw around 20miliamps. The chart below shows the power draw when operational.

Component	Current Draw	Total Draw
SX Processor	3.5 A @ 12VDC	3.5 A @12VDC
Camera 1	1.0 A @ 12VDC	4.5 A @12VDC
Camera 2	1.0 A @ 12VDC	5.5 A @12VDC
Camera 3	1.0 A @ 12VDC	6.5 A @12VDC
Camera 4	1.0 A @ 12VDC	7.5 A @12VDC

NOTE: *These calculations do NOT include load from the MDC, Touchscreen monitor, or GPS antenna*

Inventory Lists

Below are the two most common system architectures.

Mobile Law Enforcement Package (Client/Server architecture):

- Mobile ALPR Camera(s) with appropriate infrared illumination
- Mobile ALPR Processor with camera, HDMI, Display Port, and USB 3.0 ports
- Mobile ALPR Processor power cable (three wire)
- Camera cables/connector(s)
- Accessory Kit including Antennas (when applicable)
- Garmin GPS Antenna (16x HVS)
- CAT 5E network cable (25ft.)
- ALPR/OCR Engine specifically for customer region inside the SX4e
- Lightbar Mounting Bracket(s) and Plate(s) for approved lightbar assemblies
- OPTIONAL – Mobile Mounting Bracket
- OPTIONAL – Garmin 16 GPS mount, trunk clip

NOTE: *Approved lightbar assemblies include Federal Signal, Whelen Liberty, Justice and Edge, Code3 Defender, Tomar, and other 13.25-inch and 16.25-inch bars. Non-approved lightbar mounting designs are available but may incur a design charge. Please check with your Sales representative.*

Mobile Law Enforcement Package (Stand-alone architecture):

- Mobile ALPR Camera(s) with appropriate infrared illumination
- Mobile ALPR Processor with camera, HDMI, Display Port, and USB 3.0 ports
- Mobile ALPR Processor Power cable (three wire)
- Camera cable/connector(s)
- Accessory Kit including Antennas (when applicable)
- Garmin GPS Antenna (16x HVS)
- 10.4 Inch Touch Screen Monitor with HDMI and two USB cables (25ft. ea)
- DC-DC power adapter for the touch screen monitor
- License Plate Capture Software (PAGIS) on the SX Processor
- ALPR/OCR Engine specifically for customer region on the SX Processor
- Lightbar Mounting Bracket(s) and Plate(s) for approved lightbar assemblies
- OPTIONAL – Mobile Mounting Bracket
- OPTIONAL – Third party mounting bracket for 10.4 inch monitor (based on vehicle)

NOTE: *Approved lightbar assemblies include Federal Signal, Whelen Liberty, Justice and Edge, Code3 Defender, Tomar, and other 13.25-inch and 16.25-inch bars. Non-approved lightbar mounting designs are available but may incur a design charge. Please check with your Sales representative.*

PHYSICAL INSTALLATION

This section discusses the aspects of the unboxing and physical installation of the ALPR system and its components.

Unpacking the ALPR System

Carefully unbox the ALPR platform, its components, as well as any other products included in the shipment. Inspect each item for any damage caused by shipping prior to installation.

Damaged or Missing Item

If an ordered product is missing, or was damaged during shipping, it cannot be used for installation. Immediately call ALPR Support at (833) 747-7577 Option 2 or email Support@PIPSTechnology.com to generate a support case (Please reference the order number).

Planning the ALPR System Installation

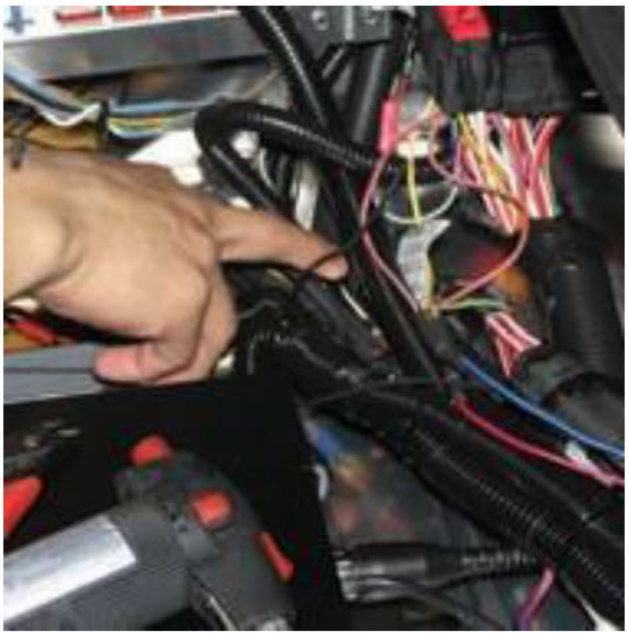
Be sure to assess the vehicle type before moving forward with any installation. Certain vehicle types may require variations of the installation process. For example, the lengths of wiring/cabling needed for an SUV are generally greater than what's needed for a sedan. Understanding these details ahead of time are highly recommended.



Shown - Ford Police Interceptor Utility and Police Interceptor Sedan. Photo courtesy of Ford Motor Company.

Assess Existing On-Board Systems

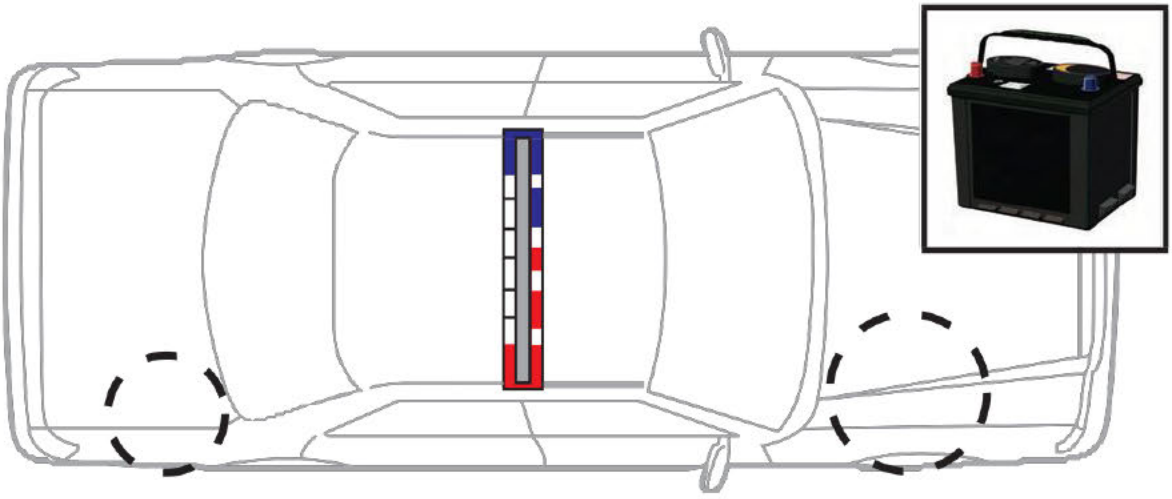
Before any installation steps, the installer should fully understand how each on-board system, radio, laptop, lightbar, etc., has been wired in the vehicle. He/she should then plan the Mobile ALPR Processor installation to take advantage of any existing power taps, wire runs, or other outfitter wiring systems. **NOTE**: To prevent malfunction or potential electrical damage, the installer should also take care to not overload any of the existing vehicle circuits.





Assess Power Source

Most police package vehicles have power distribution in the trunk or in the back of the vehicle. This is the preferred power source for the Mobile Processor. If a power tap is not found, the power must be run to the battery. Be sure to add an in-line fuse at the battery. **NOTE**: For more detail refer to Appendix B and C



Unpacking the Mobile Cameras

Each camera and mounting bracket are packaged individually. Best practice recommends the agency keep the shipping box of each bracket and camera in the unlikely event the unit needs to be returned. If it's not possible to temporarily save the shipping containers, they should be sent to an appropriate recycling center.

Record Each Serial and Model Number

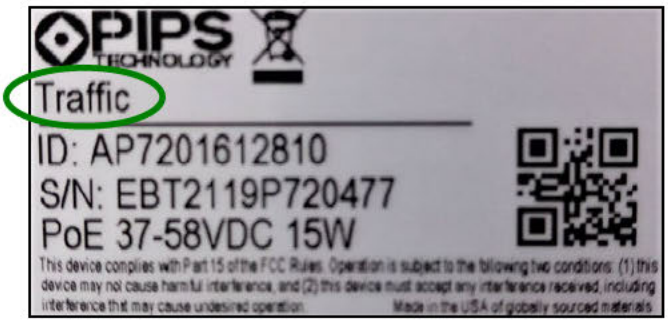
Note the serial and model numbers on the label of the product housing and record it for reference.
IMPORTANT: Please have the model and serial numbers available whenever Customer Support is contacted.

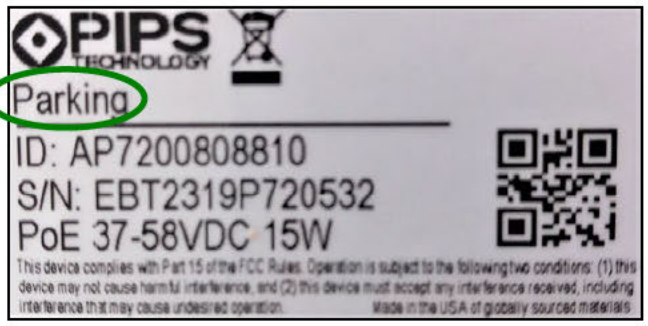
Identify Each Camera

Before mounting cameras to the vehicle, they should be checked for any damage, identified to confirm illumination uniformity, and assigned to the proper mounting locations based on lensing. The steps to identify the cameras and lensing are below:

1. Locate the Identification Label (Contains Serial and Model/ID Number)
2. The Label should say "Traffic" or "Parking"
    a. Traffic cameras are designed to view plates farther down the adjacent lanes
    b. Parking cameras are designed to view plates closer to the ALPR vehicle
3. Make note of the ID Number (This is the "Model Number")
4. Use ID/Model number information to select each camera position

How to Read the ID/Model Number: Example: AP7201612810
[Product: AP720] + [IR Lens: 16] + [OV Lens: 12] + [Illumination Wavelength: 810]





General Camera Layout

The proper mounting location is extremely important to overall function. Placing a camera in the wrong position on the vehicle will reduce the ALPR performance to almost zero. Below is the most common mounting layout:

1. The front left, and front right cameras are nearly always Traffic cameras.
2. The right rear side camera is nearly always a Parking camera and aimed perpendicular to the vehicle.
3. The left rear side camera can either be a second perpendicular parking camera or it can be a rear facing traffic camera.
    a. The advantage of the rear facing camera is its ability to capture rear plates of opposing traffic. This is especially useful in rear license plate only states.

For more detailed mounting information, refer to the alignment section.

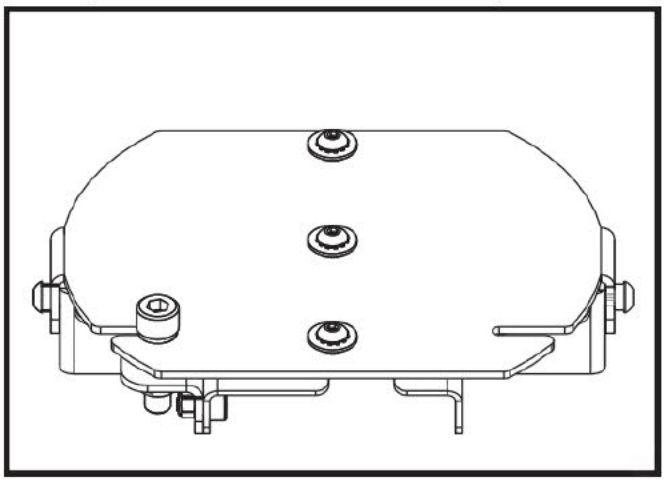
Preparing the Zero-Clearance Bracket

Once the proper camera configuration is determined for the vehicle, it's time to prepare the mounting brackets. There are two bracket configurations, a driver's side or left-handed bracket, and a passenger's side or right-handed bracket. When viewing the bracket from the rear and face up, the right-hand bracket will have the adjustment screw on the right. Since all brackets come this way, the installer will need to manually configure any required left-hand brackets.

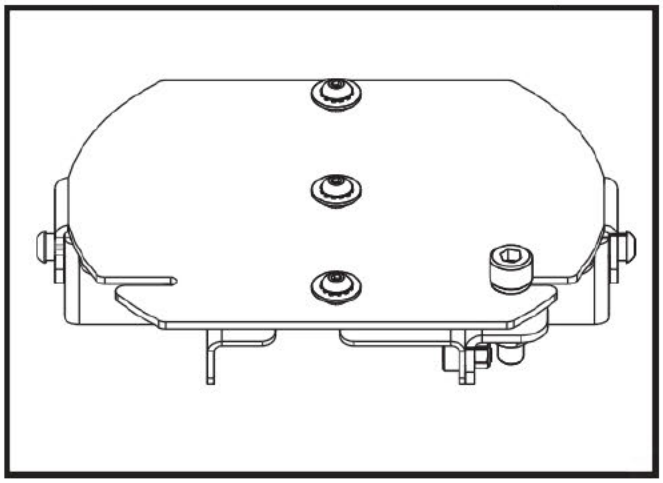
PRO-TIP: To assist with maintenance, PIPS recommends the use of an anti-seizing agent on all screws/bolts for the entire light bar and bracket system.

NOTICE: Zero-clearance brackets only ship with lightbar mounting configurations. Be sure to work with the Sales Department to procure the proper packages for each vehicle.

Left-Hand or Driver's Side Bracket



Right-Hand or Passenger's Side Bracket



Typical Camera and Bracket Configurations

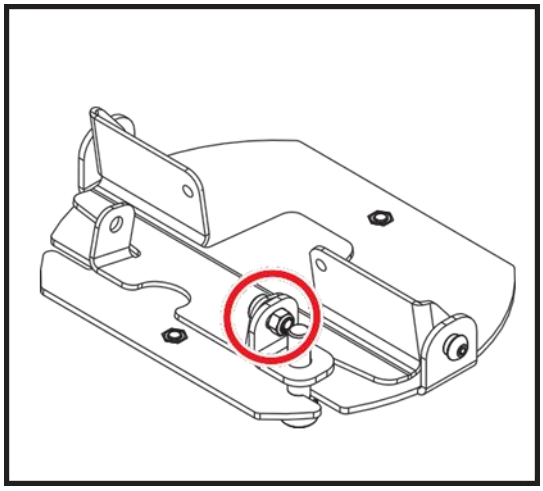
The chart below illustrates the combination of the camera position and the corresponding bracket configuration.

Camera location	Camera type	Bracket type	Camera number
Front/Left	Traffic	Left-hand	1
Front/Right	Traffic	Right-hand	2
Rear/Left	Traffic	Left-hand	3
Rear/Left	Parking	Left-hand	3
Rear/Right	Parking	Right-hand	4

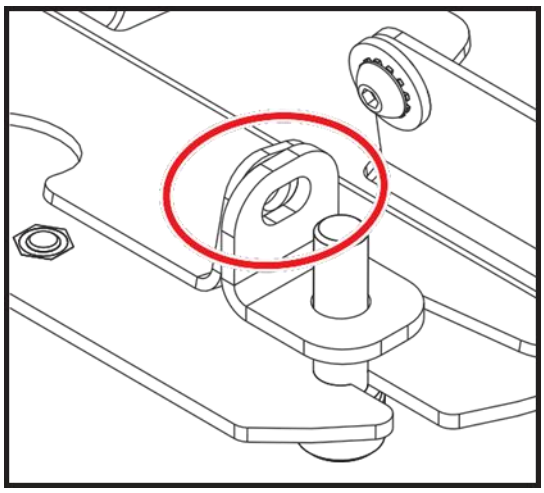
Changing the Orientation of the Zero-Clearance Bracket

In order to convert one or more of the right-hand brackets to left-hand brackets, follow the steps below:

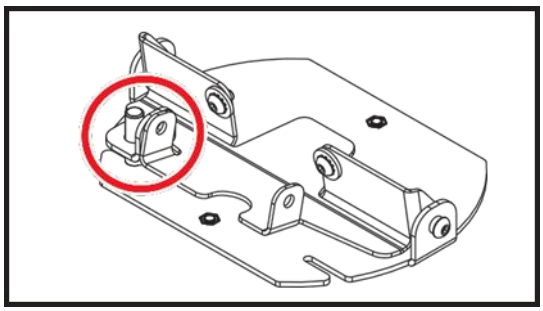
1. Locate the pivot screw on the bracket



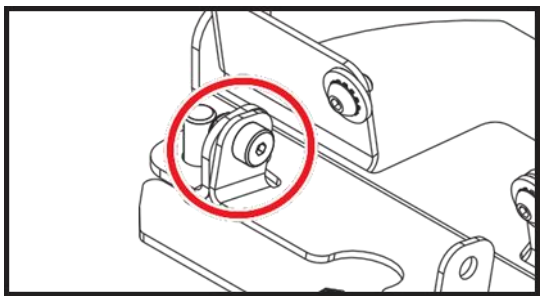
2. Remove the pivot screw from the bracket



3. Slide the pivot screw bracket from the slot and move it to the opposite side of the assembly

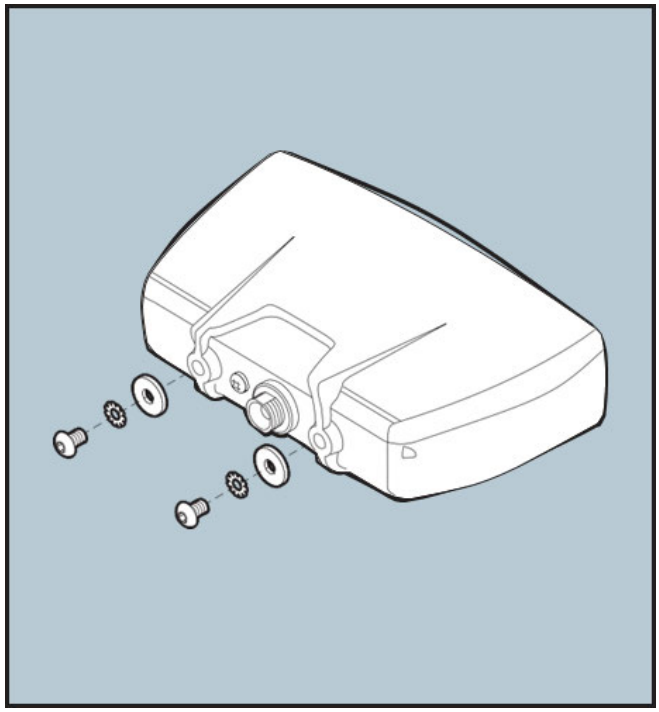


4. Reattach the pivot screw to complete the conversion



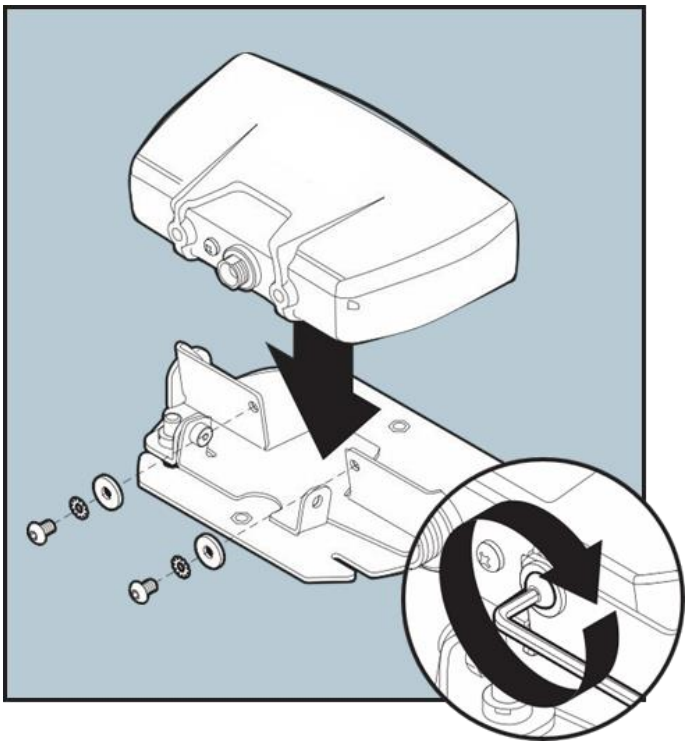
Attaching the Zero-Clearance Bracket to the Camera

Once all the brackets are assembled, the mobile cameras should be mounted to the brackets.



1. Remove the screws, star washers, and flat washers from the mounting holes at the rear of the camera.

2. With the camera and bracket upside down, install the zero-clearance bracket by sliding the bracket tongue into the camera groove. The camera groove is located on the top rear of the camera.



3. When the tongue is fully seated in the groove, place the star washers and flat washers on the screws. Tighten the screws in the mounting holes.

Mobile ALPR Mounting Solutions

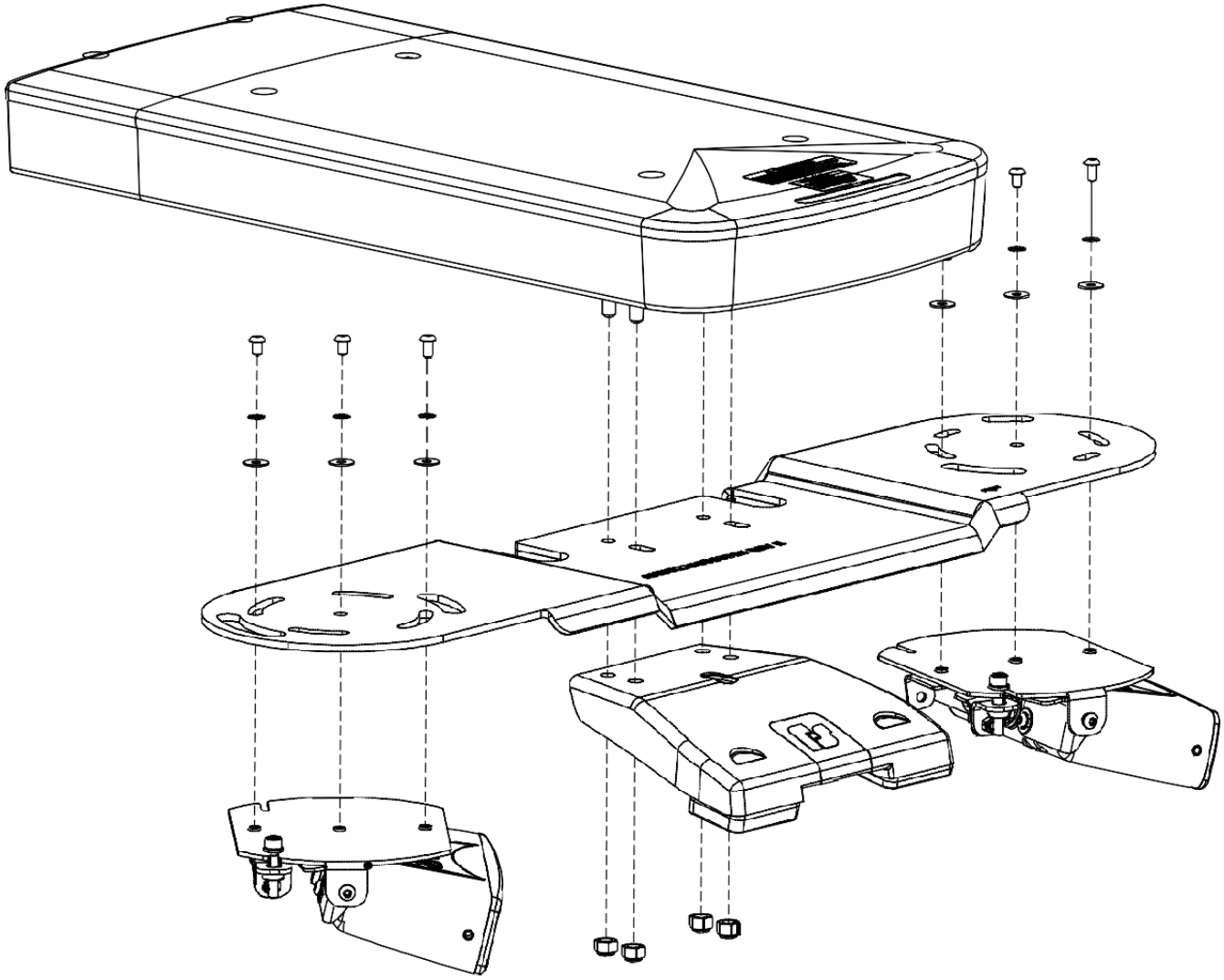
Below are examples of some of the mounting options available.

Supported Lightbar Mounting Options (Manufacturers):

- Federal Signal: Legend, Integrity, Argent, Vista, Raydian, Valor, Vision
- Code3: Defender 13.25 inch & 18 inch wide models
- Whelen: Edge, Justice, Liberty, Legacy, Freedom
- Tomar lightbars
- Unmarked Vehicle lightbar, Federal Signal product

Supported Non-Lightbar Mounting Options:

- Trunk Mount, Single or Dual Options
- Magnet Mounts (supports most vehicles with metallic/ferrous panels)
- Gutter Mounts (support Ford Police Interceptor models and Chevy Tahoe)



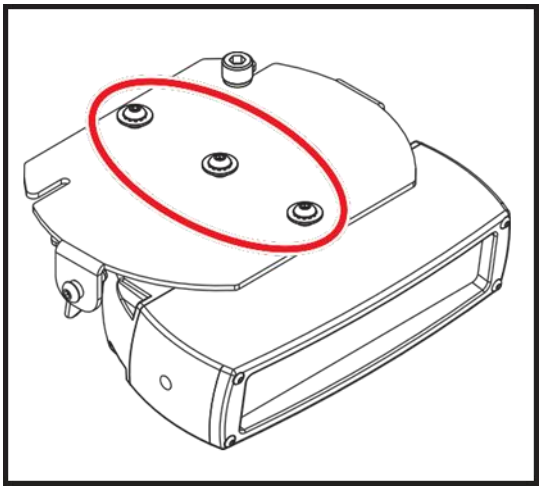
Shown - Classic Lightbar Bracket (Federal Signal "LEGEND")

Mounting the Camera Assembly to the Vehicle

The camera mounting assembly is then installed to the mounting plate attached to the lightbar.

NOTE: Due to the large number of variations between lightbars and mounting plates, this document only illustrates how to attach the camera mounting assembly to an existing mounting plate

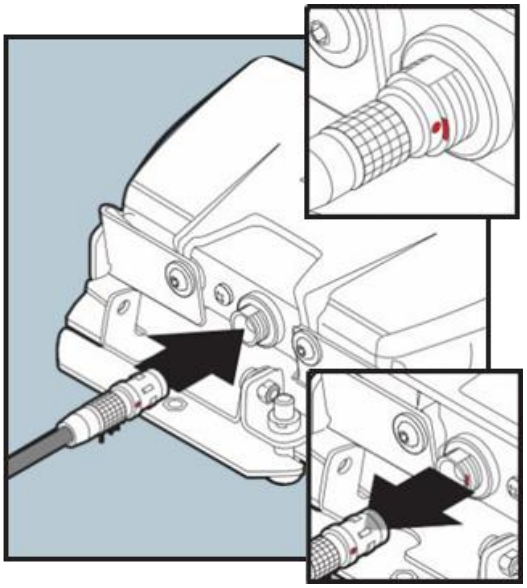
1. With the camera bracket attached to the camera, remove the three screws, star washers, and flat washers.



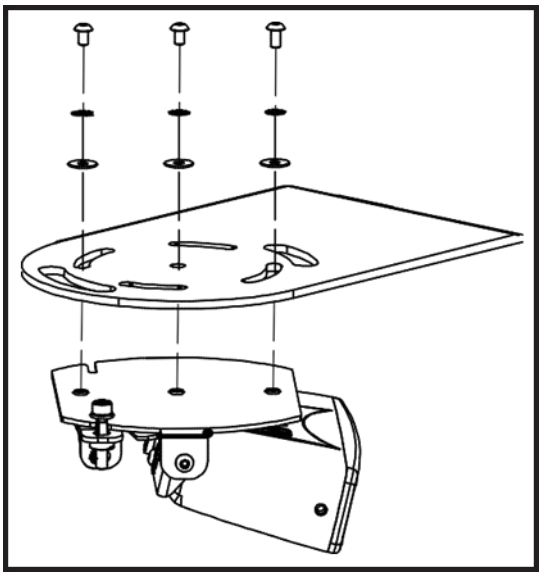
2. Connect the camera cable to the camera:
Align the red dot on connector with red mark on the port and connect using minimal force.

DO NOT FORCE OR TWIST THE CONNECTION. If the connector does not snap in easily, pull the connector out and realign.

PRO-TIP: PIPS recommends use of a bit of di-electric grease in and on the cable connectors.

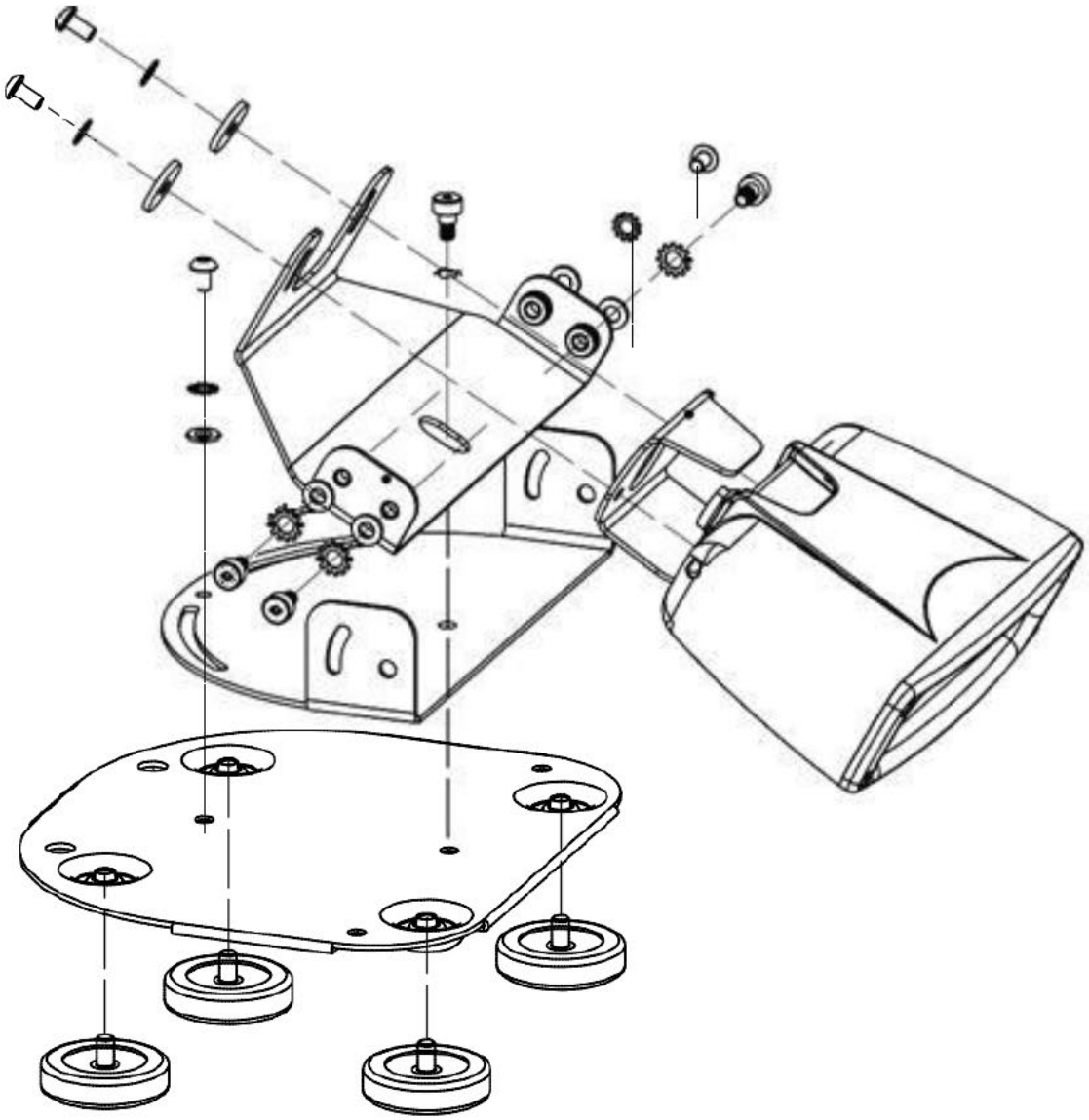


3. Attach the camera mounting assembly/plate to the lightbar bracket. **NOTE**: If the camera isn't perfectly secure, use the stabilizing foot included with the bracket to provide additional stability.



Attaching a Camera to Non-Lightbar Mounts

All Non-Lightbar mounting solutions utilize the Auxiliary 3 axis mounting plate. Once the camera is securely attached to the Aux mounting plate, attach it to the base plate of your bracket.



Shown – Magnet Mount

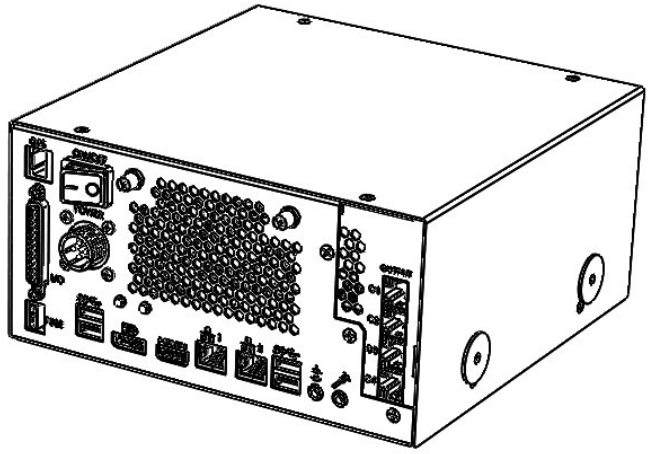
Mounting the Mobile Processor

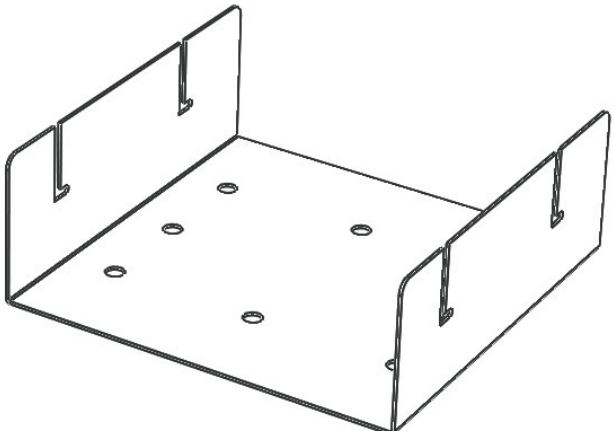
Understanding the vehicle and its current systems is a must when selecting the mounting location of the SupeRex (SX) Processor. Below are the key considerations:

- If the vehicle does not have a utility drawer/tray, be certain of all vehicle systems before drilling or mounting.
- The SX Processor and its bracket can be safely mounted in any orientation.
- Mount the unit with easy access to the rear panel and cables for maintenance/service.
- Be sure to leave adequate room for ventilation, cabling, and any maintenance needs.
- If the vehicle has a utility drawer/tray, mount the SX with enough clearance for ventilation, cabling, and service.
- Before mounting, physically place the SX in the mounting space to properly assess clearance or any dangers.
- Mount the bracket first, then secure the Mobile Processor to the bracket.

Additional Mounting Bracket Considerations:

- The Mobile Processor bracket comes with eight pre-drilled holes (0.375 in dia.). Use at least four of them to mount the bracket to the utility tray or trunk surface.
- For utility tray mounting, secure the unit using at least four 1/4-20UFC-2A bolts with appropriate washers and lock nuts. Hardware not provided.
- For direct trunk surface mounting, secure the unit using at least four #14 (or #16) sheet metal screws with appropriate washers. Hardware not provided.





WIRING AND CONNECTIONS

This section discusses the proper wiring and physical connections to the Mobile Processor. PIPS highly recommends the agency review the owner's manual of the ALPR vehicle to be certain of how to safely run cables and avoid vehicle/equipment damage. The agency is also responsible to fully understand how to safely tie into the on-board electrical systems in the vehicle.

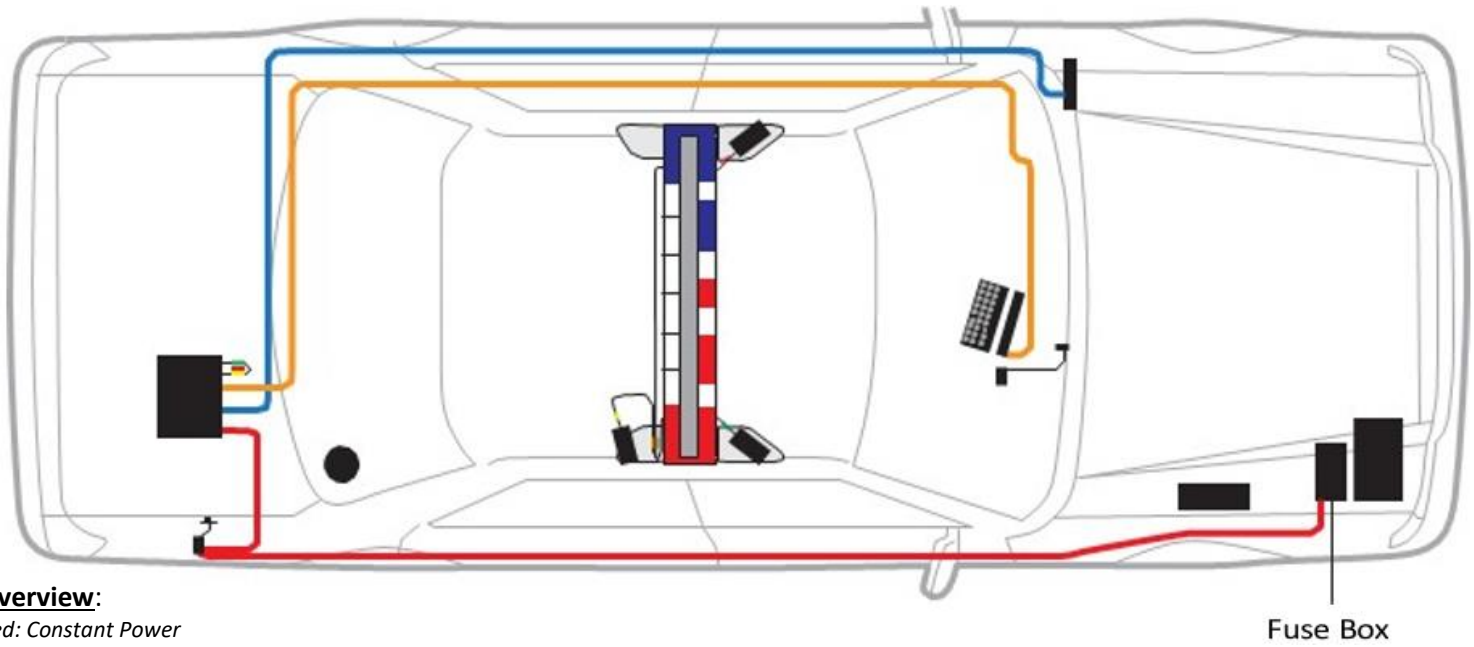
NOTE: Failure to adhere to this recommendation may immediately void all warranties and maintenance agreements.

The Power Wiring

The power cable provided with the Mobile Processor is a 3-wire connector. **NOTE**: The provided length of cable may not fit all vehicles. If wires must be extended, use 14 gauge or heavier. Min draw on 1 Cam system= 4.5AMPS, Max draw on 4 Cam system is 7.5AMPS.

1. Route the red wire (positive) from processor to a constant battery source. For example, a fused connection to the battery or to a vehicle power terminal block. Recommended fuse 20 amps.
2. Route the black wire (ground) from processor to vehicle ground tap.
3. Route the blue wire (remote) from processor to vehicle's ignition (key) source in the fuse panel or police packaging wiring harness. Recommended fuse 5 amps.





Overview:

Red: Constant Power
Blue: Remote/Ignition source
Black: Ground (barely visible off side of Processor)
Gold: Network (CAT5) to laptop or HDMI cable to front touchscreen

The GPS Antenna

The included GARMIN GPS antenna is a powerful omnidirectional receiver that can be mounted in any location with a line of sight to the sky.

1. Locate a position in, or on, the ALPR vehicle with a line of sight to the sky. Common zones are front dash, rear dash, rear window ledge, or on top of the vehicle.

2. Attach the hook side of hook-and-loop take to the underside of the GPS module.

3. Mount the antenna and route the GPS cable to the SX Processor.



GPS 16xHVS: Black PVC-jacketed, 5-meter, foil-shielded, 8-conductor 28 AWG with RJ-45 termination is waterproof up to 1m. Standby Current: < 10 microAmps

The Mobile Camera Cables

As mentioned previously, it's extremely important to review the vehicle manual when running the mobile camera cables.

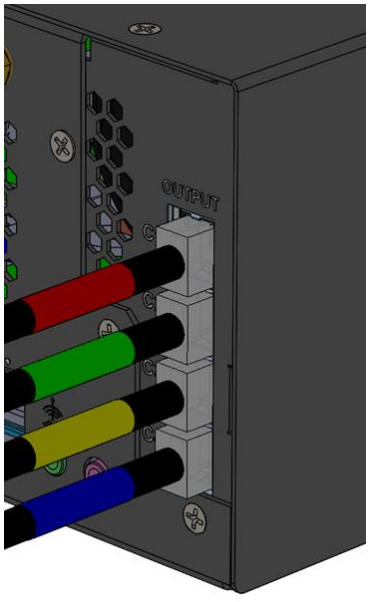
1. Locate the colored indicator rings that came with the Mobile Processor shipment.
2. Band and layout the camera cables to ensure the proper cables are going to the correct camera locations.
3. When run through the vehicle, be certain the cables do not get pinched or impede any of the vehicle airbags.

Color Coded Cable Rings:
Red: Front Left Camera
Green: Front Right Camera
Yellow: Rear Left Camera
Blue: Rear Right Camera

Connecting Camera Cables to the Processor

Connecting the P720 camera cables to the Mobile Processor is straight forward and as easy as plugging in a network cable. After the cables have been safely run through the vehicle, simply plug in the network (RJ45) connector to the appropriate camera port on the Processor (labeled C1-C4).

- Camera 1 Front Left (C1) = Red
- Camera 2 Front Right (C2) = Green
- Camera 3 Rear Left (C3) = Yellow
- Camera 4 Rear Right (C4) = Blue



Connecting the GPS Antenna to the Processor

After the antenna is placed with a line of site to the sky and its cable is securely run back to the Processor, simply plug in the RJ45 connection to the port labeled "GPS" located in the upper left corner of the rear I/O panel.

CAUTION: Plugging the GPS antenna into the wrong port may cause equipment damage and immediately void all warranties. Do **NOT** plug the GPS cable into a NIC or camera port. Do **NOT** plug a camera or network cable into the GPS port.

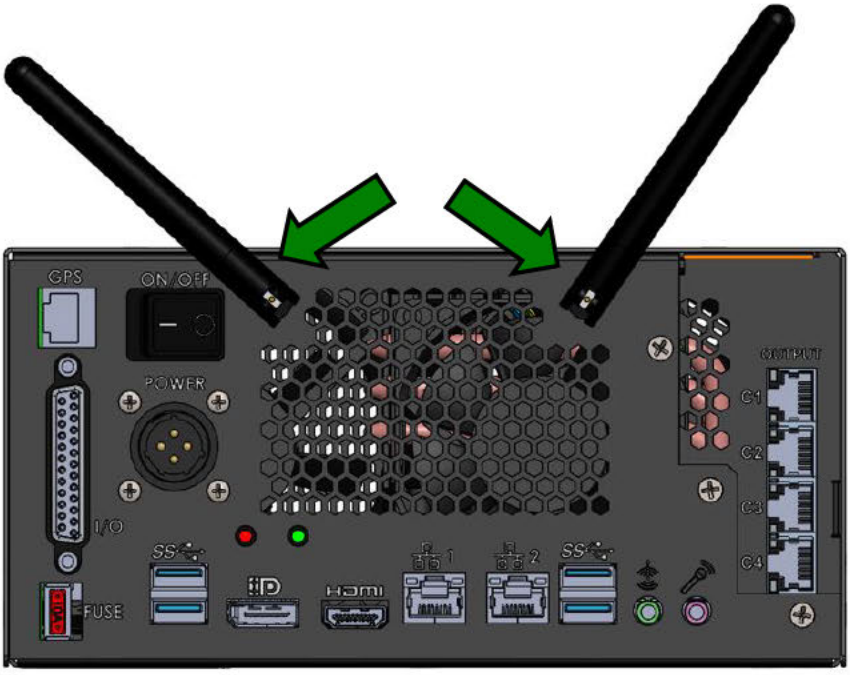


Connecting the Networking Elements to the Processor

The next step is to connect the networking option to the Processor. The most common method is a physical CAT5/6/7 cable from the Processor's NIC port 1 to an MDC/Laptop in the front of the vehicle.

NOTE: The on-board NICs are auto-switching. Meaning the agency can use either a standard network cable or a cross-over cable with no issues.

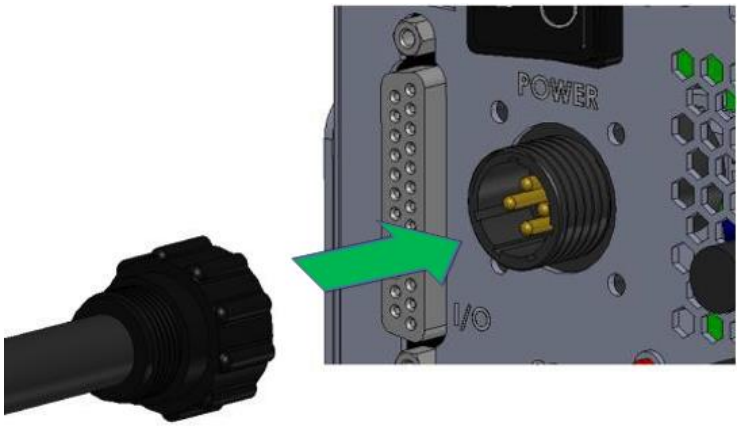
OPTION: In less than 1% of domestic orders, the Mobile Processor is built with Wi-Fi connectivity enabled. If the agency ordered this option, locate the two antennas from the accessories kit shipped with the Processor and install them to the Wi-Fi Networking Posts at the back of the Processor as shown below.

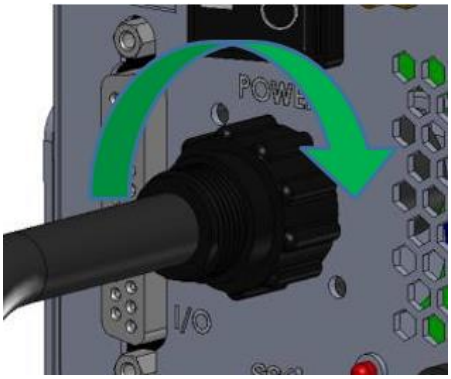


Connecting the Power Cable to the Processor

The last step in connecting all the cables to the Processor is to attach the power cable.

1. Align the notch on the power cable with the connection on the Processor
2. Insert the power cable onto the connection – DO NOT FORCE THE CABLE
3. After seating the cable properly, tighten the screw coupling/locking nut until snug – DON'T OVER TIGHTEN



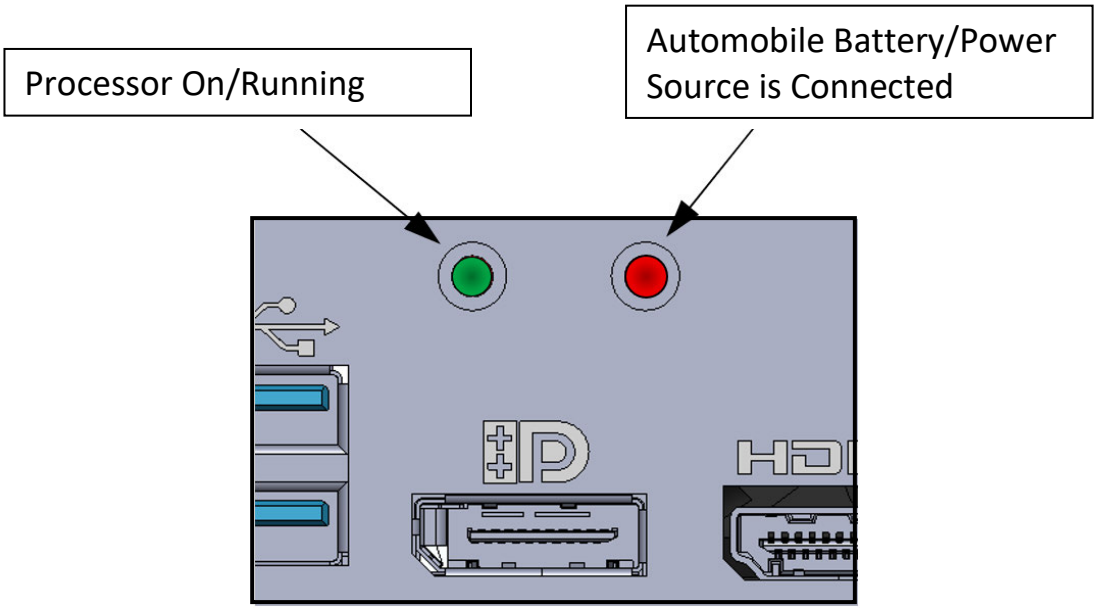


Confirming the Power Status

With all the vehicle wiring complete and the cables connected to the Processor, flip the power switch on the Processor to the On position and start the vehicle. Information on the status lights is below.

- The ignition sensitive fuse (blue wire) will register the start of the vehicle and energize the Processor
- Both the Red and Green LED status lights should illuminate
- The unit will POST and play audible tones (and the fans should spin)
- When ignition power is removed, the Processor will begin its shutdown process, indicated by the green LED flashing
- When the shutdown timer has finished, the unit will completely shut down, indicated by the green LED going out
- Conversely when the ignition is activated, the green light will come on.

NOTE: It is normal for the red LED to stay illuminated. Expected power draw while in standby is roughly 20-40 milliamps.



ALIGNMENT

The purpose of this section is to provide the best practices for the proper alignment of the PIPS Mobile ALPR Dual-Lens Cameras. The more accurate the alignment and illumination, the more effective the ALPR system will be. The values below should be considered as a baseline for general alignment and positioning of the cameras. Based on varying agency vehicles, mounting locations, and use-case scenarios, some fine tuning may be required.

ALIGNMENT PROCEDURE

The steps below assume the ALPR system has been successfully installed, the SX Processor is properly communicating with the cameras, and PAGIS (or Mobile Toolkit) is properly configured and functioning. NOTE: The greater the care taken during this process, the more accurately the ALPR system will perform in the field.

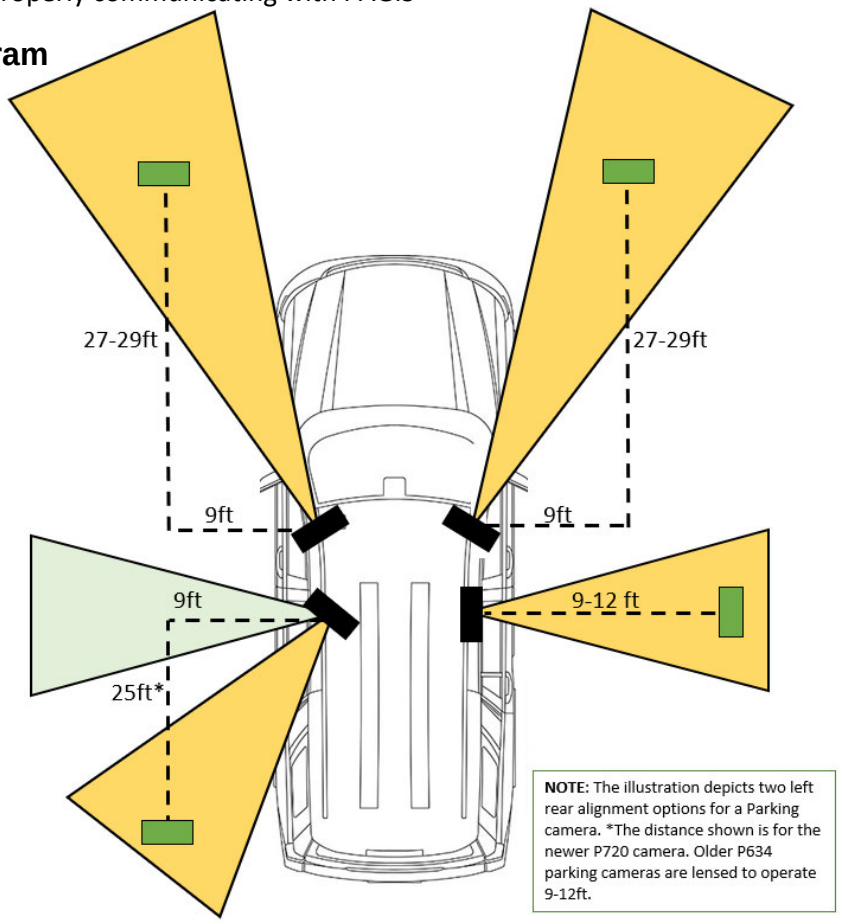
Alignment Requirements

- Large flat area without incline/decline (Ideal dimensions: 30 feet wide by 50 feet deep)
- No atmospheric conditions like fog or rain
- MEASURE ALL DISTANCES FROM THE CAMERA (NOT THE VEHICLE)
- Tripods or stands are stable and place the center of the License Plate at 32 inches above the ground

Tools Required

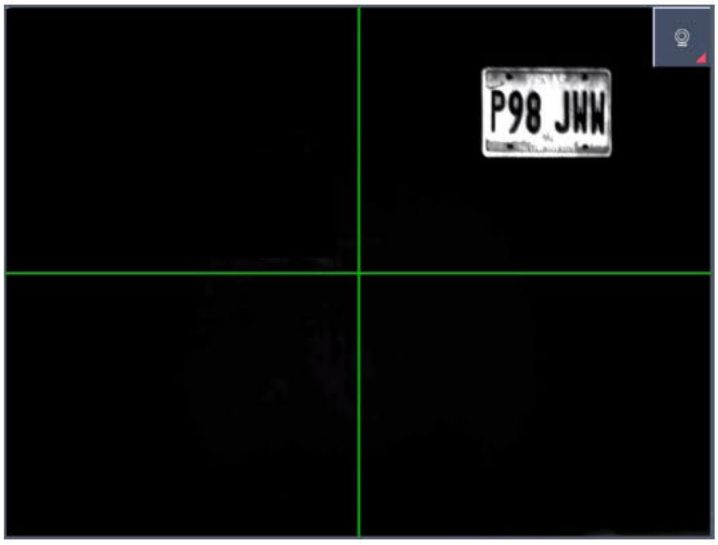
- Step Ladder
- #3, #3.5, and #4 hex/Allen wrench
- Chalk or Tape to mark the ground for template plate distances
- Tripod, tall parking cone, or box to secure test plates at 30-36” above the ground
- Tape measure or distance wheel
- Test license plate
- A configured MDC properly communicating with PAGIS

Distance Marker Diagram



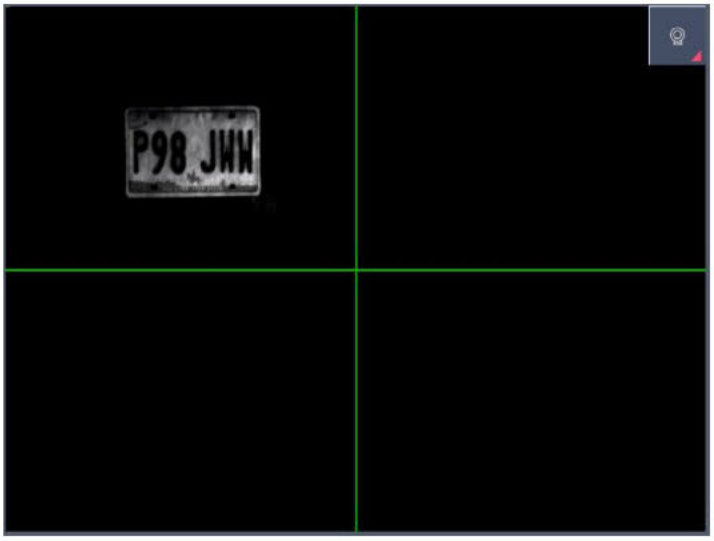
Aligning the Front Left Camera

- Place the completed plate stand on the distance marker
- Launch PAGIS from the MDC
- Login with Admin rights
- Click the Settings button from the top navigation menu (PAGIS 2.12 and above)
- Scroll down on the right-side menu and select “Cam Setup”
- Click the camera name to be aligned
- Use the camera view toggle button to confirm the proper camera is selected then switch the view to Infrared (IR)
- Loosen the mounting screws on the camera bracket just enough to allow for movement
- While monitoring the IR camera feed, position the camera so the plate is viewed as shown below
- Once set, tighten the mounting screws on the bracket to lock the camera in place



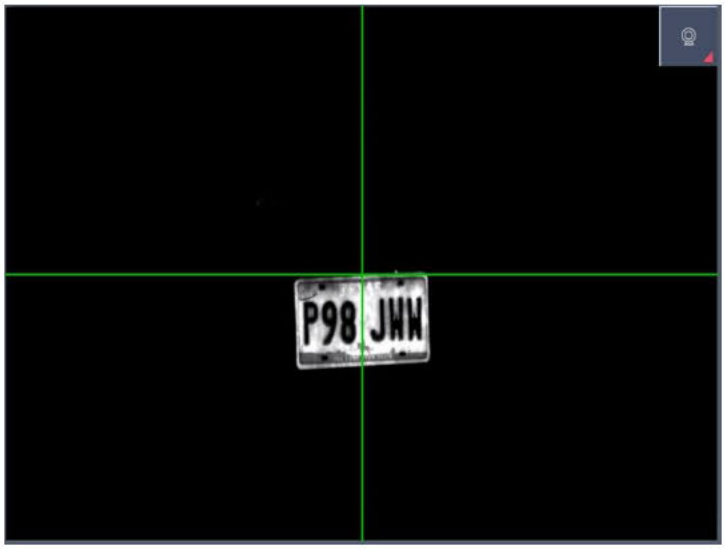
Aligning the Front Right Camera

- Use the preparatory alignment steps from above
- While monitoring the IR camera feed, position the camera so the plate is viewed as shown below
- Once set, tighten the mounting screws to lock the camera in place



Aligning the Right Rear Parking Camera

- Measure 10-12ft to the right side of the vehicle (from the parking camera)
- Place a completed plate stand at the mark
- Launch PAGIS from the MDC
- Login with Admin rights
- Click the Settings button from the top navigation menu (PAGIS 2.12 and above)
- Scroll down on the right-side menu and select "Cam Setup"
- Click the camera name to be aligned
- Use the camera view toggle button to confirm the proper camera is selected then switch the view to Infrared (IR)
- Loosen the mounting screws on the camera bracket just enough to allow for movement
- While monitoring the IR camera feed, position the camera so the plate is viewed as shown below
- Once set, tighten the mounting screws on the bracket to lock the camera in place



Aligning the Left Rear Camera

- Parking Option: Follow the steps for the Right Parking Camera
- Rear Facing Parking Camera Option: Measure 9 feet out and 25 feet down the lane
- Rear Facing (Third) Traffic Camera Option: Follow all steps for front left camera
    - Launch PAGIS from the MDC
    - Login with Admin rights
    - Click the Settings button from the top navigation menu (PAGIS 2.12 and above)
    - Scroll down on the right-side menu and select "Cam Setup"
    - Click the camera name to be aligned
    - Use the camera view toggle button to confirm the proper camera is selected then switch the view IR
    - Loosen the mounting screws on the camera bracket just enough to allow for movement
    - While monitoring the IR camera feed, position the camera so the plate is viewed as shown below
    - Once set, tighten the mounting screws on the bracket to lock the camera in place

CALIBRATING EXPOSURE TABLES

Proper plate illumination is necessary for the mobile ALPR system to function correctly. Administrators should take care not to under or over saturate the plate with Infrared (IR) light. Use the steps below to discover the plate "standard" and then select values just above, and just below that starting point to account for varied environmental conditions over time.

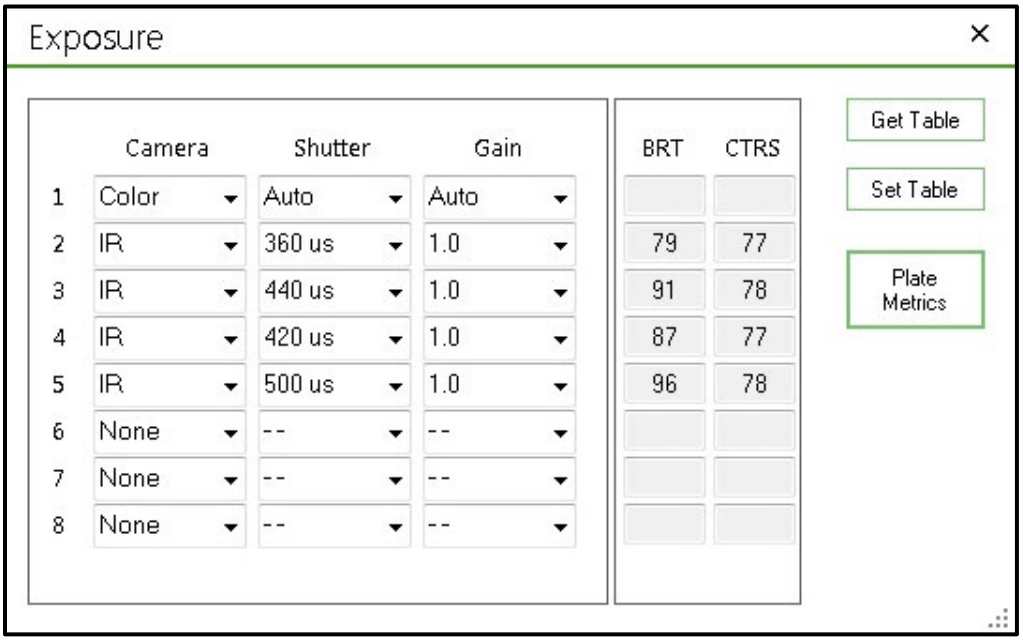
Exposure Table Best Practices

- Only calibrate 1 license plate at a time
- Only use a Gain setting of 1 or 1.5 (values above 1.5 amplify visual "noise" and could lead to misreads)
- Use 1 Color setting and 4 IR settings

Setting the Exposure Table/Plate Illumination

1. Remote Desktop to the SX4e
2. Open Tools from the Desktop
3. Launch Mobile Toolkit
4. The default view is the Infrared (IR) feed of the left front camera (Input 1)
5. Use the Input menu to navigate to the camera to be configured
6. Then from the Settings Menu, select "Exposure"
7. Be sure the plate is clearly viewable for the distance to be calibrated
8. Click the "Get Table" button to import the current exposure settings from the camera
9. Next, use the "Plate Metrics" button to analyze the current illumination
10. Adjust the exposure settings to increase or decrease illumination as necessary
    a. Increasing the Exposure will increase the Brightness (BRT) and Contrast (CTRS)
    b. Ideal BRT is above 60 **NOTE**: BRT over 90 begins to over-saturate the plate and could lead to misreads
    c. Ideal CTRS is roughly 80 (the higher the contrast the better)
11. Be sure to re-run Plate Metrics after each adjustment to the exposure table
12. Once the ideal value is discovered, fill in the other IR fields with values just above, and just below this ideal setting to account for varied atmospheric possibilities
13. Leave the Color setting to "Auto"
14. When all values are selected, click the "Set Table" button to save the changes
15. Then move on to the other cameras

NOTE: In order to read plates two lanes over, the exposure settings will need to be close to the maximum settings. This will over-expose some of the near lane plates and is the tradeoff made by agencies looking to expand ALPR coverage. An example of those settings is below.



MAINTENANCE AND SERVICE

This section discusses the general service and maintenance of the Mobile ALPR System.

Qualifications

To properly install or service the ALPR system, the technician must have a good understanding of automotive electrical systems as well as a proficiency in maintaining computer systems and networks in a mobile environment.

Servicing Mobile ALPR Cameras

Establishing a regular maintenance schedule for the Mobile ALPR cameras extends the life of the system and ensures safety. Periodically check the Mobile ALPR cameras to ensure the camera lenses are clean, all LEDs illuminate when the system is operating, and that all mounted hardware is securely fastened to the vehicle. Also, inspect the camera front cover for cracks, crazing (hairline cracks), discoloration, and other defects.

CAUTION: DO NOT open the camera housing. Each camera is nitrogen purged to remove moisture. If the camera is opened moisture will enter the camera resulting in potential damage to the electronics and accumulation on the lenses. If the camera is opened the warranty is void. For service, support, or replacement please contact Customer Support.

Cleaning Mobile ALPR Cameras

The lens of the camera should be cleaned before each use. Accumulation of insects, road grime, and other debris can obstruct the camera and reduce the plate read capability. To clean the lens, do not use an alcohol or ammonia based cleaner like Windex. Cleaners containing these compounds can damage the polycarbonate cover. PIPS Recommends use of a microfiber cloth and a mild soap and water solution.

Servicing the Mobile ALPR Processor

The housing of each Processor is sealed. If the seals are broken, the warranty of the unit will be void. Software and firmware can be updated at the direction of Customer Support.

Servicing the 10.4 inch Touchscreen Monitor

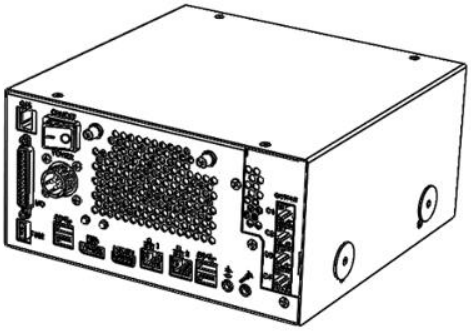
If monitor issues develop, first check the power and video connections. Make sure the cords are connected properly and are not twisted. Then clean the touchscreen. The touchscreen monitor should be cleaned before each use. Oils from fingers accumulate on the screen and can erode performance. To clean the screen DO NOT USE an alcohol or ammonia based cleaner. Cleaners containing these compounds can damage the touch screen. Use of an anti-fog, anti-static cleaner and a microfiber cloth.

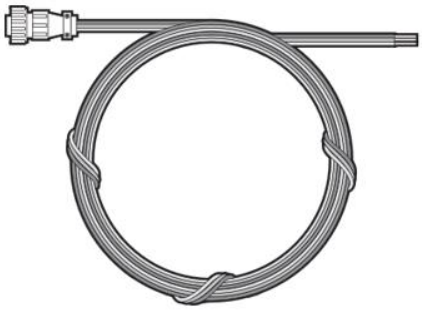
Cleaning the Vehicle

When washing the vehicle, it's best to avoid automatic car washes that use the older rotating nylon bristles. The fibers can become lodged in the camera brackets and misalign the cameras or damage the acrylic cover plate. Automatic car washes that use Soft Cloth or touchless (high pressure spray) can be used as they do not pose a risk to the cameras. For non-lightbar mounting solutions, it is not recommended to use rotating car wash systems for any brackets that use magnets to secure them to the vehicle.

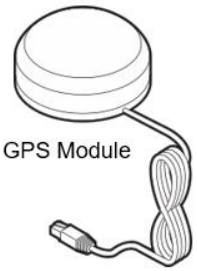
APPENDIX A – ALPR COMPONENTS

Standard Components

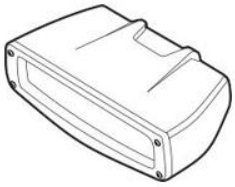




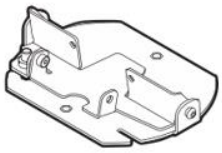
Mobile ALPR Processor
Power Cable



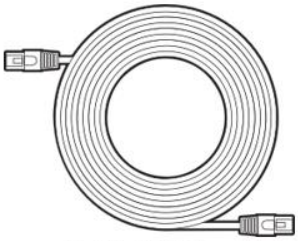
GPS Module



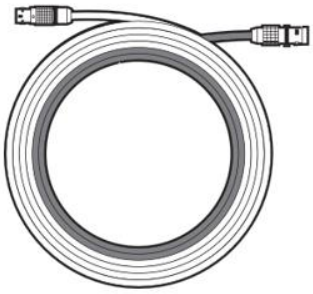
Camera
(1-4 per Processor)



Right-Hand Bracket
(1 per Camera)



Mobile ALPR Processor
Ethernet Crossover Cable



Camera Cable
(1 per Camera)

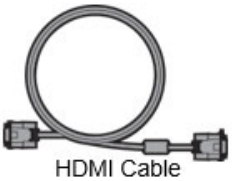
Optional with Stand-Alone Configuration



DC-DC Power Cable

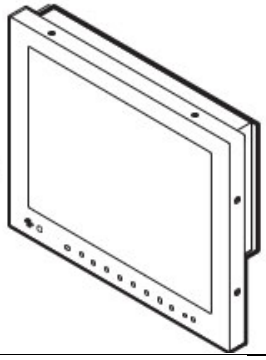


USB Cable
(2 per system)

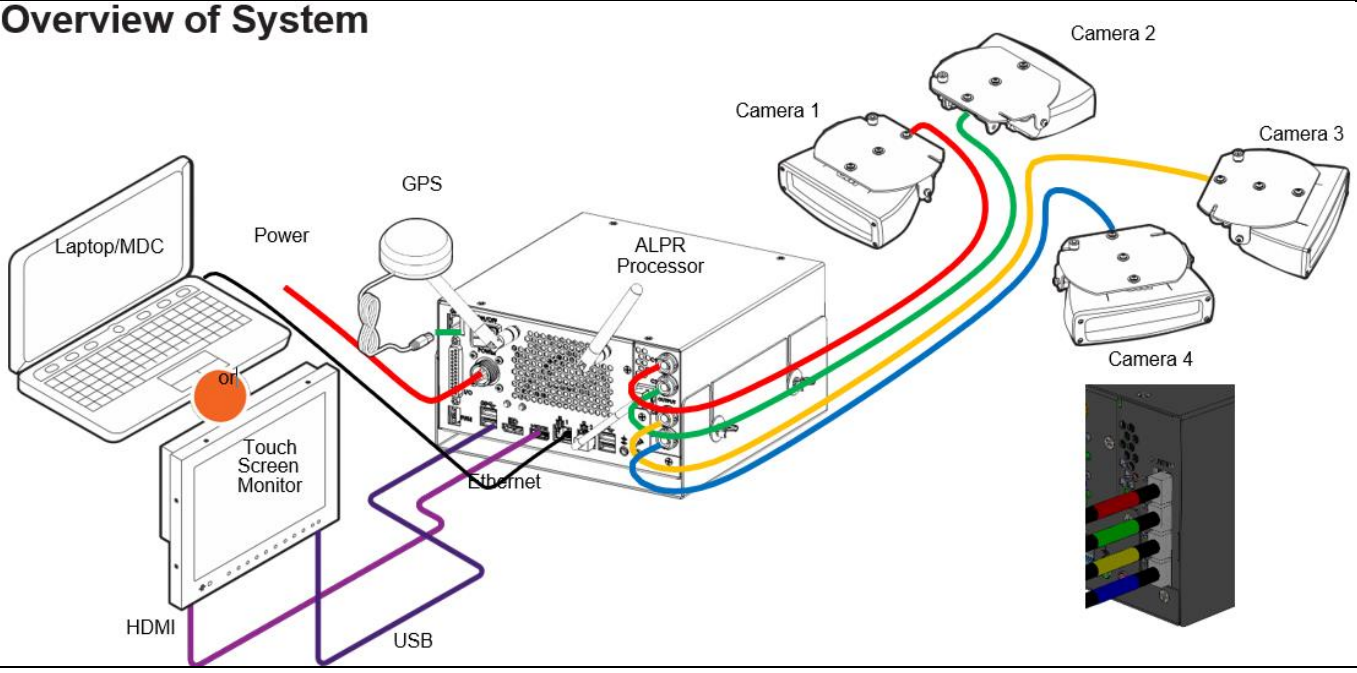


HDMI Cable

Touch Screen Monitor
(Mounting bracket provided by others)

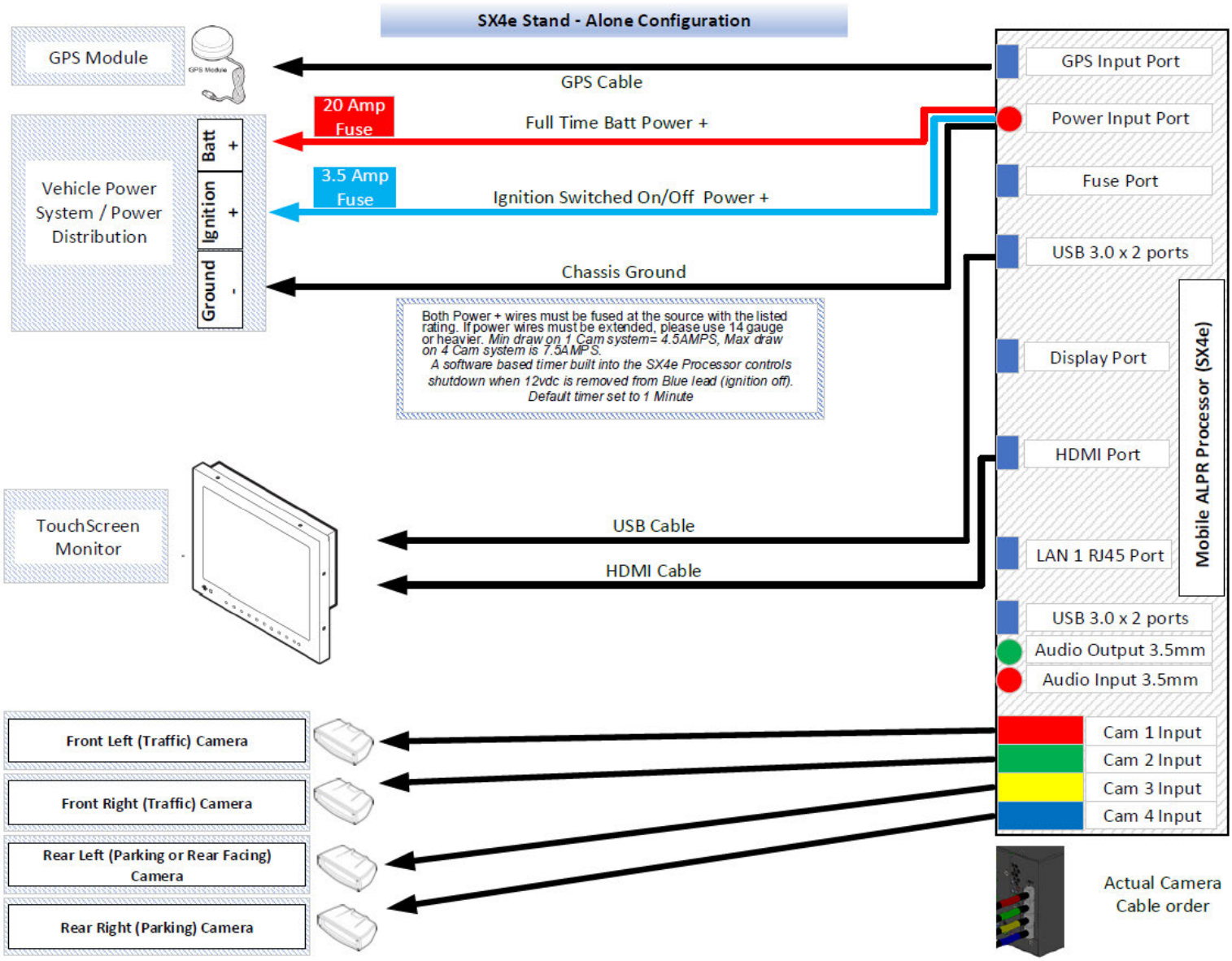


Overview of System



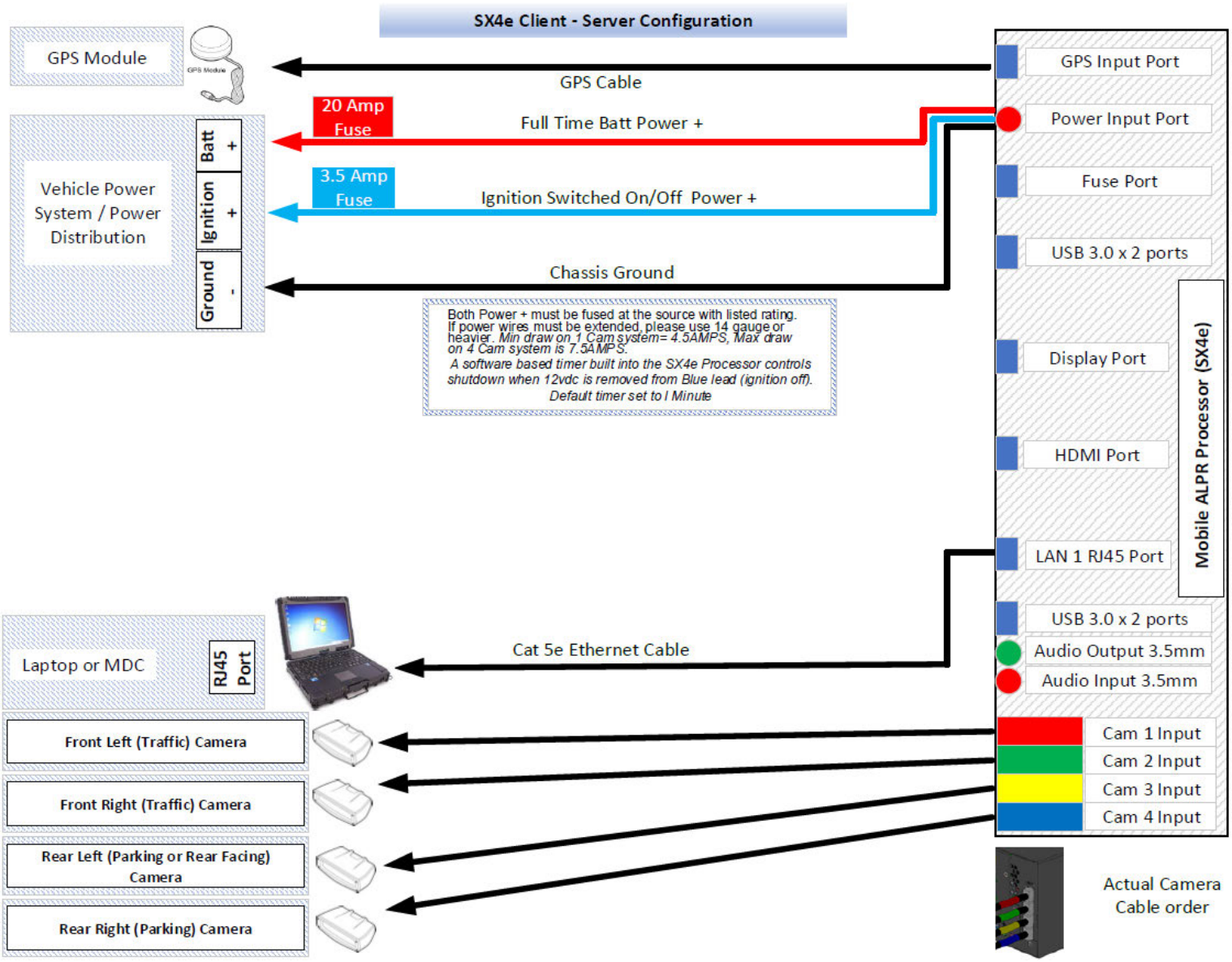
APPENDIX B – WIRING DIAGRAM

Below is the wiring diagram for a Stand-Alone Processor.



APPENDIX C – WIRING DIAGRAM

Below is the wiring diagram for client/server (VPRelay mode) used with a laptop in the front of the vehicle.



UTMC ALPR Protocol

A UTMC Technical Guide
Library reference ***TR007.001c***

Updated July 2020
Cover + 31 pages

Written by UTMC © Copyright UTMC Ltd
Developed in part with PIPS Technology

List of contents

1 Introduction **3**
1.1 About this document 3
1.2 Status of this document 3
1.3 Context 3
1.4 Web service interfaces 4

2 Camera to Instation **5**
2.1 Introduction 5
2.2 PlateRead 5
2.3 ALPR diagnostics 6
2.4 Machine diagnostics 7
2.5 Logs 8
2.6 Images 8
2.7 Camera and Configuration 9
2.8 Configuration request 11
2.9 Heartbeat message 11

3 Instation To Camera **13**
3.1 Introduction 13
3.2 Configuration 13
3.3 Log request 14
3.4 Configuration request 14
3.5 Image request 15
3.6 Acknowledgement 16

4 Tag Hashing algorithm **17**
4.1 About the algorithm 17
4.2 Example 17

Appendix 1 PlateRead Element **19**

Appendix 2 ALPRDiagnostic Element **21**

Appendix 3 MachineDiagnostic Element **23**

Appendix 4 Image Element **25**

Appendix 5 Camera Configuration Elements **26**
A5.1 Camera Element 26
A5.2 Lane Element 27
A5.3 Configuration Element 28

Appendix 6 ImageRequest Elements **31**
A6.1 TimeRangeImageRequest 31
A6.2 PriorVRNImageRequest 31
A6.3 InstanceSetImageRequest 32
A6.4 ContextImageRequest 32

1 Introduction

1.1 About this document

1.1.1 UTMC is a UK-led initiative which provides and maintains a technical framework for traffic management and related systems. It is geared to producing open specifications geared to the needs of real world projects, delivered through an efficient and innovative supply market. UTMC specifications are endorsed by the UK Department for Transport and are published on the UTMC website at: http://www.utmc.uk.com.

1.1.2 To help users get the best out of the UTMC Technical Specification, we provide a set of guidance documents addressing some of the associated issues, ranging from non technical aspects such as procurement policy and operations, to technical aspects such as database design and communications network configuration.

1.1.3 This document is a guidance document primarily for developers, and is concerned with expanding on the technical implementation of UTMC protocols within an ALPR system.

1.2 Status of this document

1.2.1 This document is based on the previous version, TR007 001b, produced by the UTMC ALPR Working Group (2009-2010).

1.2.2 UTMC gratefully acknowledges the work of the members of the Working Group in compiling this guidance and the associated elements of the Technical Specification.

1.3 Context

1.3.1 This protocol is for use by ALPR cameras when connecting to UTMC systems as used by numerous authorities across the UK, with the goal of achieving interoperability between suppliers. Although the primary aim has been to provide standardized ALPR data for journey time systems, the scope of the protocol includes the provision of additional data meeting NAAS requirements (for example images) to satisfy Police requirements in the event that Local Authorities and the Police wish to share cameras.

1.3.2 The UTMC ALPR protocol was developed within the following framework:

- This standard utilises non-proprietary elements and is based on XML. It is recognised that the communications costs associated with the use of XML may be higher at present than those for a less verbose protocol. However, it is hoped that the ease of use and the wide support of XML will lead to the ready exploitation of a forward-looking XML based open standard, particularly in the light of ongoing reductions in communication costs.

- The focus of this protocol is Camera to Instation and Instation to Camera communications. In parallel, a set of attribute extensions have been developed for the Common Database CCTV Data Object, which allow the Instation to add distilled ALPR data to the CDB. This document does not deal with Instation to Instation Journey Time Exchange.

- This protocol should be formed with some consideration of existing protocols and guidance – UTMC, Datex and possibly NTCIP.

- This protocol should be scalable. Elements such as image transfer may not be a requirement of all users. The protocol should be developed in a way to ensure that such additions are optional.

1.4 Web service interfaces

1.4.1 All web interfaces are SOAP (Simple Object Access Protocol) based and are described in WSDL (Web Services Description Language).

1.4.2 To summarise the Instation WSDL, the interface allows the camera to send XML element: <CameraToInstation> and in reply receives an XML element: <InstationToCamera>.

1.4.3 The camera WSDL allows the Instation to send XML element: <InstationToCamera>.

1.4.4 It should be noted that SOAP headers are not included in the UTMC ANPR WSDL files (camera.wsdl and instation.wsdl) or in the xml excerpts shown below. SOAP headers must therefore be generated for any SOAP-compliant implementation.

1.4.5 Both <CameraToInstation> and <InstationToCamera> elements have a mandatory version number attribute:

- SchemaVersion, indicating the version number of the element which contains it (SchemaVersion is a string containing dot-separated numbers (starting with 1.0). The first digit indicates a major revision, the second indicates updates to that revision.)

1.4.6 The xml excerpts shown below relate to V1.2 of the UTMC ALPR Protocol.

2 Camera to Instation

2.1 Introduction

2.1.1 This XML element is intended for transmitting all information from Camera to Instation. It allows for sending: plate data, ALPR and machine diagnostics, proprietary logs, images, current Camera configuration and request for configuration in any combination.

2.1.2 The option must be provided to use Gzip compression of the entire Camera to Instation element. The protocol does not provide for enabling or disabling this feature - it must be enabled or disabled by a commissioning engineer, either on-site or via a remotely connected engineering application.

2.1.3 Mandatory elements are:

- CameraID to identify the Camera
- TimeStamp which is the date and time of message creation

2.1.4 For clarity, each type of information payload is discussed separately; however messages may use any combination of elements.

2.1.5 All array elements include an optional attribute "ManufacturerSpecific" (not shown in the examples) which enables the communication of additional information outside the scope of the pre-defined attributes.

2.2 PlateRead

2.2.1 An optional array of plate read results may be included. For each entry in the array, the following are mandatory:

- InstanceID to identify the plate read event;
- TimeStamp which is the date and time of the sighting;
- LaneID representing the lane in which the plate was travelling;
- VehicleDirection representing the direction the vehicle was travelling in the lane;
- PlateNotRead, a flag to indicate a vehicle has been detected but no plate read.

2.2.2 The following is an example message containing a single plate read.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CameraToInstation xmlns=" http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <CameraID>0</CameraID>
    <TimeStamp>2009-06-29T12:01:59.377+01:00</TimeStamp>
    <PlateReadArray>
        <PlateRead>
            <InstanceID>0</InstanceID>
            <TimeStamp>2009-06-29T12:01:59.379+01:00</TimeStamp>
            <TimeStampError>5</TimeStampError>
            <LaneID>0</LaneID>
            <VehicleDirection>U</VehicleDirection>
            <XYType>OSGB</XYType>
            <XCoord>123456.7</XCoord>
            <YCoord>654321.0</YCoord>
            <PlateNotRead>false</PlateNotRead>
            <VRN>A123BCD</VRN>
            <VRNConfidence>85</VRNConfidence>
```

```
                <Tag>1234</Tag>
                <TagConfidence>90</TagConfidence>
                <Classification>1</Classification>
                <Country>GBR</Country>
                <Make>Ford</Make>
                <Model>Focus</Model>
                <Colour>Red</Colour>
                <Velocity>50</Velocity>
                <VelocityError>5</VelocityError>
            </PlateRead>
        </PlateReadArray>
</CameraToInstation>
```

2.2.3 Where the Camera has been configured to send plate reads immediately, the <PlateReadArray> element will only contain a single <PlateRead> element. Where the Camera is configured to send batches of plate reads, multiple <PlateRead> elements will be present. It is mandatory that each <PlateRead> element contains at least one of <VRN> or <Tag>.

2.2.4 See section 4 for an explanation of the hashing algorithm which is used to convert the <VRN> element to a hashed tag (the <Tag> element) for the purposes of journey time or origin-destination applications.

2.2.5 These elements are described in more detail in Appendix 1.

2.3 ALPR diagnostics

2.3.1 An optional array of ALPR diagnostics may be included (one entry per lane). For each entry in the array, the following are mandatory:

- TimeStamp which is the date and time of end of the diagnostic period;
- DiagnosticType representing whether the entry is a routine diagnostic or an alarm;

2.3.2 The following is an example message containing all defined ALPR Diagnostic objects:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CameraToInstation xmlns=" http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <CameraID>0</CameraID>
    <TimeStamp>2009-06-29T12:01:59.377+01:00</TimeStamp>
    <ANPRDiagnosticArray>
        <ANPRDiagnostic>
            <TimeStamp>2009-06-29T12:01:59.379+01:00</TimeStamp>
            <DiagnosticType>routineDiagnostic</DiagnosticType>
            <LaneID>0</LaneID>
            <MeanVRNConfidence>82</MeanVRNConfidence>
            <MeanTagConfidence>85</MeanTagConfidence>
            <MeanPlateContrast>56</MeanPlateContrast>
            <MeanCharacterHeight>15</MeanCharacterHeight>
            <MeanHorizontalAngle>8</MeanHorizontalAngle>
            <MeanVerticalAngle>2</MeanVerticalAngle>
            <MeanTrajectoryOffset>2</MeanTrajectoryOffset>
            <MeanTrajectoryAngle>11</MeanTrajectoryAngle>
            <MeanVelocity>45</MeanVelocity>
            <MeanVelocityError>4</MeanVelocityError>
```

```
                <PlateToTriggerRatio>90</PlateToTriggerRatio>
                <PlatesNoCountryRatio>3</PlatesNoCountryRatio>
                <PlatesTowardsRatio>43</PlatesTowardsRatio>
                <PlatesAwayRatio>45</PlatesAwayRatio>
                <MeanIRLevel>53</MeanIRLevel>
                <MeanExposure>350</MeanExposure>
                <MeanGain>-10</MeanGain>
            </ANPRDiagnostic>
        </ANPRDiagnosticArray>
</CameraToInstation>
```

2.3.3 These elements are described in more detail in Appendix 2.

2.4 Machine diagnostics

2.4.1 An optional array of machine diagnostics (describing hardware, software and communications performance) may be included. For each entry in the array, the following are mandatory:

- TimeStamp which is the date and time of the end of the diagnostic period;
- DiagnosticType representing whether the entry is a routine diagnostic or an alarm;
- HostName representing the host to which communications diagnostics relate

2.4.2 The following is an example message containing all proposed Machine Diagnostic objects:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CameraToInstation xmlns=" http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <CameraID>0</CameraID>
    <TimeStamp>2009-06-29T12:01:59.377+01:00</TimeStamp>
    <MachineDiagnosticArray>
        <MachineDiagnostic>
            <TimeStamp>2009-06-29T12:01:59.379+01:00</TimeStamp>
            <DiagnosticType>routineDiagnostic</DiagnosticType>
            <MeanCPUTemperature>56</MeanCPUTemperature>
            <MeanTotalCurrent>120</MeanTotalCurrent>
            <MeanIlluminatorTemp>70</MeanIlluminatorTemp>
            <MeanIlluminatorCurrent>90</MeanIlluminatorCurrent>
            <IlluminatorUsage>123</IlluminatorUsage>
            <MeanIlluminatorOutput>90</MeanIlluminatorOutput>
            <LastResetTime>2009-06-29T12:01:59.379+01:00</LastResetTime>
            <NoOfHardwareErrors>0</NoOfHardwareErrors>
            <MeanSignalStrength>-36</MeanSignalStrength>
            <HostName>192.168.1.1</HostName>
            <MeanCommsLag>23</MeanCommsLag>
            <WorstCommsLag>50</WorstCommsLag>
            <NoOfCommsResends>3</NoOfCommsResends>
            <NoOfCommsFailures>1</NoOfCommsFailures>
            <NoOfCommsReconnects>2</NoOfCommsReconnects>
            <MeanSyncDifference>40</MeanSyncDifference>
            <WorstSyncDifference>123</WorstSyncDifference>
            <LastSyncTime>2009-06-29T12:01:59.379+01:00</LastSyncTime>
            <SupplyVoltage>98</SupplyVoltage>
            <TamperAlarm>normal</TamperAlarm>
```

```
            </MachineDiagnostic>
        </MachineDiagnosticArray>
</CameraToInstation>
```

2.4.3 These elements are described in more detail in Appendix 3.

2.5 Logs

2.5.1 An optional array of log messages (representing logged events such as power up, configuration change or communication error) may be included. For each entry in the array, the following is mandatory:

- TimeStamp which is the date and time relating to the log message;

2.5.2 The following is an example message outlining the format of a Log Array:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CameraToInstation xmlns=" http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <CameraID>0</CameraID>
    <TimeStamp>2009-06-29T12:01:59.377+01:00</TimeStamp>
    <LogArray>
        <Log>
            <TimeStamp>2009-06-29T12:01:59.379+01:00</TimeStamp>
            <InstanceID>0</InstanceID>
            <LogMessage>System Restart</LogMessage>
        </Log>
    </LogArray>
</CameraToInstation>
```

2.5.3 The <LogArray> element may contain any number of <Log> elements. LogMessage elements may contain XML or plain text in proprietary format, as long as XML formatting rules are strictly followed.

2.6 Images

2.6.1 An optional array of camera images may be included. For each entry in the array, the following are mandatory:

- TimeStamp which is the date and time at which the image was captured;
- ImageType representing the type of the image e.g. plate patch, ALPR image etc;

2.6.2 The following is an example message containing binary images. Five types of image can be sent: PlatePatch, ALPR Image, Overview Image, Context Image or Context Overview Image:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CameraToInstation xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <CameraID>0</CameraID>
    <TimeStamp>2009-06-29T12:01:59.377+01:00</TimeStamp>
    <ImageArray>
        <Image>
            <InstanceID>0</InstanceID>
            <TimeStamp>2009-06-29T12:01:59.379+01:00</TimeStamp>
```

```
            <VRN>A123BCD</VRN>
            <LaneID>0</LaneID>
            <ImageType>platePatch</ImageType>
            <ImageFormat>jpeg</ImageFormat>
            <BinaryImage>[IMAGE DATA]</BinaryImage>
        </Image>
        <Image>
            <InstanceID>0</InstanceID>
            <TimeStamp>2009-06-29T12:01:59.379+01:00</TimeStamp>
            <VRN>A123BCD</VRN>
            <LaneID>0</LaneID>
            <ImageType>ANPRImage</ImageType>
            <ImageFormat>gif</ImageFormat>
            <BinaryImage>[IMAGE DATA]</BinaryImage>
        </Image>
        <Image>
            <InstanceID>0</InstanceID>
            <TimeStamp>2009-06-29T12:01:59.379+01:00</TimeStamp>
            <VRN>A123BCD</VRN>
            <LaneID>0</LaneID>
            <ImageType>overviewImage</ImageType>
            <ImageFormat>tiff</ImageFormat>
            <BinaryImage>[IMAGE DATA]</BinaryImage>
        </Image>
    </ImageArray>
</CameraToInstation>
```

2.6.3 These elements are described in more detail in Appendix 4.

2.6.4 It should be noted that InstanceID is not required for an ad-hoc context image or any image that may be requested from the Instation where there is no association with a vehicle, and therefore no VRN has been collected with a corresponding Instance ID. However, where an image relates to a plate read, the InstanceID for the plate read is included in the image attributes.

2.7 Camera and Configuration

2.7.1 Optional Camera and Configuration elements may be included in response to a ConfigRequest issued by the Instation via the InstationToCamera element. The following is mandatory in the Camera element:

- HardwareUniqueID which represents a globally unique identifier for the camera

2.7.2 At least one Lane element per camera is mandatory. The following are mandatory in each Lane element:

- LaneID representing the lane relative to the camera to which the lane config applies
- LaneNumber representing the lane position in the carriageway
- LaneDirectionTypeID representing the direction of travel of the carriageway lane
- NormalVehicleDirection - whether vehicles normally travel towards or away from the camera

2.7.3 The following is an example message outlining a Camera and Configuration response to an Instation ConfigRequest, which includes both Camera and Configuration elements:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CameraToInstation xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <CameraID>0</CameraID>
    <TimeStamp>2009-06-29T12:01:59.377+01:00</TimeStamp>
    <Camera>
        < HardwareUniqueID>CA_Traffic:Evo8:7205/0219</ HardwareUniqueID>
        <ShortDescription>My Short description</ShortDescription>
        <LongDescription>My long description</LongDescription>
        <XYType>OSGB</XYType>
        <XCoord>123456.7</XCoord>
        <YCoord>654321.0</YCoord>
        <Height>3.5</Height>
        <TypeID>7</TypeID>
        <MobileCamera>false</MobileCamera>
        <SoftwareVersion>2.1.1</SoftwareVersion>
        <LaneArray>
            <Lane>
                <LaneID>0</LaneID>
                <LaneNumber>1</LaneNumber>
                <LaneDirectionTypeID>5</LaneDirectionTypeID>
                <NormalVehicleDirection>towards</NormalVehicleDirection>
            </Lane>
        </LaneArray>
    </Camera>
    <Configuration>
        <HostName>HOST1</HostName>
        <SendVRNs>true</SendVRNs>
        <SendTags>false</SendTags>
        <SendPlatePatches>false</SendPlatePatches>
        <SendANPRImages>false</SendANPRImages>
        <SendOverviewImages>false</SendOverviewImages>
        <SendPlatesNotRead>false</SendPlatesNotRead>
        <SendANPRDiagnostics>true</SendANPRDiagnostics>
        <SendMachineDiagnostics>true</SendMachineDiagnostics>
        <SendIncrementalLog>true</SendIncrementalLog>
        <SendPeriodicContextImage>true</SendPeriodicContextImage>
        <UseReportingOffset>false</UseReportingOffset>
        <SendHeartbeat>true</SendHeartbeat>
        <StreamPlates>false</StreamPlates>
        <HeartbeatInterval>300</HeartbeatInterval>
        <PlateSendInterval>60</PlateSendInterval>
        <ReportingOffset>15</ReportingOffset>
        <ANPRDiagsSendInterval>1800</ANPRDiagsSendInterval>
        <MachineDiagsSendInterval>3600</MachineDiagsSendInterval>
        <IncrementalLogInterval>600</IncrementalLogInterval>
        <ContextImagePeriod>900</ContextImagePeriod>
        <MaxPlatesToSend>200</MaxPlatesToSend>
        <MinANPRDiagnosticSamples>10</MinANPRDiagnosticSamples>
        <CurrentDateTime>2009-06-29T12:01:59.379+01:00</CurrentDateTime>
    </Configuration>
</CameraToInstation>
```

2.7.4 Elements that are part of the <Camera> element are not configurable by the instation and should be set up on installation of the physical camera by manufacturer specific means (for example pre-configured at the factory or entered by the commissioning engineer).

2.7.5 A number of different lanes may be configured for one camera, however note that the <Configuration> element has no attributes which are lane-specific.

2.7.6 In the <Camera> element, at least one <Lane> element is mandatory. It is anticipated that <Lane> attributes will be entered into the camera by the commissioning engineer – these are not downloadable from the Instation.

2.7.7 Where there are attributes in the <Configuration> element which are not supported by a particular camera, the camera may omit these from the response.

2.7.8 A camera must maintain separate Configuration objects for each host. It will only accept the Configuration for a particular host from that host itself, and will only push a Configuration to the host to which it applies.

2.7.9 The <Camera>, <Lane>, and <Configuration> elements are described in more detail in Appendix 5.

2.8 Configuration request

2.8.1 The following is an example message outlining a request by the Camera for an update of its current Configuration:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CameraToInstation xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <CameraID>0</CameraID>
    <TimeStamp>2009-06-29T12:01:59.377+01:00</TimeStamp>
    <ConfigRequest/>
</CameraToInstation>
```

2.8.2 This is an empty element used by the Camera for requesting the current configuration from the Instation, for example on Camera startup.

2.8.3 The ConfigRequest is directed to a particular host, which will return the Configuration relating only to that host. Where a camera is configured to report to multiple hosts, it is not permitted for one host to have the ability to change the Configuration of another.

2.9 Heartbeat message

2.9.1 The following is an example message outlining a heartbeat, which comprises a CameraToInstation element which is empty apart from the mandatory CameraID and Timestamp attributes:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CameraToInstation xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <CameraID>0</CameraID>
    <TimeStamp>2009-06-29T12:01:59.377+01:00</TimeStamp>
</CameraToInstation>
```

2.9.2 Where a Camera is connected via a network which does provide a fixed IP address (for example some mobile networks), it may not be possible for the Instation to initiate a data transaction with a Camera (it may be impossible to determine the IP address allocated by the network). The Camera should therefore be configured periodically to send a ‘Heartbeat’ message to allow the Instation to respond with a message to the Camera. This heartbeat message is essentially an empty message which must be sent if no other messages have been sent within a configurable period of time (<HeartbeatInterval>).

3 Instation To Camera

3.1 Introduction

3.1.1 The <InstationToCamera> element is intended primarily for transmitting information from the Instation to the Camera in response to a SOAP call containing the <CameraToInstation> element. It allows for any combination of: a camera configuration, a configuration request, an image request or a log request to be sent. None of these elements is mandatory, hence the <InstationToCamera> element may also be sent empty to provide a receipt acknowledgement.

3.1.2 The option must be provided to use Gzip compression of the entire Instation to Camera element. The protocol does not provide for enabling or disabling this feature - it must be enabled or disabled by a commissioning engineer, either on-site or via a remotely connected engineering application.

3.1.3 Whereas this element is used in response to a <CameraToInstation> element, it mostly contains requests for data from the camera, for the reason that cameras are often connected via mobile networks where the Instation is unable to initiate a TCP/IP connection. Requests for data are therefore 'piggybacked' onto the acknowledgements sent by the Instation to the Camera.

3.1.4 Where the network connection allows the Instation to initiate a TCP/IP connection, the <InstationToCamera> element may also be transmitted on an ad-hoc basis as a SOAP call from the instation to the camera.

3.1.5 All array elements include an optional attribute "ManufacturerSpecific" (not shown in the examples) which enables the communication of additional information outside the scope of the pre-defined attributes.

3.2 Configuration

3.2.1 The Instation may push a new or revised configuration to the camera either at will or in response to a <ConfigRequest> from the camera. It is only possible to push that configuration which is specific to the sending host.

3.2.2 The following is an example message outlining a Configuration response to a camera ConfigRequest (none of the <Configuration> elements is mandatory):

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<InstationToCamera xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <Configuration>
        <HostName>HOST1</HostName>
        <SendVRNs>true</SendVRNs>
        <SendTags>false</SendTags>
        <SendPlatePatches>false</SendPlatePatches>
        <SendANPRImages>false</SendANPRImages>
        <SendOverviewImages>false</SendOverviewImages>
        <SendPlatesNotRead>false</SendPlatesNotRead>
        <SendANPRDiagnostics>true</SendANPRDiagnostics>
        <SendMachineDiagnostics>true</SendMachineDiagnostics>
        <SendIncrementalLog>true</SendIncrementalLog>
        <SendPeriodicContextImage>true</SendPeriodicContextImage>
        <UseReportingOffset>false</UseReportingOffset>
        <SendHeartbeat>true</SendHeartbeat>
        <StreamPlates>false</StreamPlates>
```

```
            <HeartbeatInterval>300</HeartbeatInterval>
            <PlateSendInterval>60</PlateSendInterval>
            <ReportingOffset>15</ReportingOffset>
            <ANPRDiagsSendInterval>1800</ANPRDiagsSendInterval>
            <MachineDiagsSendInterval>3600</MachineDiagsSendInterval>
            <IncrementalLogInterval>600</IncrementalLogInterval>
            <ContextImagePeriod>900</ContextImagePeriod>
            <MaxPlatesToSend>200</MaxPlatesToSend>
            <MinANPRDiagnosticSamples>10</MinANPRDiagnosticSamples>
            <CurrentDateTime>2009-06-29T12:01:59.379+01:00</CurrentDateTime>
        </Configuration>
</InstationToCamera>
```

3.2.3 This is exactly the same <Configuration> element as used for the <CameraToInstation> child element for transmitting the camera's current configuration.

3.2.4 The protocol does not provide for the addition of new hosts to the camera - these must be added or removed by a commissioning engineer, either on-site or via a remotely connected engineering application.

3.2.5 Where there are attributes in the <Configuration> element which are not supported by a particular camera, they will be ignored by the camera.

3.3 Log request

3.3.1 The Instation may request log records from the camera for a specific time period. In the <LogRequest> element, the following (which are the only attributes) are mandatory:

- StartTime which is the date and time at which log records should start;
- EndTime which is the date and time at which log records should end.

3.3.2 The following is an example message containing a response request from the Instation for provision of a Log by the camera:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<InstationToCamera xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <LogRequest>
        <StartTime>2008-11-14T10:50:30.952Z</StartTime>
        <EndTime>2008-11-14T10:50:30.952Z</EndTime>
    </LogRequest>
</InstationToCamera>
```

3.4 Configuration request

3.4.1 The following is an example message outlining a request by the Instation for a camera to upload its current Configuration:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<InstationToCamera xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <ConfigRequest/>
</InstationToCamera>
```

3.4.2 The <ConfigRequest> is an empty element identical to the same child element of the <CameraToInstation> element. (see 2.8).

3.4.3 The <ConfigRequest> is issued by a particular host, and the camera will return only the Configuration relating only to that host.

3.5 Image request

3.5.1 The Instation may request (retrospectively) images related to plate reads which have been stored in a camera. It may also request ad-hoc context images which are not connected with plate reads. There are four different classes of request, depending on the criteria which the Instation wishes to use to identify the required images:

- TimeRangeImageRequest: request images from a specific time period
- PriorVRNImageRequest: request a specific quantity of the most recent images
- InstanceSetImageRequest: request the images for a specific list of plate reads
- ContextImageRequest: request immediate images from one or more camera sensors

3.5.2 Only one of these ImageRequest classes should be used per <InstationToCamera> response, otherwise the instation will not know to which request the images sent by the camera relate.

3.5.3 The following is an example outlining a request from an Instation to a camera requesting the provision of images from a specific time period:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<InstationToCamera xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <TimeRangeImageRequest>
        <StartTime>2008-11-14T10:50:30.952Z</StartTime>
        <EndTime>2008-11-14T10:50:30.952Z</EndTime>
        <ImageTypeArray>
            <ImageType>platePatch</ImageType>
            <ImageType>overviewImage</ImageType>
        </ImageTypeArray>
    </TimeRangeImageRequest>
</InstationToCamera>
```

3.5.4 The following is an example outlining a request from an Instation to a camera requesting a specific quantity of recent images ending at a particular InstanceID:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<InstationToCamera xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <PriorVRNImageRequest>
        <NoOfPriorVRNs>10</NoOfPriorVRNs>
        <EndInstanceID>123456</EndInstanceID>
        <ImageTypeArray>
            <ImageType>platePatch</ImageType>
            <ImageType>overviewImage</ImageType>
        </ImageTypeArray>
    </PriorVRNImageRequest>
</InstationToCamera>
```

3.5.5 The following is an example outlining a request from an Instation to a camera requesting the provision of images for a specific set of plate reads:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<InstationToCamera xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <InstanceSetImageRequest>
        <InstanceIDArray>
            <InstanceID>123456</InstanceID>
            <InstanceID>123454</InstanceID>
            <InstanceID>123452</InstanceID>
        </InstanceIDArray>
        <ImageTypeArray>
            <ImageType>platePatch</ImageType>
            <ImageType>overviewImage</ImageType>
        </ImageTypeArray>
    </InstanceSetImageRequest>
</InstationToCamera>
```

3.5.6 The following is an example outlining a request from an Instation to a camera requesting immediate context images:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<InstationToCamera xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <ContextImageRequest>
        <ImageTypeArray>
            <ImageType>contextImage</ImageType>
            <ImageType>contextOverviewImage</ImageType>
        </ImageTypeArray>
    </ContextImageRequest>
</InstationToCamera>
```

3.5.7 These elements are described in more detail in Appendix 6.

3.6 Acknowledgement

3.6.1 The following is an example message outlining an acknowledgement, which comprises an <InstationToCamera> element that is empty:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<InstationToCamera xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
</InstationToCamera>
```

3.6.2 Where the Instation receives a <CameraToInstation> message and does not require any further information from the camera, the <InstationToCamera> response will be an empty element which provides the camera with an acknowledgment that its transmission has been received.

4 Tag Hashing algorithm

4.1 About the algorithm

4.1.1 Journey time systems based on ALPR require cameras to recognise a plate at two or more locations and to return the recognised plate details to the instation. Although the full plate registration number can be returned to the instation for character by character matching, this may be undesirable in some circumstances. Additionally, to maintain driver and vehicle anonymity, it may be desirable to encrypt or otherwise change the plate string such that the actual registration number cannot be recovered.

4.1.2 ALPR systems are never 100% accurate. Read errors do occur. It is desirable to minimise the effect on the system of these read errors. For example the character D may be read correctly at one location and then the same character may be read as an O at a subsequent location.

4.1.3 The hashing algorithm firstly reduces the possible effect of plate read errors by replacing any characters likely to be confused with one another by a single character. So for example any occurence of O, D, 0 or Q in a plate is replaced with the character O. The following table lists all such substitutions:

ALPR reads character	Reported as
O D 0 Q	O
I 1	I
S 5	S
V Y	V
3 8 B	3
2 Z	2
E F	E
G C	G
H M N W	H

4.1.4 The resultant plate string is then hashed down to a binary number of 24 bits. The hash algorithm chosen is "one_at_a_time_hash". This algorithm has been chosen after reviewing the performance of a large number of algorithms over a database of about 100,000 UK plates and selecting the algorithm which provided the best distribution of hash values.

4.1.5 The "one_at_a_time_hash" hash algorithm was developed by Bob Jenkins. The original reference for the algorithm is: http://www.burtleburtle.net/bob/hash/doobs.html

4.2 Example

4.2.1 Example code (C language) for character substitution and the hash process is shown below.

```
static const char *mixups[] =
{
    "OD0Q", "I1", "S5", "VY", "38B", "2Z", "EF", "GC", "HMNW",
};
#define    NMIXUPS    9

void merge_ambiguous_characters(char *plate)
{
short  i;
char   *cp;

    while(*plate)
    {
        for(i=0; i<NMIXUPS; ++i)
        {
            cp = mixups[i];
            if(ismember(*plate, cp))
            {
                *plate = *cp;
            }
        }
        ++plate;
    }
}


// this function returns the 24 bit hash value directly

unsigned long hash(const char *plate)
{
unsigned   len;
unsigned   hash, i;
const int  hashbits = 24;
char       merge_plate[12];
#define    hashsize(n) ((unsigned)1<<(n))
#define    hashmask(n) (hashsize(n)-1)

    strcpy(merge_plate,plate);
        merge_ambiguous_characters(merge_plate);
    len = strlen(merge_plate);
    for (hash=0, i=0; i<len; ++i)
    {
        hash += merge_plate[i];
        hash += (hash << 10);
        hash ^= (hash >> 6);
    }
    hash += (hash << 3);
    hash ^= (hash >> 11);
    hash += (hash << 15);
    return (hash & hashmask(hashbits));
}
```

Appendix 1 PlateRead Element

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
InstanceID	DYNAMIC	A unique plate reference number for this camera. InstanceID should be incremented for each plate read until the holding variable (typically INT32) wraps, i.e. it is not just unique for a particular timestamp.	uInteger	Y	Combined with CameraID and TimeStamp at Instation to form a unique EventID
TimeStamp	DYNAMIC	ISO 8601 UTC date/timestamp for time of sighting	DateTime	Y	1ms resolution For dateTime format, see section 3.2.7 (dateTime) of W3C document “XML Schema Part 2 - Datatypes Second Edition“
TimeStampError	DYNAMIC	Estimated worst case timestamp error in ms	Integer		
LaneID	DYNAMIC	Camera Lane to which configuration item(s) relate	uInteger	Y	0 is the leftmost lane in the camera field of view. This ID is relative to the camera, not the actual lanes of the carriageway
VehicleDirection	DYNAMIC	Whether vehicle travelling toward or away from camera	Enumerated	Y	e.g. towards, away, unknown. i.e. towards = front plate, away = rear plate
XYType	STATIC	Reference co-ordinate system for XY location	Enumerated		e.g. OSGB or WGS84 (NB OSGB refers to OSGB36 datum)
XCoord	STATIC	X co-ordinate of camera location	Float		e.g. Longitude or Easting (Degrees + decimal degrees for longitude)
YCoord	STATIC	X co-ordinate of camera location	Float		e.g. Latitude or Northing (Degrees + decimal degrees for latitude)
PlateNotRead	DYNAMIC	A vehicle has been detected, but a plate cannot be found or, if found, cannot be recognised	Boolean	Y	Allows an InstanceID to be generated and a PlateRead record to be sent where no plate has been read.
VRN	DYNAMIC	Recognised licence number	Character		No whitespace characters
VRNConfidence	DYNAMIC	Probability that licence number is correct	Percent		0 to 100%
Tag	DYNAMIC	Hashed value formed from VRN	uInteger		In the range 0 to 2^{24} - 1

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
TagConfidence	DYNAMIC	Probability that tag value is correct	Percent		0 to 100%
Classification	DYNAMIC	Class of the recognised vehicle e.g. car, van lorry	uInteger		Numeric values only representing a classification scheme determined by the user.
Country	DYNAMIC	ISO 3166-1 three character country code	Character		e.g. GBR, FRA, DEU
Make	DYNAMIC	Make of Vehicle (Manufacturer)	Character		
Model	DYNAMIC	Model of Vehicle	Character		May be text (e.g. Mondeo) or number (e.g. 520)
Colour	DYNAMIC	Colour of vehicle	Enumerated		See list of standard colours (table below)*
Velocity	DYNAMIC	Estimated vehicle speed in kph	uInteger		
VelocityError	DYNAMIC	Estimated velocity error (magnitude) in kph	uInteger		Mean of the magnitudes of the +ve and -ve error estimates at 95% confidence interval

* A standard set of colours is used as follows:

Red		Green		Dark Purple		Light Brown
Light Red		Light Green		Grey		Dark Brown
Dark Red		Dark Green		Light Grey		Magenta
Orange		Blue		Dark Grey		Turquoise
Light Orange		Light Blue		Gold		
Dark Orange		Dark Blue		Silver		
Yellow		Violet		White		
Light Yellow		Purple		Black		
Dark Yellow		Light Purple		Brown		

Appendix 2 ALPRDiagnostic Element

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
TimeStamp	DYNAMIC	ISO 8601 UTC date/timestamp for end of diagnostic period	DateTime	Y	1ms resolution
DiagnosticType	DYNAMIC	Whether a routine diagnostic or an alarm (warning or fault)	Enumerated	Y	Enumerated type having values "routineDiagnostic", "alarmWarningSet", "alarmWarningClear", "alarmFaultSet","alarmFaultClear"
LaneID	DYNAMIC	Camera Lane to which the Diagnostics relate	uInteger		0 is the leftmost lane in the camera field of view. This ID is relative to the camera, not the actual lanes of the carriageway
MeanVRNConfidence	DYNAMIC	Average Probability that licence number is correct	Percent		0 to 100%
MeanTagConfidence	DYNAMIC	Average Probability that tag value is correct	Percent		0 to 100%
MeanPlateContrast	DYNAMIC	Average plate patch contrast	Percent		0 = all black, 100 = all white
MeanCharacterHeight	DYNAMIC	Average VRN character height in pixels	uInteger		
MeanHorizontalAngle	DYNAMIC	Average character angle to horizontal in degrees	Integer		±90 degrees
MeanVerticalAngle	DYNAMIC	Average character angle to vertical in degrees	Integer		±90 degrees
MeanTrajectoryOffset	DYNAMIC	Average trajectory distance from image centre	Integer		As a percentage of the horizontal image size. -ve for left of centre, +ve for right of centre
MeanTrajectoryAngle	DYNAMIC	Average angle of trajectory to horizontal in degrees	WholeDegrees		Horizontal right to left is zero, increasing anti-clockwise to 360. Values between 180 and 360 for vehicles travelling away from camera.
MeanVelocity	DYNAMIC	Average estimated vehicle speed in kph	uInteger		
MeanVelocityError	DYNAMIC	Average velocity error at 95% confidence interval	uInteger		Value in kph (mean of velocity error magnitude estimates)
PlateToTriggerRatio	DYNAMIC	Ratio of plates recognised to objects detected	Percent		0 to 100%

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
PlatesNoCountryRatio	DYNAMIC	Ratio of plates with unidentified country to all plates	Percent		0 to 100%
PlatesTowardsRatio	DYNAMIC	Ratio of plates towards camera to total plates	Percent		0 to 100%
PlatesAwayRatio	DYNAMIC	Ratio of plates away from camera to total plates	Percent		0 to 100%
MeanIRLevel	DYNAMIC	Average illuminator output level (percentage of max)	Percent		For frames selected for plate recognition
MeanExposure	DYNAMIC	Average exposure time in microseconds	uInteger		For frames selected for plate recognition
MeanGain	DYNAMIC	Average camera gain in dB where max gain is 0dB	Integer		For frames selected for plate recognition

Appendix 3 MachineDiagnostic Element

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
TimeStamp	DYNAMIC	ISO 8601 UTC date/timestamp for end of diagnostic period	DateTime	Y	1ms resolution
DiagnosticType	DYNAMIC	Whether a routine diagnostic or an alarm (warning or fault)	Enumerated	Y	Enumerated type having values "routineDiagnostic", "alarmWarningSet", "alarmWarningClear", "alarmFaultSet","alarmFaultClear"
MeanCPUTemp	DYNAMIC	Average processor board temperature in degrees	Integer		Can be +ve or -ve
MeanTotalCurrent	DYNAMIC	Average current drawn by camera including illuminator in mA	uInteger		Purpose: to identify reduction in illuminator current. Max value is 99,999mA
MeanIlluminatorTemp	DYNAMIC	Average illuminator temperature in degrees	Integer		Can be +ve or -ve
MeanIlluminatorCurrent	DYNAMIC	Average illuminator current in mA (during on-time)	uInteger		Max value is 99,999mA
IlluminatorUsage	DYNAMIC	Total illuminator usage (amps x hours) - cumulative	uInteger		As an indication of illuminator lifetime used
MeanIlluminatorOutput	DYNAMIC	Average illuminator light output as percentage of max when new	Integer		May be > 100%
LastResetTime	DYNAMIC	Date & Time of last CPU reset	DateTime		May be outside this diagnostic interval
NoOfHardwareErrors	DYNAMIC	Number of hardware errors detected	uInteger		
MeanSignalStrength	DYNAMIC	Average signal strength (wireless comms) in dB	Integer		Range is -999dB to 0dB
HostName	DYNAMIC	Name of host to which diagnostics relate	Character	Y	IP address or DNS name
MeanCommsLag	DYNAMIC	Average "round trip" communications delay in ms	uInteger		
WorstCommsLag	DYNAMIC	Worst case "round trip" communications delay in ms	uInteger		
NoOfCommsResends	DYNAMIC	Number of messages re-sent	uInteger		e.g. After failure to open host port
NoOfCommsFailures	DYNAMIC	Number of messages deleted from send buffer after repeated re-send failures	uInteger		
NoOfCommsReconnects	DYNAMIC	Number of reconnections to wireless network	uInteger		

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
MeanSyncDifference	DYNAMIC	Average time correction upon re-synchronisation in ms	Integer		This is a signed value, where a negative difference means the camera clock was fast, and a positive difference means it was slow.
WorstSyncDifference	DYNAMIC	Worst case time correction upon re-synchronisation in ms	Integer		This is a signed value, where a negative difference means the camera clock was fast, and a positive difference means it was slow.
LastSyncTime	DYNAMIC	Date & Time of last successful re-synchronisation	DateTime		May be outside this diagnostic interval
SupplyVoltage	DYNAMIC	Percentage of nominal system SELV supply voltage	Integer		May be >100%
TamperAlarm	DYNAMIC	Indication of unauthorised access to the equipment	Enumerated		Has 3 enumerated values: "normal", "enclosureBreachAlarm", "unauthorisedCommunicationAlarm"

Appendix 4 Image Element

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
InstanceID	DYNAMIC	Unique reference number for this camera to VRN record for a plate in the image	uInteger		
TimeStamp	DYNAMIC	ISO 8601 UTC date/timestamp	DateTime	Y	1ms resolution
VRN	DYNAMIC	Recognised licence plate number	Character		No whitespace characters. Allows images to be transmitted belatedly without the Host needing to refer to a database table referenced by InstanceID in order to associate VRN with images.
LaneID	DYNAMIC	Camera Lane to which image relates	uInteger		0 is the leftmost lane in the camera field of view. This ID is relative to the camera, not the actual lanes of the carriageway
ImageType	DYNAMIC	Whether the image is: a Plate patch (a close-cropped image of the plate as used for recognition) an ALPR image (the full image from which the plate patch has been taken) an Overview image (a visible image of the vehicle to which the plate read relates) a Context image (an uncropped image not related to a plate read) For cameras having separate ALPR and Overview sensors, context images by default relate to the ALPR sensor, but context images from the Overview sensor are also handled.	Enumerated	Y	Format: either "platePatch", "ALPRImage", "overviewImage", “contextImage” (from ALPR sensor) or “contextOverviewImage” (from Overview sensor).
ImageFormat	DYNAMIC	Encoding format of the image e.g. jpeg, tiff	Enumerated		Enumerated type having values "fits", "g3fax", "gif", "ief", "jp2", "jpeg", "jpm", "jpx", "t38", "tiff", "tiff-fx". (These formats are recognised MIME media types maintained in the IANA protocol registry: www.iana.org/assignments/media-types/image/).
BinaryImage	DYNAMIC	Jpeg image base-64 encoded	Binary		

Appendix 5 Camera Configuration Elements

A5.1 Camera Element

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
CameraID	STATIC	Unique identifier for the camera within a system	Character	Y	Local to Instation/Database Cross-reference to definition unique within a system can be compared in use to a "local IP Address"
HardwareUniqueID	STATIC	Globally unique identifier for the camera	Character	Y	Variable length up to 256 characters. Comprises three colon-separated fields i.e. "ManufacturerName:Model:FreeText". Each field any length with no whitespace allowed. ManufacturerName is mandatory, Model is optional - if null is signified by consecutive colons "ManufacturerName::FreeText". Strings must be alphanumeric and may include punctuation marks except colon.
ShortDescription	STATIC	Brief description of camera location	Character		
LongDescription	STATIC	Detailed description of camera location	Character		
XYType	STATIC	Reference co-ordinate system for XY location	Enumerated		e.g. OSGB or WGS84 (NB OSGB refers to OSGB36 datum)
XCoord	STATIC	X co-ordinate of camera location	Float		e.g. Longitude or Easting Degrees + decimal degrees for longitude
YCoord	STATIC	Y co-ordinate of camera location	Float		e.g. Latitude or Northing Degrees + decimal degrees for latitude
Height	STATIC	Height of camera above local ground level	Float		Measured in metres e.g. Height above Lowest road surface in multi-level junction

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
TypeID	STATIC	Type of equipment from generic list	uInteger		Generic ALPR = 5, IR = 6, IR+colour = 7, colour = 8
MobileCamera	STATIC	Whether the camera is mobile or fixed	Boolean		Assume fixed if attribute is absent
SoftwareVersion	STATIC	Software version number of the application generating the machine diagnostics (manufacturer specific)	Character		e.g. 3.5.15.72

A5.2 Lane Element

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
LaneID	STATIC	Camera Lane to which configuration item(s) relate	uInteger	Y	0 is the leftmost lane in the camera field of view This ID is relative to the camera, not the actual lanes of the carriageway
LaneNumber	STATIC	Position of the Lane in relation to the total number of lanes in the carriageway	uInteger	Y	In the range 0 to 99 Lane 0 is the first lane on the left in the direction of travel
LaneDirectionTypeID	STATIC	Direction of the carriageway lane in which vehicles normally travel (Note that this attribute relates to the direction taken by vehicles, not the direction in which the camera is pointing.)	uInteger	Y	e.g. 3 = clockwise, 4 = anticlockwise, 5 = northbound etc Format: see Direction_TypeID in CCTV ALPR Extensions Global Support Object
NormalVehicleDirection	STATIC	Direction relative to the camera in which vehicles normally travel	Enumerated	Y	e.g. towards, away, both "Both" applies for a single track road or tidal lane in a multi-lane road

A5.3 Configuration Element

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
HostName	CONFIG	Name of host to which configuration item(s) relate	Character		The fully qualified host URL or endpoint is set at time of commissioning.
SendVRNs	CONFIG	Whether to send VRN data (true/false)	Boolean		Following config items per host
SendTags	CONFIG	Whether to send Tag data (true/false)	Boolean		
SendPlatePatches	CONFIG	Whether to send plate patch images (true/false)	Boolean		
SendANPRImages	CONFIG	Whether to send full frame ALPR images (true/false)	Boolean		
SendOverviewImages	CONFIG	Whether to send full frame Overview images (true/false)	Boolean		
SendPlatesNotRead	CONFIG	Whether to send PlateRead records where PlateNotRead attribute is true	Boolean		See PlateRead attribute “PlateNotRead”
SendANPRDiagnostics	CONFIG	Whether to send ALPR diagnostics (true/false)	Boolean		
SendMachineDiagnostics	CONFIG	Whether to send machine diagnostics (true/false)	Boolean		
SendIncrementalLog	CONFIG	Whether to send an incremental log file (additions since last send)	Boolean		
SendPeriodicContextImage	CONFIG	Whether to send periodic context images (true/false)	Boolean		Note that in multiple sensor cameras, the sensor from which the context image is to be taken is determined by manufacturer-specific means. For example an image from the overview sensor may be returned during the day and an image from the ALPR sensor at night.

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
UseReportingOffset	CONFIG	Whether the camera should utilise the ReportingOffset (true/false)	Boolean		If false, permits the randomisation of reporting times by another method (for example by starting reporting intervals relative to the last camera power-on or reset) without the need to configure each camera with an individual ReportingOffset. Avoids cameras all reporting at the same time if no ReportingOffset is configured or a default value is assumed.
SendHeartbeat	CONFIG	Whether a generic wrapper should be sent periodically irrespective of whether there is data to send (true/false)	Boolean		Allows the sending of heartbeats to be turned on and off explicitly, rather than relying on whether a HeartbeatInterval has been configured.
StreamPlates	CONFIG	Whether to send a PlateRead record as soon as a plate is recognised (true/false)	Boolean		
HeartbeatInterval	CONFIG	Send at least one generic wrapper during this interval in seconds	uInteger		Maximum value 86400 seconds (=1 day)
PlateSendInterval	CONFIG	Reporting interval for sending VRN and/or tag data in seconds	uInteger		The end of the PlateSendInterval should be aligned with the time of transmission determined by the ReportingOffset, to ensure that the latest plate data is always reported as soon as possible.
ReportingOffset	CONFIG	Reporting time offset as percentage of appropriate send interval	Percent		Relative to a reporting interval commencing at midnight
ANPRDiagsSendInterval	CONFIG	Reporting interval for sending ALPR diagnostics in seconds	uInteger		
MachineDiagsSendInterval	CONFIG	Reporting interval for sending machine diagnostics in seconds	uInteger		
IncrementalLogInterval	CONFIG	Reporting interval for sending incremental log in seconds	uInteger		
ContextImagePeriod	CONFIG	Time interval at which a single context image is returned in seconds	uInteger		Single image only - not a batch

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
MaxPlatesToSend	CONFIG	Maximum number of VRNs/Tags to send per reporting interval	uInteger		Applies when StreamPlates is false - send up to this number of captured plates during a plate reporting interval.
MinANPRDiagnosticSamples	CONFIG	Minimum vehicles to be included in ALPR diagnostic averages	uInteger		Roll samples over from one interval to next
CurrentDateTime	CONFIG	DateTime value to set real time clock. The presence or absence of this attribute in the InstationToCamera response determines whether the Camera clock should be set or not.	DateTime		For dateTime format, see section 3.2.7 (dateTime) of W3C document “XML Schema Part 2 - Datatypes Second Edition“

Appendix 6 ImageRequest Elements

A6.1 TimeRangeImageRequest

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
StartTime	DYNAMIC	ISO 8601 UTC date/timestamp	DateTime	Y	1ms resolution
EndTime	DYNAMIC	ISO 8601 UTC date/timestamp	DateTime	Y	1ms resolution
ImageTypeArray	DYNAMIC	Array element containing 0 to n ImageTypes (list of the types of images required)	Character		See ImageType attribute of Image element (contextImage and contextOverviewImage will be ignored)

A6.2 PriorVRNImageRequest

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
NoOfPriorVRNs	DYNAMIC	Number of most recent VRN instances for which images are required	uInteger	Y	
EndInstanceID	DYNAMIC	The set of images to be sent should end with this InstanceID	uInteger		Used in conjunction with NoOfPriorVRNS to determine the latest InstanceID which should be sent in the set of images defined by these two attributes.
ImageTypeArray	DYNAMIC	Array element containing 0 to n ImageTypes (list of the types of images required)	Character		See ImageType attribute of Image element (contextImage and contextOverviewImage will be ignored)

A6.3 InstanceSetImageRequest

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
InstanceIDArray	DYNAMIC	InstanceArray element containing 0 to n Instance IDs for this camera of VRN records of the plates for which images are required	uInteger	Y	
ImageTypeArray	DYNAMIC	Array element containing 0 to n ImageTypes (list of the types of images required)	Character		See ImageType attribute of Image element (contextImage and contextOverviewImage will be ignored)

A6.4 ContextImageRequest

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
ImageTypeArray	DYNAMIC	Array element containing 0 to n ImageTypes (list of the types of images required)	Character		See ImageType attribute of Image element (anything other than contextImage or contextOverviewImage will be ignored)

THE COMMONWEALTH OF MASSACHUSETTS
EXECUTIVE OFFICE OF PUBLIC SAFETY AND SECURITY
Department of Criminal Justice Information Services
200 Arlington Street, Suite 2200, Chelsea, Massachusetts 02150, MASS.GOV/CJIS
TEL: 617-660-4600 • TTY: 617-660-4606 • FAX: 617-660-4613

Deval L. Patrick, *Governor* | Andrea J. Cabral, *Secretary of Public Safety and Security* | James F. Slater, III, *Acting Commissioner*

EXECUTIVE OFFICE OF PUBLIC SAFETY AND SECURITY DEPARTMENT OF CRIMINAL JUSTICE INFORMATION SERVICES AUTOMATIC LICENSE PLATE RECOGNITION SYSTEMS CENTRAL REPOSITORY COMPANION POLICY

PURPOSE

To establish guidelines and best practices for data use, maintenance, training, and data storage associated with the usage of the Commonwealth Criminal Justice Information Automatic License Plate Recognition Systems Central Repository (Central Repository) by Massachusetts law enforcement agencies.

OVERVIEW

An Automatic License Plate Recognition (ALPR) system is a computerized system that uses high-speed digital cameras combined with sophisticated computer algorithms capable of converting the images of license plates to electronically readable data. The ALPR system captures an infrared image of a license plate and converts it to a text file using Optical Character Recognition (OCR) technology. The technology also compares the digital images of license plates to lists of known plates of interest. Currently, the ALPR is being utilized by many law enforcement and criminal justice agencies in the Commonwealth, which maintain the captured information in a database.

The Central Repository is a centralized data warehouse that stores ALPR information contributed by law enforcement and public safety agencies from the agency's database. By allowing the agencies to share and access the stored information, local, state and federal law enforcement agencies are provided accurate information to be used for official and legitimate law enforcement operations and public safety purposes. Guidelines for submission and retrieval of license plate data for all participating departments are included in the Commonwealth of Massachusetts Global Justice and Public Safety Information Sharing Policy of the Massachusetts Department of Criminal Justice Information Services (DCJIS), which is incorporated by reference, and this ALPR Central Repository Companion Policy. ALPR systems are dependent upon the networking system of Commonwealth's Criminal Justice Information System (CJIS) and all participating agencies and users agree to the terms of these policies.

DCJIS Enhancing Public Safety Through Information Exchange

POLICY

It is the policy of the DCJIS to utilize the technology only in furtherance of official and legitimate law enforcement operations and public safety. Recognizing privacy implications, it is further the policy of DCJIS to ensure the protection of data. Thus, all users of the Central Repository are expected to abide by the guidelines set forth herein when using the Central Repository.

ACRONYMS AND DEFINITIONS

Agency ALPR Administrator: An employee of a Participating Agency designated by that agency to be responsible for the management of its authorized users and the user accounts at the Participating Agency.

Authorized User: An individual designated by a law enforcement agency and properly trained in the use and operational protocols of the ALPR. Only authorized employees who have an approved login and password will be allowed to access or use information in the Central Repository.

Contributing Agency: An agency that contributes ALPR data to the Central Repository.

Non-Contributing Agency: An agency that may access, but does not contribute data to, a data application or system maintained or operated within the DCJIS network or system.

Participating Agency: Either a contributing or non-contributing party that utilizes the Central Repository.

Source Agency: The agency that originally recorded and contributed data to a data application or system maintained or operated within the DCJIS network or system.

PROCEDURES

1. Standard of Use

Central Repository ALPR data shall be accessed and used only for official and legitimate law enforcement operations and public safety and may only be used based on specific and articulable facts of a concern for safety, wrongdoing, criminal investigations, Department-related civil investigations, or pursuant to a court order.

Searches of historical Central Repository ALPR data shall be done in accordance with this policy.

Only users who have been designated by their law enforcement department and properly trained in the use and operational protocols of the ALPR systems shall be permitted to use the Central Repository. DCJIS administrators shall ensure that any changes in hardware, software or law are communicated to all participants. Only authorized employees who have an approved login and password (Central Repository Authorized Users) will be allowed to access or use information in the Central Repository.

When a enforcement action, investigation, or prosecution results from the Repository ALPR data, the information contained in it will be preserved by the agency accessing the information.

Requests for searches of Central Repository ALPR data may be made by authorized members of the Contributing Party or Non-Contributing party subject to the provisions of this policy.

2. Login Application Process

a) Each Contributing and Non-contributing Party shall designate an Agency ALPR administrator to be responsible for management of user accounts at that agency. All authorized users shall be limited to current employees who are legally authorized to review criminal justice information for crime prevention and detection purposes. Each potential user shall submit a request for a login and password to the Agency ALPR Administrator. The Agency ALPR Administrator shall have discretion to deny or revoke individual access.

3. Login Assignment

a) Each Authorized User will be issued a user login and a default password by the Agency ALPR Administrator. Upon logging into the Repository for the first time, each Authorized User shall change the default password to another DCJIS-compliant password.

b) Each Agency ALPR Administrator is responsible for the timely removal of any login accounts as Authorized Users leave their agency.

c) An Authorized User shall not access the Central Repository by using a name and password that was assigned to another user. An Authorized User shall not give his or her password to another person, including another user, to access the system.

4. ALPR Central Repository Data Query Logs

a) An automated log will be maintained for each transaction, which will include the name of the individual accessing the data, along with the date and time of access.

b) Requests to review stored ALPR data and search results will be recorded and maintained in appropriate case files.

c) ALPR Data Query Logs shall be maintained and secured.

d) Audits of the ALPR systems and the central repository shall be conducted by the DCJIS.

5. ALPR Data Sharing and Dissemination

a) Each Contributing Agency authorizes the release of its information as outlined in this Policy to any other criminal justice agency that may participate in the Central Repository in the future.

b) A Contributing Party that does not want certain information from its ALPR system to be shared is responsible for filtering out such information before entering it into the Central Repository.

c) The information contributed to the Central Repository is limited to ALPR data.

d) Central Repository ALPR data can be accessed, retrieved, or shared for official and legitimate law enforcement operations or public safety purposes only.

6. Ownership of Data

a) Each Contributing Party will retain sole responsibility, ownership, management control, and disposition over the information it contributes or allows access to. All system entries will be identifiable to the Contributing Party, and the content of the contributed information remains the sole responsibility of the Contributing Party and is under that Contributing Party's management control.

b) It shall be the responsibility of the party requesting or using the data to confirm the accuracy of the information with the Source Agency before taking any enforcement-related action.

7. Retention of Data

a) Data from field ALPRs will be transferred/uploaded to the Department's server at a time to be determined by the Agency ALPR Administrator.

b) ALPR data shall be stored in the Central Repository for a period of one year except in the following circumstances:

i) Alert data associated with an enforcement action, investigation, or prosecution shall be maintained for one year or until a final disposition has been reached in the particular case, whichever is longer.

ii) Alert data associated with an arrest will be maintained in the criminal case file and retained for the maximum period of time associated with such record.

iii) Alert data associated with criminal investigations will be maintained in the criminal case file and retained for the maximum period associated with such record.

iv) If it is reasonable to believe and the ALPR data will become evidence in a criminal or civil action, the record will be maintained until it is no longer reasonable to believe it will become evidence in a criminal or civil action.

v) Whenever otherwise directed by the ALPR Administrator.

CONFIDENTIALITY OF INFORMATION

Information in the Central Repository is confidential and is not subject to public disclosure, except as required by law. Only Authorized Users are allowed to view and use the information, otherwise, the information shall be kept confidential.

ACKNOWLEDGEMENT OF TERMS AND CONDITIONS OF USE

The Agency ALPR Administrator shall provide a copy of the terms and conditions of the Massachusetts Public Safety Information Sharing Global Policy and this ALPR Central Repository Companion System Policy to all Authorized Users when they are issued a login ID for the system. Each Authorized User shall sign an acknowledgement stating, "I have received a copy of the terms and conditions of usage of the Central Repository. I agree to comply with the terms and conditions and I understand that any violation of the terms and conditions may lead to disciplinary action and/or criminal prosecution." The Agency ALPR Administrator shall maintain the signed acknowledgements at all times.

POLICY REVIEW

The Commissioner of the Department of Criminal Justice Information Services is responsible for the annual review of this policy.





PIPS TECHNOLOGY™
DETECTION INNOVATION

Back Office System Software

User's Manual
Version 3.5 or above

NEOLOGY™ MOBILITY TECHNOLOGIES

Table of Contents

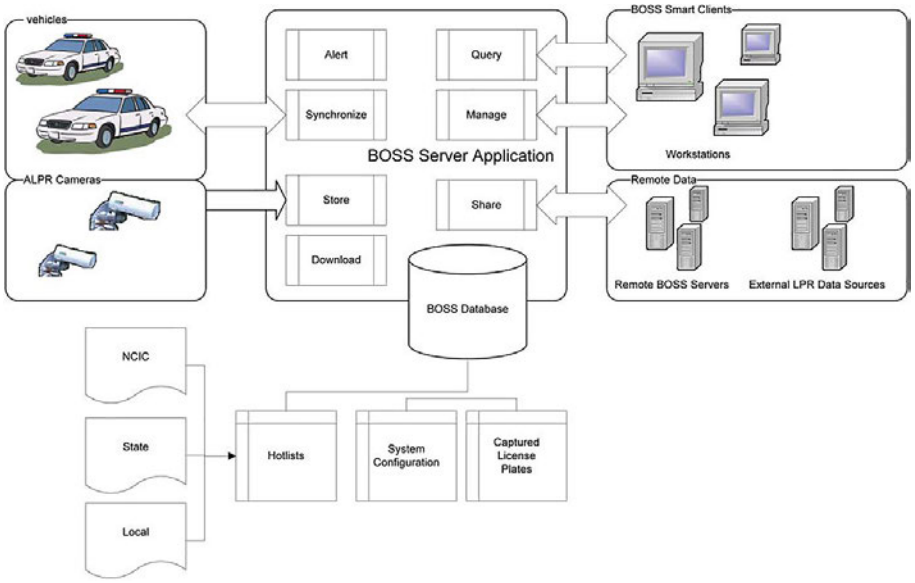
1 Introduction 4
1.1 The Design of PIPS Back Office System Software Version
2 Logging In 5
2.1 PIPS Back Office System Software Administrator Login 5
2.2 User Login 5
2.3 Login Dialog 5
2.3.1 Storing Username and Password 6
2.3.2 BOSS Client Connection Settings 6
3 Application Layout 7
3.1 Components of the BOSS Application Screen 7
3.2 The BOSS Home Screen 8
3.3 Help Documentation 9
3.4 Minimizing the BOSS Application 9
4 BOSS Access Permissions: Users/Groups/Roles 10
4.1 Permission Levels 10
4.2 Permissions 10
4.3 Roles 11
4.4 Groups 12
4.4.1 Creating a New Group 12
4.4.2 Parent Groups 13
4.4.3 Deleting a Group 13
4.5 Users 14
4.5.1 Creating a New User 14
4.5.2 Deleting a User 15
4.5.3 Importing Users from Active Directory 16
4.6 Access Permission Example 17
4.7 Preferences 18
4.7.1 Changing User Preferences 18
5 Devices and Sites 19
5.1 Devices 19
5.1.1 Device Status 20
5.1.2 Defining a Device 20
5.1.3 Editing a Device 21
5.1.4 Enabling and Disabling a Device 21
5.1.5 Deleting a Device 22
5.2 Sites 22
5.2.1 Default Sites 22
5.2.2 Creating a Site 23
5.2.3 Deleting a Site 23
6 BOSS Data Sharing 24
6.1 Configuring BOSS to Allow Remote BOSS Queries 24
6.2 Configuring BOSS to Access a Remote BOSS Server 24
7 Hotlists 25
7.1 Creating a New Hotlist 25
7.1.1 Configuring Basic Hotlist Settings 25
7.1.2 Defining the Hotlist Data Source 27
7.1.3 ZIP Compressed Hotlist Files 29
7.1.4 Defining Hotlist Source Credentials 29
7.1.5 Defining Hotlist Advanced Options 31
7.2 Enabling and Disabling a Hotlist 32
7.3 Modifying Hotlist Entries 32
7.3.1 Querying Hotlist Entries 33
7.3.2 Editing a Hotlist Entry 34
7.3.3 Adding a Hotlist Entry Manually 34
7.3.4 Deleting a Hotlist Entry 35
7.4 Targets 35
7.4.1 Creating a New Target 36
7.4.2 Deleting a Target 36
8 Hotlist Formatters 37
8.1 Creating a New Formatter for Hotlists 37
9 Alerts 38
10 Dispatch 39
10.1 Dispatch Settings 40
10.2 Dispatch Hits 41
10.3 Dispatch Reads 41
10.4 Manual Entries 41
10.4.1 Adding a Manual Read 42
10.4.2 Correcting Reads 42
11 Querying Stored Data 43
11.1 Wildcards 43
11.2 Quick Search Bar 43
11.2.1 Quick Search Fields 43
11.3 Query Result Navigation Icons 43
11.4 Advanced Reads Queries 44
11.4.1 Performing an Advanced Reads Query 44
11.4.2 Entering Advanced Reads Query Criteria 45
11.4.3 Managing Query Results 46
11.5 Multiple Query Tabs 46
11.6 Cross-Referencing External Data 47
11.7 Working with Queried Reads. 48
11.7.1 Viewing Query Results 48
11.7.2 Query Results Actions 49
11.7.3 Viewing Read Details 49
11.8 Favorites 52
11.8.1 Creating a New Favorite 52
11.8.2 Activating a Favorite 52
11.8.3 Deleting a Favorite 53
12 Reports 54
12.1 Running a System Report 54
12.2 Viewing and Printing Reports 54
12.2.1 Viewing the Login Statistics Report 55
13 Client Tools 56
14 Archiving Data 57
15 System Settings 58
15.1 Sessions 58
15.1.1 Viewing and Disconnecting Sessions 58
15.1.2 Workstation Power Management and Sessions 58
15.2 Dispositions 59
15.2.1 Defining a New Disposition 59
15.2.2 Deleting a Disposition 59
15.3 System Parameters 60
15.3.1 Editing System Parameters 60
15.3.2 List of BOSS System Parameters 60
15.3.3 Branding 62
15.4 Roles 63
15.4.1 Adding New Roles 63
15.4.2 Deleting Roles 63

15.5 Report Management ... 64
15.5.1 Assigning Permissions to Access Reports ... 64
15.6 Translations ... 64
15.6.1 Entering a New Translation ... 65
15.7 Justifications ... 66
15.7.1 Entering a New Justification ... 66
15.7.2 Deleting Justifications ... 66
17 Appendix: Installation and Configuration Guide ... 67
17.1 Installing the BOSS Server Application Files ... 68
17.1.1 Running the Installer ... 68
17.1.2 PIPS License Agreement ... 69
17.2 BOSS Version 3.2 and Above License Key Management ... 70
17.2.1 Activating the License Key ... 70
17.2.1.1 Activating the License Key over the Internet ... 71
17.2.1.2 Activating the Software with a License File. ... 72
17.2.1.3 Request a License File to Activate the License ... 72
17.2.2 Updating a License Key ... 73
17.3 Map Display Options with BOSS ... 74
17.3.1 U.S. Census Bureau TIGER Maps ... 74
17.3.2 Advanced Mapping with Microsoft Bing Maps ... 74
17.4 Configuring the BOSS Server Application ... 74
17.4.1 The BOSS Controller Application ... 74
17.4.1.1 Starting the BOSS Controller ... 74
17.4.1.2 Status Colors ... 74
17.4.1.3 Right-Click Menu ... 75
17.4.1.4 Starting the BOSS Service ... 75
17.4.1.5 Stopping the BOSS Service ... 75
17.4.2 BOSS Configuration ... 76
17.4.2.1 Activating the Configuration Wizard ... 76
17.4.2.2 BOSS Configuration Wizard ... 76
17.4.2.3 SQL Server Configuration ... 77
17.4.2.4 Resetting the Administrator Password ... 78
17.4.2.5 Network Port Settings ... 78
17.4.2.6 Regional Hotlist Formatters ... 80
17.4.2.7 NCIC Hotlist Formatters ... 80
17.4.2.8 TIGER Maps Configuration ... 81
17.4.2.9 Finishing Configuration ... 81
17.5 Installing the BOSS Smart Client Application ... 82
17.5.1 Installation over the Web ... 82
17.5.2 Stand-Alone Installation ... 82
17.6 Configuring Client Tools ... 82
18 Troubleshooting ... 84
19 Appendix: Plug-Ins ... 87
19.1 The BOSS Truck Drayage Utility ... 87
19.2 The BOSS LPRD Plug-In ... 87
19.3 The BOSS DEA Plug-In ... 87
20 Appendix: BOSS Mantis ... 88
20.1 How Dose Mantis Work ... 88
20.2 Mantis Security and Encryption ... 89
20.3 Mantis Requirements ... 90
20.4 Mantis Installation ... 90
20.5 Mantis Configurations ... 90
20.6 Mantis Search Features. ... 91
20.6.1 Mantis Search Definitions ... 91
20.7 Additional Mantis Parameters ... 92
20.8 Mantis Configuration Troubleshoot ... 92
20.8.1 Mantis Log Messages Catalog ... 93
Glossary ... 95

1 INTRODUCTION

This document serves as a user's manual for the PIPS Back Office System Software (BOSS) version 3.5 or above and describes the various features and functionality of the application. BOSS is a management and administration tool for the PIPS Automatic License Plate Recognition (ALPR; also known as ANPR, or Automatic License Number Recognition) systems. The BOSS server application provides an interface for user maintenance, data queries, import and export of data, and dispatch functions. BOSS lets an Administrator specify the databases used by both mobile and fixed camera installations. BOSS retrieves these databases on a regular schedule; manages the users of the PIPS PAGIS systems and BOSS Smart Client workstations; provides a central repository for data collected by mobile PAGIS deployments and fixed camera installation; provides reporting and data management tools; provides hit detection and dispatch functions for fixed camera installations; and allows for data mining and data sharing with other agencies.

The following schematic shows how the BOSS server application works together with Smart Client workstations, various data sources, PAGIS, and the full line of ALPR cameras to create a comprehensive solution.



1.1 The Design of PIPS Back Office System Software Version 3.5 and Above

The design of BOSS version 3.5 or above offers ease of accessibility with a user-friendly look and feel. Large, easy-to-identify icons provide intuitive navigation, and the frequently used elements are readily available. The user interface (UI) is very recognizable and comfortable, particularly for users already familiar with Windows-based applications, including Microsoft® Office software, or the Mobile Pagis Software. In addition, users can enter a minimum amount of information to add a data object, with the ability to include more details if needed.

2 LOGGING IN

2.1. PIPS Back Office System Software Administrator Login

During each new installation of the PIPS Back Office System Software, a default user of “admin” is created, with the password of “admin1.” The installer or designated BOSS Administrator can log in with this account to create additional users and otherwise configure the system. It is important that the “admin” password be changed to protect the system’s security. Likewise, it is equally as important to keep this and all passwords confidential to protect the security of the BOSS system. Section 17, Installation and Configuration, offers more information on setting up users and passwords.

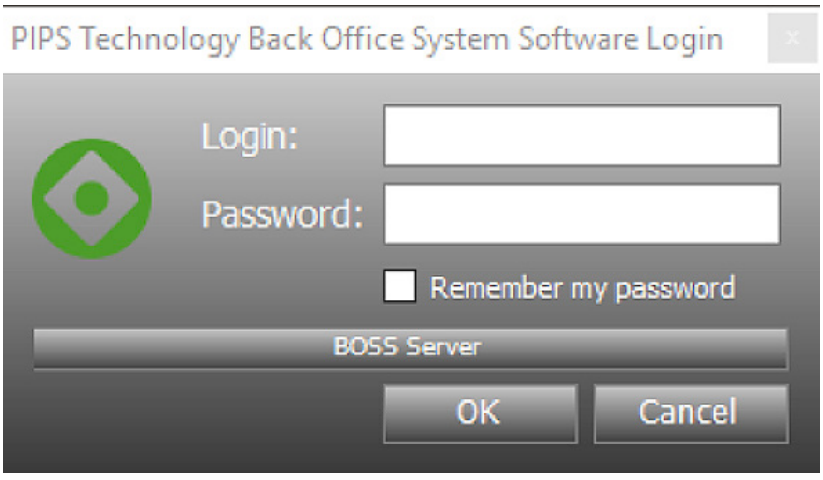
2.2 User Logins

The PIPS Back Office System Software will require a user to log in with a username and password only if there is no BOSS user matching the current Active Directory user login. In other words, if the username currently logged into Windows matches a username in the BOSS system, the user is automatically logged into the application when it is started, and no login screen will appear.

For example, if user “bsmith” is logged in using Windows Domain Authentication through Active Directory (“logged into Windows”), when the BOSS Smart Client is started, and a “bsmith” user exists within the BOSS system, no login screen will appear; the application will authenticate the user and load automatically. If a user logs onto Windows with a name that is not an exact match to a username in the BOSS system, or is not logged into the same Windows Domain, a login screen will appear. The user will then need to enter a correct BOSS user name and password in order to enter the application.

Note: In order for a user to be automatically logged into BOSS, the Active Directory user must be in the same Windows domain as the PIPS™ Back Office System Software server.

2.3 Login Dialog



1. Enter your username in the Login field.

2. Enter the correct password in the Password field.
Note: Passwords are case sensitive.

3. Click OK to complete the login process.

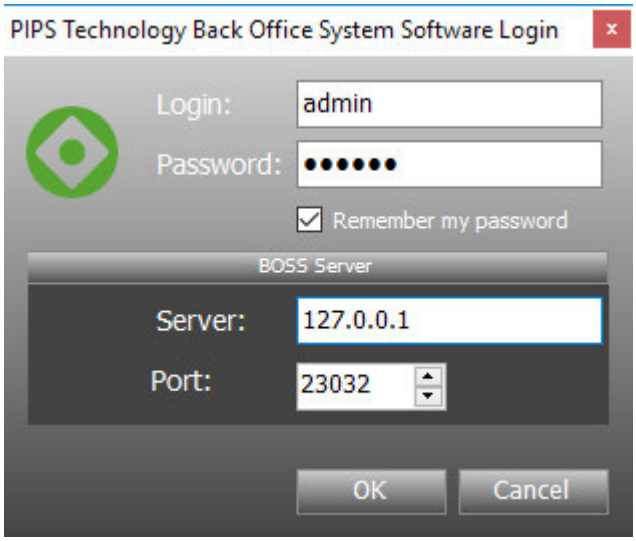
2.3.1 Storing Username and Password

Select the Remember my password option to save the password to the computer's local Windows registry and automatically fill in both Login and Password fields on subsequent logins.
Selecting this option only remembers the login information for the current Windows User on the local computer. It will not apply to a different Windows user logged in the same computer and will not apply to the same user logging in a different computer. This option need not be checked every time. Once checked, the option will stay that way until it is deselected during a login.

Note: The username and the password are stored in the Windows Registry. This can be a security risk. It is recommended that you not use the Remember my password option unless the Windows workstation can be secured against unauthorized access.

2.3.2 BOSS Client Connection Settings

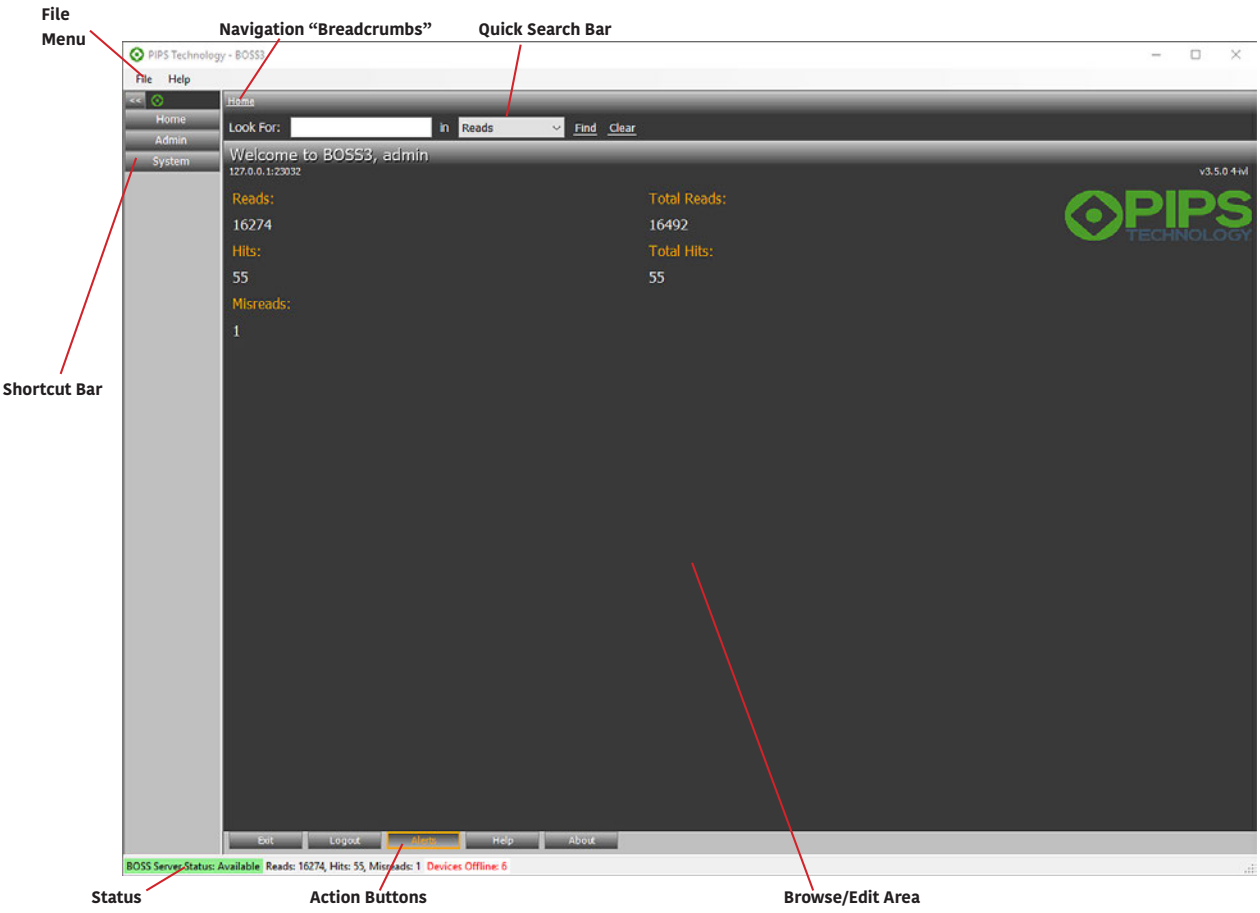
Click the BOSS Server button on the Login screen to view or change the client connection settings.



Server – IP address, computer name, or DNS address can be used in the Server field as long as the client can reach the server using the value entered.
Port – The default port used for connecting to the BOSS server is 23032. This should only be changed here if the BOSS server has been configured to use a non-default port.

3 APPLICATION LAYOUT

3.1 Components of the BOSS Application Screen



File Menu – The File menu of the application resides in the very top left of the application window. The File menu is always visible and available regardless of the screen or shortcut selected. The Exit option is available through this menu.

Navigation – The navigation "breadcrumbs" appear at the top of the BOSS screen as different actions are selected. By clicking on the links it is possible to backtrack to a previous screen.

Shortcut Bar –The Shortcut bar (the panel on the left of the screen) contains icon buttons for the various operations available. The shortcut icons are divided into three categories: Home, Admin, and System. Each time the application is started, all of the categories are closed with no shortcuts displayed. Click on any of the three headings to access the shortcuts within that category. The actual categories and shortcuts that appear depend on the logged-in user's privileges.

The Shortcut bar can be collapsed entirely to provide a larger space for the Browse/Edit area by clicking the << button at the top left of the screen. To expand the Shortcut bar again, click the >> button.

Browse/Edit Area – The widest portion of the application window, the Browse/Edit area is where data is displayed for viewing or editing. The actual data displayed here depends upon the shortcut icon that is selected from the Shortcut bar.

Quick Search Bar – Directly above the Browse/Edit Area, the Quick Search bar allows for simple, immediate queries of BOSS data. Using the Quick Search bar simply involves typing the text to query in the Look For field and selecting the type of data (reads, hits, etc.) to search in the drop-down box.

Action Buttons – These are the buttons directly below the Browse/Edit area. These buttons will differ depending on the shortcut icon selected. The actual buttons that appear will also vary depending upon the user's privileges.

Status Bar – This is the area along the very bottom of the application window that displays the following system information:

- **BOSS System State (Available or Offline):** "Available" status indicates that the client is currently communicating with the BOSS server application and the server is running. This status is highlighted with a green background. "Offline" status indicates that the client is currently not able to communicate with the BOSS server and is highlighted with a red background. In this event, the BOSS UI will continue to check for the BOSS server to become available again. After three attempts to reconnect, the user will be notified that the connection could not be re-established and will be provided further instructions on how to proceed.
- **Reads:** The total number of reads currently contained in the BOSS system.
- **Hits:** The total number of hits currently contained in the BOSS system.
- **Misreads:** The total number of misreads currently contained in the BOSS system.
- **Devices Offline:** The number of fixed camera devices that are currently identified as offline.

3.2 The BOSS Home Screen

The BOSS Home screen is displayed within the Browse/Edit area upon login. The top banner displays the username of the current BOSS user, the BOSS server address, and current system statistics. Statistics may take a few moments to update after login. The action buttons, described below, are displayed along the bottom of the screen. The actual buttons that display will vary depending upon the user's privileges.

Exit – Exit the BOSS application.

Logout – Log out from the current session to the Login screen.

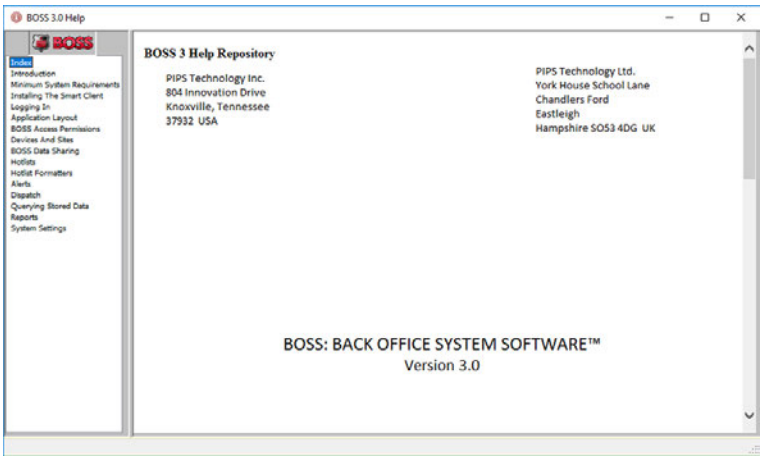
Alerts – Toggle dispatch alerts on (orange highlight) and off. This button will not be displayed if the user is not authorized to access the dispatch screen, or if the user has not chosen to receive dispatch alerts in Preferences (Section 5.3).

Help – Activate the help system.

About – Display application information.

3.3 Help Documentation

BOSS provides a help document accessible in the client application. To access help, select Help in the File menu area or press the F1 button. A help document will be displayed in a browser window and is indexed and searchable for ease of use.



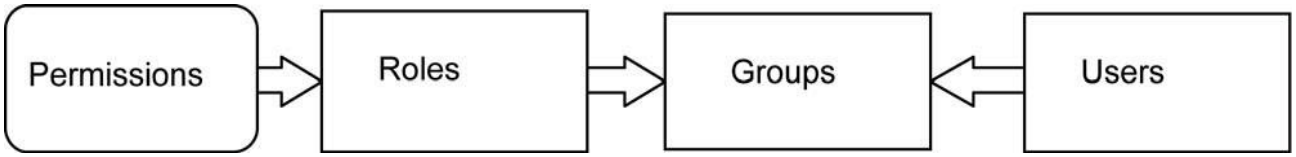
3.4 Minimizing the BOSS Application

The BOSS application can be minimized to the Windows System Tray using the Windows minimize button on the right upper corner of the BOSS application window. To restore the BOSS application, click on the BOSS PIPS icon. When the application is minimized, real-time alerts will still be displayed.



4 BOSS ACCESS PERMISSIONS: USERS/GROUPS/ROLES

Access permissions to various functions (such as reports or dispatches) in BOSS are administered through users, groups, and roles. Each individual who will use the BOSS software must log in via a user account. Each user account is assigned to a group. Every group is assigned a role (such as Administrator or Dispatcher), which determines the set of functionality to which the group's members will have access:



The security parameters defined in a role apply to a user via the group to which the user belongs.

4.1 Permission Levels

The following table lists the levels that apply to permissions:

LEVEL	EXPLANATION
No Access*	No permissions to the function
Read Only	View-only permissions to the function. Add/Change/Delete are not permitted.
Full Access	Complete permissions to the function. View/Add/Change/Delete are permitted.

**When a user's effective permissions to a function are No Access, the function is not visible to the user. For example, if a user has No Access privileges to the System function, the System category is not displayed.*

4.2 Permissions

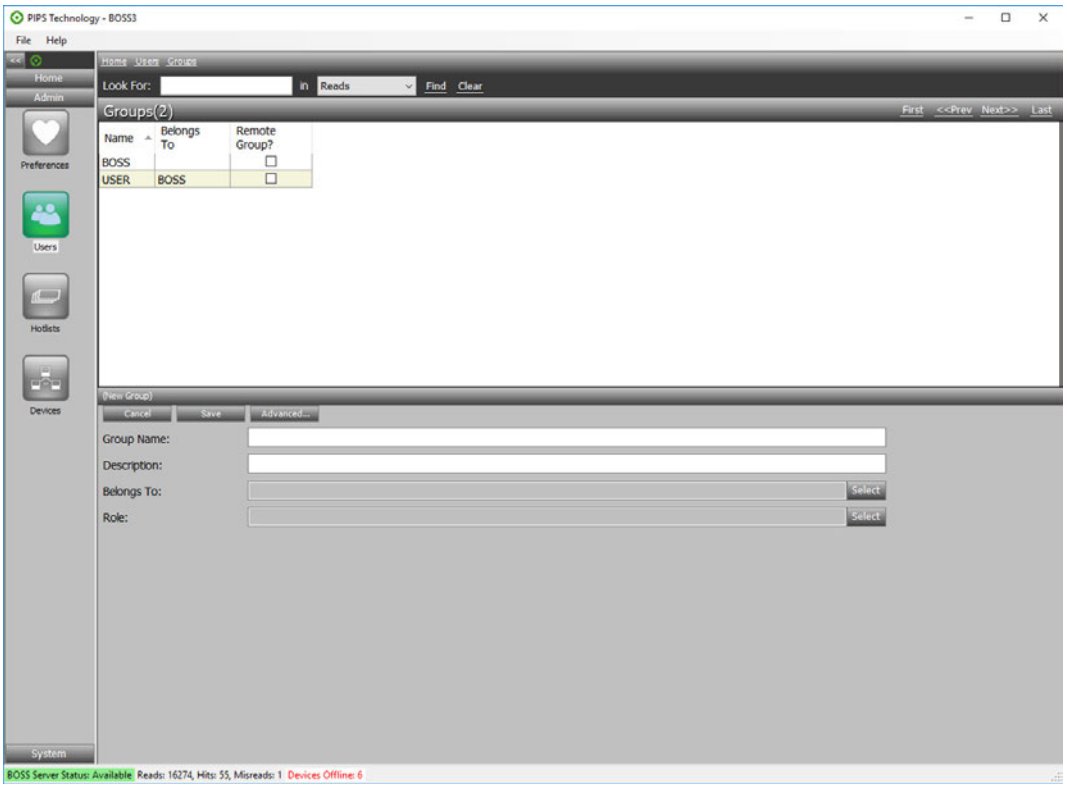
The following table lists the functions that are controlled by permissions levels:

PERMISSION	EXPLANATION
Reads	Plate read information
Dispatch	Real-time monitoring and hit alerts
Users	Groups and user accounts
Hotlists	Hotlists (plates of interest)
Devices	Sites and ALPR camera devices
System	System configuration options

See Section 15.4, Roles, for more information on setting permissions.

4.3 Roles

Roles are access permission profiles. BOSS comes with several predefined roles. A BOSS Administrator is able to add additional roles to the system. A BOSS Administrator is also able to alter and delete any roles. Roles define a permission level for different functions of the system. See Section 15.4, Roles, for additional information.



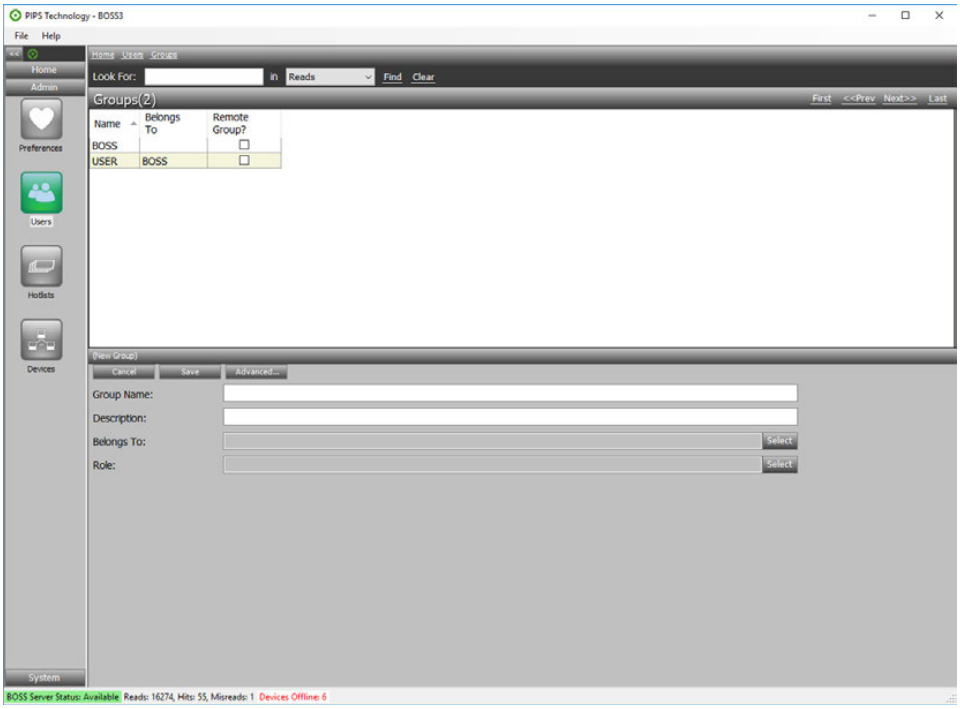
The following roles are installed by default in a BOSS system:

- System Administrators
- User
- Dispatcher
- Group Administrators
- Device Administrators
- Hotlist Administrators

See System Settings section for Role definitions and changes.

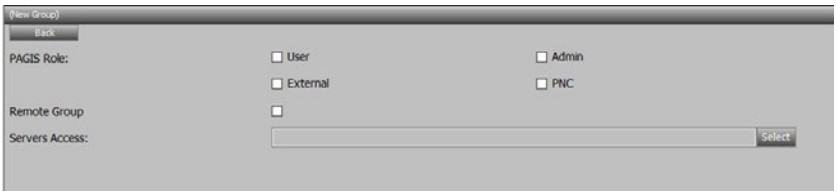
4.4 Groups

Groups are collections of users that have the same permissions. Groups provide an efficient way to organize users, for example by organizational units, and easily assign permissions to those users. Using groups is optional. A default group named “BOSS” automatically exists within a BOSS system, and user accounts will belong to the “BOSS” group by default. The BOSS group cannot be deleted.



4.4.1 Creating a New Group

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Users** shortcut. A list of all current users will display in the Browse/Edit area.
3. Click the **Groups** button at the bottom of the Browse/Edit area. A list of all current groups will display in the Browse/Edit area.
4. Click the **New** button. The New Group Entry screen will display.
5. In the Group Name text box enter a name for the group. (**Note:** The group name must have a minimum of three characters.)
6. In the Group **Description** text box enter a description of the group (optional).
7. Each group, except for the default BOSS group, is required to have a parent group. In the Belongs To field, click the **Select** button to view a list of all existing groups. Click on the desired group and click the **Save** button to select. The name of the selected group will display in the Belongs To field as the parent group.
8. Assign a role to the group. In the Role field, click the **Select** button to select from the existing roles. Click the desired role from the list and click the **Save** button to make the selection. The name of the selected role will appear in the field.
9. Click the **Advanced**... button to access additional, optional settings for the new group.



4.4.1 Creating a New Group (continued)

PAGIS Role (User/Admin/External/PNC) – Check desired PAGIS roles to grant the new group for the associated permissions in Pagis. Please refer to the Pagis User's Manual for more information.

Remote Group – Select this option to designate the group as remote. When a BOSS Administrator wants to give access to another BOSS system for remote queries ("data sharing," see Section 6), a login must be created and assigned to a group that is flagged as a remote group. The remote BOSS Administrator will then create a remote site with credentials for that login.
Servers Access – This option allows for defining which, if any, sites will be accessible by this group. Click the Select button to access a list of sites.

Note: There are two sites defined by default: Manual Entries and Unassigned. If no additional sites have been defined, only the default values are available in this field. Click each desired site and click the **Save** button to complete the selection process. If one site is selected the name of that system will appear in the Server Access field. More than one site can be selected.

Log Queries – This option, when selected, will result in the logging of all queries made by all users of the group. This information is then available via the audits report. **WARNING:** *This can potentially be a very large amount of data. Select this option with care.*

a. Configure these Advanced User settings as desired.

b. Click the **Back** button to return to the main New Group Entry screen

10. Click **Save** to complete creating the new group, or click **Cancel** to clear the new group.

4.4.2 Parent Groups

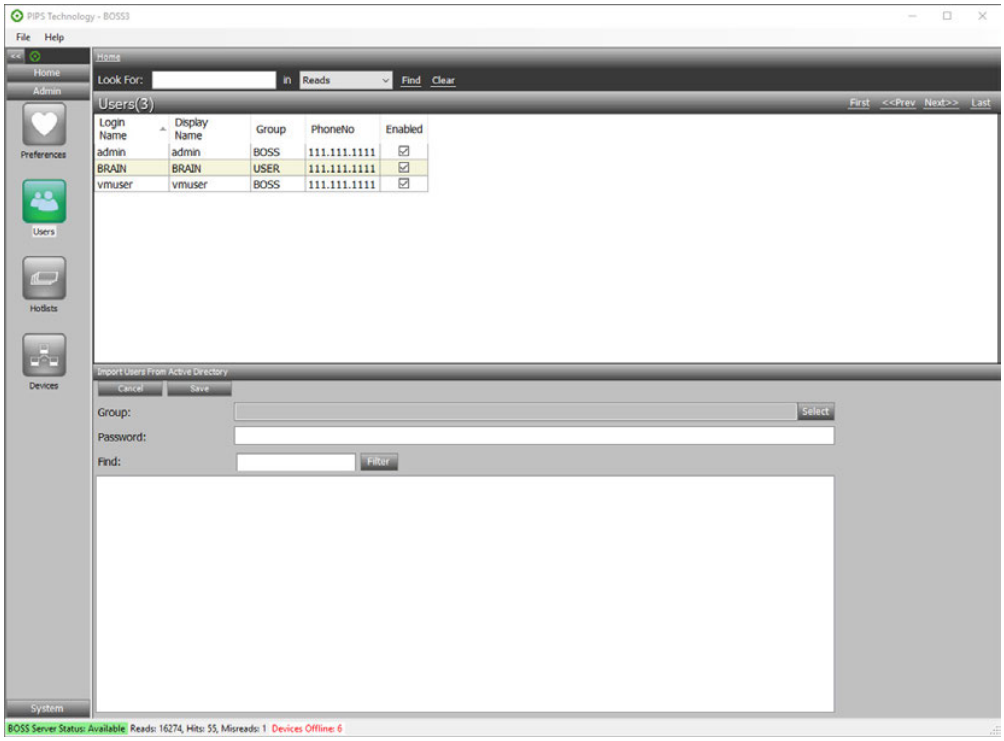
When creating a new group, you must select a parent group (the Belongs To field). BOSS uses a parent-child group structure as an organizational mechanism. This allows the BOSS Administrator to arrange groups into collections based on location, job role, or any other applicable criteria. In BOSS, the parent group can be selected in order to easily reach the entire collection of groups under that parent. This can be especially helpful in large installations with a large number of groups.

4.4.3 Deleting a Group

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Users** shortcut.
3. Click the **Groups** button at the bottom of the Browse/Edit area. A list of all existing groups will display in the Browse/Edit area.
4. Click to select the desired group from the list.
5. Click the **Delete** button.
6. Click **OK** in the confirmation dialog to complete the operation.

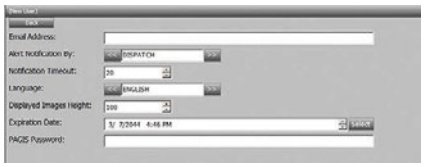
WARNING: Any users currently assigned to the deleted group will be assigned to the default "BOSS" group. You should empty the group by assigning all of its users to different groups prior to deleting it.

4.5 Users



4.5.1 Creating a New User

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Users** shortcut. A list of all existing users will display in the Browse/Edit area.
3. Click the **New** button at the bottom of the Browse/Edit area. The New User Entry screen appears.
4. Enter a **Login Name** for the new user. This is the name the user will enter when logging into the BOSS application. (The login name must be at least three characters.)
5. Enter a **Display Name** for the new user (optional).
6. Enter a **Password** for the new user. (The password must be at least six characters with one Cap, one number and one special symbol.) The strong password requirement cannot be disabled.
7. Select a **Group** for the user. Click the **Select** button to access a list of all groups. Click on the desired group and click the **Save** button to complete the selection.
8. Enter a contact **Phone Number** for the user (optional). This field is for informational purposes only; in case the BOSS Administrator needs to contact the user.
9. Click the **Advanced**... button to access additional, optional settings for the new user. Configure these advanced user settings as desired.



4.4.1 Creating a New Group (continued)

Email Address – Email address or addresses associated with the user. BOSS alerts for the user are sent to the email addresses specified here. Multiple addresses should be separated with a comma.
Alert Notification By – A user can be configured to receive BOSS alerts through the Dispatch application, email, or both. Click the <<
or >> buttons to cycle through the options, stopping at the desired selection.
Notification Timeout – The cutoff time from the time when a hit occurred after which an alert will no longer be sent to the user. For example, if the notification timeout is 20 minutes and a plate of interest is detected at 12:00 pm, notification is not sent to the user after 12:20 pm. This timeout prevents alerts being sent for events that are delayed in arrival to BOSS.
Language – The language preference for the user. The default value is English.
Displayed Images Height – This setting defines the vertical size in pixels of the images (reads and hits) that will display for the user on the Dispatch and Reads screens.
Expiration Date – Date for the user account to automatically be disabled. If no expiration is desired, simply leave this field at its default value (30 years from current date).
PAGIS Password – The user's Pagis password. Strong password requirement not utilized for this field.

Note: The user must be in a group that has been granted PAGIS permissions in order for the user to log in to PAGIS.

---

10. Click the **Back** button to return to the main New User Entry screen.
11. Click the **Save** button to complete creating the new user.

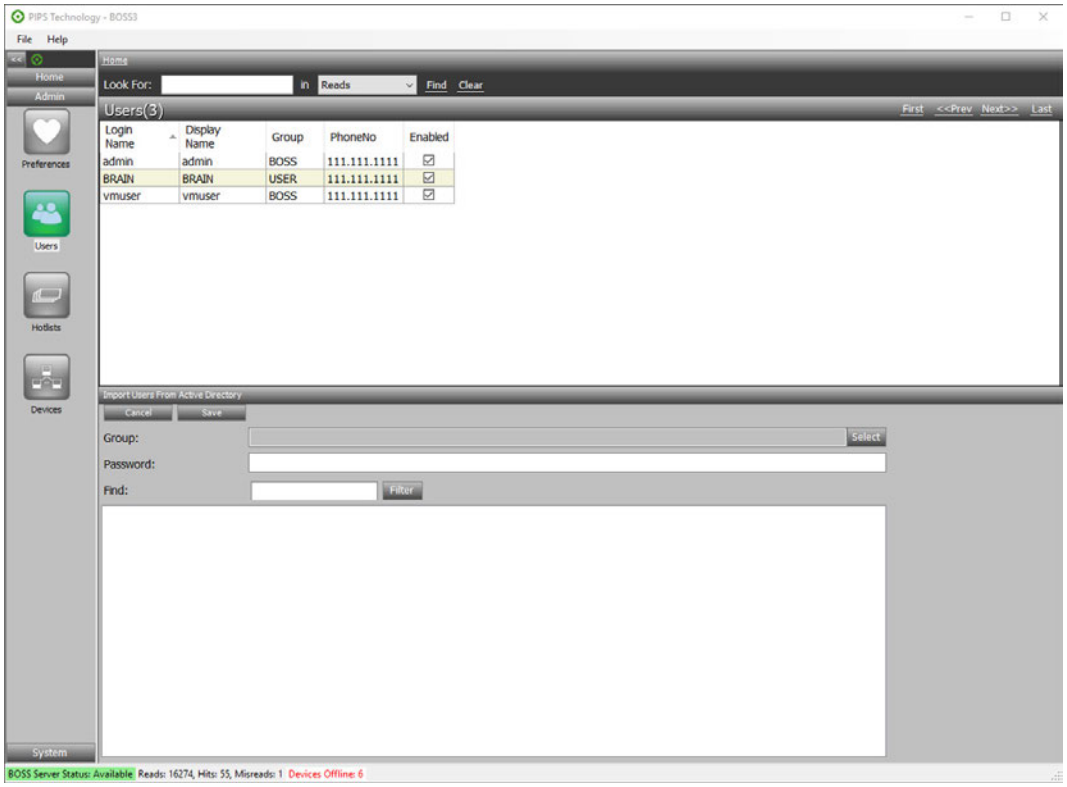
4.5.2 Deleting a User

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Users** shortcut. A list of all existing Users will display in the Browse/Edit area.
3. Click the desired user in the list.
4. Click the **Delete** button at the bottom of the Browse/Edit area.
5. Click **Yes** to confirm the operation.

4.5.3 Importing Users from Active Directory

BOSS allows user logins to be imported from Microsoft Active Directory (AD) service.

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Users** shortcut.
3. Click on the **Import** button.



4. Select the BOSS group that will receive the imported logins. Click the **Select** button to display available groups and **Save** to commit the selection.
5. Enter the default password for the imported logins in the Password field.
6. Browse for the desired users, **or** type in the desired login name (full or partial) in the Find field and press the **Filter** button.
7. Click on the checkbox in front of the desired usernames to select users to be imported to BOSS.
8. Click on **Save** to import the users from Active Directory.

Note: A Windows login cannot have any punctuation included or problems will occur with reads queries being performed.

4.6 Access Permissions Example

The previous sections have described how BOSS user security is designed, using roles, groups, and user accounts. This section presents a working example that integrates the information in this chapter.

A BOSS Administrator creates a role, names the role “Temporary Workers,” and defines the new role to have very limited permissions, as follows:

Reads	Read Only
Dispatch	Read Only
Users	No Access
Hotlists	No Access
Devices	No Access
System	No Access

Then the Administrator creates a group called “Temps.” When creating the group, a role is required. The Administrator selects the new role just created “Temporary Workers,” which assigns the permissions, defined above, to the new group.

Next, the Administrator creates a user account, “Jsmith,” for a temporary worker. While creating the new user, the Administrator is required to select a group for the user, and assigns the user to the “Temps” group just created. The user “Jsmith” has now been created with the permissions shown above because he belongs to the group called “Temps” and that group was assigned the “Temporary Workers” role.

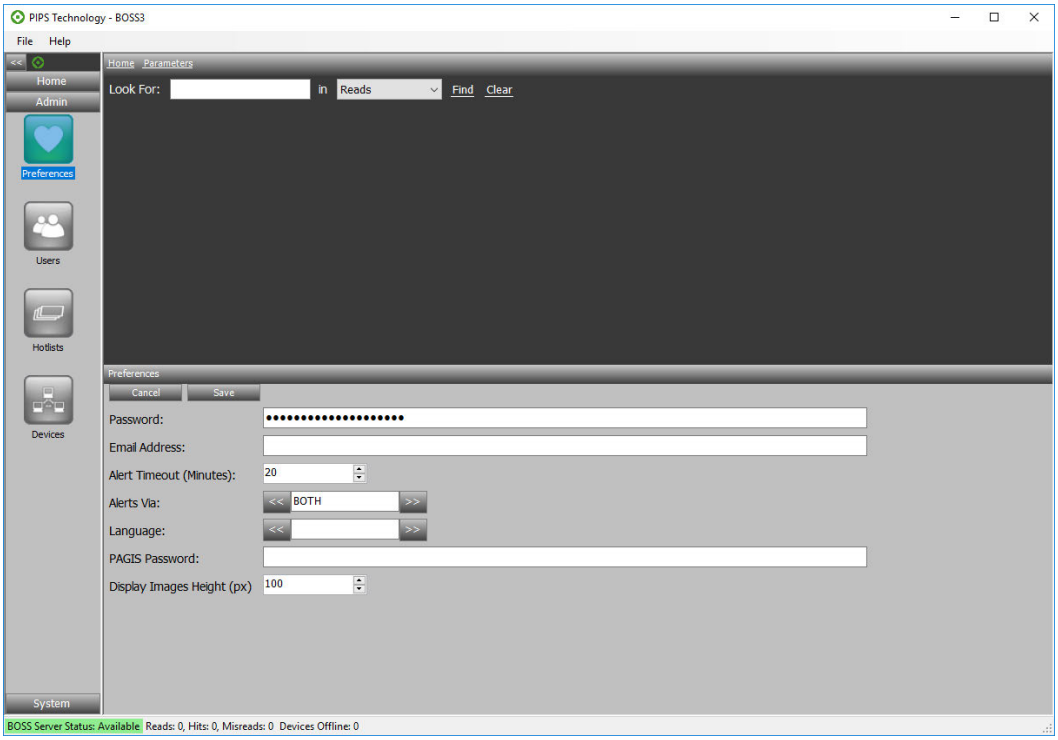
As this example shows, this security design allows reusability of security roles because a BOSS Administrator can define a set of permissions in a role, and that role can be assigned to multiple groups.

4.7 Preferences

The Preferences section allows for changing settings for the currently logged-on BOSS user, such as the password and email addresses.

4.7.1 Changing User Preferences

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Preferences** shortcut. The Preferences Entry screen appears at the bottom of the Browse/Edit area.
3. Modify the preferences settings as desired and click the **Save** button.



Password – Login password for the BOSS user. For security purposes, the existing password does not display on screen.
Email Address – Email address or addresses associated with the user. BOSS alerts for the user are sent to the email addresses specified here. Multiple addresses should be separated with a comma.
Alert Timeout (Minutes) –The cutoff time for older hits to alert the user.
Alerts Via – A user can elect to receive BOSS alerts through the Dispatch screen, emails, or both.
Language – Language preference for the user. The default value is English.
PAGIS Password (PAGIS Password) – The Pagis Software password for the user.

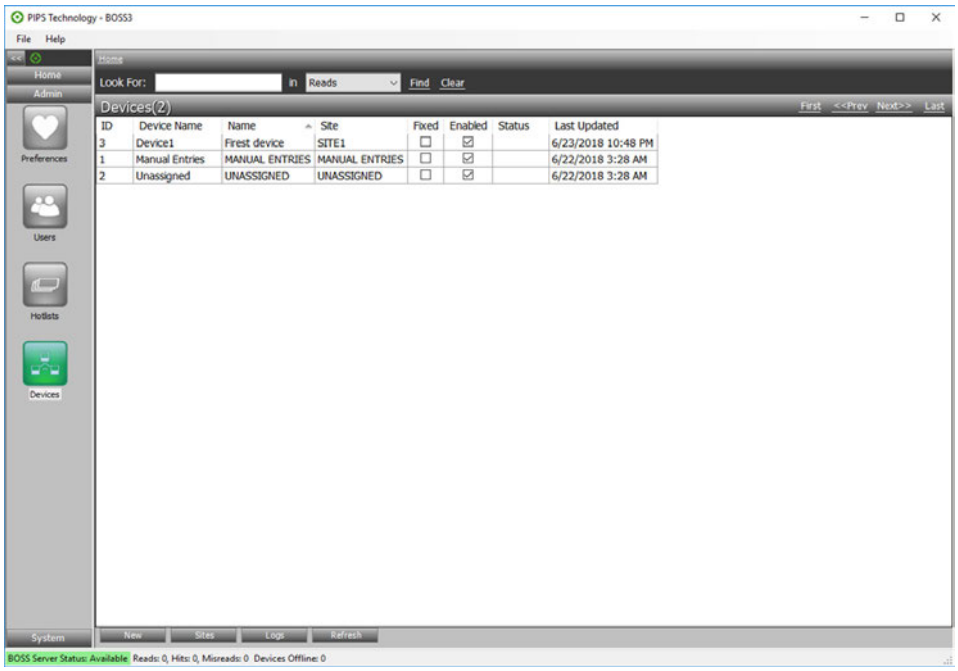
Note: The user must be in a group that has been granted PAGIS permissions in order for the user to log in to PAGIS.

Display Images Height (px) – This setting defines the size in vertical pixels of the images (reads and hits) that will display for the user in the Dispatch and Reads Query sections.

5 DEVICES AND SITES

5.1 Devices

A BOSS device is any source that can input reads into the system. Typically, a device is a camera—either fixed or mobile. Another source for reads is manual entry, in which a BOSS user types the information for a read into the BOSS Dispatch screen .A new BOSS installation automatically contains two default devices, Manual Entries and Unassigned. A BOSS Administrator creates additional devices applicable to his/her organization.



5.1.1 Device Status

To see the current devices in your system with information about their status:

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Devices** shortcut.

The devices will be listed in rows with the following column headings:

Device Name – The name assigned to the device, used in the device selections and is the description of the device. The list will always include Manual Entries and Unassigned.

Name – The name that is given to the device.

Site – The group of devices to which this device belongs. Sites can be grouped by geographical location or other criteria.

See Section 5.2, Sites.

Fixed – This box will be checked if the device is fixed camera, rather than a mobile camera. Enabled – This box will be checked if the device is currently enabled (see Section 5.1.4). Status – The Status field can display the following messages:

Device Added – If the device is newly added to the list, this message will display.

5.1.1 Default Devices (continued)

Offline – This device is a previously connected fixed camera that is not currently connected to BOSS.
Online Heartbeat – BOSS has detected a ping from a fixed camera.
Online Synced – The device's connection with BOSS has been established. This is shown for PAGIS mobile devices only and may not change when the device is offline.
Updated – Information has been sent from BOSS to the device, and the device is up to date.
Received Logins – Updates to the device included logins that were successfully sent to the device.
Received Source – BOSS has found the hotlist source file that it needs in order to send the updated hotlist to the device. Received Source may not be displayed due to timing or events.
Received Hotlist – The hotlist scheduled to be successfully sent has been sent to the device.
Received Hotplates – BOSS is sending "pages" of hotplates for a large hotlist, and the last page was successfully received.
Received Targets – The update to the device included targets that were successfully sent.

5.1.2 Defining a Device

Note: Devices will be defined automatically when a PIPS device, such as an ALPR camera, connects to BOSS the first time. Normally, there is no need to define devices in advance.

---

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Devices** shortcut. A list of existing devices will appear in the Browse/Edit area.
3. Click the **New** button.
4. Enter a name for the new device. (The name must be at least three characters long.) Note that the name **CANNOT BE CHANGED** once the device has been created.
5. Enter a **Description** for the new device. (The description must be at least three characters long.)
6. Select **Mobile** or **Fixed** in the Type field. By default, **Fixed** is selected. To change the current selection, click the **left** or **right** arrow.
7. Select a **Site**. Click the **Select** button next to the Site field to display a list of all available sites. Click on the desired site in the list and click the **Save** button.

Note: In addition to the two default sites, Manual Entries and Unassigned, which are created automatically when a new BOSS system is installed, other sites can be created by an authorized BOSS user. See Section 5.2, Sites, for more information.

---

8. Select **Owners**. Owners are groups that can access this device. For PAGIS units, user logins are sent only to devices where the group is an owner of the device. Click the **Select** button next to the Owners field to display a list of all BOSS groups. Select each desired group by clicking the checkbox. When the desired groups are selected, click the **Save** button. The group name(s) selected will be displayed in the Owners field.

9. Select **Latitude** and **Longitude** values for the geographical location of a device by typing in a value or using the up and down controls on each field to increase or decrease the value. Note that some devices, such as PAGIS units with a GPS attached, will automatically send the latitude and longitude of the device to BOSS.
10. Click the **Advanced** button to display additional options for the device.
    No Reads Alert – Defines how long the device must remain with no reads coming in before the system shows the device as offline.
    Alert Email – The email address or addresses to which alerts associated with this device should be sent.
    Retain Reads – The length of time that reads from this device should be saved in the BOSS database. The Retain Reads setting must be longer or equal to the Retain Images setting.
    Retain Images – The length of time that pictures captured by this device should be saved in the BOSS database.
    Retain Hits – The length of time that hits captured by this device should be saved in the BOSS database.
    SpikeStore – The PIPS High Resolution ANPR/ALPR Camera P382 and the PIPS Compact ANPR/ALPR Camera P372 (formerly the Spike P382 and P372 cameras) allow captured images to be stored in an on-board USB flash drive to be retrieved on demand. Setting a device as a SpikeStore device causes BOSS to attempt to retrieve images from the storage device when the read is requested for viewing.
11. When Advanced Options have been set as desired, click **Back** to return to the New Device screen.
12. Click the **Save** button to complete creation of the new device. The new device will now appear in the devices list above.

5.1.3 Editing a Device

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Devices** shortcut. A listing of all devices appears in the Browse/Edit area.
3. Click the desired device to select it. Details for the selected device appear in the Browse/Edit area.
4. Click the **Edit** button.
5. The Device Edit screen appears in the lower portion of the screen.
6. Modify fields as desired and click the **Save** button.

5.1.4 Enabling and Disabling a Device

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Devices** shortcut. A listing of all devices appears in the Browse/Edit area.
3. Click the desired device to select it. Details for the selected device appear in the Browse/Edit area.
4. Click the **Edit** button.
5. The **Device** Edit screen appears in the lower half of the screen.
6. Click the **Disable/Enable** button. The change will immediately close the edit window and return to the Devices screen. It will also take effect immediately.

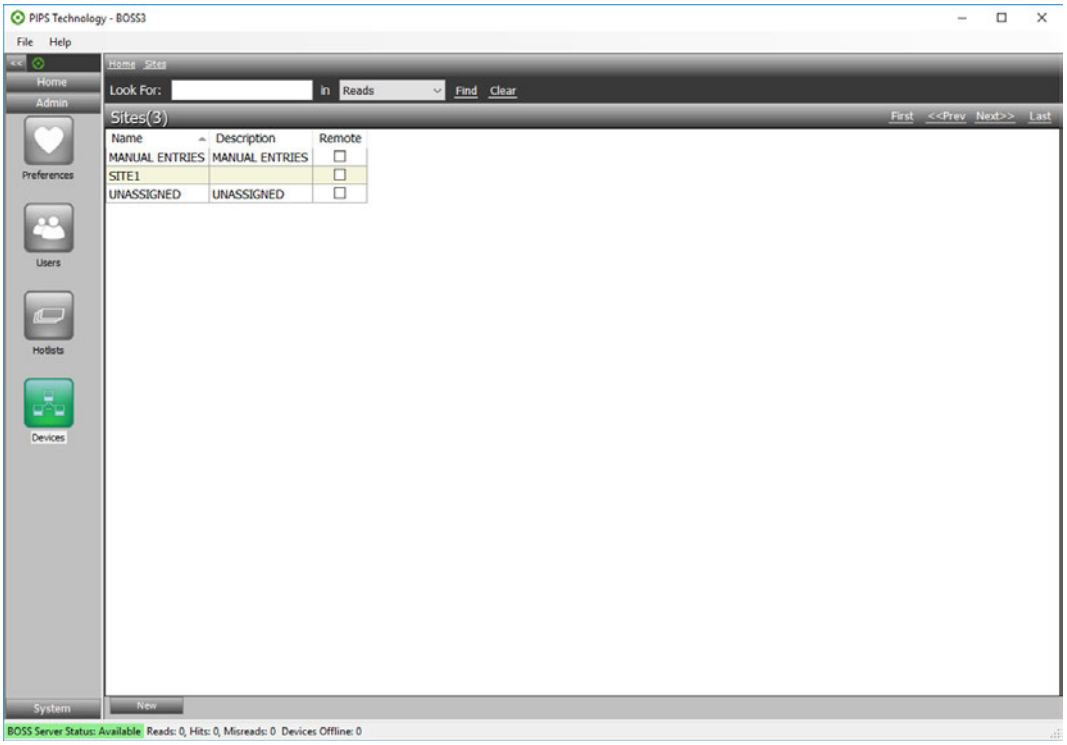
5.1.5 Deleting a Device

Note: It is strongly recommended that **devices are never deleted.** If a device is deleted, queries can no longer be performed using the device as a criterion. Instead of deleting a device, it should be disabled or given a new description.

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Devices** shortcut. (A listing of all existing devices will display in the Browse/Edit area).
3. Click the desired device in the listing.
4. Click the **Edit** button.
5. Click the **Delete** button at the bottom of the Browse/Edit area.
6. Click **Yes** to confirm the operation.

5.2 Sites

A site is a mechanism for organizing devices. This allows a BOSS Administrator to arrange devices into groups according to convenience, such as geographical area or a facility. The ability to group or arrange devices can be quite useful in large installations where there are many devices. Each device created must be assigned to a site.



5.2.1 Default Sites

A new BOSS site automatically contains two default sites, Manual Entries and Unassigned. Normally, a BOSS Administrator will want to create additional sites applicable to an organization.

5.2.2 Creating a Site

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Devices** shortcut.
3. Click the **Sites** button at the bottom of the screen. A list of existing sites will appear in the Browse/Edit area.
4. Click the **New** button at the bottom of the screen.
5. Enter a name for the new site. (The name must be at least three characters long.) Note that the name cannot be changed once the site is created.
6. Enter a description for the site. (The description must be at least three characters long.)
7. Select the parent site for the site. BOSS allows organizing sites into tree-like hierarchies. Click the **Select** button next to the Belongs To field, and select one site from the list. Click the **Save** button to complete the selection. The site name will appear in the Belongs to field.
8. Check the **Remote** option to designate the site as a remote site. (Remote sites are explained in Section 6, BOSS Data Sharing.)

5.2.3 Deleting a Site

Note: It is strongly recommended that sites are never deleted. If a site is deleted, queries can no longer be performed using the site as a criterion. Instead of deleting a site, it is recommended that devices assigned to it should be moved to another site.

---

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Devices** shortcut. A listing of all existing devices will display in the Browse/Edit area.
3. Click the **Sites** button at the bottom of the screen. A listing of existing sites will appear in the Browse/Edit area.
4. Click the desired site in the listing and click the **Edit** button.
5. Click the **Delete** button at the bottom of the Browse/Edit area. Click **Yes** to confirm the operation.

6 BOSS DATA SHARING

BOSS allows "linking" of multiple BOSS systems for data-sharing purposes. When a user issues a query from the Smart Client application that includes a remote site, the query is submitted to the local BOSS server, which in turn makes a query to the remote BOSS server(s). The combined results from all the sites are then returned to the Smart Client. **Data from remote sites is not stored in the local BOSS server.**

The following configuration steps need to be taken to permit BOSS data sharing:

6.1 Configuring BOSS to Allow Remote BOSS Queries

1. Create a BOSS user for remote access. This user account is a "proxy" the local BOSS server will use for all requests from a remote site. This user account will have "Reads" privileges by default; no other privileges need to be given. The user must be assigned to a remote group. (See Section 4.4, Groups, for information about flagging a group as remote.)
2. Give the username and password for this "proxy" user to the BOSS Administrator at the remote BOSS system. The remote BOSS will need to be configured to access this BOSS system, described in the next section.

Note: It is best to create a dedicated user account for remote sites—one that will not be used by an actual user to log in and access the application.

6.2 Configuring BOSS to Access a Remote BOSS Server

1. Obtain username and password from BOSS Administrator at the remote site.
2. Create a site for the remote BOSS server and select the **Remote** option.
3. Enter the remote site IP address and BOSS service port (23032 by default).
4. Add the username and password provided.
5. For each group that is allowed to query the remote BOSS server, assign the remote server to the user via the **Servers Access** option. (See Section 4.4, Groups, for information on selecting Servers Access.)
6. Log out of the application.
7. Log back on using the provided username and password. The Remote BOSS server can then be queried by selecting the desired servers in the Reads Query screen.

Note: BOSS version 3.2 and above only supports data sharing with servers running BOSS 3.0 and above.

---

7 HOTLISTS

A hotlist is a database that contains license plates of interest. When reads from license plate readers arrive at the BOSS server application, they are compared against hotlist records to find matches. Various hotlists can be enabled on a BOSS system and used in this comparison. In addition, hotlists can be assigned individually to specific devices. Only reads from those devices will be compared against these hotlist records. Typical hotlists include stolen vehicles, amber alerts, wants and warrants, etc. When the system reads in a plate that is determined to be a match to a hotlist entry in a hotlist, the BOSS application informs the user either with an alert sound and a pop-up window displaying a picture of the vehicle, or via email, depending on the user's preferences (see "Alerts via" in Section 5.3, Preferences).

A hotlist can be a database imported from an external source, such as another law enforcement agency. It can also be a list created by the local BOSS Administrator. For the BOSS server application to be able to understand how to import the hotlist records into the database, there are three different format types that exist in a BOSS system. In addition, there are several specific formats that are pre-defined and available by default when a new BOSS system is installed (see Section 8, Hotlist Formatters).

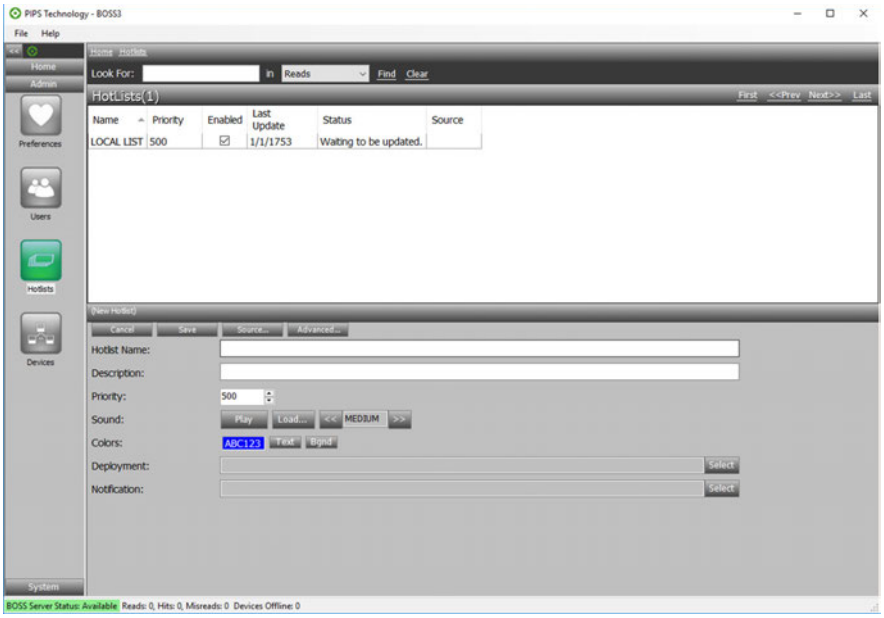
7.1 Creating a New Hotlist

There are three general areas to complete when creating a new hotlist:

- Configure basic settings
- Define a source file location with credentials when necessary.
- Define advanced settings (optional).

7.1.1 Configuring Basic Hotlist Settings

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Hotlists** button. Currently existing Hotlists appear in the Browse/Edit area.
3. Click the **New** button at the bottom of the Browse/Edit area. The New Hotlist Entry form appears.



4. Enter a **Hotlist Name** for the hotlist. It must be at least three alphanumeric characters, and it cannot be an existing hotlist name.
5. Enter a **Description** for the hotlist (optional).

6. Select a **Priority** for the hotlist. When there are multiple hits/alerts, the priority determines which alert will occur first. (The lower the number, the higher the priority.)
7. Select a **Sound** for alerts resulting from this hotlist (optional). Click the **Load** button to select a wave sound file (*.wav). To test the selected sound, click the Play button. Optionally, one of the three default sounds may be selected, **Low, Medium**, or **High** alert.
8. Select **Colors** for the alert if desired (optional). The default is white text on a royal blue background. Custom color settings affect the entries in dispatch. The background color also applies to alerts given in PAGIS.
9. Click the **Text** button to select a color for the text.
10. Click the **Bgnd** (Background) button to select a color for the background.

Note: Currently selected text and background colors are displayed in the sample box (showing "ABC123").

---

11. Select devices for **Deployment**. Click the **Select** button to select devices from the list of those currently available. Click the checkbox next to a device in order to select it. When desired devices are checked, click the **Save** button to make the selection. One or more devices can be selected, and they will be displayed in the Deployment field.

Note: Deployment means distributing the hotlist to a device or devices. Only the devices where a hotlist is deployed will produce hits from the hotlist.

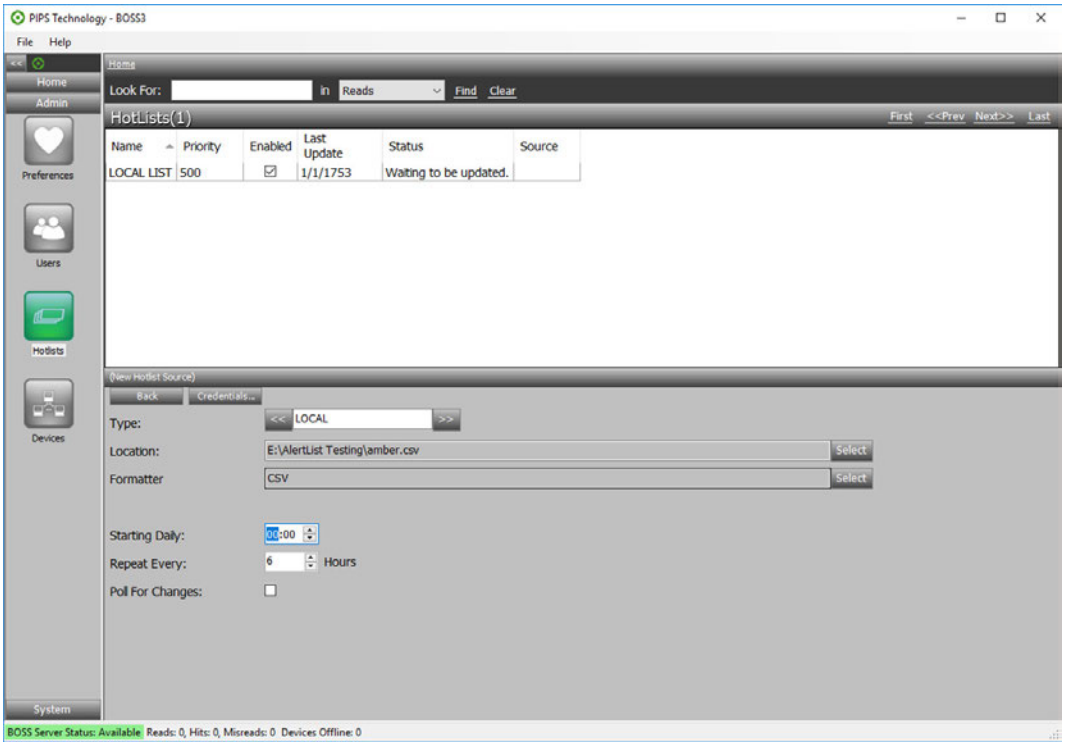
---

12. Select groups for Notification. Click the **Select** button to see a list of all BOSS groups. Click the checkbox next to a group to select the group. When you select a parent group, child groups are automatically selected. When desired groups are checked, click the **Save** button to make the selection.

Note: In order to receive alerts for hits on the hotlist, the user must be in the notification list of the hotlist. For more information see Section 7.1.5, Defining Hotlist Advanced Options.

7.1.2 Defining the Hotlist Data Source

1. On the New Hotlist Entry screen, click the **Source**... button to open the screen shown in the lower half of the following image:

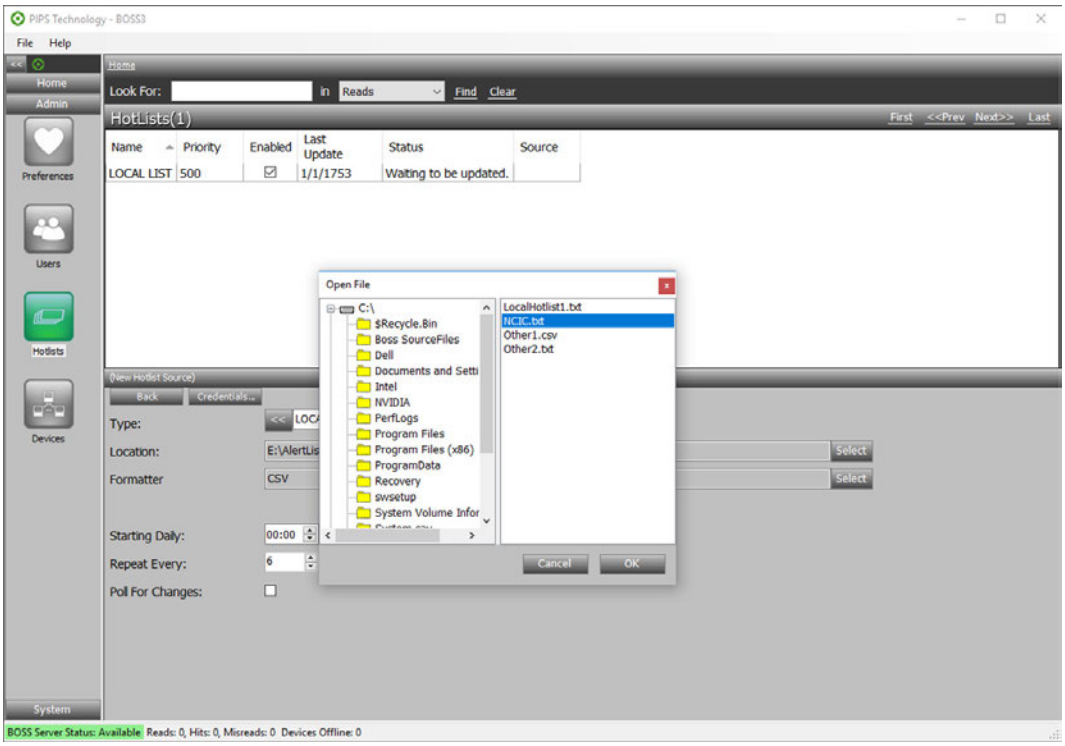


2. Choose the appropriate entries for each of the fields that describe the new hotlist:
   Type (**Network** or **Local**) – A local source means that the file is stored on the BOSS server's Windows file system. A network source means that the hotlist source resides outside the BOSS server.

Note: If a Local source is selected, the source file location (folder) must be accessible to the Windows process running the BOSS server application ("PIPS BOSS3" Windows service).

Location – Enter the location of the hotlist file. Click the **Select** button to the right of the location field.

For a local source, a file dialog will display, allowing you to navigate to a path and select a file.



For a network source, select one of the default locations displayed (if applicable), **or** type in the location of the source:

HTTP – The location format must be in Hypertext Transfer Protocol (HTTP) format: “http://server:port/path.” There are a few predefined HTTP locations (such as CA DOJ) included in BOSS. These locations can be accessed with the **Select** button. Boss also supports FTP & SFTP, examples : “ftp://server:21/path” , : ftp://server:22/path.

Remote BOSS System – The location format must be “boss://server:port/hotlist,” where “hotlist” is the hotlist name on the remote system.

Note: The remote system hotlist name **MUST** be alphanumeric and **CANNOT** contain any spaces.

Formatter – Formatter defines the way a hotlist database file is parsed into discrete fields. Click the **Select** button next to the Formatter field. A list of available formatters appears. Click on the desired formatter and click the **Save** button to make the selection. The name of the selected formatter will appear in the field.

Note: Normally one of the several default formatters included with BOSS is sufficient. A new custom formatter can be created if necessary. See Section 8.1, Creating a New Formatter for Hotlists, for more information.

7.1.2 Defining the Hotlist Data Source (continued)

Starting Daily – Specify the time of day the hotlist should begin updating each day. The time is formatted as hours:minutes in the 24-hour clock, i.e., between 00:00 and 24:00 can be selected.
Repeat Every – Specify the time interval, in hours (1 – 24), between updates.

OR

Poll for Changes – If you choose this setting, BOSS will check for updates to the hotlist approximately every 30 seconds. When this option is selected, the **Starting Daily** and **Repeat Every** options are disabled.

Note: If **Poll for Changes** is selected, and the hotlist source resides on the network, BOSS will attempt to make a network connection every 30 seconds. This frequency may add significantly to network traffic. Use with caution.

7.1.3 ZIP Compressed Hotlist Files

BOSS will automatically recognize and extract a hotlist data file contained in a ZIP archive file, such as Windows Explorer compressed (zipped) folder.

Note: There can be only one file in the ZIP archive.

7.1.4 Defining Hotlist Source Credentials

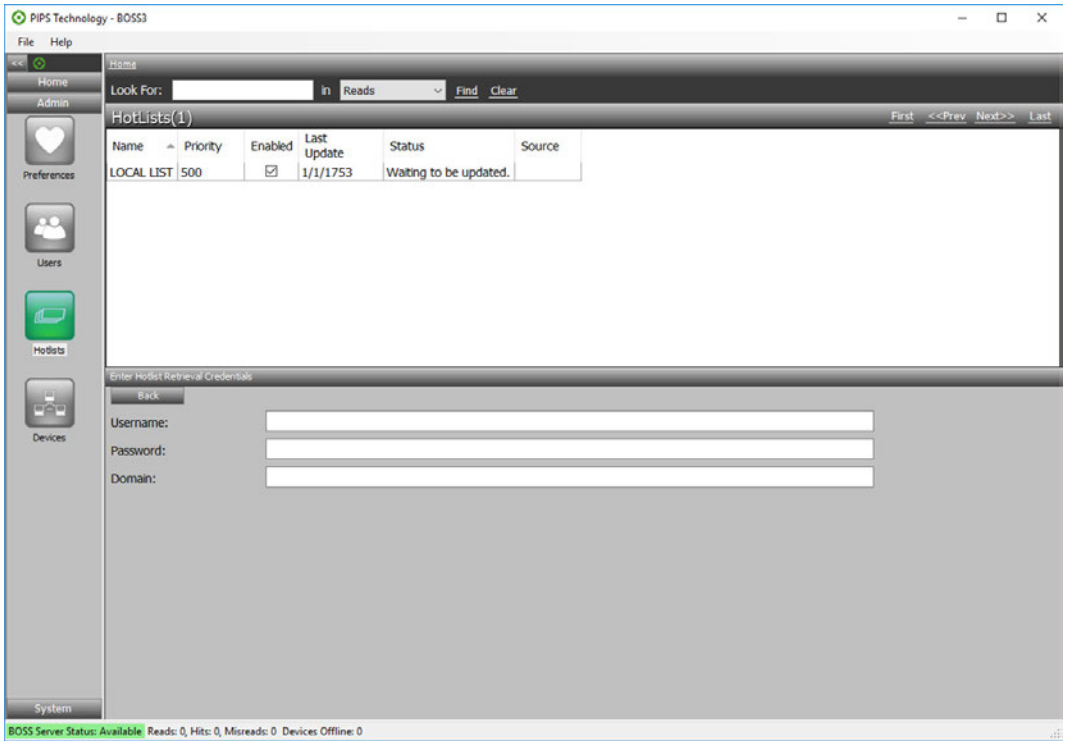
Some sources will require credential settings (e.g., login information) in order to allow BOSS to access that data. To enter the **Credentials** Settings screen from the Hotlist Source screen, click the Credentials button.
The credentials depend on the source type as follows:

Network-HTTP – If the HTTP (website) source defined requires login information, it should be entered in the Credentials Setting screen. This information will include username and password. The domain field may be necessary as well. Consult the Administrator of the HTTP source for required login information.

Network-Remote BOSS system – A username and password valid on the remote BOSS system must be entered (as in remote sites configuration, described in Section 6.0, BOSS Data Sharing). Consult the Administrator of the remote BOSS system for a username and password.

To set credentials for a source:

1. Click the **Credentials** button. The Credential Input screen appears.
2. Enter the username, password, and domain information applicable to the source you are specifying.
3. Click the **Back** button to return to the Source Entry form.
4. Click the **Back** button again to return to the New Hotlist Entry screen.



Advanced Options are values that allow you to further define details of the new Hotlist. To access the Advanced Options, click the **Advanced**... button.

Covert – A covert hotlist is one that contains sensitive information that should only be available to certain user groups. The effects of defining a hotlist as covert are as follows:

- A Hit on covert hotlist will not be alerted to users in mobile vehicle “Pagis”, unless the logged-in user is a Pagis administrator.
- A hit on the covert hotlist will not be alerted in the Boss application, regardless of the user’s alert preference. Hit alerts for covert hotlist can be send via email.
- When reads are queried, git information on covert hotlist will be displayed only to users in the Notification list for the hotlist. Other users will see that the read is a hit, but no information will be shown.
- Hit information for hits from covert hotlist will not be sent to remote Boss servers.

Whitelist – This option, when selected, defines the hotlist to be a whitelist, which works in reverse to a normal hotlist. A whitelist defines a list of plates that are **authorized** and not of concern. When a whitelist is active, license plates read that do **not** match an entry on the list will trigger a hit/alert.

7.1.5 Defining Hotlist Advanced Options (continued)

An example of whitelist use might be a secure parking lot where fixed camera devices are monitoring vehicles entering. Authorized plates will match entries in a whitelist hotlist. If a plate is read that does not match an entry in the whitelist, an alert occurs.

Whitelists and hotlists can be active simultaneously for a device.

Note: Whitelist support in PAGIS requires a separate license. If you do not have the license and wish to use whitelists, please contact your PIPS sales representative for further information.

Ext Trigger – This option, when selected, sets the External Trigger flag on a hotlist when it is passed to PAGIS. It is only supported in PAGIS version 2.6.6 or above and will have no effect on earlier versions of the software.
One Time – This option, when selected, specifies that the hotlist data should only be accessed from its defined source one time; no subsequent updating will occur after the initial import.
Alert Timeout – This setting allows you to define how current a hit (from this hotlist) must be in order to cause an alert. This primarily pertains to information coming in from mobile units, where there may be a large delay. Alert Timeout can be specified in minutes, hours, days, or months.
Delete Inactive – BOSS updates hotlists in an incremental manner, and instead of deleting hotlist entries that no longer exist, non-existent entries are marked as "inactive." If the entry subsequently becomes valid, the entry is marked as active again. The Delete Inactive value determines how long inactive entries are kept in the BOSS hotlist database.
Notify Email – One or multiple email addresses may be defined to receive an alert when there is a hit. Multiple

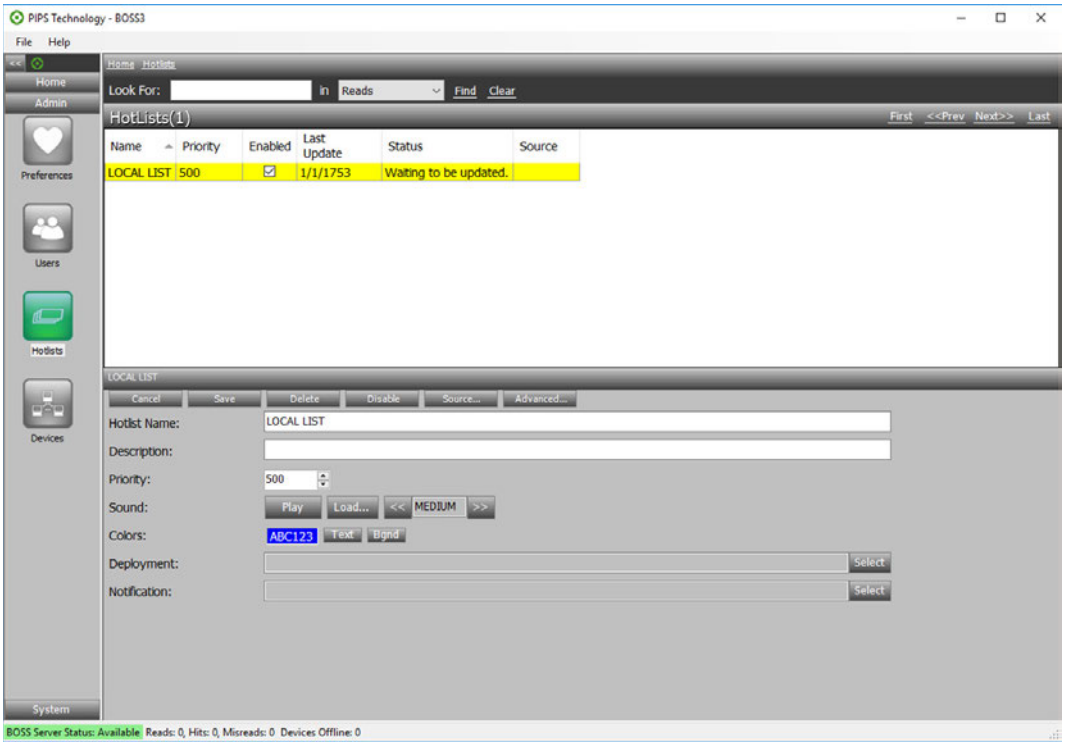
Note: If PAGIS mobile units are used, this value should be set to the longest time between begin shift downloads to PAGIS.

email addresses can be entered in the field, separated by a comma.
Remote Alerts To – Select the remote sites in which to send alerts. When a BOSS system sends an alert to a remote system, it is sent as a read; the remote BOSS system then determines whether to treat the read as a hit.

Note: This setting is only applicable if remote sites are defined.

Expires – Determines the date that the hotlist will stop importing data from its source. For a hotlist that is intended to be permanent, leave the expiration at the default value, 30 years from current date.

7.2 Enabling and Disabling a Hotlist



1. Select the **Admin** category on the Shortcut bar.
2. Click the **Hotlists** shortcut. A list of all hotlists appears in the Browse/Edit area.
3. Click the desired hotlist. Details for the selected hotlist appear in the Browse/Edit area.
4. Click the **Edit** button.
5. The Hotlist Edit screen appears in the lower half of the screen.
6. Click the **Disable** or **Enable** button.

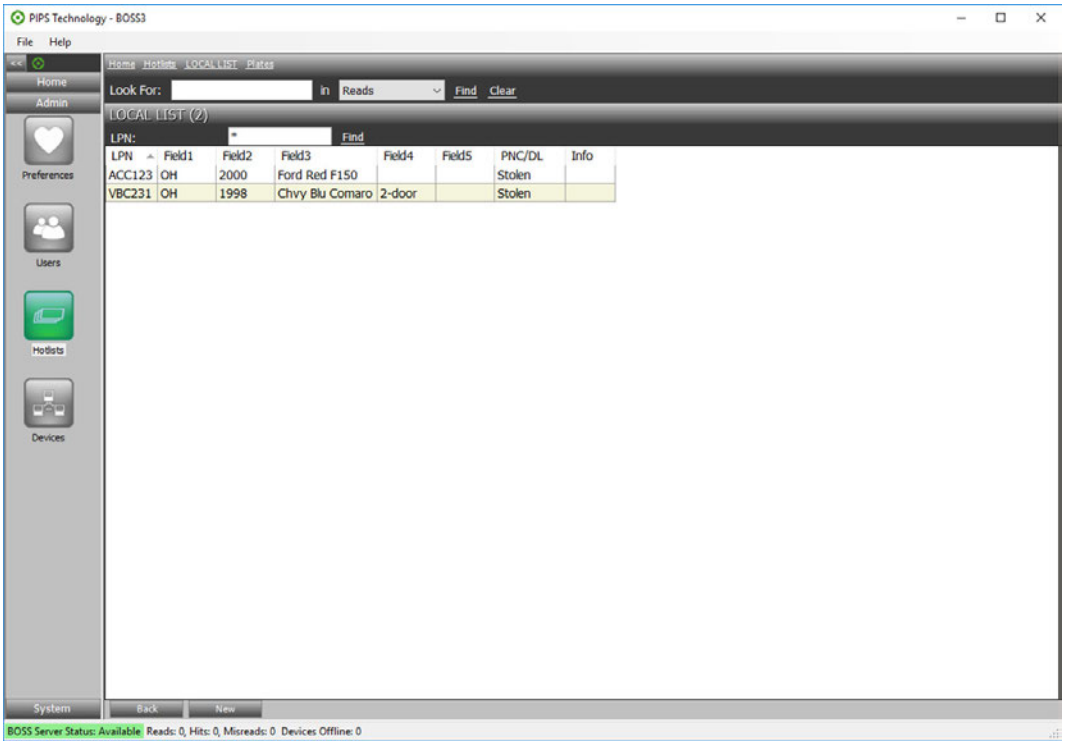
7.3 Modifying Hotlist Entries

BOSS allows viewing, adding, editing, and deleting hotlist entries.

Note: If the hotlist is set to update automatically, any changes to that hotlist made from within the BOSS User Interface application will be lost at the next automatic update.

7.3.1 Querying Hotlist Entries

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Hotlists** shortcut. A listing of all hotlists appears in the Browse/Edit area.
3. Click the desired hotlist. Details for the selected hotlist appear in the Browse/Edit area.
4. Click the **Plates** button.
5. The Hotlist Plates screen will be displayed.

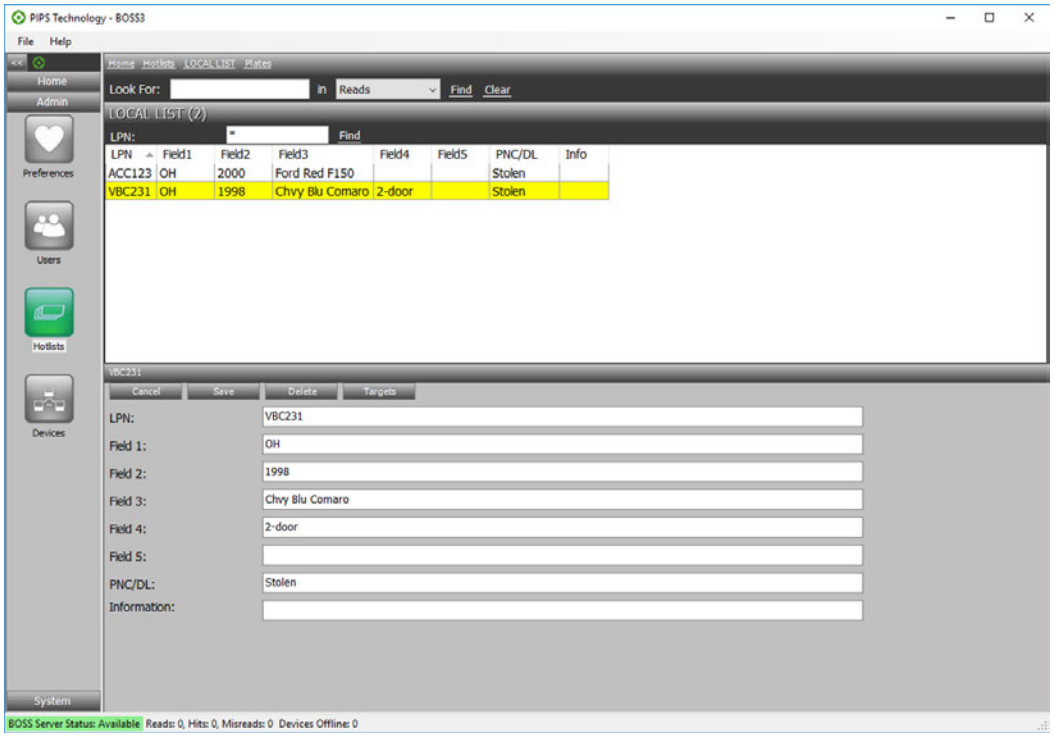


6. Type in the full or partial plate text to search for in the LPN field. (Wildcard searches are supported. See Section 11.1, Wildcards, for more information.)
7. Click on **Find**. License plates that match the criteria will be displayed. Note that only the first 1,000 matching license plates will be shown.

7.3.2 Editing a Hotlist Entry

1. Retrieve hotlist plates as instructed in the previous section.
2. Click on the row showing the desired plate.
3. The Plate Edit form will be displayed at the bottom of the screen.
4. Edit the field values as desired.
5. Click **Save** to save changes.

Note: Manually edited hotlist entries will be lost the next time the hotlist is updated.



7.3.3 Adding a Hotlist Entry Manually

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Hotlists** shortcut. A listing of all hotlists appears in the Browse/Edit area.
3. Click the desired hotlist to select. Details for the selected hotlist appear in the Browse/Edit area.
4. Click the **Plates** button.
5. Click the **New** button. The Plate Edit form will be displayed at the bottom of the screen.
6. Enter the **LPN** (mandatory) and other fields (optional).
7. Click **Save** to save changes.

Note: Manually edited hotlist entries will be lost the next time the hotlist is updated.

7.3.4 Deleting a Hotlist Entry

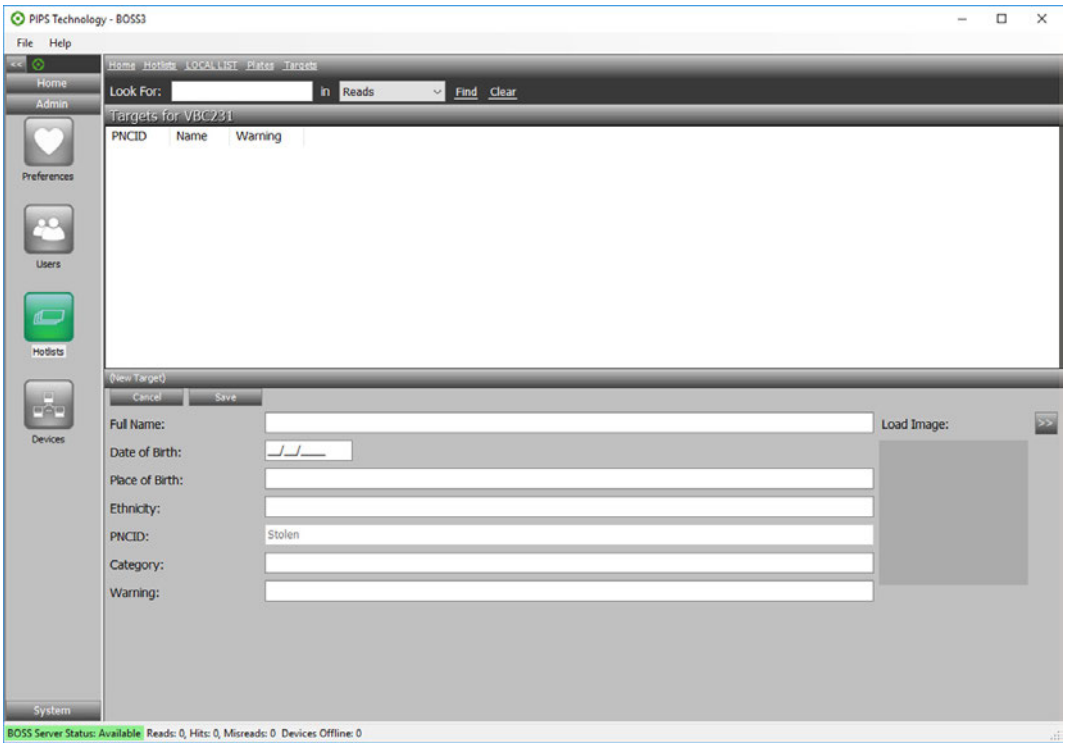
1. Retrieve hotlist plates as instructed in the Querying Hotlists Entries section.
2. Click on the row showing the desired plate. The Plate Edit form will be displayed at the bottom of the screen.
3. Click the **Delete** button.
4. Click **Yes** to confirm the deletion.

Note: Manually deleted hotlist entries may be re-added the next time the hotlist is updated.

7.4 Targets

Targets are individuals of interest associated with a license plate. Target information is downloaded to the PAGIS mobile application from BOSS.

1. Retrieve hotlist plates as instructed in Section 7.3.1, Querying Hotlists Entries.
2. Click on the row showing the desired plate.
3. The Plate Edit form will be displayed at the bottom of the screen.
4. Click the **Targets** button. Information about the target will display.



7.4.1 Creating a New Target

1. Click the **New** button.
2. The Target Edit form will be displayed.
3. Fill in the fields, listed below, with appropriate values.

   Full Name – The first and last name of the target. Date of Birth – The date of birth of the target.

   Place of Birth – The location where the target was born.

   Ethnicity – The ethnicity (race or national origin) of the target.

   PNCID – This field can be used to enter any type of identification number that is available. In the UK this is the Police National Computer identification number of the target. This field is linked to the PNCID field in the hotlist information in the PAGIS application. *See the sample INI configuration file in Section 5 of the Pagis Software User's Manual.*

   Category – The category of the target, such as Felon, Suspect, etc.

   Warning – The warning information to display to the officer.

   Load Image – An image of the target, such as a DMV photo or "mugshot," can also be associated with the Target record. Upload an image by clicking on the Select button and browsing to the image file. Supported formats include JPG, GIF, or BMP.
4. Click the **Save** button.

7.4.2 Deleting a Target

1. Access the Targets screen as described above.
2. Click the row containing the target to be deleted.
3. The Target Edit form will be displayed.
4. Click the **Delete** button.
5. Click **Yes** to confirm deletion.

8 HOTLIST FORMATTERS

Hotlist Formatters define the structure of source data that is imported into BOSS Hotlists. BOSS includes several default formatters when the software is installed. There are three types of formatters:

CSV (comma-separated values) – A flat text file containing one line for every record. Each field in the record is separated by a comma.

Fixed Length – A flat text file containing records that are all the same length. No separator characters are used to determine where each field ends and another begins, but rather, field and record lengths are known up front. In a fixed length file, padding spaces are used where necessary, to accomplish the correct field length.

NCIC (United States National Crime Information Center) – The NCIC database is a computerized index of criminal justice information (i.e., criminal record history information, fugitives, stolen properties, missing persons, etc.), that is available to law enforcement agencies 24 hours a day, 365 days a year. Several NCIC import sources/formats exist within BOSS.

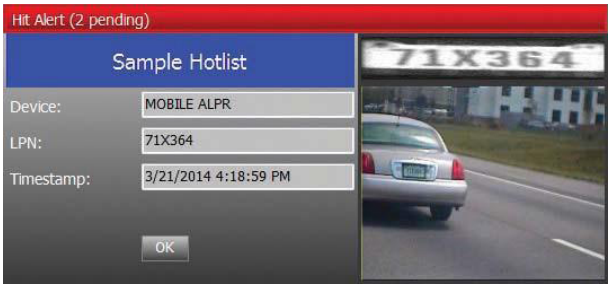
8.1 Creating a New Formatter for Hotlists

Normally, when creating a new hotlist, you will find that one of the default formatters can be used. However, BOSS does give you the flexibility to create new hotlist formatters. Creating a new formatter or modifying an existing formatter should be approached with caution and is beyond the scope of this manual. For more information, please contact PIPS™ Technical Support.

9 ALERTS

BOSS can provide real-time alerts on-screen, via the BOSS User Interface application, or through email. In order to receive alerts through the BOSS application, **the logged-on user must be in a group that is assigned the Dispatch permission**. Email alerts can be sent to any BOSS user or email recipient.

A real-time alert for a hit can pop up on the screen at any time when the BOSS application is running, regardless of which screen the user has active. A sound associated with the hit will be played. Alerts will be queued until the user acknowledges them by clicking **OK**. Real-time alerting in the BOSS application can be turned off by clicking on the **Alerts** toggle button on the BOSS Home screen. The settings for real-time alerts can be modified through the Dispatch screen, (see Section 10, Dispatch).

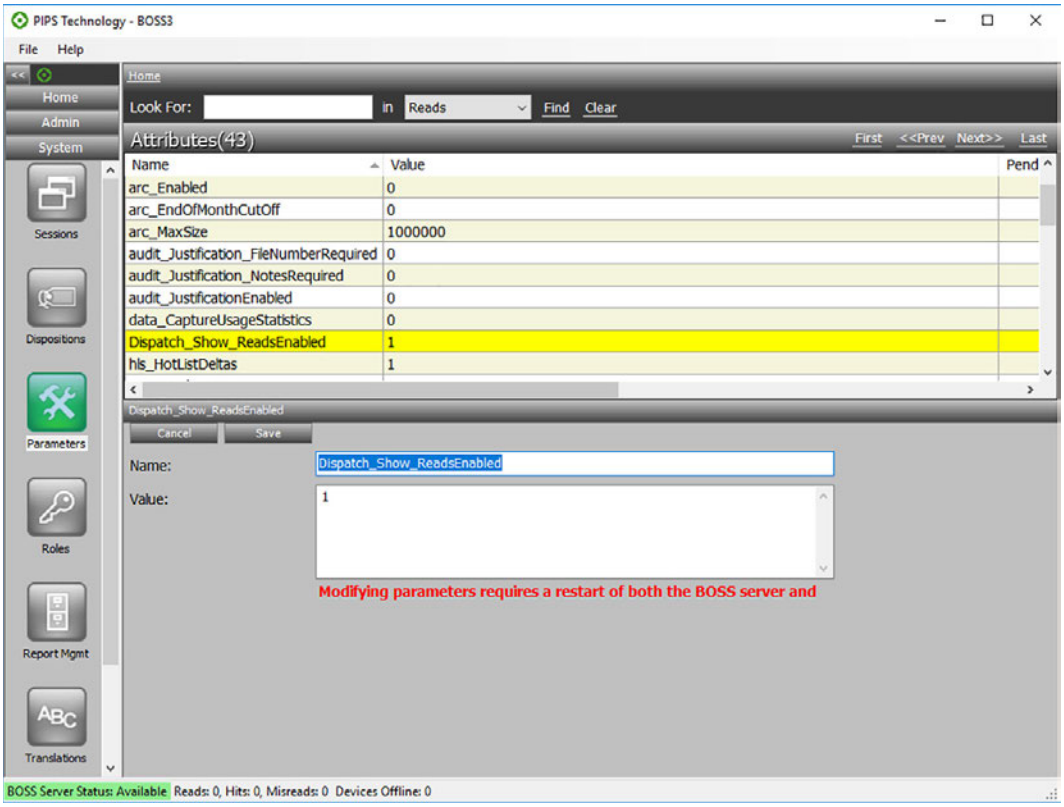


10 DISPATCH

The Dispatch screen is a tool often used by first responder dispatchers. It enables them to easily view hits, monitor reads, and correct license plates as they enter the BOSS system. The information displayed is as near to real time as possible. For ease of viewing, there are three configurations that can be set:

- If only the hits are set to display, they will appear on the whole screen.
- Similarly, if only the reads are set to display, they appear on the whole screen.
- Of the dispatcher is monitoring both hits and reads, then the hits will be displayed on the top half of the screen and the reads will be displayed on bottom half.

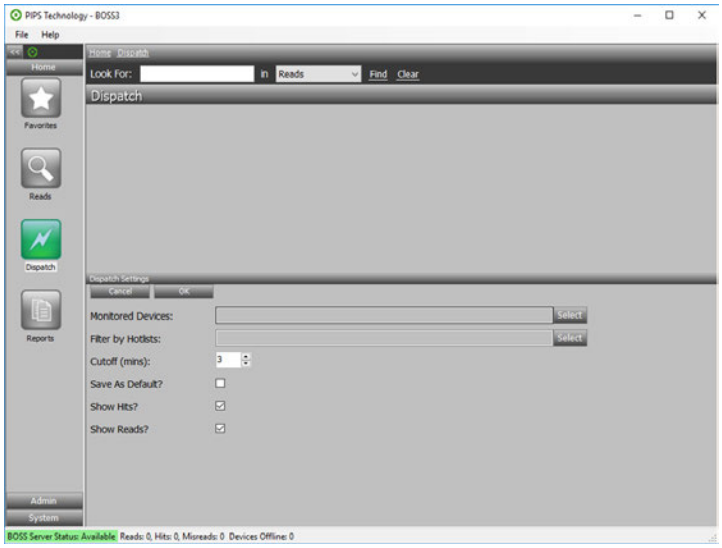
Note: By default, the ability to monitor reads via dispatch is disabled for new Boss installations, this feature can be turned back on by editing the Boss parameter “Dispatch_Show_ReadsEnabled” and setting the value to 1 for on. The Boss service must be restated for this to take effect.



10.1 Dispatch Settings

Dispatch Settings allow you to choose the information shown on the Dispatch screen.

1. Select the **Home** category in the Shortcut bar.
2. Click the **Dispatch** shortcut.
3. Click the **Settings** button in the bottom of the Browse/Edit area.



4. The following settings are available on the Dispatch screen. Change these settings as desired:

   Monitored Devices – Camera sources can be selected or deselected from a pick list to control which ones will supply reads (and resulting hits) to the Dispatch screen. Individual dispatchers can focus on particular camera inputs by selecting/deselecting any combination of sources (one, multiple, or all) for monitoring.

   In large BOSS systems, it may not be practical for a single dispatcher to monitor all sources simultaneously. An organization may choose to assign individual dispatcher personnel to different sources or may select to focus on particular sources during certain time periods or events.

   Filter by Hotlists – Hotlists may be selected to only show hits from designated hotlists. If there are no hotlists selected, hits from the monitored devices will be displayed.

   Cutoff (mins) – The cutoff setting determines how current from the present time a hit or read must be in order to display on the dispatch screen This setting determines the number of minutes before data is discarded from the on-screen display. The maximum time is 10 minutes.

   Save As Default – If checked, the current settings are saved and restored the next time the user logs in. Note that selected devices will always default to the devices where the user is configured to receive notifications in the Hotlist settings. See additional information on notifications in Section 7.1.1, Configuring Basic Hotlist Settings.

   Show Hits? – If checked, hits will display in rows in the top section of the Dispatch screen as they occur. If this option is deselected, rows of hits are not displayed in this section of the Dispatch screen. However, pop-up alerts will still display for hits, regardless of this setting.

Note: If the Alert Toggle button is set to the Off position, hits and reads will not display in the Dispatch screen. See Section 9, Alerts, for additional information.

   Show Reads? – If checked, all reads included in the devices selected in the Monitored Devices field display in the dispatch screen. By default, this option is not selected.

Note: Monitoring reads may slow down the BOSS server. It is recommended that reads are only monitored for diagnostics purposes.

5. Click the **Save** button for the changes to take effect.

10.2 Dispatch Hits

For each row, the columns displayed are:

Device – The device where the read originated.
LPN – The license plate characters read in by a camera or manually entered by a user.
Timestamp – Date and time when the read occurred.
Syntax – The state or region of the plate, if available.
Misread – If checked, indicates that the hit resulted from a read that was marked as a misread. Manual – If checked, indicates that the hit resulted from a manual entry (put in by a BOSS user). Patch – A thumbnail image of the license plate.
Overview – Color overview picture of the vehicle.
Hotlist – The name of the hotlist from which the hit occurred.
Field1 ... Field5 – Fields originating from the hotlist. The content and meaning of these fields vary depending on the composition of the hotlist.
PNC/DL – This field can be used for a driver's license (DL) number in US installations, but primarily used in United Kingdom installations for storing the UK Police National Computer identification number.
Info – Commonly contains additional text associated with the hit record. When the hotlist source contains additional fields, the information from those fields is all stored in this one field.
Priority – Priority assigned to the hotlist, with a lower number being given a higher priority.
Annotation – Notes associated with the read. Annotations are entered by BOSS users.

10.3 Dispatch Reads

For each row, the columns displayed are:

Device – The device where the read originated.
LPN – The license plate characters read in by a camera or manually entered by a user.
Syntax – The state or region of the plate, if available. Timestamp – The date and time when the read occurred. Patch – A thumbnail image of the license plate.
Overview – Color overview image of the vehicle.
Misread – If checked, indicates that this record was marked as a misread.
Hit – If checked, indicates this read resulted in a hit.
Manual – If checked, indicates this read was input manually by a BOSS user, rather than originating from a device.
Annotation – Notes associated with the read. Annotations are entered by BOSS users.

10.4 Manual Entries

There may be times when a read must be manually entered or when a camera does not correctly read a plate. For example, if there was an obstruction between the camera and the plate, then characters may be missed in the read. For this reason, manual entries can be completed by an authorized user via the Dispatch screen.

10.4.1 Adding a Manual Read

1. From the Dispatch screen, click the **Add** button. The Manual Entry screen appears in the lower half of the Browse/Edit area.

Note: The **Add** button will only be present if the logged in user has the Edit Access permission to reads.

2. Enter the plate characters in the LPN field.
3. Click the **Select** button to the right of the disposition field.
4. Select the desired disposition(s) and click the **Save** button to complete the selection.
5. Click the **Save** button to finish saving the manual entry. If the "Manual Entries" device is not being monitored, the manual entry will not appear in the Dispatch screen.

10.4.2 Correcting Reads

1. From the Dispatch screen, click the Add button. The Manual Entry screen appears in the lower half of the Browse/Edit area.
2. Enter the plate characters in the LPN field.
3. Click the **Select** button to the right of the disposition field.
4. Select the desired disposition(s) and click the **Save** button to complete the selection.
5. Click the **Save** button to finish saving the manual entry. If the "Manual Entries" device is not being monitored, the manual entry will not appear in the Dispatch screen.

11 QUERYING STORED DATA

The Reads screen allows for searching and viewing past read records on a local server or on a remote server that has granted access. Reads can be quickly searched by entering a license plate number. This screen also allows for more advanced queries where data can be filtered based on additional fields such as date ranges, location, and radius. Additionally, the Reads screen allows you to perform multiple queries with the use of tabs.

For the queried results returned, there are no limits to the number returned from a local server. To limit the impact on outside systems, there is a limit of 1,000 records returned from a remote server. A maximum of 1000 records will be displayed per page.

Note: Depending on factors such as the size of the BOSS database, the speed of the server, the bandwidth of the connection between client and server, and the parameters of the query, there may be a delay before the results are displayed. A status bar will display that shows that the query progress.

11.1 Wildcards

Wildcards are special characters that represent any alphanumeric character and can be used in searches and queries. Wildcards can make finding a match easier because they can define a portion of the criteria to be ambiguous. Wildcards supported in BOSS are described in the following table.

WILDCARD USED	REPRESENTS
a%	Any values that start with the letter “a”
a	Any values containing “a”
% or *	Any/all values
a_	Any values that are exactly two characters long and start with “a”
_a*b	Any values that have “a” as the second letter and end with “b”
[abc]*	Any values that start with “a”, “b” or “c”

11.2 Quick Search Bar

The Quick Search bar is always visible and available on the top of the BOSS screen regardless of the category or shortcut currently selected. This feature allows for quick, simple searches of various BOSS data.

1. Type the value to search for in the Look For field. This value can include wildcard characters. Multiple values can be entered separated by a comma (e.g., ABC123, XYZ234). However, wildcard values cannot be used when searching for multiple values.
2. In the “In” drop-down box select an area to search. The available options are **Reads**, **Hotlists**, **Users**, **Group Users**, **Groups**, **Devices**, and **Sites**. These areas are described below.
3. Click the Find link to initiate the search. The results will be displayed in the Browse/Edit area of the screen.

11.2.1 Quick Search Fields

When performing a query using the quick search feature, keep in mind that the search is performed in one significant area that can be selected. The search is then run against the significant field in that area, not all fields in that area. For example, when performing a quick search in Users, the text entered is compared against the Username field of all user records.

However, it is not compared to the display names for users. The following is a list of the fields used in the Quick Search:

SEARCH IN AREA	FIELD USED FOR SEARCH
Reads	LPN
Users	Username
Groups	Group Name
Site	Site Name
Hotlists	Hotlist Name
Group Users	Group Name
Devices	Device Name

11.3 Query Result Navigation Icons

Just above the query results are navigation icons that facilitate moving through the data results. These icons can be very useful for larger result sets, providing an easy way to move through records.



Move to the very beginning of the data results, i.e., the first record.



Move forward through the data results.



Move backward through the data results.



Move the very end of the data results, i.e., the last record.

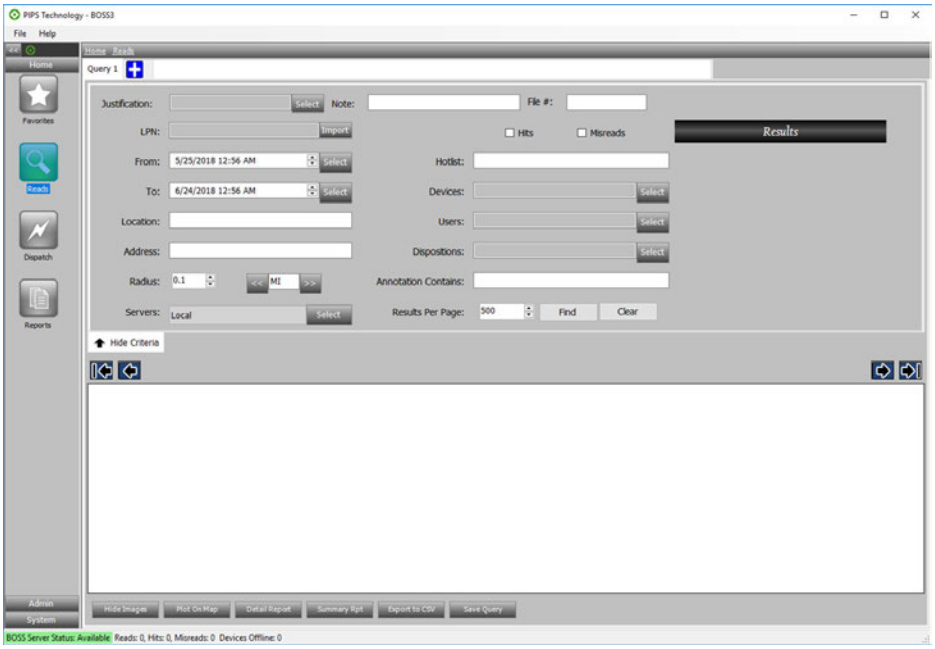
11.4 Advanced Reads Queries

The Reads screen allows for searching and viewing past read records. Reads can be quickly searched by entering a license plate number. The Reads screen also allows for more advanced read queries where data can be filtered based on additional fields such as date ranges, location, or radius. As indicated earlier, a maximum of 1000 records will be displayed.

11.4.1 Performing an Advanced Reads Query

1. Select the **Home** category on the Shortcut bar.
2. Click the **Reads** shortcut.
3. Enter desired query criteria (see the following section, 11.4.2, Entering Advanced Reads Query Criteria). All fields do not have to be filled in. Leaving a query field blank simply means there will be no filtering on that field.
4. Click the **Find** button to run the query.

11.4.2 Entering Advanced Reads Query Criteria



The query criteria fields are:

LPN – Full or partial (using wildcards) license plate number.
From – The start date and time for reads to be retrieved. Either click the **Select** button to display a calendar for quick selection, or type in the date.
To – The end date and time for reads to be retrieved. Either click the **Select** button to display a calendar for quick selection, or type in the date.
Location – The location as entered in the PAGIS application (see the Pagis Software User's Manual for more information).
Near Address – An address to use as the center of a radius search. The address format depends on the mapping system used but typically street name, house number, city and state, or zip code can be entered.
Radius – When a Near Address filter is entered, the search radius from the center point must be entered here.
Servers – Information can be queried from one or more remote BOSS servers. Click the Select button to display a list of authorized BOSS servers.
Justifications – Select the justification that best describes the purpose for the query being performed. This field will only be displayed if Justifications have been enabled in the System Parameters. See Sections 15.3.2, List of BOSS System Parameters, and 15.7, Justifications, for more information.
Justification Note – Enter any additional information necessary to more accurately document the query being performed. This field will only be displayed if Justifications have been enabled in the System Parameters. See Sections 15.3.2, List of BOSS System Parameters, and 15.7, Justifications, for more information.
Hits Only – If checked, only hits are queried.
Misreads Only – If checked, only reads that are marked as misreads are queried.
Hotlist – A search on hits can be limited to a specific hotlist, which can be entered here.
Devices – A query can be narrowed to reads originating from a particular device. Click the Select button to display a list of devices, select one or more.
Users – A query can be narrowed to reads originating by a particular user. Click the Select button to display a list of users and select one or more.

Note: The username can also be typed in.

Dispositions – A query can be narrowed to reads with a particular disposition. Click the **Select** button to display a list of dispositions. Then select one or more dispositions.

Annotation Contains – If text is entered in this field, only reads that contain the text in the annotation field are queried.

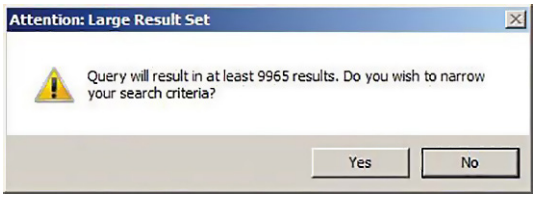
Results Per Page – The maximum number of reads that will be displayed. The default is 500, the maximum is 1,000.

Clear – If clicked, the fields on the current tab will be returned to their default values.

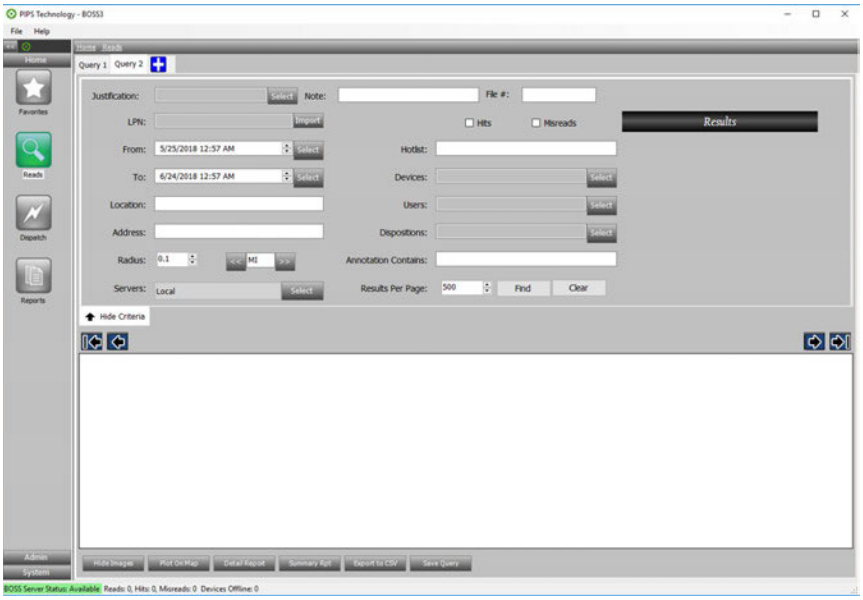
11.4.3 Managing Query Results

With the ability to obtain any number of results from a local server comes the option to narrow the potential results to be returned. If a large number of results will be returned based on the criteria entered, a message is displayed asking if the search criteria should be narrowed. If you select **Yes**, the search criteria is redisplayed offering the chance to make any necessary changes to reduce the results. If you select **No**, the query is performed based on the current criteria selections.

Note: A large number of results can take several minutes to be displayed.



11.5 Multiple Query Tabs



With Query tabs, users can perform multiple queries at a time. By clicking on the last tab, which contains the plus icon, you can access additional Reads Query screens. Enter the desired search criteria on each new screen to obtain additional information through the varying results. Each query can be given a descriptive name by right-clicking on the tab, and obsolete queries can be removed the same way.

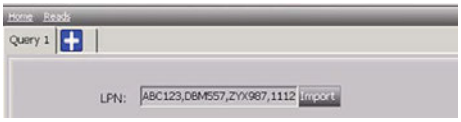
11.6 Cross-Referencing External Data

BOSS allows cross-referencing external data, such as DMV information. To query BOSS based on external information, take the following steps:

1. Create a CSV text file containing the license plate numbers to be cross-referenced. **The license plate number must be in the first field.**
2. Open the Reads Query screen.
3. Click the **Import** button next to the LPN field.



4. Click **Open** to import the plate numbers. A maximum of 50 plate numbers can be referenced at a time. Imported plate numbers will show up in the LPN field:

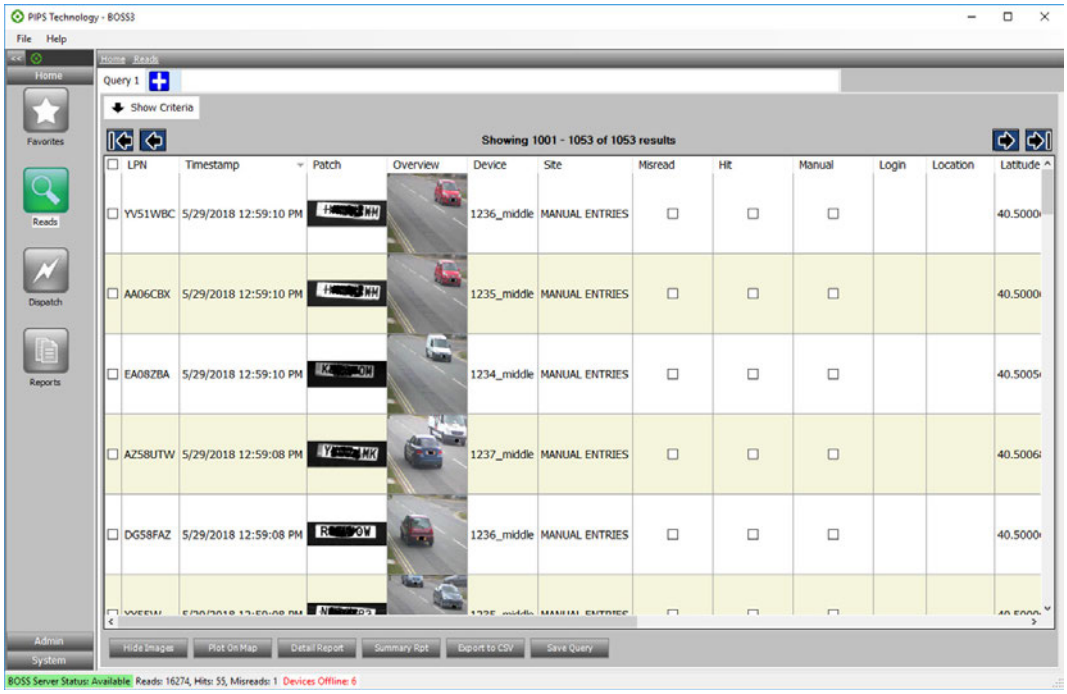


5. Enter other query criteria, as needed, and click **Find** to run the query.

11.7 Working with Queried Reads

11.7.1 Viewing Query Results

The results of both Quick Searches and Advanced Reads Queries are presented in the same manner.



The columns displayed are:

LPN – The plate text (characters) read in by a camera or manually entered by a user.
Timestamp – The date and time when the read occurred.
Patch – A thumbnail image of the license plate. Overview – The color overview picture of the vehicle. Device – The device where the read originated.
Site – The site where the read originated.
Misread – Indicates whether the read was marked as a misread by a user.
Hit – Indicates whether the read is a hit.
Manual – Indicates whether the read was entered manually.
Login – The username logged into the device at the time the read originated.
Location – The location entered in the PAGIS system. See the Pagis Software User's Manual for more information.
Latitude – The latitude coordinates of the device at the time the read originated. Longitude – The longitude coordinates of the device at the time the read was originated. Hotlist – The name of
the hotlist that produced the hit.
Field1 ... Field5, PCNID, Information – Information from the hotlist that produced the hit.
Annotation – Annotations entered for the read.
Server – The name of the server that has provided this information. This can be a local or remote server.

11.7.2 Query Results Actions

There are several button options available at the bottom of the Reads Query Results screen that offers additional uses of the data results.



Hide Images/Show Images – Used to remove the image columns, patch and overview, from the view. This can be done to provide more room for text fields to be displayed. When clicked, the Hide Images button's caption changes to Show Images. When the button is clicked again, images will again be displayed.

Plot On Map – When clicked, any selected records will be plotted on a map. One or multiple records can be selected by clicking the checkbox in the first column of the record. To select all of the records, click the checkbox in the headings column.

Detail Report – Click to generate a detailed report of selected reads. To select one or more records, click the checkbox in the first column of the record. To select all of the records on the current page, click the checkbox in the headings column. Use the navigation buttons to move to additional pages to select additional records.

Summary Rpt – Click to get a summary report of selected reads. To select one or more records, click the checkbox in the first column of the record. To select all of the records on the current page, click the checkbox in the headings column. Use the navigation buttons to move to additional pages to select additional records. To include all results choose the All Results option in the Reads Summary Detail Report option box.

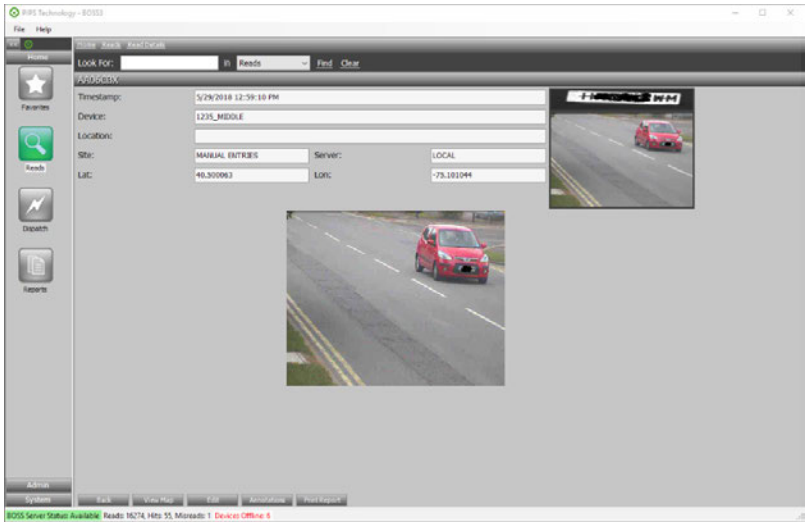
Export to CSV – Click to save the results to a file in a CSV format. Select to save the current page or all results provided. Use the navigation buttons to move to additional pages to select additional records.

Save Query – Click to save the query criteria as a favorite for future use. See Section 11.8, Favorites, for more information.

11.7.3 Viewing Read Details

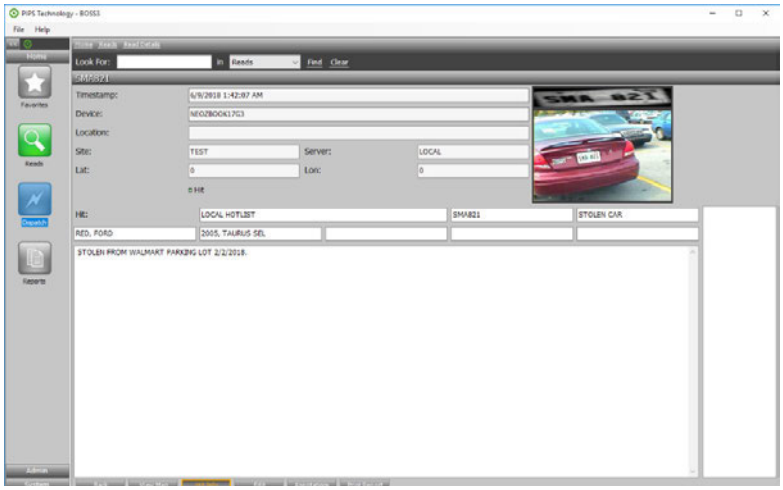
Click a row in the query results to view the details of the record.

The Read Details screen displays the license plate text in the title. The timestamp, originating device, site, and geographical coordinates are displayed below. The plate patch and vehicle color overview images are on the right.

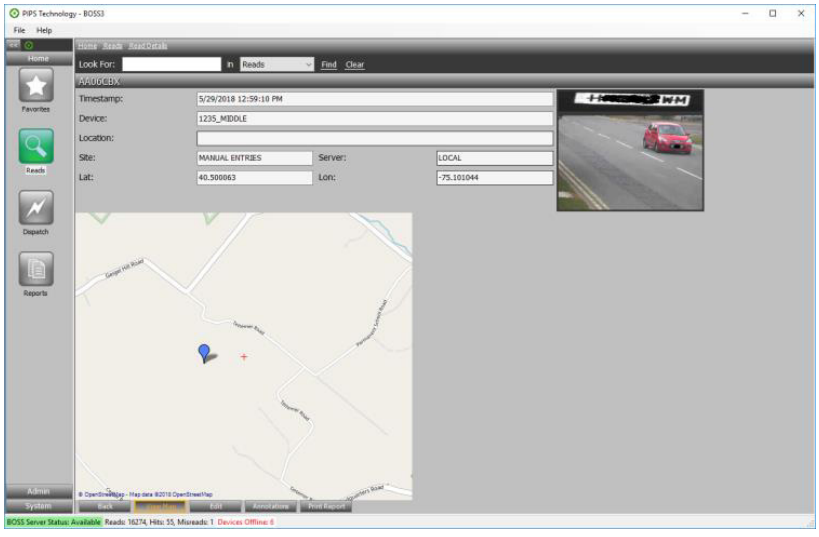


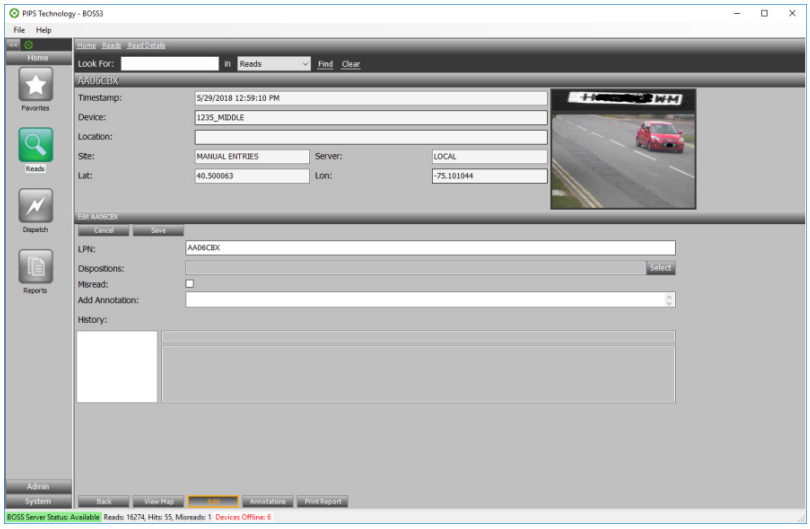
The vehicle color overview picture can be enlarged by clicking on the picture. Use a mouse scroll wheel or the cursor up and down keys to resize the image. Left-click on the enlarged image to close. Right-click on the image to copy the image to the Windows Clipboard.

If the read is a hit, details of the hit can be displayed by clicking on the Hit Info button at the bottom of the screen.

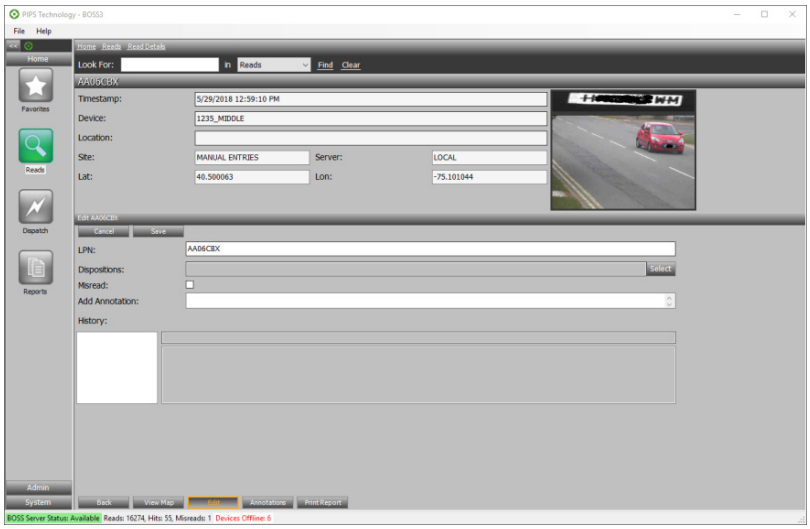


A map plotting the location where the read occurred can be displayed by clicking on the View Map button.

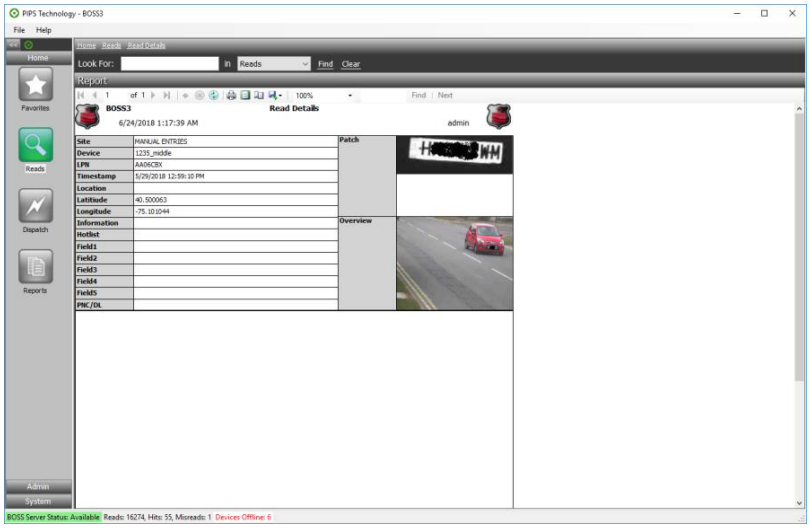




Use the Edit button to correct the plate text and/or assign a disposition and annotation to the read. Click on Save to save the changes. The plate text can also be marked as misread if the read information is found to be incorrect.



Annotations associated with the read can be viewed by clicking on the Annotations button.



A report containing the read's details can be printed by clicking on the Print Report button.

11.8 Favorites

Favorites are read queries that use specified criteria, which have been saved. Favorites can be reused, which allows the user to quickly perform frequently needed queries without having to define the parameters each time. Favorites are specific to each user.

11.8.1 Creating a New Favorite

1. Select **Home** on the Shortcut bar to access its icons.
2. Click on the **Read** shortcut.
3. Enter the desired query parameters in the Browse/Edit area (e.g., data range, location, radius, servers).
4. Click the **Go** button to run the query.
5. When the query results window appears, click the **Save Query** button.
6. A dialog box will appear, prompting for a name. Enter a descriptive name for the new favorite.
7. Select the Use Relative Date Range option if desired.

   Use Relative Date Range Option – If this option is selected when saving a query, and when the resulting favorite query is run in the future, it will use a From and To date and time range relative to the From and To date and time entered for the original query. It will not use the actual range entered in the original query. Also, it is important to remember that the time span between the From and To date and the time range used is relative to the date and time when the original query was run.

   Consider a query that is saved as a favorite and originally defined on 8/9/20xx to search reads between 8/02/20xx and 8/8/20xx (the prior week). If the Relative Date Range option is selected, the query is saved to always run against the prior week rather than those actual dates. If the Favorite option is invoked on 12/3/20xx, it will return results from 11/26/20xx through 12/2/20xx. It is important to note that the results will be relative to the actual time of the original query and when it is rerun. Suppose you run a query at 5 pm today to search for reads occurring between 9 am and 5 pm and save it as a favorite. When you run the query again tomorrow, it will search for reads that occurred eight hours **before** the current time, which may not necessarily fall between 9 am and 5 pm.
8. Click **OK** to complete. The query definition is now saved as a favorite and can be accessed at any time.

11.8.2 Activating a Favorite

1. Select the **Home** category in the Shortcut bar (if not already selected).
2. Click the **Favorites** shortcut.
3. A listing of all favorites is displayed in the Browse/Edit area.
4. Click the desired favorite. (The selected favorite will be highlighted in yellow.)
5. Click the **Go** button in the bottom area of the Browse/Edit area.
6. The query results will appear in the Browse/Edit area.

11.8.3 Deleting a Favorite

1. Select the **Home** category in the Shortcut bar (if not already selected).
2. Click the **Favorites** shortcut.
3. A listing of all favorites is displayed in the Browse/Edit area.
4. Click the desired favorite. The selected favorite will be highlighted in yellow.
5. Click the **Delete** button in the bottom area of the Browse/Edit area.
6. Press **Yes** to confirm deletion.

12 REPORTS

Several reports are included, automatically, with a new BOSS installation. These reports are available for use as soon as a BOSS Administrator assigns role permissions to the reports.

12.1 Running a System Report

1. Select the **Home** category on the Shortcut bar.
2. Click the **Reports** shortcut.
3. The Browse/Edit area will display a list of available reports. (Reports to which the user does not have permissions are not displayed.)
4. Click the desired report. The selected report is highlighted in yellow. Parameters for the report appear in the bottom of the Browse/Edit area.
5. Select **Date Range**. All reports call for From and To dates to define the time range for the report data. By default, the values in these fields define a report for the most recent two weeks. You can change these dates by typing different information into these fields, using the **Up/ Down** arrow keys to the right of the field or by clicking the **Select** button to the right of the field and selecting a date on the calendar and then clicking the **Save** button.
6. Some reports also permit you to filter report results by user(s). For example, the pictures report, which reports pictures taken in PAGIS, allows you to define one or more users to report on.
7. Once desired parameters are selected for the report, click the Go button. The report screen immediately displays, indicating that the server is generating the report until results are displayed.

12.2 Viewing and Printing Reports

The Report screen displays the date and time the report was generated and the title of the report in the heading area. When you place your mouse above a shortcut on the Report Shortcut bar, a label appears indicating what the shortcut button does. Note that some of the buttons on the Shortcut bar are not relevant to BOSS reports and are therefore disabled.
The Report Results Shortcut bar icons are as follows:



First Page – Return to the first page of the report.
Previous Page – Go to the previous page of the report.
Page Input – In this text box, type in a particular page number to bring up on screen.
Next Page – Go to the next page of the report.
Last Page – Go to the last page of the report.
Stop Rendering – This button can be used to cancel the report processing. This can be helpful if a large report was initiated, but is no longer desired.
Refresh – Refresh the report using the most current BOSS data.
Print – Print the report.
Print Layout – Toggle between available print layouts.
Page Setup – Choose among the options for standard page setup, such as page orientation, and paper size.
Save As – Excel/PDF/Word – Save the current results to a Microsoft Excel (.xls), an Adobe Portable Document Format (.pdf) or a Microsoft Word (.doc) document.
Width Zoom Setting – This drop-down list allows you to select a zoom view for the report results on the screen.

12.2.1 Viewing the Login Statistics Report

1. Select the **Admin** category on the Shortcut bar.
2. Click the **Devices** shortcut.
3. Click the **Logs** button at the bottom of the screen.



4. Click **Go** to view the Login Statistics Report.
   Begin Date – Select the start date for the report.
   End Date – Select the end date for the report.
   Selected Users – Select the users to include in the report. Click the **Select** button. Click the checkbox of the desired user. Click on the **Save** button.

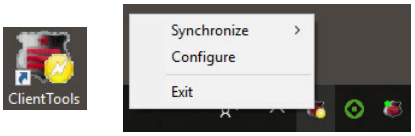
13 CLIENT TOOLS

The Client Tools utility is used to transfer any necessary files needed for a shift from BOSS to an PAGIS system that is being run in the Disk Sync mode. After the completion of a shift, Client Tools can then be used to transfer read data files captured during a shift into BOSS. The utility is configurable and processes files stored on a local, network, or USB flash drive. Like Smart Client, the Client Tools utility does not have to be run on the BOSS server; it can be configured to access the server via an IP Address.

Client Tools does not have a customary interface. Once the utility is started, the Client Tools icon will appear in the Windows System Tray.

Before use, Client Tools must be configured, which is described in Appendix 17. Once the Client Tools has been configured, it can now be used to synchronize information between BOSS and PAGIS:

1. To start, right-click on the **Client Tools** icon.

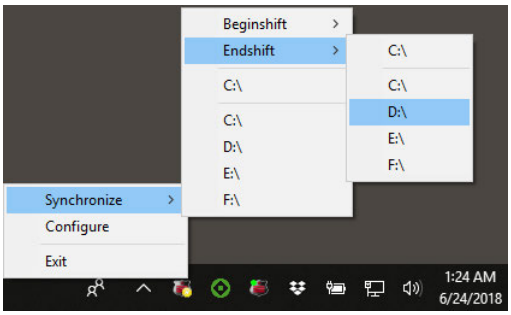


2. Select **Synchronize**. The next menu displayed is divided into three sections.

   a. The first section allows the user to select either **Create Begin Shift Files or Synchronize End Shift Files**. When either option is selected, the next menu is displayed. It is divided into two sections; it is the bottom two sections of the previous menu and functions the same way.

   b. The second section displays the path defined during configuration. This is a shortcut to perform Begin Shift and End Shift at the same time, storing the Begin Shift files in the defined location and processing the End Shift files at the defined location. If there are no End Shift files to process, this feature will be complete after the Begin Shift file is created. No error message will be displayed if the End Shift files are not found.

   c. The last section lists the drive letters currently on the workstation. If one is selected, Client Tools will perform a Begin Shift first and store the files at the root of the drive selected. Then Client Tools will check to see if there are End Shift files at that location. If found, the files will be processed. If not found, the synchronization process is complete. No error message will be displayed. This is an additional option if the configured drive is not currently available.



Note that once End Shift files have been processed, they are deleted.

14 ARCHIVING DATA

It is possible to archive reads that have accumulated in the BOSS database. Based on settings that are configurable in System Parameters, reads that meet the specified criteria are transferred from the main BOSS database to an archived BOSS database. *(See Section 15.3.2, List of BOSS System Parameters, for additional information on configuring this feature.)*

Once enabled, this process is handled by the BOSS server. There should be no noticeable difference to a user logged into a BOSS Smart Client when reviewing or reporting on stored reads. The only indication in the BOSS Smart Client that reads have been archived will be on the BOSS Home screen. The user will be able to see a calculable difference between the reads and hits counts compared to the total reads and total hits counts. The difference between the values will be the number of reads and hits stored in the archived database.

15 SYSTEM SETTINGS

15.1 Sessions

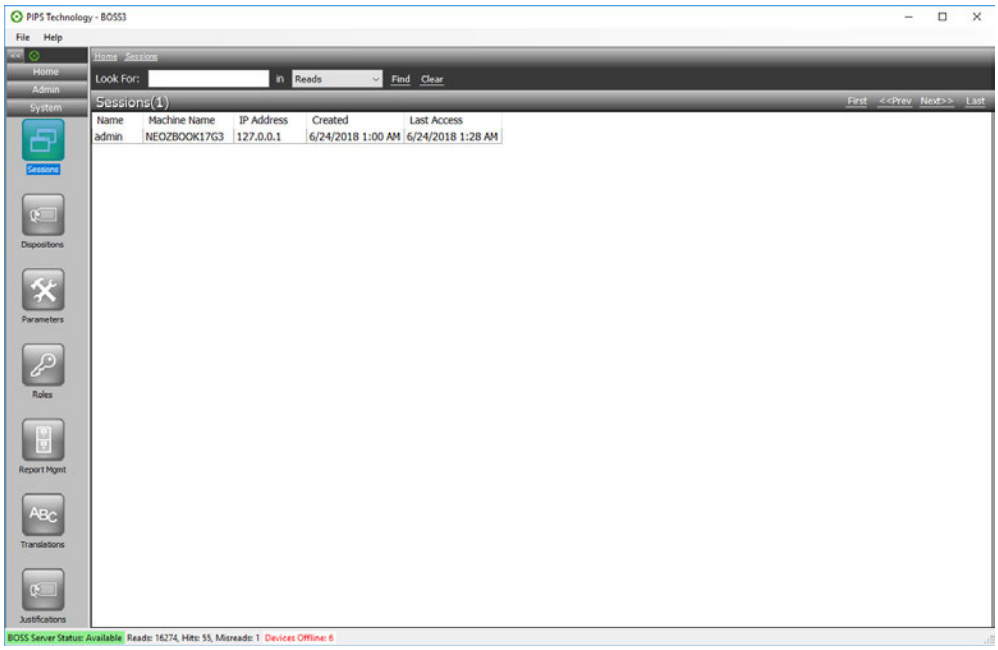
The Sessions screen allows for viewing the current list of logged-on BOSS users. Each login on each computer utilizes a concurrent license of the software. Since BOSS is licensed per concurrent active session, a BOSS Administrator may need to have a session disconnected in order to release a session license. A BOSS Administrator can force a session disconnect in the Sessions screen.

Note: BOSS allows a single "admin" login to access BOSS even if the number of concurrent sessions has been exhausted. Please see Section 2.1, BOSS Administrator Login, for more information about the "admin" username.

15.1.1 Viewing and Disconnecting Sessions

1. Select the **System** category on the Shortcut bar.
2. Click the **Sessions** shortcut. A list of current user sessions appears in the Browse/Edit area.
3. The heading in the Browse/Edit area indicates the total number of current sessions.
4. Click on a session to see details in the bottom half in the Browse/Edit area.
5. To disconnect, click the **Disconnect** button that appears in the detail area, and click **OK**.

Note: You cannot disconnect your own session in this manner. To disconnect your own session, simply log off the BOSS application.



15.1.2 Workstation Power Management and Sessions

Using Windows Power Management to hibernate or suspend a workstation running the BOSS Smart Client will cause the session in BOSS to be terminated after five minutes. When the workstation is resumed from hibernation or a suspended state, the user will have to log in to BOSS again.

15.2 Dispositions

Dispositions are pre-defined classifications that can be assigned to hits. “Arrest Made,” “Vehicle Recovered,” “Surveillance Established” are examples of dispositions. A BOSS Administrator is able to define any number of dispositions for her system. Users can then use those dispositions to specify the action taken or the status of the hit. A new BOSS system will have a Default Disposition category that includes one disposition of “No Action.” Additional categories can be defined as needed.

15.2.1 Defining a New Disposition

1. Select the **System** category on the Shortcut bar.
2. Click the **Dispositions** shortcut. A list of all current dispositions appears in the top of the Browse/Edit area.
3. Click the **New** button in the bottom of the Browse/Edit area.
4. Enter a name for the disposition. If adding it to the default category, simply enter the name of the disposition. If adding it to a new category, the format of the name should be [Category : Disposition Name], i.e., **Auto :Vehicle Recovered**.
5. Enter a **Description** for the new disposition.
6. Specify a **Priorit**y for the disposition. (A lower number means a higher priority.)
7. Select the **Back Office Only** option if the disposition should not be available only in the Correct Reads screen in BOSS, and not exposed in PAGIS.



15.2.2 Deleting a Disposition

1. Select the **System** category in the Shortcut bar (if not already selected).
2. Click the **Dispositions** shortcut.
3. A list of all dispositions is displayed in the Browse/Edit area.
4. Click the desired Disposition. The selected disposition will be highlighted in yellow.
5. Click the **Delete** button in the bottom area of the Browse/Edit area.
6. Press **Yes** to confirm deletion.

15.3 System Parameters

System Parameters allow for configuration parameters for a BOSS system. System parameters only need to be configured during initial system configuration and normally do not need to be modified again after that.

15.3.1 Editing System Parameters

1. Select **System** from the left Shortcut bar.
2. Click on the **Parameters** button in the Shortcut bar.
3. Click on the desired parameter in the right Browse/Edit window. The bottom pane of the Browse/Edit window will display the entry field for the selected parameter.
4. Modify the parameter value as desired and click the **Save** button.

15.3.2 List of BOSS System Parameters

arc_ActiveRetentionDays – This setting dictates how long reads will be maintained in the BOSS database. After reads have been stored for this time, they will be moved to the archived database, creating space for additional reads in the main database. The default setting is 730 days but can be varied based on the size and needs of the system.
arc_ArchiveDBRetentionDays – This setting dictates how many days to retain an archived database. After an archived database has been stored for this time it will be removed, creating space for additional archived databases. The default setting is 0 days, which indicates that the archived databases will never be removed, but the number of days can be modified based on the size and needs of the system.
arc_DatabaseLocation – This setting allows the user to specify where the archived databases should be saved. A blank entry will save them in the SQL default location.
arc_Enabled – To allow the BOSS server to archive aged reads and free up space, enable archiving by setting this to 1. When archiving is not desired, this setting should be 0.
arc_EndOfMonthCutOff – This setting forces a restriction on the size of the archived databases, so that nothing will be added after the end of each month. The default setting is disabled (0). To enable the setting, change the value to 1.
arc_MaxSize – This setting allows the Administrator to determine the number of reads that can be stored in the archived database. The default value is 1 million and can be varied based on the size and needs of the system. Once an archived database has reached this maximum number of records, a new archived reads database will be created.
audit_Justification_FileNumberRequired – When this setting is enabled (1), users performing read queries are required to enter a file number.This information will also be listed in the audit report. The default setting is disabled (0).
audit_Justification_NotesRequired – When this setting is enabled (1), users performing read queries are required to enter a justification note. This information will also be listed in the audit report. The default setting is disabled (0).
audit_JustificationEnabled – When this setting is enabled (1), users performing read queries are required to select a pre-defined justification. This information will also be listed in the audit report. The default setting is disabled (0).
data_CaptureUsageStatistics – When this setting is enabled (1), information sent from a PAGIS device that has been modified due to Privacy settings will still be utilized to generate usage statistic reports. The default setting is disabled (0).
hls_HotListDeltas – When this setting is enabled (1), updated hotlists will be deployed in full. Changing the setting to disabled (0) will cause only the changes made in the updated hotlists to be deployed.
Password_Expiration_Days-Number of days a password is allowed to remain unchanged. Value “1”=enabled, “0”=disabled.

15.3.2 List of BOSS System Parameters (continued)

Proxy_uri/proxy_username /proxy_password/proxy_domain – These settings are only necessary if there is a proxy server involved that requires authentication for connection. Enter a valid Uniform Resource Identifier (URI), username, password, and domain in the associated fields to allow communication through the proxy server. Consult the network Administrator for proxy authentication information

purge_Minutes – This setting is the time, in minutes, between each session of purging or archiving. The default value is 15 minutes and is configurable to any value of 1 minute or greater.

purge_ReadCount – This setting is the number of records to be processed by the purging or archiving process per session. It can be any value, but setting it according to system limitations is recommended because the process can be resource intensive if set too high.

readQuery_fromDate – This setting allows the user to adjust the default From date on the Reads Query screen. Any value can be entered and it is used to decrement from today. Example – a value of 7 would result in a from date seven days earlier than today.

readQuery_toDate – This setting allows the user to adjust the default to date on the Reads Query screen. Any value can be entered and it is used to incremented from today. Example – a value of 7 would result in a to date seven days later than today.

Recent_Read_Time- Time in min. of how long to hold reads in the "Recent reads" table for hit evaluation.

Recent_Reads_Amt- Number of records to delete from "Recent reads" if older then Recent read time.

ResendEmailNotice- Resend Offline notification on Fixed Camera after this amount of time has expired.

rq_ReaperHours – This setting manages how long to retain a temporary database table created when running certain read queries. This allows the user to continue to review the results of those queries for a longer time. The default is a minimum of 48 hours, and there is no maximum value.

smtp_AlertTemplate- Default email template, definitions listed in table below.

smtp_SenderName – In order for the BOSS server to send alerts to email addresses, the SMTP settings must be configured correctly. The SMTP sender field should contain the username that will appear in the from field on an email generated by the BOSS system.

smtp_Server – The name or IP address of the SMTP server should be entered here. The name or address used here must be one by which the SMTP server can be reached from the BOSS server. This field must be populated correctly in order for the BOSS system to send any alerts to email addresses.

smtp_SSL – If Secure Sockets Layer (SSL) is used on your SMTP server, the value of this field should be set to 1. If you do not use SSL, this field should be set to 0.

smtp_SubjectTemplate – This field sets the subject line of alert emails generated by BOSS. The following entry in the field incorporates both static text and a BOSS field variable as well: BOSS alert FROM [SRC].

TOKEN	DESCRIPTION	TOKEN	DESCRIPTION
[LPN]	license plate	[FD1]	field1
[STE]	site	[FD2]	field2
[SRC]	device	[FD3]	field3
[LOC]	location	[FD4]	field4
[LAT]	latitude	[FD5]	field5
[LON]	longitude	[PNC]	PNCID/DL
[HOT]	hotlist name	[INF]	information

smtp_UserName/smtp_password – The SMTP username and password fields should contain a valid SMTP username and associated password for sending alerts through the SMTP (email) server. Normally, a BOSS Administrator coordinates with his SMTP Administrator to create a special SMTP user that will be used exclusively for BOSS alerts.

Soap variables- All are now legacy features not currently used.

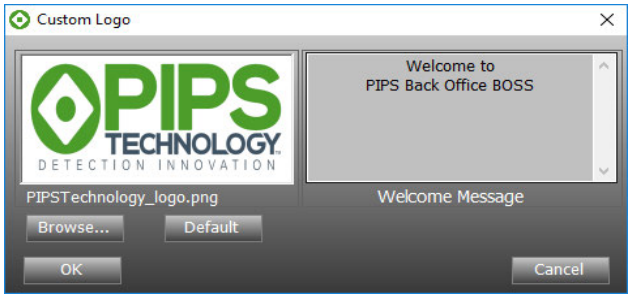
verint_HotlistsMonitored- Enter hotlist by name separated by commas.

verint_NotificationConfigured- Indicates whether the Verint notifier should be used.

15.3.2 Branding

BOSS allows the BOSS Administrator to upload a logo image and a welcome message that is displayed to BOSS users on the Home screen. To define the image and message:

1. Select **System** from the left Shortcut bar.
2. Click on the **Parameters** button in the Shortcut bar.
3. Click on **Branding**.
4. If needed, click **Default** to remove current custom settings.
5. Pick the desired logo image using the **Browse**... button.
6. Type in a message in the Welcome Message box.



Browse – Select an image file (JPEG, GIF, BMP) to be displayed on the home screen. The largest recommended image size is 120 by 380 pixels.

Default – Remove the custom logos and texts.

Welcome Message – A custom welcome message can be typed in here.

7. Click **OK** to save changes, or **Cancel** to discard changes.

15.4 Roles

In addition to the default roles that are automatically created by BOSS, the Administrator can create and configure custom roles as needed. *See Section 4.2, Permissions, for more information.*



15.4.1 Adding New Roles

1. Select the **System** category on the Shortcut bar.
2. 2. Click the **Roles** shortcut. The Browse/Edit area will display a list of existing roles.
3. 3. Click on the **New** button. The New Role entry window will be displayed in the bottom of the window.
4. 4. Enter the name of the new role and assign the desired permissions.
5. 5. Click the **Save** button.

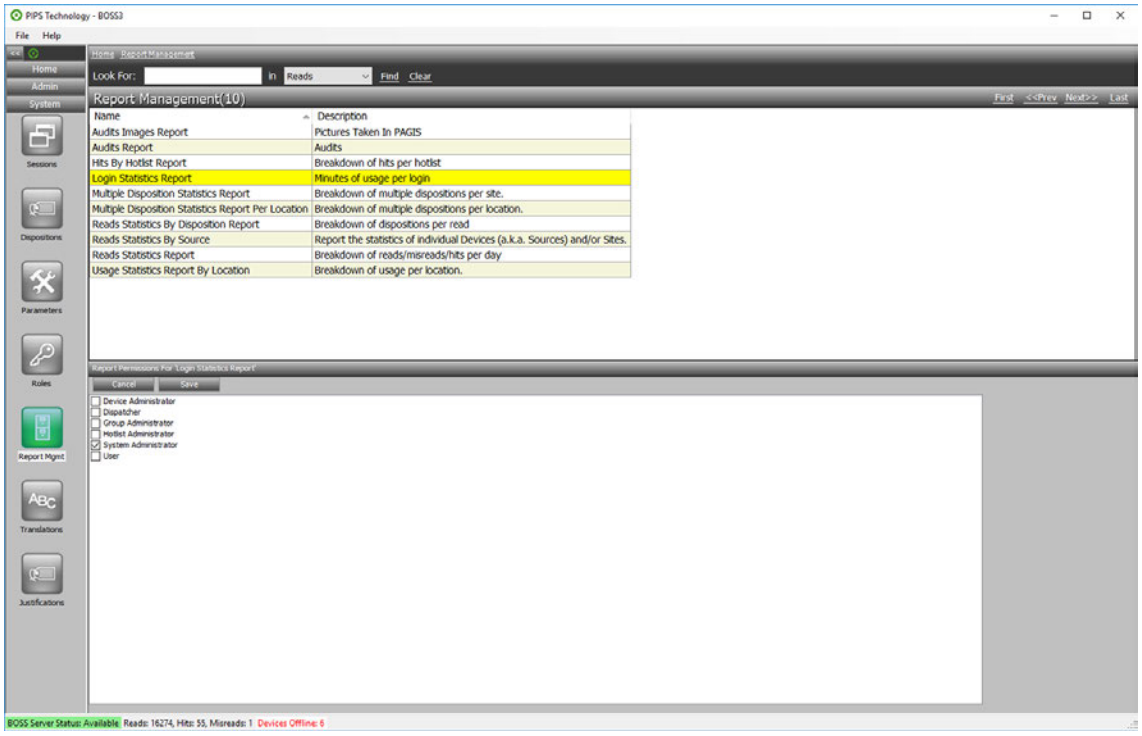
15.4.2 Deleting Roles

1. Select the **System** category on the Shortcut bar.
2. 2. Click the **Roles** shortcut. The Browse/Edit area will display a list of existing roles.
3. 3. Click on an existing role and the edit window will be displayed in the bottom of the window.
4. 4. Click the **Delete** button. Click **Yes** when prompted to complete the operation.

15.5 Report Management

15.5.1 Assigning Permissions to Access Reports

1. Select the **System** category on the shortcut bar.
2. Click the **Reports Mgmt** shortcut. The Browse/Edit area will display a list of available reports.
3. Select a report by clicking the name in the list. The selected report will be highlighted in yellow.
4. Current report permissions for the type of report chosen display in the bottom of the Browse/Edit area. Each BOSS role is listed along with a checkbox. Click a role in the list to select. Click a second time to change an unchecked box to a checked box.
5. After selecting the desired permissions for the report, click the **Save** button.



15.6 Translations

Across various organizations and agencies, terminology related to BOSS can differ significantly. For this reason, a new function added in the BOSS version 3 series gives customers flexibility in naming conventions used in the application. The Translations function provides for changing wording on BOSS screens, which allows a customer to tailor screen labeling to correspond to their own vernacular. Text items in the translations editor correspond to labels on BOSS screens. Authorized users can change these text items as necessary.

Note: This feature is not intended as a replacement for language-specific versions of BOSS. For international versions of BOSS, please contact PIPS™ Technical Support.

15.6.1 Entering a New Translation



1. Select the **System** category on the Shortcut bar.
2. Click the **Translations** shortcut. A list of all current translations appears in the top of the Browse/Edit area.
3. Click the **New** button and the new Translations Entry screen appears in the bottom area.
4. Enter an existing label from the BOSS application in the Caption field, using the exact case and spelling that normally appears on the screen.
5. Enter the desired replacement text in the Translation field.
6. Click the **Save** button to complete the operation.

Note: The user must log off and on again for translation to take effect in the current session.

For Example: A customer preferring to see a label of “Plate” where the software normally uses the term “LPN” would use the translations feature to create the replacement for their installation. The translation Entry Caption field would contain “LPN,” while the Translation field would contain the replacement term “Plate.”

15.7 Justifications

To ensure that sensitive information is being kept secure, systems can be configured to require that users who are performing queries on reads have a valid reason for doing so. Enabling the audit Justification Enabled parameter requires users to justify their reason for querying reads. There are five justifications created by default: Audit, BOLO Post Scan Query, Crime Scene Query, Test and Trend Analysis. These queries will also be documented in audit reports.



15.7.1 Entering a New Justification

1. Select the **System** category on the Shortcut bar.
2. 2. Click the **Justifications** shortcut. A list of all existing justifications appears in the top of the Browse/Edit area.
3. 3. Click on the **New** button. The Justifications Entry screen appears in the bottom area.
4. 4. Enter a justification. There is no validation on the entry for this field.
5. 5. Click the **Save** button to complete the operation.

15.7.2 Deleting Justifications

1. Select the **System** category on the Shortcut bar.
2. 2. Click the **Justifications** shortcut. A list of all existing justifications appears in the top of the Browse/Edit area.
3. 3. Click on the justification to be deleted. The Justifications Edit screen appears in the bottom area.
4. 4. Click the **Delete** button. Click on **Yes** when prompted to complete the operation.

17 APPENDIX: INSTALLATION AND CONFIGURATION

This section is intended for authorized personnel in installation and configuration of a BOSS system. The information in this guide is organized sequentially, in the order that steps would be performed when initially setting up a new BOSS system, with the first section describing the software installation process, and the subsequent sections describing configuration options for a BOSS system.

Upon initial installation of a new BOSS system, the BOSS server application must be configured using the BOSS Controller application. BOSS Administrators may also find the need to modify configuration settings after the system has already been in use. Therefore, the configuration section can be used as an ongoing reference for authorized personnel responsible for maintaining the system.

Note: It is critical that only an IT Administrator or other knowledgeable personnel attempt configuration modifications to a BOSS system. Incorrect configuration settings can cause serious issues with operation and/or adversely affect data integrity. When in doubt, you should consult PIPS Technical Support before making system configuration changes.

OS feature requirements

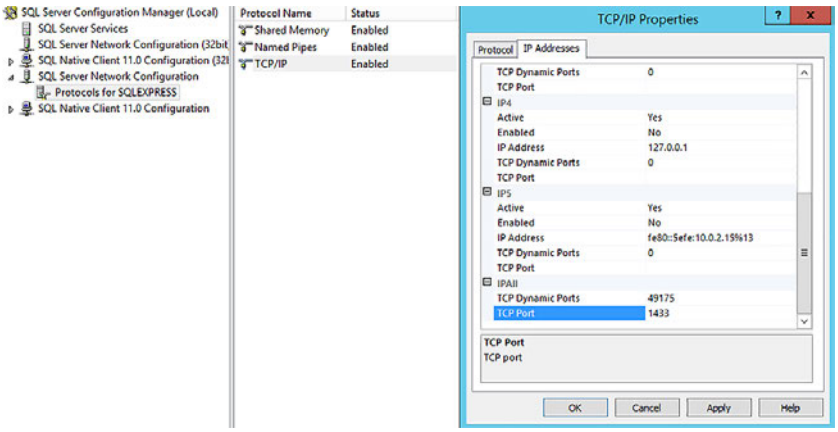
- Windows server 2008 or newer.
- Net. TCP Port Sharing Service must be enabled and running.
- Framework .Net 4.0.

SQL Server Requirements

1. SQL version 2012 or newer required.
2. 2. SQL login account “NT AUTHORITY\SYSTEM” is required to be mapped to Boss3 database as db_owner. For system with existing “Boss3” databases this should be applied prior to Boss software installation. For new installation this can be applied after the Boss service has ran for the first time and created the Boss3 database. See- “Common issues”

Settings under SQL Server Configuration Manger:

3. “SQL Server Network Configurations” Name Pips must be enabled.
4. “SQL Server Network Configurations” TCP/IP must be enabled, with “IP All” set to port 1433.
5. SQL restart required after changes.



17.1 Installing the BOSS Server Application Files

17.1.1 Running the Installer

This guide assumes that the Microsoft SQL Server 2012 or newer instance has already been installed and is available. If the SQL Server is not available, stop now and continue installation after the SQL Server has been installed. To install the Microsoft SQL Server, please follow the instructions provided by Microsoft.

Note: 1. It is recommended that antivirus utilities be disabled during the install.

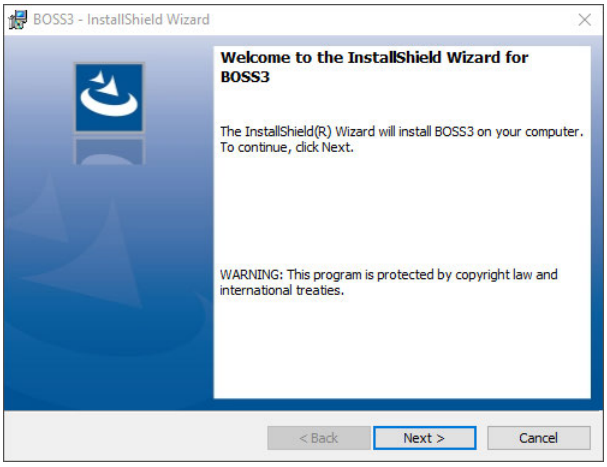
To commence the installation:

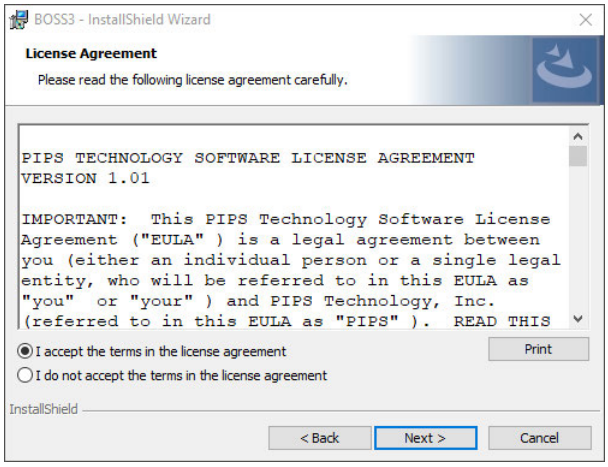
1. Select the link supplied by PIPS to the BOSS installation application.
2. Run the BOSS Setup executable.

Note: Right-click on the installer icon and select Run As Administrator.

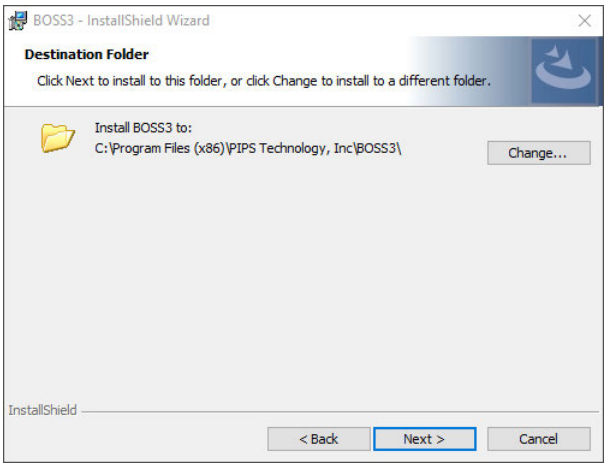
17.1.2 License Agreement

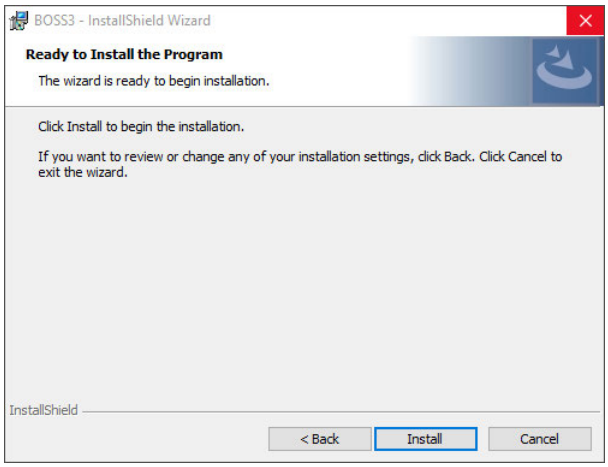
1. Click **Next** then check the license agreement checkbox to acknowledge agreement with the license terms.
2. Click **Next** to continue.



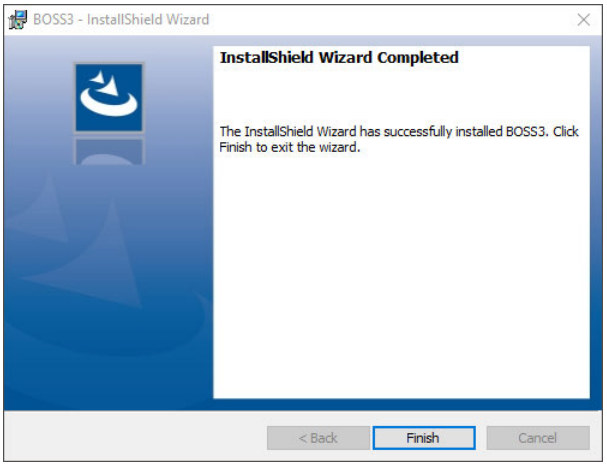


3. Accept the default installation file path or change.
4. Click “Next” to proceed to “Install”





5. When the Installation Complete message is displayed, click **Finish** to proceed to the Licensing.

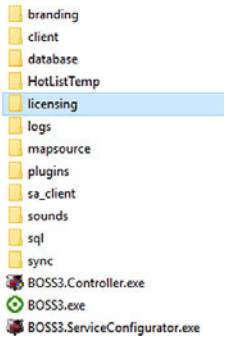


17.2 License Key Management

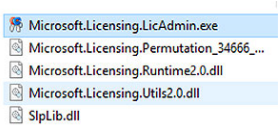
17.2.1 Activating the License Key

Following a new installation, a valid BOSS license key must be entered. There are three options available discussed in the sections below that can be used to activate the license. For upgrades or reinstallation on same server this step is not required as the licensing tool will automagical re-acquire the licensing code.

1. Navigate to the licensing folder in the BOSS3 installation folder.



2. Start Microsoft License Manager (Microsoft.Licensing.LicAdmin.exe). This must be run as an Administrator.



3. In the License Manager User interface, select **File → Activation Wizard** to install the new license
4. When the Activation Wizard dialog opens select one of the following:
   a. I want to activate the software over the Internet. *See Section 17.2.1.1.*

   or

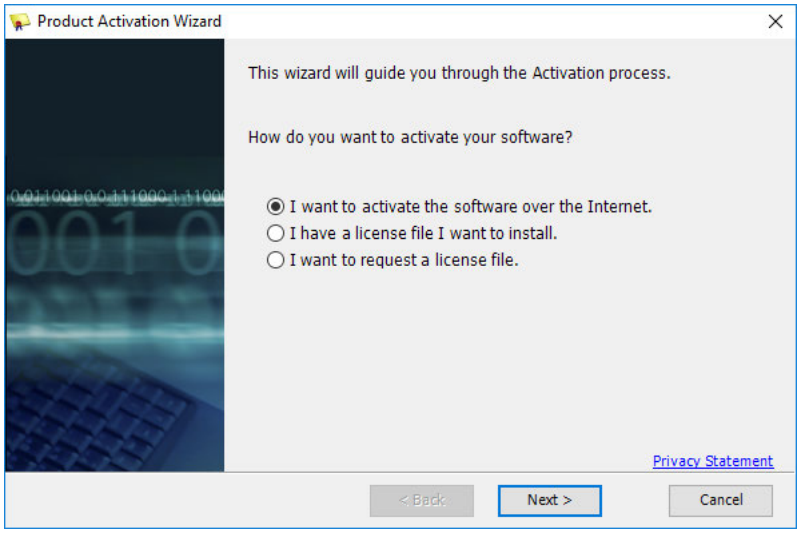
   b. I have a license file I want to install. *See Section 17.2.1.2.*

   or

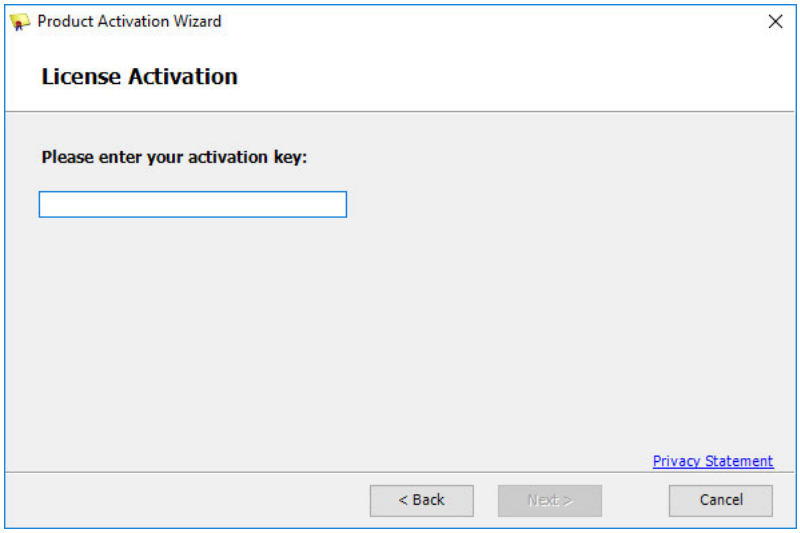
   c. I want to request a license file. *See Section 17.2.1.3.*

17.2.1.1 Activating the License Key over the Internet

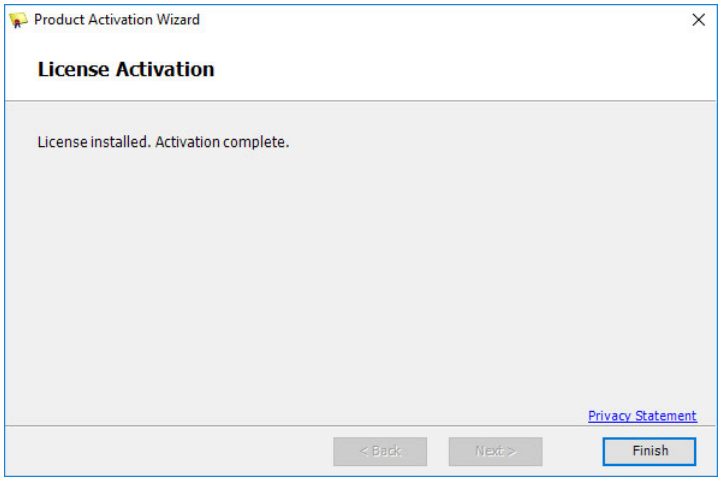
1. Check **I want to activate the software** over the Internet.
2. Click **Next** to continue.



3. Enter the activation key provided by PIPS and click **Next**.



4. The license key will be activated over the Internet. The following screen will display. Click **Finish** to continue.



17.2.1.2 Activating the Software with a License File

1. Check I have a license file I want to install.
2. Click **Next** to continue.
3. Navigate to the location of the license file and select it.
4. Click **Next** to continue.
5. When the activation is completed click **Finish**.

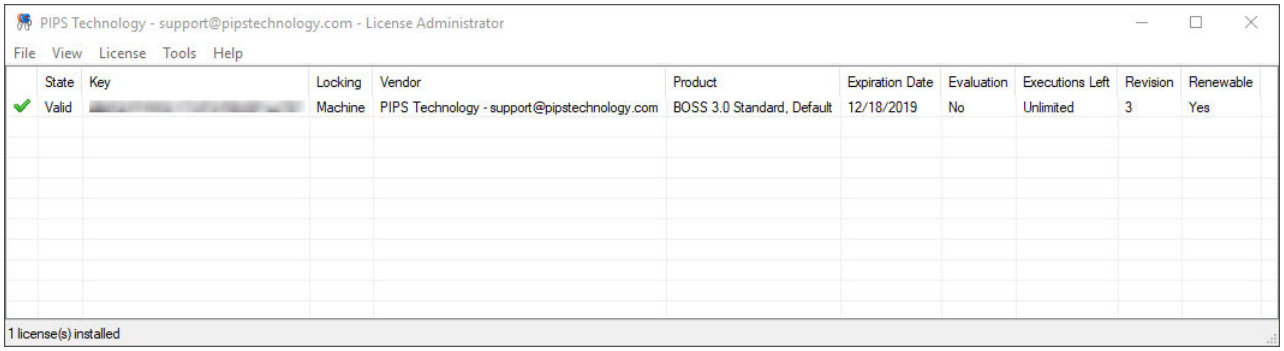
17.2.1.3 Request a License File to Activate the License

1. Click **I want to request a license file**. Press Next.
2. Enter the license key you received previously. Press **Next**.
3. In the screen that displays, copy the text block highlighted (starts with "—BEGIN Request") to the clipboard and paste it into an email. Send the email to PIPS Technical Support (support@pipstechnology.com).
4. Close the Activation Wizard by clicking the **Finish** button.
5. You will be sent an activation file via email. Extract the license file (*.bin) and copy it to a folder on the computer where BOSS is installed. Return to Section 17.2.2 and follow the steps to activate the license.

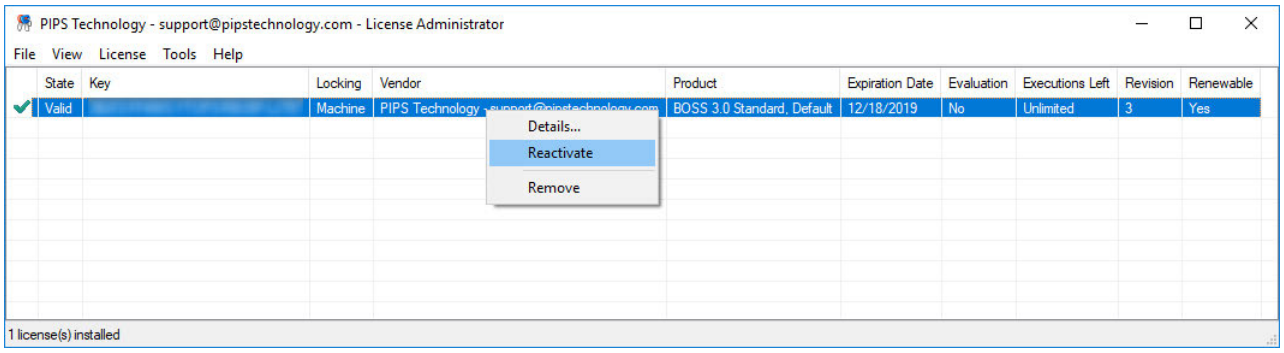
17.2.2 Updating a License Key

If the BOSS license key becomes invalid, or if the license is upgraded, follow these steps to reactivate a BOSS license key:

1. Start Windows Explorer on the BOSS server.
2. Navigate to the folder where the BOSS server application is installed (by default C:\Program Files\PIPS Technology, Inc\BOSS3).
3. Locate the licensing folder as described in Section 17.2.1.
4. Open the folder and right click on the application Microsoft.Licensing.LicAdmin.exe. Select to run as the Administrator. You will see the following screen:



5. Select the license key. Right-click, and from the context menu, select Reactivate.



6. Click Next.
7. When the Installation Complete message is displayed, click Finish.

17.3 Map Display Options with BOSS

BOSS can display collected plate read information plotted on a map. There are two different mechanisms for displaying maps within the BOSS Smart Client application.

17.3.1 U.S. Census Bureau TIGER Maps

U.S Census Bureau TIGER Maps now discontinued.

17.3.2 Advanced Mapping with Internet Maps

PIPS provides an option to purchase an "Advanced Mapping" feature with BOSS. This option enables integration of Maps, an Internet-based service that BOSS can use to display maps in the Smart Client application.

Note: In order to use Advanced Mapping, the BOSS Smart Client will need an unimpeded Internet connection.

17.4 Configuring the BOSS Server Application

After the BOSS installation is completed, the application must be configured using the BOSS Controller program. The following sections explain how to use this program as well as the configuration settings that are available.

17.4.1 The BOSS Controller Application

17.4.1.1 Starting the Boss Controller

BOSS Controller (BOSS3.Controller.exe) is the application used to configure and control the BOSS service. The BOSS Controller is installed on the server computer along with the server application. After the installation is complete the Controller program will start automatically. If this is a new installation the license will need to be activated first. Choose to configure BOSS at a later time by clicking on Cancel.

The shortcut to the BOSS Controller program can be found on the desktop or in the All Programs → PIPS Technology → BOSS3 menu. Right-click on the Controller icon and select Run As Administrator. When the BOSS Controller program is started an icon for the application will appear in the Windows System Tray at the lower right corner of the desktop.

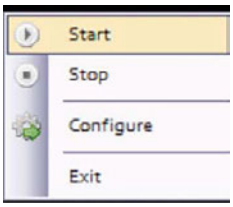


17.4.1.2 Status Colors

The icon for the Controller program includes a "traffic light" that uses a color indicator to show the status of the BOSS service application. When the BOSS service application is running, the indicator is green. When the BOSS service application is not running, the indicator is red. Yellow color indicates that the application is changing state (starting or stopping).

17.4.1.3 Right-Click Menu

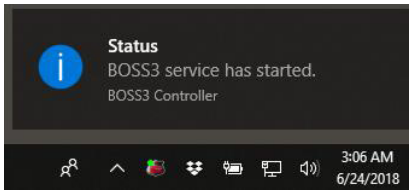
When you right-click the BOSS Controller System Tray icon, a pop-up menu will appear:



Start	Start the BOSS service.
Stop	Stop the BOSS service.
Configure	Present the BOSS Configuration Wizard.
Exit	Close the BOSS Controller application. (Note: This closes the BOSS Controller program, but does not stop the BOSS Service.)

17.4.1.4 Starting the BOSS Service

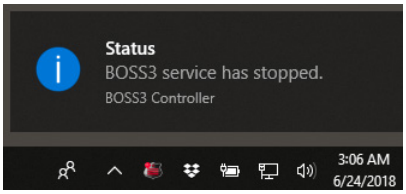
When the **Start** action is selected, and the service starts successfully, a Success message will be displayed:



The traffic light in the BOSS Controller icon will turn green to indicate the status.

17.4.1.5 Stopping the BOSS Service

When the **Stop** action is selected, and the service stops successfully, another Success message will be displayed, and the traffic light changes to red:

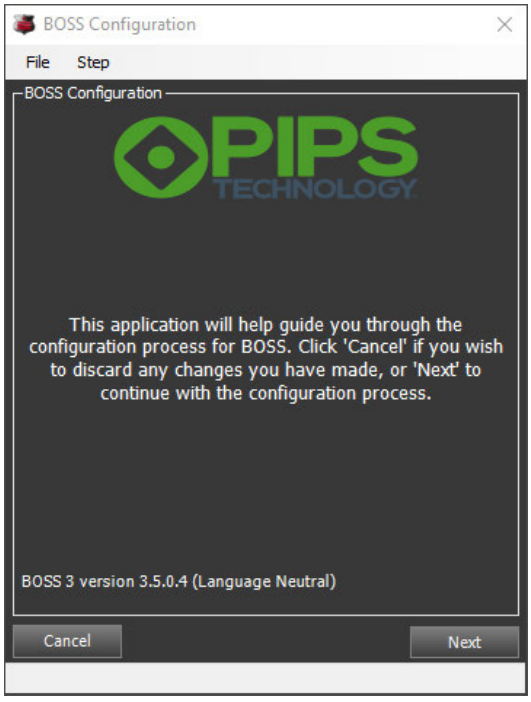


17.4.2 BOSS Configuration

17.4.2.1 Activating the Configuration Wizard

1. Right-click the **Controller System Tray** icon.
2. Select the **Configure** option. The Configuration Wizard options are explained in the following sections.

17.4.2.2 BOSS Configuration Wizard



Step through all configuration screens in the BOSS Configuration Wizard by simply clicking the **Next** button on this first screen. Click **Next** on each subsequent screen after entering in the desired settings. Note: This step-by-step process is recommended when you are configuring the system for the first time.

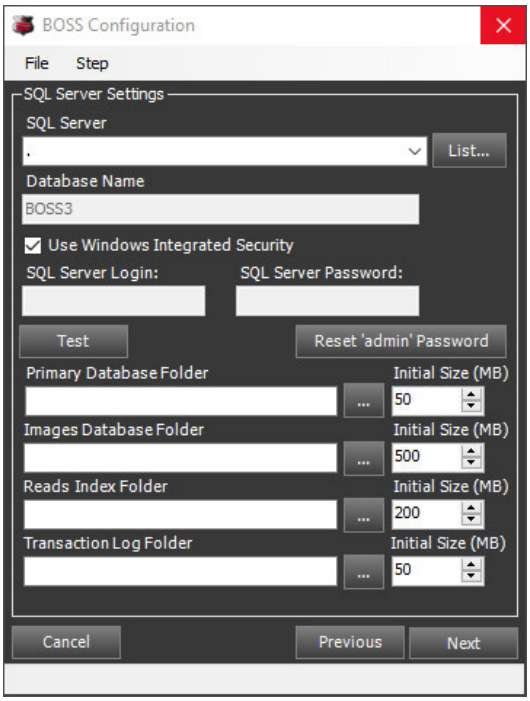
OR

Click the **Step** menu option to access the configuration menu and proceed to the step choice.

For each configuration step (described in Sections 17.4.2.3 – 17.4.2.9), clicking **Next** will take you to the next configuration screen, clicking **Previous** will take you to the previous one, and clicking Cancel will clear any changes you have made on the current screen.

17.4.2.3 SQL Server Configuration

SQL Server configuration is required for a new BOSS system, in order to specify the location and necessary authentication information for the SQL database.

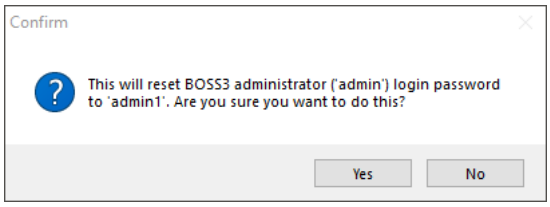


SQL Server – Select the SQL Server instance for BOSS. Press **List** to choose from a list of available SQL Servers. The SQL Server Browser service must be running at this point. You may also type in the server IP address or host name. Enter a dot "." to use a local SQL Server that is running on the same machine as the BOSS service.
Use Windows Integrated Security – If checked, BOSS will use Windows Integrated Security to access the SQL Server database.
SQL Server Login and SQL Server Password – If Windows Integrated Security is not selected, enter the SQL Server username and password provided for BOSS to use to access the database.
Test – The **Test** button can be used to test the SQL Server settings currently in place. The Test button initiates a connection. A message box will appear to indicate whether the test connection fails or succeeds.
Database file locations: BOSS database can be divided among multiple locations as follows if necessary. When selecting a folder path for the database files keep in-mind that the folder path is referenced from the standpoint of the SQL server location.
Primary Database Folder – The drive and folder where the BOSS primary database will reside.
Images Database Folder – The drive and folder where the BOSS will store images.
Reads Index Folder – The drive and folder where BOSS will store database indices for stored plate reads.
Transaction Log Folder – The drive and folder where BOSS will store the database transaction log file.
Initial Database Sizes - By Default Boss will predefines the sizes as indicated in the controller.



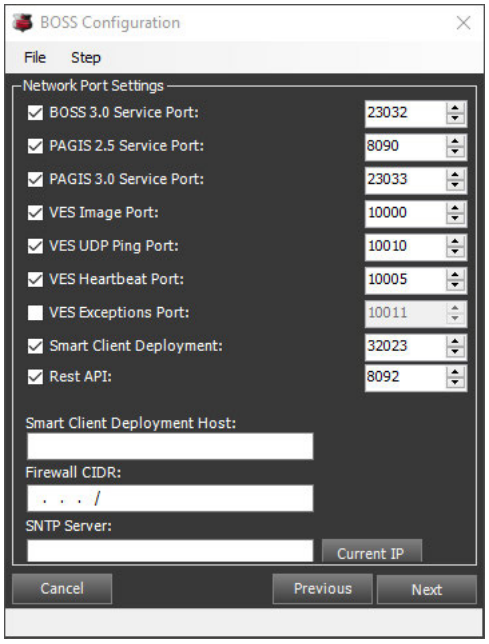
17.4.2.4 Resetting the Administrator Password

If you have forgotten the BOSS administrator (admin) password, you can press the **Reset 'admin' password** button to reset the password to "admin1."



Pressing **Yes** will immediately reset the password.

17.4.2.5 Network Port Settings



BOSS uses a number of TCP/IP and UDP network ports for communication between server and client applications and server and license plate reading devices.

17.4.2.5 Network Port Settings (continued)

FIELD	DESCRIPTION	DEFAULT PORT
BOSS 3.0 Service Port	TCP/IP port used to provide access for BOSS Smart Clients	**23032**
PAGIS 2.5 Service Port	TCP/IP port used to provide access for older mobile client versions older than Pagis 2.6.8	**8090**
PAGIS 3.0 Service Port	TCP/IP port used to provide access to various mobile client versions	**23033**
VES Image Port	TCP/IP port used to receive reads from fixed cameras	**10000**
VES UDP Ping Port	UDP port used to receive keep alive ping messages from fixed cameras	**10010**
VES Heartbeat Port	TCP/IP port used to receive heartbeat status messages from fixed cameras	**10005**
VES Exceptions Port	TCP/IP port used to receive exceptions messages from fixed cameras	**10011**
Smart Client Deployment	TCP/IP port used for BOSS client installations via BOSS server	**32023**
REST API Port	HTML port used for the communication between the BOSS service and newer versions of PAGIS	**8092**

If the checkbox in front of the port name is left unchecked, the corresponding connection will be disabled.

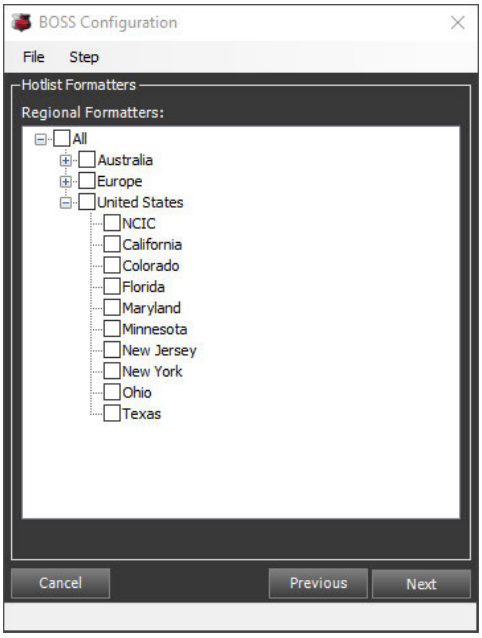
Smart Client Deployment Host – If this information is entered, BOSS Smart Clients will use the given hostname to distribute the smart client application. This can be left blank to use the local host name.

Firewall CIDR – BOSS provides a built-in firewall for incoming fixed camera connections. If a value is entered, only cameras with an IP address matching the CIDR will be allowed to connect. CIDR (Classless Inter-Domain Routing) is a standard industry method for specifying a range of included IP addresses. The format of the CIDR entry is A.B.C.D/N, in which the dotted decimal portion before the "/" is interpreted, like an IPv4 address, as a 32-bit binary number that has been broken into four octets. The value of N indicates the number of shared initial bits, counting from the left-hand side of the address.

For Example: For an entry of 10.200.200.255/24, the CIDR value 24 leaves 8 bits that can be changed. Therefore, addresses 10.200.200.x are permitted addresses.

SNTP Server – BOSS has a built-in time service. The fixed ANPR/ALPR cameras do not support automatic daylight savings time (DST) adjustment. The BOSS time service provides a customized SNTP service for these cameras in order to support DST. To use the built-in time service, Windows Time Service has to be disabled in the Services Control panel, and the BOSS time server IP address entered in this field.

17.4.2.6 Regional Hotlist Formatters

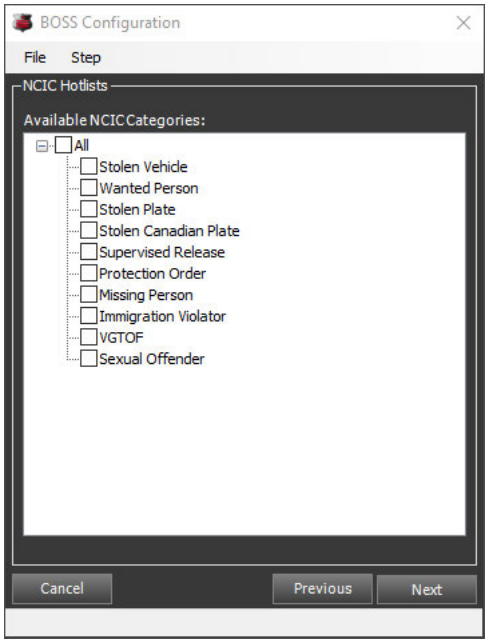


The BOSS allows the selection of predefined hotlist formatters. These formatters define the input format (structure) of hotlist data files. Custom formatters can be defined via the BOSS Smart Client application *(see Section 13 of this manual for more information)*. Also, when installing BOSS in the United States, National Crime Information Center (NCIC) data formatters can be selected for specific states (see section following).

To select or unselect formatters, click on the formatter title to add or remove a check mark. Additional formatters can be added to a system as needed. These will be provided by PIPS Technical Support upon request.

17.4.2.7 NCIC Hotlist Formatters

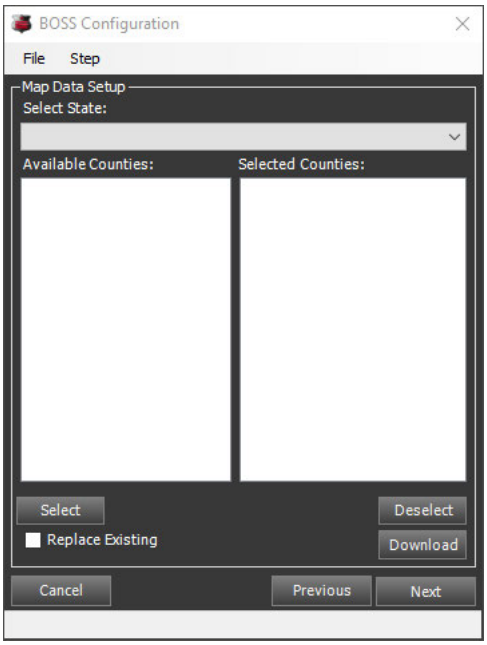
BOSS supports hotlist import in the United States National Crime Information Center data format. This option is available only in the United States.



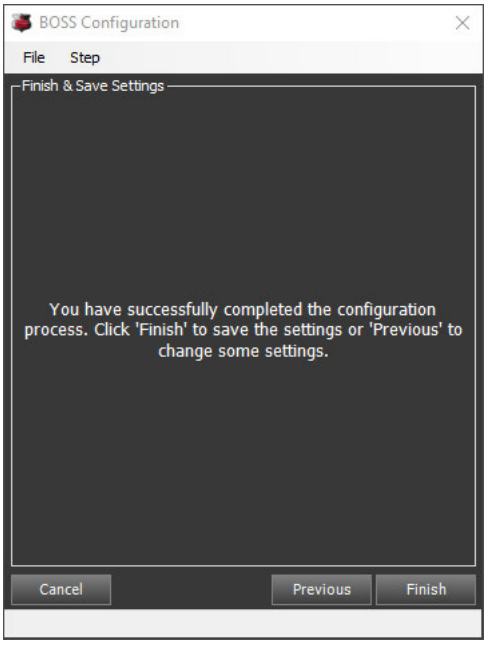
To configure formatters for the desired categories, check those categories. Once the desired categories have been selected, press **Next** to proceed.

17.4.2.8 Map Data Setup

U.S Census Bureau TIGER Maps now discontinued. Do not utilize this section, click “Next”



17.4.2.9 Finishing Configuration



Click **Finish** to complete configuration. BOSS will save the chosen configuration.

17.5 Installing the BOSSUI Smart Client Application

17.5.1 Installation over the Web

To initiate a web installation on a workstation, start up Microsoft Internet Explorer and navigate to this web address: **http://{boss_server_ IP_address}:32023/publish.htm**, where {boss_server_IP_address} is the address of the server running the BOSS server application.

For Example: To install the Smart Client on the BOSS server itself, navigate to http://127.0.0.1:32023/publish.htm. The installation webpage will be presented. The advantage of installing the Smart Client over a web browser is that the application will automatically check for updated versions every time it is started.

17.5.2 Stand-Alone Installation

The BOSS Smart Client is a zero-administration desktop application meant for administration of the BOSS server application and querying data collected in the BOSS database as described in this manual. The BOSS Smart Client is installed as a single executable program. This program can be copied to any Windows workstation, or to a shared network drive.

To install the stand-alone application:

1. Start Windows Explorer on the BOSS server.
2. Navigate to the folder where the BOSS server application is installed (**by default C:\Program Files\PIPS Technology, Inc\BOSS3**)
3. Locate folder **sa_client.**
4. Copy the **sa_client** folder to the workstation or shared network folder of choice.

17.6 Configuring Client Tools

Client Tools is used to transfer any files needed during an Pagis shift from BOSS to an Pagis system that is being run in the Disk Sync mode. *See Section 13, Client Tools, and the Pagis Software User's Manual.*

Client Tools does not have a customary interface. Once the utility is started, the Client Tools icon will appear in the Windows System Tray. Before use, Client Tools must be configured and can be quickly completed with the simple configuration wizard provided:

1. To start the wizard, right-click the icon and select **Configure**. The initial screen provides information about the tool.
2. Click **Next** to continue the configuration, or **Cancel** to exit the wizard.
3. Enter a path so that Client Tools knows where to store the files it creates and where to look for files to process. This path can be a local, network, or external drive. Enter the path or click on the … button and browse to the location.
4. If the Begin Shift files that Client Tools creates need to be encrypted, click **Encrypt Output**. Click **Previous** to return to the previous screen, or click **Next** to continue.
5. The data used to create the Begin Shift files is created and managed in BOSS. Client Tools needs to know where the BOSS Server is located. Enter the server IP and the port to use to connect to it. Click **Previous** to return to the previous screen, or click **Next** to continue.
6. The final screen provides additional information on how to use the wizard. Click **Previous** to return to the previous screen, or click **Finish** to save the changes and exit.

Common Issues

Missing Permissions on the database user

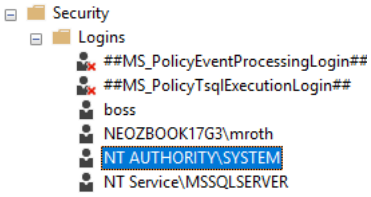
PIPS Boss service does not start: If the service does not start after two tries, go to the logs file located in "C:\Program files(x86)\PIPS Technology, Inc\BOSS3\logs", there look for the following message:

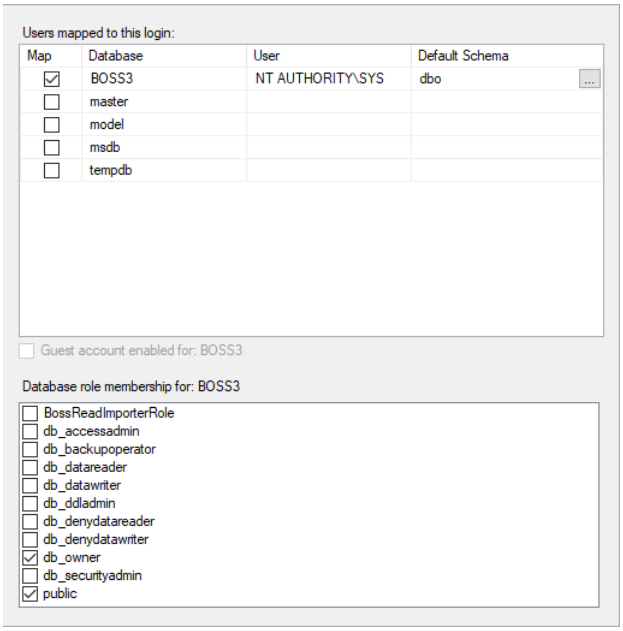
a. The server principal "user" is not able to access the database "BOSS3" under the current security context:
This problem is caused by missing permissions in the database user you are using.
To fix this problem you need to go to the Microsoft SQL Server Management Studio application and connect with a user with sysadmin privileges, inside the object explorer expand the folder Security, within the logins folder identify your user, right click on the user and select Properties. Inside "Server Roles" mark the sysadmin box.
After this restart the BOSS service.

The Underlying Provider failed

When a read query is made, the application shows the message **The Underlying Provider failed**

a. Inside the logs file, look for the line with the message "Login failed for user" identify the user, example- "Login failed for user 'NT AUTHORITY\SYSTEM". If this occurs log into SQL Studio Manager and map the BOSS3 Db to that account, also add the membership role of "db_owner" to the account.





Failed login

Check that the service is running, and the credentials are valid, also, check the server configurations, if you have localhost instead of 127.0.0.1 replace it for 127.0.0.1. If the problem persists go to the logs file and identify the error and contact PIPS customer support support@pipstechnology.com.

Relocating BOSS3 database

- When an upgrade requires you to move your existing BOSS3 database to a new location follow the recommend step in our "PIPS Relocate Boss Data Files" document for step by step instructions.

18 Appendix: Troubleshooting

When troubleshooting an issue, always start by looking for error messages in the Server log file, usually found at ...\PIPS Technology, Inc\ BOSS3\logs\BOSSServerLog.txt. Proceed based on the following information, recognizing that escalation may be necessary. If so, obtain a copy of the complete error message and include it with all escalated documentation.

ISSUE REPORTED	EXPLANATION	STEPS TO CORRECT
Just after an installation/upgrade, the UI won't start.	It takes several moments for the BOSS Server to be completely started and ready for information to be accessed.	After starting the BOSS server, wait for several moments before attempting to start the UI. If this is an upgrade this could be several minutes while the database is being updated.
I start the BOSS Controller, but it stops a moment later. The following error message may display "Error: Error in BOSS3 Controller. Please check the log files." (New installation scenario)	The license was not activated. When checking the BOSS Server Log, there will be two error messages : – 'Licensed for 0 concurrent clients' and – 'Failed to set registry parameter [_tmpbaliked a63] to value System.Byte[].'	Return to the licensing activation and updating checklist. (*See Section 17.2, BOSS Version 3.2 and Above License Key Management.*)
I start the BOSS Controller, but it stops a moment later. The following error message may display "Error: Error in BOSS3 Controller. Please check the log files." (Upgrade scenario)	The Upgrade Tool must be run before starting the Controller.	Run the Upgrade Tool. (*See Section 17.7 The BOSS Upgrade Tool.*)
I start the BOSS Controller, but it stops a moment later. The following error message may display "Error: Error in BOSS3 Controller. Please check the log files." (Other scenario)	If the Upgrade Tool has been run, there may be a problem with the database.	Look for error messages in the BOSS Server Log. Provide this information to Technical Support.
A fixed camera won't connect.	The firewall could be blocking the communications.	Ensure that the firewall is allowing communications through the VES ports, found in the BOSS Configuration Controller on the Ports screen.
PAGIS won't connect.	The firewall could be blocking the communications.	– Ensure that the firewall is allowing communications through the REST API (for PAGIS 2.7.x) and PAGIS 3.0 Service (for versions of PAGIS) ports, found in the BOSS Configuration Controller on the Ports screen. – Ensure that the device has been enabled in the BOSS UI Devices screen.
Hotlist will not update.	There is typically a problem with the source file.	– If it is a network hotlist, ensure that the site can be reached by entering the address in a browser. – If a local hotlist, ensure that the file is on the system and can be opened.
The NCIC Hotlist formatter that I need is not available. (New installation scenario)	The NCIC formatters were not added during the initial installation.	Stop the BOSS Service. Go to the Configure option on the BOSS Controller. Step to the NCIC screen. Select the desired NCIC formatters. Click **Save** and exit. Restart the BOSS Service. The formatters will now be available.

ISSUE REPORTED	EXPLANATION	STEPS TO CORRECT
I am unable to see reads/hits in the Dispatch screen.	The time on the read/hit coming in must be relatively close, within a couple of minutes, to the BOSS server time.	For a mobile ALPR system, correct the time on the laptop or ALPR processor. A fixed camera can be configured to use a time server. If issue persists, the server that BOSS is running on could also be configured to sync with a time server.
An error message, "Compressed method not supported," was found in the BOSS Server Log.	There are various reasons that this message can occur.	Obtain a copy of the complete error message. Provide this information to Technical Support.
An error message, "Transaction has aborted," was found in the BOSS Server Log.	There are various reasons that this message can occur.	Obtain a copy of the complete error message. Provide this information to Technical Support.
An error message. "Error #nn appeared in the db for Stored Procedure xxxx on line nn." was found in the BOSS Server Log.	An error occurred when running the stored procedure listed in the message.	Obtain a copy of the complete error message. Provide this information to Technical Support.
An error message, "Timeout expired. The timeout period elapsed prior to completion of the operation or the server is not responding," was found in the BOSS Server Log.	A SQL timeout error has occurred.	Obtain a copy of the complete error message. Provide this information to Technical Support.
An error message, "SNTP server not started, could not bind to InterNetwork 0.0.0.0:123," was found in the BOSS Server Log.	This is an expected error message that occurs when BOSS has not been configured to access a time server.	If no time server has been configured, this message can be ignored. If one has been configured, this needs to be escalated for further assistance.
After a new installation, the BOSS server stops running with an error message, "Failed in working with the database. Ensure connectivity is properly defined. Try running the BOSS Controller again and checking settings," was found in the BOSS Server Log.	When BOSS was started, there was a connection issue between it and the SQL Server.	Start by checking the information in the Controller. If that is all correct, then check to ensure that the SQL Server is running. If no issues are found there contact Technical Support Obtain a copy of the complete error message.
After a new installation, the BOSS Server stops with no error message in the BOSS Server Log.	The server needs to be run with Administrator privileges.	The server should be restarted in the Console as an Administrator. If running BOSS as a service then the BOSS Controller must be run as Administrator.
Error message in BOSS Server Log says that the file "httpconfig.exe" cannot be found.	This is an error that can occur when the system has not been updated in some time. It has been seen for other uncertain reasons as well.	Obtain a copy of the complete error message. Provide this information to Technical Support.
After a new installation, the BOSS Server starts but stops moments later. The BOSS Server Log contains the error message. "The system cannot find the file specified Additional Exception Message: Unhandled exception from 'Name:BOSS3.exe. There are no context policies." However, no file is listed in the message.	This typically occurs on older systems, especially Windows Server 2003, or systems that have not been updated for a while.	The file httpcfg.exe needs to be copied into the c\Windows\System32 directory.
The BOSS Server won't start, and there is an error message, "Transport Manager failed to listen on the supplied UIR using the NetTcpPortSharing service: failed to start the service because it is disabled," in the BOSS Server Log.	The NetTcpPortSharing Service is not running.	Obtain a copy of the complete error message. Provide this information to Technical Support.
The BOSS server stops running, and there is an error message, "Cannot open database "<Database Name>," in the BOSS Server Log.	There is an issue with the connection between the BOSS server and the SQL Server.	Start by checking the information in the Controller. If correct, then check to ensure that the SQL Server is running. If no issues are found contact Technical Support. Obtain a copy of the complete error message.

ISSUE REPORTED	EXPLANATION	STEPS TO CORRECT
The BOSS Server won't start and there is an error message "A file activation error occurred. The physical file name '<filename>' may be incorrect." in the BOSS Server Log.	There could be multiple reasons, but it is probably due to a database connection issue.	Obtain a copy of the complete error message. Provide this information to Technical Support.
When running the upgrade tool, an error message is displayed. A message is included in the BOSS Server Log: "Current upgrade state: One of the upgrade scripts failed to run as expected. Please contact support for direction."	This most likely occurred due to upgrading from an old version of BOSS.	Obtain a copy of the complete error message. Provide this information to Technical Support.
An unexpected response or behavior occurs in BOSS, and there is an error message, "Object reference not set to an instance of an object," in the BOSS Server Log.	This is a generic error message that can occur for various reasons.	Unless the issue has an obvious cause contact Technical Support. Obtain a copy of the complete error message.
The following error message, "Discarding tmp buffer because it's corrupted," has been found in the BOSS Server Log.	This message is associated with a database issue.	Obtain a copy of the complete error message. Provide the information to Technical Support.
The following error message, "SMTP server is not defined, email alerts disabled," has been found in the BOSS Server Log.	This message is informational indicating, as it states, that an email server has not been configured.	If attempts have been made to configure an email server and this error message occurs, recheck the settings and the server. If the error remains contact Technical Support.
The BOSS Service stops running, and the BOSS UI indicates that the server is not available. The following error message, "Cannot access a disposed object," is found in the BOSS UI Log.	This is an informational message provided by the UI confirming that it is no longer able to communicate with the BOSS server.	Restart the BOSS server and the BOSS UI will reconnect. If this does not correct the issue contact Technical Support.
The following error message, "The socket connection was aborted," is found in the BOSS UI Log.	This is an informational message provided by the UI confirming that it is no longer able to communicate with the BOSS server.	Restart the BOSS server, and the BOSS UI will reconnect. If this does not correct the issue contact Technical Support.
A problem occurs while adding a hotlist and the following error message "Invalid object name '<hotlist name here>'," has been found in the BOSS Server Log.	This indicates that there is an issue with the hotlist formatter being used.	Confirm that the correct formatter is being used. If so, confirm the source file is formatted correctly. If so, contact Technical Support. Provide a copy of the full error message.
While installing BOSS, an error message displays: "Error opening file for writing: <File Name>."	This indicates that the application listed in the error message is still running.	Check the Windows System Tray for any BOSS applications still running on the system. Close the application(s) and continue the installation.
The BOSS applications are installed under one user, but are not found when another user logs in.	The application was not installed using administrative privileges.	The application will need to be uninstalled and reinstalled using administrative privileges.
While using Client Tools to create Begin Shift files, an error message displays: "Client has not been activated on the server."	Mobile devices must be enabled on BOSS to synchronize data to it. This message is displayed the first time that Client Tools is used to create Begin Shift files because it has not been enabled yet.	Configure Client Tools on BOSS (see Section 17.6) so that BOSS adds Client Tools as a device.
When using Client Tools to synchronize End Shift files to BOSS, the following error message displays: "Error: Could not find <file and path name>."	Client Tools was unable to find the End Shift files to be processed at the defined path.	Check that the location assigned for the End Shift file matches the location chosen when Client Tools was configured. If it does not, move the file to the configured location.

19 Appendix: Plug-Ins

BOSS allows the use of third-party code via a plug-in that serves the needs of BOSS customers with specific data requirements. Once a plug- in is created and compiled, a copy of the DLL and any other necessary files can be copied to the plug-ins directory under BOSS. BOSS will automatically detect the existence of the plug-in at that point and permit reads to be passed to the ReceiveData method of your plug-in.

The functions of the currently available BOSS plug-ins are described in Sections 19.1 and 19.2. For more information and guidance on installing a plug-in, contact PIPS Technical Support for guidance.

19.1 The BOSS Truck Drayage Utility

Regulation of diesel-fueled heavy-duty trucks and a Drayage Truck Registry (DTR) were implemented by the California Air Resources Board (ARB) to help reduce both emissions from these vehicles and public exposure to contaminants in those emissions. Drayage trucks subject to regulation (Class 7 and Class 8) are registered and information about them is maintained on an ARB web service.

The Truck Drayage Utility is BOSS plug-in that provides access to the ARB web service. The utility is designed to contact the web service, retrieve data, and add it to a comma-separated values file. In BOSS, the Hotlist Administrator will then create a whitelist that uses this CSV file as the source file.

The connection to the ARB web service (managed by the Windows Task Scheduler) can be made once daily for a full download of the data, with subsequent connections allowed no more frequently then every 30 minutes for updates. This whitelist can then be deployed to a mobile or fixed camera in the monitored area. If a plate is read that is not included on the whitelist, a notification will be displayed in BOSS. Appropriate action can be taken at that time.

If the ARB web service is unavailable and downloads cannot be completed, the BOSS whitelist will not be updated. There will also be warning messages in the BOSS log such as “Could not connect to <web service address>. TCP error code nnnnn: <Error description>.” If this occurs, the utility will try again in 30 minutes. If the errors persist, it may be necessary to seek assistance.

19.2 The BOSS LPRD Plug-in

The BOSS LPRD plug-in relays the reads the BOSS server receives on to the national database at the Automated Regional Justice Information System (ARJIS), a joint powers agency that facilitates information-sharing among more than 70 law enforcement agencies—local, state, and federal—in the two California counties (San Diego and Imperial) that border Mexico. ARJIS operates a secure intranet (ARJISnet) with more than 11,000 users in San Diego County alone.

19.3 The BOSS DEA Plug-in

The BOSS DEA plug-in writes LPR messages to the file system as reads are received by the BOSS server. Those files will then be available for the Drug Enforcement Agency, DEA, File Transporter to act upon.

20 Appendix: BOSS Mantis

The Mantis service adds analytical analyses to new and existing read images within BOSS providing the user the ability to search based on vehicle Type, Brand, Color & Unique markings. BOSS Mantis is an additional PAID service that can be enabled on BOSS versions 3.6.x.x and above, older version of BOSS can support this feature by upgrading, providing they meet the system

20.1 How Dose Mantis Work

The service is hosted in the Amazon Web Services (AWS) Elastic Compute Cloud (EC2) platform, running in instances comprised mainly by Graphics Processing Units (GPUs). The only information sent to the Mantis endpoint is the vehicle image, known as the Overview image by the BOSS. Communication between BOSS and Mantis is performed as a client-server architecture, meaning the Mantis server uses the 443 (https) port to allow clients to reach the Mantis endpoint.

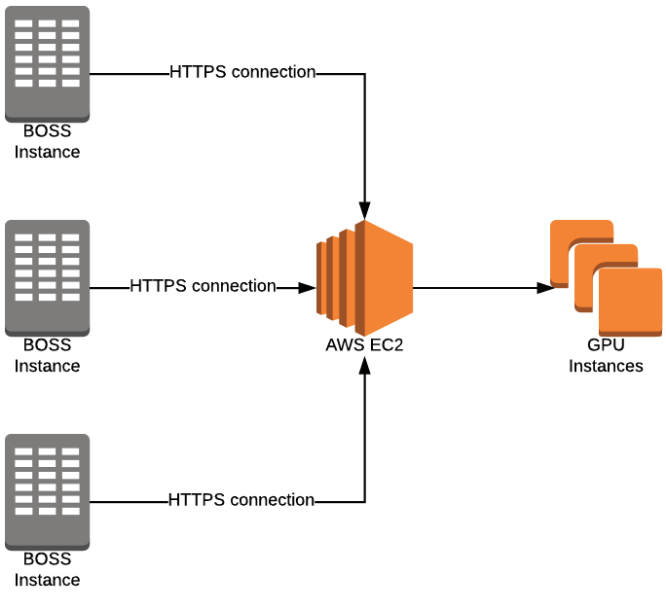


Figure 1 Multiple BOSS instances connected to the Mantis API.:

The information between BOSS and Mantis flows only in one way, this means that only BOSS clients can send data to Mantis, where it will be processed, and a response will be received by the BOSS server. Mantis cannot reach the BOSS Server or perform any kind of operations on the user's behalf over the data stored inside BOSS.

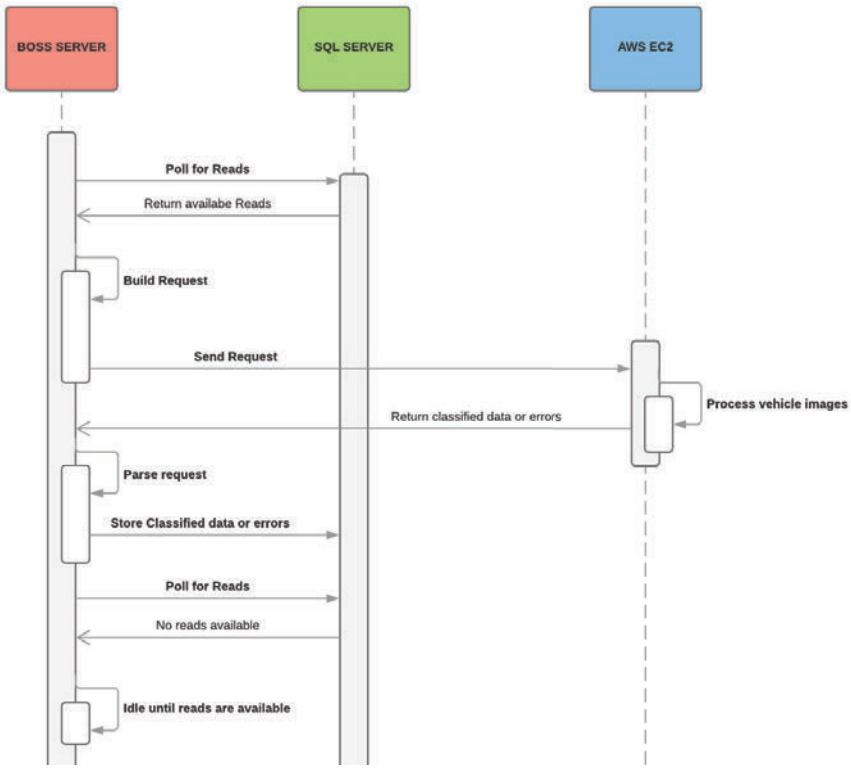


Figure 2 Sequence diagram for the current BOSS-Mantis Integration

20.2 Mantis Security and Encryption

As a summary description for the HTTPS protocol, its security is that of the underlying TLS (Transfer Layer Security) cryptographic protocol, where a certificate is used to authenticate the server, thus, the data flow between the client and the server is encrypted.

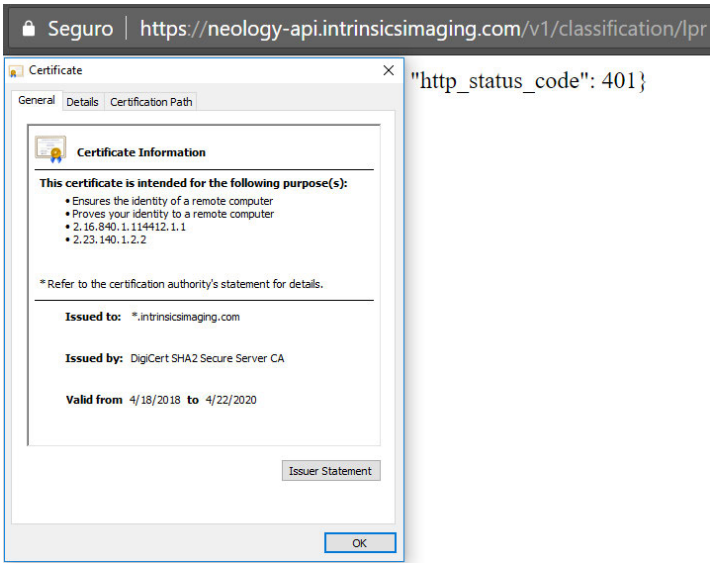


Figure 3 Available details for the certificate on the Mantis-Neology endpoint

20.3 Mantis Requirements

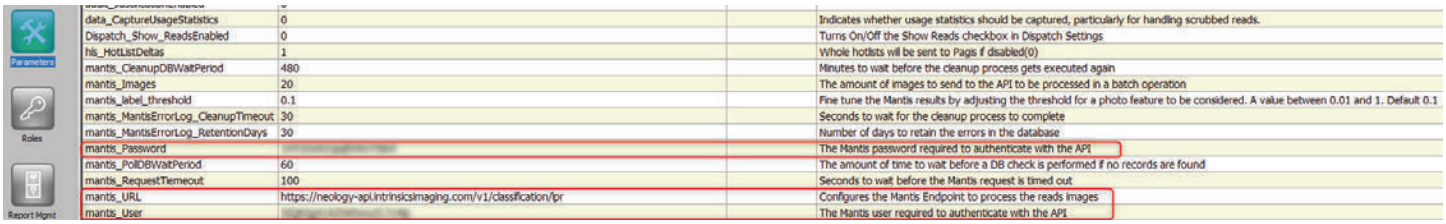
1. BOSS version 3.6 or newer.
2. Open communication to Mantis API URL (https://neology-api.intrinsicsimaging.com/v1/classification/lpr) via port 443.
3. Mantis Licensing feature required.
4. A valid Mantis User name and password. User name and password provided at time of licensing purchase.

20.4 Mantis Installation

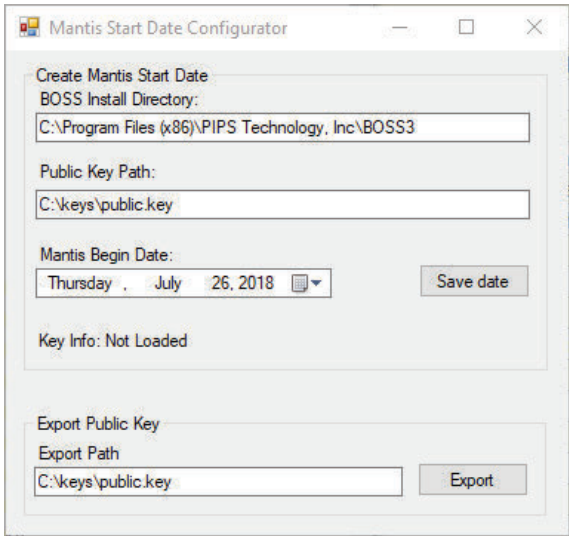
1. To upgrade or install Mantis version of BOSS follow the installation steps provide under Appendix 17. If upgrading from previous BOSS version you will also need to reactive your existing license to reflect the addition of the Mantis feature, see section 17.2.2.
2. Once BOSS is installed or upgraded, start the BOSS service to perform additional Mantis configurations.

20.5 Mantis Configurations

1. Start and login to the BOSS UI, navigate to System > Parameters.
2. In the Attributes table, look for the entries with the following names:
    - **a. mantis_User:** Assign the provided Mantis user name here.
    - **b. mantis_password:** Assign the provided Mantis user password here.
    - **c. mantis_URL:** Set the Mantis URL here. https://neology-api.intrinsicsimaging.com/v1/classification/lpr

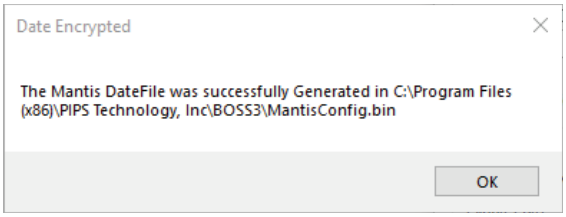


3. Additional parameters can be configured, see Mantis Parameters for details.
4. Once all the entries were assigned their corresponding values, close the BOSS UI and stop the BOSS service.
5. Download and place the “MantisStartDateGenerator.exe” file in the root BOSS3 folder, this executable is sperate from the BOSS installer and will need to be downloaded and placed manually.
6. Start the “MantisStartDateGenerator.exe” utility with administrator permissions.



7. Set the BOSS Install Directory to the Path of the folder where BOSS was installed.:

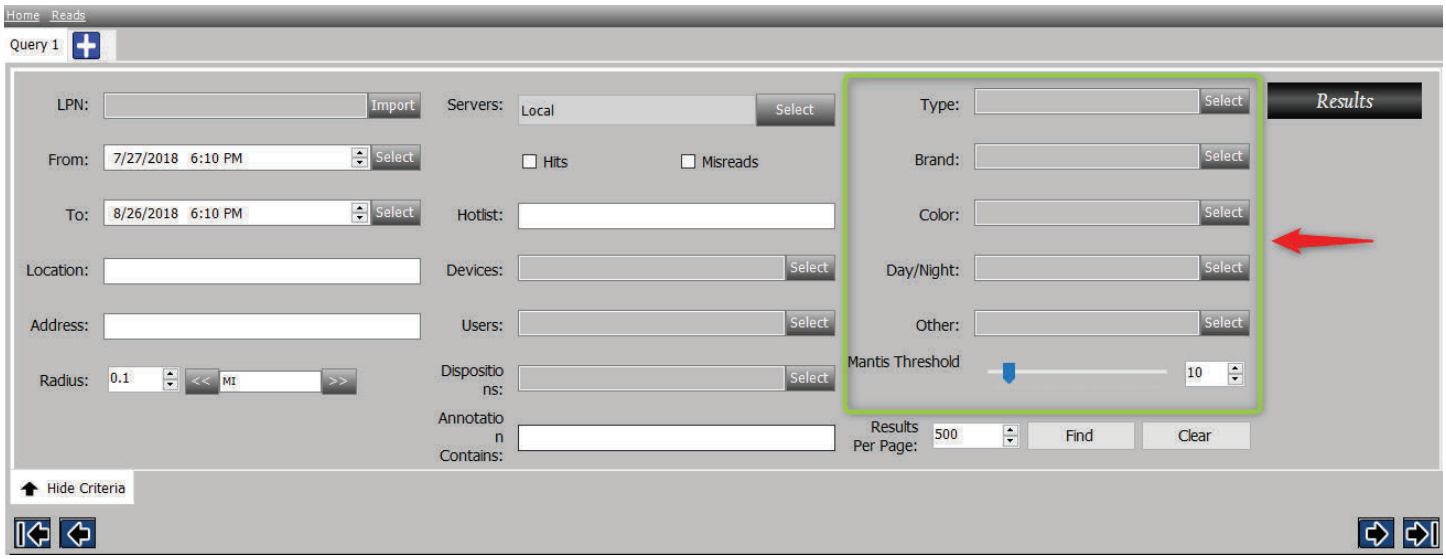
8. Set the Export Public Key path to a folder where you can access the generated public key, then click the Export button, and verify that the key was exported to the path.
9. Select a date that you want Mantis to take as the begin date for reads to be retrieved “Mantis Begin Date”. Reads that entered the system before this date, won’t be processed.
10. Click the Save date button to create the “MantisConfig.bin” file in the installation directory. A message confirming the file creation will appear.



11. Start the BOSS service.
12. When BOSS is started, the existing reads in the BOSS database will be sent to and processed by the Mantis API. The results will be stored on the local database.
13. Start and login to the BOSS UI.

20.6 Mantis Search Features

The Mantis fields should be visible in the right side of the reads panel in the BOSS UI. In case the fields are not available, diagnose the possible problems in the Mantis Configuration Troubleshoot section 20.8.



20.6.1 Mantis Search Definitions

- **Type=** Vehicle configuration style, i.e. Car, Box-Truck, Full-Size-Van, Hatchback, Minivan, Other-Truck, Pickup, Sedan, Suv.
- **Brand=** Vehicle manufacture.
- **Color=** Vehicle primary color.
- **Day/Night=** Vehicle capture in day or night.
- **Other=** Includes additional vehicle identifiers such a roof racks, spare-time, spoiler, ect...
- **Threshold=** Adjust the threshold slide bar to increase or decrease the confidences level of the Mantis search criteria based on selected filters, 1 being the lowest and 100 the highest confidence level available. When threshold is utilized in searches a new “Confidence” column will appear in the results, a user may now use this column to further sort the results by descending or ascending order.

20.7 Additional Mantis Parameters

As a summary description for the HTTPS protocol, its security is that of the underlying TLS (Transfer Layer Security) cryptographic protocol, where a certificate is used to authenticate the server, thus, the data flow between the client and the server is encrypted.

Parameter Name	Description	Default value
mantis_URL	The URL for the Mantis endpoint. The latest value should be available in this document. See Ports configuration for the corresponding value or ask a PIPS Technology representative.	None
mantis_User	Part of the credentials provided, it may be referenced also as the Mantis API key.	None
mantis_Password	Part of the credentials provided, it may be referenced also as the Mantis API password.	None
mantis_Images	The number of images to send to the API to be processed in a batch operation	20 images
mantis_PollDBWaitPeriod	The amount of time to wait before a DB check is performed if no records are found	60 seconds
mantis_RequestTiemeout	Seconds to wait before the Mantis request is timed out	100 seconds
mantis_MantisErrorLog_RetentionDays	Number of days to retain the errors in the database	30 days
mantis_MantisErrorLog_CleanupTimeout	Seconds to wait for the cleanup process to complete	30 seconds
mantis_CleanupDBWaitPeriod	Minutes to wait before the cleanup process gets executed again	480 minutes
mantis_label_threshold	Fine tune the Mantis results by adjusting the threshold for a photo feature to be considered. A value between 0.01 and 1.	10% (0.1)

20.8 Mantis Configuration Troubleshoot

To trouble shoot any Mantis issue, access to the BOSS Server logs is required. The logs are available inside the logs directory, inside the installation folder, e.g. "C:\Program Files (x86)\PIPS Technology, Inc\BOSS3\logs".

Inside this folder, there are two types of outputs:

- **BOSSMantisLog.txt.*:** This files contain Mantis Service specific information.
- **BOSSServerLog.txt.*:** This files contain overall BOSS Server information.

Known errors

L	Level	Error	Description
	INFO	**Mantis Service: Not available**	The Mantis feature was not enabled in the license key with which BOSS was activated
		Solution	Contact a Neology PIPS Technology agent for information on how to request the activation of the feature in your current license key
	INFO	**Mantis configuration not loaded, the service will not be started**	This error signals missing configuration Look for the additional messages described in the following rows.
	ERROR	**Mantis endpoint not configured, shutting down service**	The mantis URL parameter was not set properly, it cannot be a null or empty value.
		Solution	Review the ports configuration and set the mantis URL parameter to the given mantis URL. If you have an outdated version of this document, contact the Neology PIPS Technology support team to get the latest information.

	ERROR	**Mantis credentials are not configured, shutting down service**	Either the mantis_User or the mantis_password parameter was not set.
		Solution	Check that these values do not have a null or empty value. If you were not provided with these credentials, contact the Neology PIPS Technology support team.
	INFO	**Due to a request error, the next Mantis request will be performed in seconds**	There are three known errors related to mantis functionality: • **Mantis Failure**: Mantis failed to process the uploaded information. This error will not be retried because with the same image, Mantis will produce the same output. • **Connection error**: There was a problem establishing a connection with the server. This batch will be retried. • **Mantis Server Error**: An exception was received from the server. This error will be retried.
		Solution	For the above three errors, the possible solutions or actions to take are described below: • **Mantis Failure:** If too many instances of this error appear, contact the support team to diagnose the error. • **Connection error:** Verify that the appropriate rules for the firewall and whitelisting for URL and ports was set. See Mantis requirements for more details. • **Mantis Server Error:** If too many instances of this error appear, contact the support team to diagnose the error.

For a full list of all the messages produced by Mantis and a more detailed explanation about them, see the Mantis Log messages catalog.

20.8.1 Mantis Log Messages Catalog

Below is a description for the messages produced by the Mantis Service. Only applicable messages will have a solution appended to them.

Glossary

Term	Definition
ALPR	Automatic license plate recognition (also called automatic number plate recognition, or ANPR)
Annotation	A note or comment that can be made about and added to a read.
Deployment	The distribution or making available of a hotlist to a device
Device	A source of ALPR data; an PAGIS unit or a fixed or mobile camera
Disposition	The classification of a hit; e.g., a recovered stolen vehicle
Fixed Camera	An ALPR camera permanently mounted above a roadway
Group	A group of BOSS users that belong together administratively
Hit	A match on a plate read against a hotlist
Hotlist	A list or database of license plates of interest, e.g., the NCIC database
Justification	A purpose for running a query on the captured data. There are several justifications included in the system by default. The BOSS Administrator can also create custom justifications to be used.
LPN	License plate number; also known as the Vehicle Plate Number
PAGIS	PIPS™ Mobile Software, the ALPR Mobile application
Local Server	A server running on a local system, in relation to the SQL server or the BOSS UI Misread A read that was marked as a misread by a user
Mobile Unit	An ALPR system with cameras, a mobile processor, and software, such as Pagis Software, installed in a vehicle
Notification	Propagation or delivery of an alert resulting from a hit
Overview	A color image of the vehicle to which the license plate is attached
Patch	A small image of the license plate
Permission	Authorization to access specified functionality in BOSS
Read	A license plate detection event that results in the plate text optical recognition and pictures being taken
Remote Server	A BOSS server that is running in another location
Role	A position, such as Administrator, with the authorization to access specified functionality in BOSS
Site	A group of related devices
Translation	The interpretation from a word in English to a word in a selected language
User	An authorized BOSS user (with a username and password)
Whitelist	In BOSS a whitelist hit is the opposite of a hotlist hit. When a license plate read does not exist in an enabled whitelist database, the same Hits (Alert) screen will be displayed.

For additional information, assistance or maintenance questions please contact Neology ALPR/ANPR Support at:
PHONE: 833-PIPS-LPR (833-747-7577)
• Option 1 for Sales
• Option 2 for Support

For the U.S/Can and all other areas:
Sales Enquiry Email: sales@pipstechnology.com
Support Request Email: support@pipstechnology.com

For Europe, Middle East and Africa:
Sales Enquiry Email: sales@pipstechnology.co.uk
Support Request Email: support@pipstechnology.co.uk

IS A TRADEMARK OF NEOLOGY INC., AND EITHER REGISTERED OR PENDING REGISTRATION IN SEVERAL JURISDICTIONS.

Neology Headquarters San Diego
Address: 12760 Danielson Ct.,
Suite A Poway, CA 92064

Neology UK Ltd
Address:Form 1 Bartley Wood Business Park
Hook, Hampshire
RG27 9UP

Neology México
Plaza Carso II, Lago Zurich No. 219-Piso 10
C.P. 11529 Ciudad de México

	BOSS 4 Annual License Subscription	MANTIS 4-D Vehicle Detection Annual Subscription	Hosted Subscription
BOSS 4 Standard Software Application For either on-premise or Neology Hosted option	x		
Free Periodic SW Enhancements and Maintenance release in line with Neology standard SW release cycle	x		
Unlimited Helpdesk Access for BOSS 4 SW Available from 08:00 to 17:00 Central Standard Time	x		
Vehicle Classification Add-in for all vehicle detections including: - Vehicle Type - Vehicle Brand - Vehicle Feature (Spoiler, roof rails etc) - Vehicle Color -		x	
Enhanced ALPR "Deep Learning" capability enabled on Neology's latest generation Mobile (Golden Eagle) and Fixed (IRIS) Camera		x	
Access to the latest OCR and Vehicle Classification algorithms for all Neology / PIPS legacy devices in line with Neology standard release cycle		x	
Application and Database Server(s) with corresponding network provided on CJIS compliant Infrastructure			x
Elastic Database retention and storage in line with subscription level			x

High Availability and Resilience to ensure 99.999% infrastructure availability with 4 layers of Severity Monitoring (Urgent, High, Medium, Low)			x
Infrastructure Security Monitoring, including annual penetration testing and patching where required			x
Proactive System Health Monitoring (database, application and infrastructure) to pre-empt incidents			x
Service Management reporting on quarterly basis			x
Out of Hours Support for Critical Severity Infrastructure Issues			x

Clear Form

BOSS4 Questionnaire

After completion and submission of this document, the delivery team will review and submit to you the recommended Systems Specifications. Further logistical planning shall proceed after delivery of the initial Systems Specifications.

BOSS4 Server Type		Software Upgrade	
On-Prem: ☐	Hosted (Cloud): ☐	BOSS Upgrade. Yes: ☐ No: ☐	Current BOSS Version:

Customer Information			
Agency Name:		Date:	
Point of Contact Name:			
Email Address:			
Phone Number:			

Items to Migrate When Upgrading					Not Applicable: ☐
Migrate Reads	Yes: ☐	No: ☐	Migrate Hits	Yes: ☐	No: ☐
Migrate Users	Yes: ☐	No: ☐	Migrate Groups	Yes: ☐	No: ☐
Migrate Roles	Yes: ☐	No: ☐	Migrate Devices	Yes: ☐	No: ☐
Migrate Sites	Yes: ☐	No: ☐	Migrate Hotlists	Yes: ☐	No: ☐

Current ALPR Data Statistics			Not Applicable: ☐
Average **Monthly Read** intake.		Average **Yearly Read** intake.	
Current number of **Devices.**		Current number of **Users.**	
Current number of **Hotlists.**		Current Data **Retention Policy.**	

5 Year Projected Growth - ALPR Statistics

Projected read estimates help us ensure the ALPR system specifications are properly configured over time. Example, if the agency currently reads 500,000 plates per month, and growth is expected to double that count in five years, the projected number would be 1,000,000 below.

Projected number of **Reads** per/month.		Projected number of **Devices.**	
Projected number of **Users.**		Projected Data **Retention Policy.**	

Data Integration

Are you planning or are you currently using any kind of third-party application to ingest data from the BOSS database? If so, please provide a detailed explanation of this process.

BOSS4 Cloud
Specifications for Requirements

Cloud Application Servers

Below, there are the minimal recommended configurations for different capacity configurations for BOSS4 hosted on Amazon Web Services infrastructure.

Application Servers Specifications				
Configuration	**Demo**	**Medium**	**Large**	**High Capacity**
ALPR Devices	1 to 3	3 to 50	50 to 150	Beyond 150
Average Daily Intake	Around 30,000 events	Around 500,000 events	Around 1,500,000 events	Beyond 1,500,000 events
Average of users querying data	3 users	15 users	25 users	Beyond 25 users
Alert list averaging	Around 1M records	Around 2M records	Around 2M records	Around 2M records
EC2 AWS Instances for Microservices	t3.small 2.5GHz Intel 2 cores 2 GB RAM Amazon Linux	t3.large 2.5GHz Intel 2 cores 8 GB RAM Amazon Linux	t3.xlarge 2.5GHz Intel 4 cores 16 GB RAM Amazon Linux	t3.2xlarge 2.5GHz Intel 5 cores 32 GB RAM Amazon Linux
EC2 AWS Instance for Controller	t2.small 3.3GHz Intel 1 core 2GB RAM Amazon Linux	t2.large 3.0GHz Intel 2 cores 8GB RAM Amazon Linux	t2.xlarge 3.0GHz Intel 4 cores 16GB RAM Amazon Linux	t2.2xlarge 3.0GHz Intel 8 cores 32GB RAM Amazon Linux
Fargate AWS Instance for Microservices	3.3GHz Intel 5 cores 8GB RAM	3.0GHz Intel 16 cores 32GB RAM	3.0GHz Intel 32 cores 32GB RAM	3.0GHz Intel 48 cores 128 GB RAM
Storage and Application Space	Amazon EBS gp2 SSD 128GB	Amazon EBS io1 SSD 256GB	Amazon EBS io1 SSD 320GB	Amazon EBS io1 SSD 512GB

This document and its contents are intended for the recipient only. Copying, redistributing, or discussing with any other party outside of the intended recipient and Neology is prohibited.

Cloud Database Service

BOSS4 uses the MongoDB engine.

Database Service Specifications				
Configuration	**Demo**	**Medium**	**Large**	**High Capacity**
ALPR Devices	1 to 3	3 to 50	50 to 150	Beyond 150
Average Daily Intake	Around 30,000 events	Around 500,000 events	Around 1,500,000 events	Beyond 1,500,000 events
Average of users querying data	3 users	15 users	25 users	Beyond 25 users
Alert list averaging	Around 1M records	Around 2M records	Around 2M records	Around 2M records
Database Server Engine	MongoDB Atlas	MongoDB Atlas MongoDB Enterprise		
Dedicated Cluster	M20 2 vCPU 4 GB RAM Network Performance 100MB	M50 8 vCPU 16 GB RAM, Network Performance 10Gbps	db.r5.4xlarge 16 vCPU 64 GB RAM Network Performance 10Gbps	db.r5.8xlarge 32 vCPU 131 GB RAM Network Performance 10Gbps
Storage	General	General	General / Local NVMe SSD	General / Local NVMe SSD
Multimedia Storage	AWS EBS General Purpose SSD (gp2)		AWS EBS Provisioned IOPS SSD (io1)	

This document and its contents are intended for the recipient only. Copying, redistributing, or discussing with any other party outside of the intended recipient and Neology is prohibited.

BOSS4 On-Premise Specifications for Requirements

On-Premise Applications Server

Below, there are the minimal recommended configurations for different capacity configurations for BOSS4 On-Premise infrastructure.

Application Servers Specifications				
Configuration	**Demo**	**Medium**	**Large**	**High Capacity**
ALPR Devices	1 to 3	3 to 50	50 to 150	Beyond 150
Average Daily Intake	Around 30,000 events	Around 500,000 events	Around 1,500,000 events	Beyond 1,500,000 events
Average of users querying data	3 users	15 users	25 users	Beyond 25 users
Alert list averaging	Around 1M records	Around 2M records	Around 2M records	Around 2M records
Operating System	Amazon Linux / Amazon Linux 2 x64 Linux x64 (RHEL/CentOS, Ubuntu, Debian, SUSE) macOS x64 Windows 10 Professional x64 Windows Server 2016 x64			
Memory	16GB	32GB	64GB	192GB
Processor	x64 2.0 GHz 8 cores o better	Server Processor x64 (Intel Xeon Gold) 2 GHz 4 cores, 8 threads, 4MB cache	Server Processor x64 (Intel Xeon Platinum) 2.4 GHz 16 cores, 32 threads, 8MB cache	Server Processor x64 (Intel Xeon Platinum) 2.4 GHz 24 cores, 48 threads, 24MB cache
Hard Drive	7200 RPM SATA3	SSD SATA3	SSD SATA3 or NVMe PCI Express	SSD SATA3 or NVMe PCI Express
Application Space	128 GB of available space	256GB of available space	320GB of available space	512GB of available space

This document and its contents are intended for the recipient only. Copying, redistributing, or discussing with any other party outside of the intended recipient and Neology is prohibited.

On-Premise Database Server

BOSS4 uses the MongoDB Database Engine.

Specifications of the Database Server				
Configuration	**Demo**	**Medium**	**Large**	**High Capacity**
ALPR Devices	1 to 3	3 to 50	50 to 150	Beyond 150
Average Daily Intake	Around 30,000 events	Around 500,000 events	Around 1,500,000 events	Beyond 1,500,000 events
Average of users querying data	3 users	15 users	25 users	Beyond 25 users
Alert list averaging	Around 1M records	Around 2M records	Around 2M records	Around 2M records
Database Engine	Mongo DB Community	MongoDB Enterprise		
Operating System	Amazon Linux / Amazon Linux 2 x64 Linux x64 (RHEL/CentOS, Ubuntu, Debian, SUSE) macOS x64 Windows 10 Professional x64 Windows Server 2016 x64			
Processor	x64 2.0 GHz 8 cores o better	Server Processor x64 (Intel Xeon Gold) 2.5 GHz 4 cores, 8 threads, 4MB cache	Server Processor x64 (Intel Xeon Platinum) 2.4 GHz 16 cores, 32 threads, 16MB cache	Server Processor x64 (Intel Xeon Platinum) 2.4 GHz 24 cores, 48 threads, 24MB cache
Memory	N/A	32 GB	128GB	256GB
Hard Drive	7200 RPM SATA3 Not suitable for camera implantation with any kind of data retention expected	SSD SATA3 RAID level redundancy and scheduled DB backups recommended *See sizing chart for storage.*	SSD SATA3 or NVMe PCI Express RAID level redundancy and scheduled DB backups recommended *See sizing chart for storage.*	SSD SATA3 or NVMe PCI Express RAID level redundancy and scheduled DB backups recommended *See sizing chart for storage.*

This document and its contents are intended for the recipient only. Copying, redistributing, or discussing with any other party outside of the intended recipient and Neology is prohibited.

BOSS4 On-Premise & Cloud Storage

The calculation of storage applies to Cloud and On-Premise configurations.

Assumptions for the calculation:

Storage of metadata per read event: 32KB
Storage of imagery per read event: 160KB

Events from Golden Eagle or P500 cameras			
# of records	Database size Metadata and indexes	Repository Size Imagery	Total
1 Million	32GB	153GB	**185GB**
5 Million	64GB	763GB	**827GB**
10 Million	320GB	1.5TB	**1.82TB**
50 Million	1.6TB	7.5TB	**6.1TB**
100 Million	3.2TB	15TB	**18.2TB**

The calculation for the storage is approximated and it can vary depending on the conditions for the processing of the indexes, Mantis Metadata, compression of the images, among others.

It is not considered the storage for the backup of the databases nor the imagery repository.

This document and its contents are intended for the recipient only. Copying, redistributing, or discussing with any other party outside of the intended recipient and Neology is prohibited.

MASSACHUSETTS STATE POLICE

EXECUTIVE OFFICE OF PUBLIC SAFETY AND SECURITY
HIGHWAY SAFETY DIVISION
FFY 2016 FUNDING PROPOSAL

ALPR TRAILER

PROBLEM STATEMENT

Law enforcement agencies throughout the nation and around the world are increasingly adopting Automated License Plate Recognition (ALPR) systems. In Massachusetts, ALPR is utilized by over 41 different public safety agencies including the MSP. ALPR systems function to automatically capture an image of the vehicle's license plate, transform that image into alphanumeric characters using optical character recognition or similar software, compare the plate number acquired to one or more databases of vehicles of interest to law enforcement and other agencies, and to alert the officer when a vehicle of interest has been observed. Currently the MSP utilize ALPR to enhance their enforcement and investigative capabilities, expand their collection of relevant data, and expedite the tedious and time consuming process of comparing vehicle license plates with lists of stolen, wanted, and other vehicles of interest.

GOALS & OBJECTIVES

ALPR is used every day in Massachusetts to generate investigative leads that assist law enforcement in solving murders, rapes, and serial property crimes, recover abducted children, detect drug and human trafficking rings, find stolen vehicles, apprehend violent criminal alien fugitives, and support terrorism investigations. With an aging population, an increasing amount of "Silver Alerts" are generated to located missing elderly individuals. Quite often these individuals are operating a motor vehicle when they become disoriented.

COUNTERMEASURE TO ADDRESS PROBLEM

To provide investigative support focusing on site specific locations and to augment security at large scale events the department proposes to deploy a trailer mounted covert ALPR system. This system would be enclosed within a speed or variable message board and deployed to such large scale events as the Boston Marathon or the July 4th Esplanade celebration. The message/speed board will provide a highway safety function while capturing the ALPR data and storing it in a central repository.

LINE ITEM BUDGET

One Kustom 850 VSM/Speed board prepped for ALPR
Two 3M model 492 ALPR Cameras

Total $50,000.00

MEASURING SUCCESS/EVALUATION METHOD

The qualitative assessment of ALPR utilization will focus on feedback from the involved stakeholders, to include local law enforcement, media, government agencies and the people we serve.

SELF-SUFFICIENCY PLAN

The Massachusetts Department of State Police supports the utilization of ALPR technology to assist in intelligence gathering in effort to prevent terrorist activity and solve criminal investigation. Without federal funding the Department cannot sustain and enhance its ALPR capabilities.

SUPPLANTING

Absent federal or grant funding, the Massachusetts State Police does not purchase ALPR equipment.

INSTITUTIONALIZED PLAN

ALPR Utilization is a fully institutionalized program of the Massachusetts State Police. It is incorporated into our daily patrol function and is enshrined in our policy and procedures.

Submitted by

Colonel Timothy P. Alben
Superintendent, Massachusetts State Police

MMARS DOCUMENT ID: ISAEPSFY16ALPRPOL16A.

5256

COMMONWEALTH OF MASSACHUSETTS
INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM

This Form is issued and published by the Office of the Comptroller (CTR) pursuant to 815 CMR 6.00 for use by all Commonwealth Departments. Departments may add non-conflicting additional terms, but changes to the official printed language of this Form shall be void.

BUDGET FISCAL YEAR: 2016	RFR REFERENCE NUMBER ENTER RFR NUMBER: OR _X_ N/A.
MMARS ALPHA *BUYER/PARENT* DEPARTMENT CODE: EPS	MMARS ALPHA *SELLER/CHILD* DEPARTMENT CODE: POL
BUSINESS MAILING ADDRESS: 10 PARK PLAZA, SUITE 3720 BOSTON, MA 02116	BUSINESS MAILING ADDRESS: 470 WORCESTER ROAD FRAMINGHAM, MA 01702
ISA MANAGER: DIANE PERRIER	ISA MANAGER: DEB BRODERICK
PHONE: **617-725-3301** FAX: 617-725-0260	PHONE: **508-820-2146** FAX: 508-820-2146
E-MAIL ADDRESS: DIANE.PERRIER@STATE.MA.US	E-MAIL ADDRESS: DEBORAH.BRODERICK@STATE.MA.US

Purpose of ISA: (Check one option only and complete applicable information) (Attachment A required for New ISAs and all ISA Amendments.)

_X_ New ISA. Current Maximum Obligation for total duration of ISA **$ 50,000.00** (Use "N/A" for Non-Financial ISA.) (Complete Attachment B)

___ Amendment to Existing ISA. What is being amended? (Attachment C required for all Federal and Bond Account Amendments)

____ Amend Budget/Accounts. Change Maximum Obligation from: $_____ to New Maximum Obligation $ _____ (Attachment B)

____ Amend Budget/Accounts. No Change in Maximum Obligation (Attachment B)

____ Amend Dates of Performance. New Dates of Service: Start Date:_____ End Date:_____ (Subject to execution dates below.)

____ Amend Scope of Services/Performance

BRIEF DESCRIPTION OF PERFORMANCE GOALS TO BE ACCOMPLISHED BY ISA, OR IF AMENDMENT, IDENTIFY WHAT IS BEING AMENDED:

FFY2016 Automated License Plate Recognition (ALPR) system, includes related equipment.
PT-16-07-01

WILL SELLER/CHILD DEPARTMENT STATE EMPLOYEES (AA OBJECT CLASS) BE FULLY OR PARTIALLY FUNDED UNDER THIS ISA? **_X_ No ___ Yes.** If Yes, Seller/Child certifies that the ISA is not being used as an alternative funding mechanism for state employees, that the identified personnel in Attachment A are necessary for completion of the ISA due to particular expertise or other factors that can not be obtained through the use of contractors, and that if federal funds are being used, funds shall not be used to supplement the regular salary or compensation of any officer or employee of the Commonwealth for services performed during their regular working hours. M.G.L. c. 29, § 6B.

ACCOUNT INFORMATION. Complete for all new ISAs and Amendments (even if account information is not changing) Check one option, indicate "add", "delete" or "no change" and enter account, fund, major program code and program code.

_X_ BGCN – non-subsidiarized (federal, capital, trust). Attachment C required for any new ISA or ISA Amendment involving federal funds.

___ BGCS – subsidiarized (budgetary)

___ Other (CT, RPO as authorized by CTR): _____.

___ Non-Financial ISA (no funds are transferred from Buyer/Parent to Seller/Child), however, resources are committed to ISA.

___ Amendment with no Accounting Changes to Budget/Accounts or to Attachments B or C. (Indicate no change below and complete account information.)

_X_ ADD __ DELETE __ NO CHANGE	Account: 80004804	Fund: 0100	Major Program Code: HSPGTS	Program Code: F16ALPR
__ ADD __ DELETE __ NO CHANGE	Account:	Fund:	Major Program Code:	Program Code:
__ ADD __ DELETE __ NO CHANGE	Account:	Fund:	Major Program Code:	Program Code:
__ ADD __ DELETE __ NO CHANGE	Account:	Fund:	Major Program Code:	Program Code:

ISA ANTICIPATED START DATE: **01/15/2015**, provided that the Seller/Child certifies that it will not incur any obligations related to this ISA prior to the date that this ISA is executed, NOR prior to the date that sufficient funding for the obligations for this ISA is available in the Seller/Child account for expenditure.

TERMINATION DATE OF THIS ISA: This ISA shall terminate on **06/30/2016** unless terminated or properly amended in writing by the parties prior to this date.

BUYER/PARENT AND SELLER/CHILD DEPARTMENT CERTIFICATIONS. IN WITNESS WHEREOF, by executing this ISA below, the Buyer/Parent and Seller/Child certify, under the pains and penalties of perjury, that Buyer/Parent and Seller/Child understand and agree that any Buyer/Parent or Seller/Child officer or employee who knowingly violates, authorizes or directs another officer or employee to violate any provision of state finance law relating to the incurring of liability or expenditure of public funds, includng this ISA, may be considered to be in violation of M.G.L. c. 29, § 66, and therefore the Buyer/Parent and the Seller/Child agree to ensure that this ISA complies with, and that all staff or contractors involved with ISA performance are provided with sufficient training and oversight to ensure compliance with 815 CMR 6.00, CTR applicable policies and the ISA Terms and Conditions which are incorporated by reference into this ISA, in addition to the performance requirements identified in Attachment A of this ISA, and that all terms governing performance of this ISA are attached to this ISA or incorporated by reference herein, and the Buyer/Parent and Seller/Child agree to maintain the necessary level of communication (including immediate notification of any amendments to accounting information, program codes or performance needs), coordination, access to reports and other ISA information, and cooperation to ensure the timely execution and successful completion of the ISA, amendments, and state finance law compliance; and that the Buyer/Parent certifies it will ensure that sufficient funds are timely made available in the Seller/Child account(s), with the proper accounting codes, prior to the Seller/Child's need to begin initial or amended performance; and that the Seller/Child will not allow initial or amended performance to begin until the ISA is executed AND the ISA Seller/Child account is sufficiently funded to support encumbrances and payments for performance (including payroll), and the Seller/Child will make encumbrances and payments (including payroll) only from the authorized ISA Seller/Child account(s) and shall not be entitled to transfer charges made from any other account not approved in writing by CTR in advance of expenditures by the Seller/Child.

BUYER/PARENT DEPARTMENT'S AUTHORIZED SIGNATURE: **DATE:** (Date must be handwritten by signatory at time of signature)	**SELLER/CHILD DEPARTMENT'S AUTHORIZED SIGNATURE:** **DATE:** (Date must be handwritten by signatory at time of signature)
PRINT NAME: ART KINSMAN	PRINT NAME:
PRINT TITLE: EXECUTIVE DIRECTOR, OFFICE OF GRANTS & RESEARCH	PRINT TITLE:

INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM
TERMS AND CONDITIONS

The following terms and conditions are incorporated by reference into any ISA.

Role of the Office of the Comptroller. All ISA fiscal transactions shall be made through the state accounting system as prescribed by the Office of the Comptroller (CTR). CTR will interpret 815 CMR 6.00 and applicable policies and take any fiscal or other actions necessary to ensure ISA compliance with state finance law, including but not limited to correcting accounting transactions, resolving ISA disputes and identifying corrective action by the Buyer/Parent or Seller/Child Departments.

Seller/Child Department Certifications. By executing an ISA the Seller/Child certifies that it is statutorily authorized to provide the type of performance sought by the Buyer/Parent, and shall at all times remain qualified to perform the ISA, that performance shall be timely and meet or exceed ISA standards, that the Seller/Child will not allow initial or amended performance to begin, may not authorize personnel or contractors to work, nor incur any obligation to be funded under an ISA prior to the execution of an ISA AND the availability of ISA funding in the Seller/Child account to support encumbrances and payments for performance. The Seller/Child will make encumbrances and payments (incuding payroll) only from the authorized ISA Seller/Child account(s) and shall not be entitled to transfer charges made from any other account not approved in writing in advance by CTR.** The Seller/Child must immediately notify CTR whenever a delay in funding is anticipated for which performance is expected. The Seller/Child is authorized to use ISA funding only for the actual costs of ISA performance and may not use ISA funds to supplement non-ISA related personnel or expenditures.

Buyer/Parent Department Certifications. Signature by the Buyer/Parent certifies that it is statutorily authorized or required to procure the type of performance required under this ISA, that the Buyer/Parent certifies it will ensure that sufficient funds are timely made available in the Seller/Child Seller/Child account(s), with the proper accounting codes, prior to the Seller/Child's need to begin intial or amended performance; that the Buyer/Parent will monitor and reconcile ISA performance in compliance with state appropriation language or federal grant requirements, communicate all fiscal information necessary for the set up of the Seller/Child account(s) including budget information, and if the ISA is funded with federal funds provide accurate accounting information in Attachment C, and immediately notify the Seller/Child of any changes in Attachment C (such as program codes) to ensure the ISA and Seller/Child account can be timely updated to avoid lapses in funding or the inability of the Seller/Child to make timely payroll and other expenditures from the Seller/Child account.

Chief Fiscal Officer. The Chief Fiscal Officer (CFO) for the Buyer/Parent and Seller/Child will be responsible for the fiscal management of ISAs within their Departments in accordance with these ISA Terms and Conditions, 815 CMR 6.00 and policies and procedures published by CTR.

ISA Manager. Both the Buyer/Parent and Seller/Childs are responsible for ensuring that the ISA Manager listed on the ISA, or ISA Amendment, is current and that the ISA Manager is an authorized signatory for the Department supported by the appropriate Security Profile. If the listed ISA Manager changes, the CFO shall be the ISA Manager until a replacement is identified in the same manner as other Written Notice.

Record-keeping and Retention, Inspection of Records. The Buyer/Parent and Seller/Child shall maintain all ISA records in such detail as necessary to support claims for payment, including reimbursement or federal financial participation (FFP), for at least seven (7) years from the last payment under an ISA Seller/Child account, or such longer period as is necessary for the resolution of any litigation, claim, negotiation, audit or other inquiry involving an ISA. In addition to any specific progress, programmatic or expenditure reports specified in Attachment A, the Seller/Child is required to provide the Buyer/Parent (and to CTR, the State Auditor and the House and Senate Ways and Means Committees upon request) with full cooperation and access to all ISA information.

Payments and Compensation. The Seller/Child may accept compensation only for performance delivered and accepted by the Buyer/Parent in accordance with the specific terms and conditions of the ISA. All ISA payments are subject to appropriation pursuant to M.G.L. C. 29, or the availability of sufficient non-appropriated funds for the purposes of an ISA. Overpayments or disallowed expenditures shall be reimbursed by the Seller/Child or may be offset from future ISA payments in accordance with state finance law and instructions from CTR.

ISA Termination or Suspension. An ISA shall terminate on the date specified, unless this date is properly amended prior to this date, or unless terminated or suspended under this Section upon prior written notice to the Seller/Child. The Buyer/Parent may terminate an ISA without cause and without penalty with at least thirty days prior written notice, or may terminate or suspend an ISA with reasonable notice if the Seller/Child breaches any material term or condition or fails to perform or fulfill any material obligation required by an ISA, or in the event of an elimination of an appropriation or availability of sufficient funds for the purposes of an ISA, or in the event of an unforeseen public emergency mandating immediate Buyer/Parent action. Upon immediate notification to the other party, neither the Buyer/Parent nor the Seller/Child shall be deemed to be in breach for failure or delay in performance due to Acts of God or other causes factually beyond their control and without their fault or negligence. Contractor failure to perform or price increases due to market fluctuations or product availability will not be deemed factually beyond the Seller/Child's control.

Written Notice. Any notice shall be deemed delivered and received when submitted in writing in person or when delivered by any other appropriate method evidencing actual receipt by the Buyer/Parent or the Seller/Child. Unless otherwise specified in the ISA, legal notice sent or received by the Buyer/Parent's ISA Manager or the CFO (with confirmation of actual receipt) through the listed fax number(s) or E-Mail address for the ISA Manager will satisfy written notice under the ISA. Any written notice of termination or suspension delivered to the Seller/Child shall state the effective date and period of the notice, the reasons for the termination or suspension, if applicable, any alleged breach or failure to perform, a reasonable period to cure any alleged breach or failure to perform, if applicable, and any instructions or restrictions concerning allowable activities, costs or expenditures by the Seller/Child during the notice period.

Confidentiality. The Seller/Child shall comply with M.G.L. C. 66A if the Seller/Child becomes a "holder" of "personal data". The Seller/Child shall also protect the physical security and restrict any access to personal or other Buyer/Parent data in the Seller/Child's possession, or used by the Seller/Child in the performance of an ISA, which shall include, but is not limited to the Buyer/Parent's public records, documents, files, software, equipment or systems. If the Seller/Child is provided access with any other data or information that triggers confidentiality requirements under FIPA, HIPPA or other federal or state laws, the Seller/Child shall be responsible for protection of this data as instructed by the Buyer/Parent.

Assignment. The Seller/Child may not assign, delegate or transfer in whole or in part any ISA, or any liability, responsibility, obligation, duty or interest under an ISA, to another Department or an outside contractor. Assumption of an ISA by a successor Department due to a legislative change in the Seller/Child or Buyer/Parent's department status shall be accomplished through the execution of a new ISA.

Subcontracting By Seller/Child. Since it is presumed that contracting through the Seller/Child is more cost effective and a better value than the Buyer/Parent directly contracting with an outside contractor(s), any subcontract entered into by the Seller/Child for the purposes of fulfilling the obligations under an ISA must be approved by the Buyer/Parent in advance of the ISA and justified as part of the ISA Attachment A. The Seller/Child is responsible for full state finance law and procurement compliance for all subcontracts, and shall supply a copy of any subcontract to the Buyer/Parent upon request.

Affirmative Action, Non-Discrimination in Hiring and Employment. In performing this ISA, the Seller/Child shall comply with all federal and state laws, rules, regulations and applicable internal state policies and agreements promoting fair employment practices or prohibiting employment discrimination and unfair labor practices and shall not discriminate in the hiring of any applicant for employment nor shall any qualified employee be demoted, discharged or otherwise subject to discrimination in the tenure, position, promotional opportunities, wages, benefits or terms and conditions of their employment because of race, color, national origin, ancestry, age, sex, religion, disability, handicap, sexual orientation or for exercising any rights afforded by law. The Seller/Child commits to, when possible, to purchasing supplies and services from certified minority or women-owned businesses, small businesses or businesses owned by socially or economically disadvantaged persons or persons with disabilities in accordance with the Commonwealth's Affirmative Market Program.

Waivers. Forbearance, indulgence or acceptance by the Seller/Child or Buyer/Parent of any breach or default in any form shall not be construed as a waiver and shall not limit enforcement remedies or allow a waiver of any subsequent default or breach.

Risk of Loss. The Seller/Child shall bear the risk of loss for any materials, deliverables, personal or other data that is in the possession of the Seller/Child or used by the Seller/Child in the performance of an ISA until is accepted by the Buyer/Parent.

Disputes. The Buyer/Parent and Seller/Child agree to take all necessary actions to resolve any dispute arising under the ISA within 30 calendar days including department head and secretariat involvement, but in no event shall a dispute remain unresolved beyond May 30th in any fiscal year, nor may the Buyer/Parent or Seller/Child allow a dispute to create a state finance law or other violation of ISA terms (such as a delay in funding, failure to timely communicate funding or program code changes, or failure to timely process ISA paperwork). Seller/Child and Buyer/Parent must immediately notify CTR to assist in resolution of the dispute and shall implement any actions required by CTR to resolve the dispute, which shall be considered final.

Interpretation, Severability, Conflicts with Law, Integration. Any amendment or attachment to any ISA that contains conflicting language or has the affect of deleting, replacing or modifying any printed language of the ISA shall be interpreted as superseded by the ISA Form as published. If any ISA provision is superseded by state or federal law or regulation, in whole or in part, then both parties shall be relieved of all obligations under that provision to the extent necessary to comply with the superseding law, provided however, that the remaining provisions of the ISA, or portions thereof, shall be enforced to the fullest extent permitted by law. The terms of this ISA shall survive its termination for the purpose of resolving any claim, dispute or other action, or for effectuating any negotiated representations and warranties.

INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM
TERMS AND CONDITIONS

ATTACHMENT A – TERMS OF PERFORMANCE AND JUSTIFICATIONS:

This Attachment Form must be used. Insert (type or copy and paste) all relevant information using as many pages as necessary. Attach any additional supporting documentation as appropriate. If Amending the ISA, completion of Sections 1, 2 and 3 identifying what is being amended and the reasons for the amendments is required. For sections 4-9 enter only the amended language in the sections being amended.

1. [REQUIRED] Purpose and other performance goals of ISA, or as amended:

   - To decrease motor-vehicle fatalities 10% from the 2009-2013 calendar base year average of 354 to 319 by December 31, 2016.
   - To decrease the number of serious traffic injuries 10% from 4,134 in 2013 to 3,721 by December 31, 2016.
   - To decrease unrestrained vehicle occupant fatalities in all seating positions 10% from the 2009-2013 base calendar year average of 108 to 97 by December 31, 2016.

2. [REQUIRED] Identify in detail, the responsibilities of the parties, the scope of services and terms of performance under the ISA, or as amended:
   The MSP seeks to enhance their enforcement and investigative capabilities through the purchase of a portable trailer equipped with an Automated License Plate Recognition (ALPR) system.

   MSP will maintain an equipment database for the life of the property as required by EOPSS.

   The Division of Field Services will ensure that all MSP personnel assigned to EOPSS/HSD grant funded enforcement initiatives are familiar with the related goals and expectations.

   With EOPSS/HSD assistance, the MSP will acknowledge EOPSS as the funding source on all news releases.

3. [REQUIRED] Identify schedule of performance or completion dates or other benchmarks for performance, or as amended:

   See Section 1 & 2.

4. [REQUIRED] Justification that use of ISA is best value vs. contract with outside vendor:
   N/A

5. Will Seller/Child department state employees (AA Object Class) be fully or partially funded under this ISA? X No ___ Yes.
   If yes, justify necessity to use state employees for the ISA vs. use of contractors (contract employees or outside vendors).

6. Subcontractors. Since it is presumed that contracting through the Seller/Child is more cost effective and a better value than the Buyer/Parent directly contracting with an outside contractor(s), any subcontract entered into by the Seller/Child for the purposes of fulfilling the obligations under an ISA must be approved by the Buyer/Parent in advance of the ISA and justified as part of the ISA Attachment A, as follows: (enter "N/A" if subcontractors will not be funded with ISA funds)
   N/A

7. Identify any equipment that will be leased or purchased by the Seller/Child using ISA funds: (The Buyer/Parent shall determine ownership of equipment purchased by the Seller/Child with ISA funds. Enter "N/A" if equipment not included in ISA.)
   ALPR system with related trailer equipment.

8. [REQUIRED] Identify the format and timing of ISA reports to the Buyer/Parent Department. Include the type of reports (e.g., progress or status, data, etc.), timing of reports (e.g., weekly, monthly, final) and the medium for submission of reports (e.g., e-mail, Excel spreadsheet, paper, telephone):

The equipment will be purchased when funds become available in MMARS. All equipment must be purchased and received prior to the close of the federal fiscal year on September 30, 2016. Invoice(s) must be submitted to EOPSS' Highway Safety Division within 30 days of the purchase(s).

The MSP will submit an Annual Report outlining the deployment and utilization associated with the ALPR system.

9. Additional ISA Terms: [Insert Terms here. Do not refer to separate attachment(s)]

General Federal Grant Conditions

The basic federal grant conditions that follow apply to all federal grants, regardless of the federal department making the funds available.

- Audit Requirement of Federal Funds
  - 2 CFR 200 (formerly OMB Circular A-133) requirements apply to each non-profit organization, each institution of higher education, and local governments as a whole when they or one of their departments receives federal funds. Any non-profit organization, institution of higher education, or local government spending more than $750,000 in federal funds *from all sources* within a 12-month period must have an audit performed on the use of the funds. OGR defines the 12-month period as July 1 to June 30. The following webpage provides the full text of this basic federal grant requirement:

    http://www.gpo.gov/fdsys/pkg/FR-2013-12-26/pdf/2013-30465.pdf

- Data Universal Number System (DUNS) and Central Contractor Registration (CCR)
  - All subrecipients of federal funds must have a nine-digit DUNS number in order. For more information: 1-866-705-5711 or http://fedgov.dnb.com/webform.
  - All subrecipients of federal funds must maintain annual registration in the System for Award Management (SAM) database: www.sam.gov.

- Transparency Act Reporting for Federal Funds
  - The Federal Funding Accountability and Transparency Act (FFATA) requires EOPSS to report on a federal website specific award and subrecipient identifying information for each award greater than $25,000 OGR makes with federal funds it received after October 1, 2010. Prior to receiving funds, each affected subrecipient must report certain information to OGR so that EOPSS can fulfill its FFATA reporting requirements. Data reported by EOPSS may be viewed at www.USASpending.gov.

- Cost Principles for Federal Grants to *State and Local Governments*
  - 2 CFR Part 225 (formerly known as OMB Circular A-87) requirements apply only to state and local government subrecipients. These regulations list and define general categories of costs that are both allowable and unallowable. Examples are included below.
    - Supplanting, including: (a) replacing routine and/or existing State or local expenditures with Federal grant funds and/or (b) using Federal grant funds for costs of activities that constitute general expenses required to carry out the overall responsibilities of State, local, or Federally recognized Indian tribal governments is unallowable.
    - The cost of alcoholic beverages is unallowable.
    - Costs incurred by advisory councils are allowable.
    - Audit costs are allowable.
    - Compensation costs are allowable so long as they are consistent with that paid for similar work in other activities of the local government.
    - Entertainment costs are unallowable.

- Equipment costs are allowable with the prior approval of OGR. Equipment having a useful life of more than one year or a current per-unit fair market value of $5,000 or more must be tracked. When replacing equipment purchased with federal funds, the equipment to be replaced may be used as a trade-in or can be sold with the proceeds used to offset the cost of the replacement equipment. In addition, during the period of the contract with OGR, insurance on the equipment is allowable.
- Travel costs are allowable if pre-approved by OGR and if they are consistent with costs normally allowed in like circumstances for non-federally funded activities. The following webpage provides the full text of this basic federal grant requirement: http://www.whitehouse.gov/omb/fedreg/2005/083105_a87.pdf.
- If a subrecipient uses grant funds to pay its employees, the subrecipient must maintain timesheets for work performed with the grant funds. Timesheets must show the hours worked and must be signed by the employee paid with the grant funds.

- Cost Principles for Federal Grants to *Non-Profit Organizations and Institutions of Higher Education* requirements apply only to the non-profit and higher education subrecipients. The CFRs referenced below list and define general categories of costs that are allowable and unallowable. The links below provide the full text of these two basic federal grant requirements.
  - 2 CFR Part 220 pertains to Educational Institutions (formerly known as OMB Circular A-21): http://www.whitehouse.gov/omb/fedreg/2005/083105_a21.pdf.
  - 2 CFR Part 230 pertains to Non-profit Organizations (formerly known as OMB Circular A-122): http://www.whitehouse.gov/omb/fedreg/2005/083105_a122.pdf.

U.S. Department of Transportation Funds

The National Highway Traffic Safety Administration (NHTSA) of the U.S. Department of Transportation offers two documents that present requirements for the use of the funds and outline the purpose of each category of grants provided.

- Urls for the two programmatic and financial guide documents from NHTSA are below.
  - Highway Safety Grant Funding Policy: http://www.nhtsa.gov/nhtsa/whatsup/TEA21/GrantMan/HTML/GrantFundPolicy_mkm_revJuly07.pdf

    Pay particular attention to the sections on: (1) allowable costs for equipment, travel, training, and consultant services; and (2) unallowable costs for equipment, facilities and construction, training and program administration.

    A more complete document on administrative requirements is found in 49 CFR Part 18 - the Uniform Administrative Requirement for Grants as promulgated by the U.S. Department of Transportation.
  - Highway Safety Grant Management Manual: http://www.nhtsa.gov/nhtsa/whatsup/TEA21/GrantMan/HTML/00_Manl_Contents1_01.html. This document provides information on each of the grant programs including Sections 154, 164, 402, 405a, 405b, 405c, 405d, 405e, 405f and 405g grant programs.

Additional current NHTSA grants management resources may be found at:
http://www.nhtsa.gov/About+NHTSA/Programs+&+Grants/Resources+Guide

In Addition to the links above, recipients of NHTSA funding must also adhere to the following conditions:

INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM
TERMS AND CONDITIONS

- **NONDISCRIMINATION (APPLIES TO SUBRECIPIENTS AS WELL AS STATES):** The State highway safety agency will comply with all Federal statutes and implementing regulations relating to nondiscrimination. These include but are not limited to: (a) Title VI of the Civil Rights Act of 1964 (Pub. L. 88-352), which prohibits discrimination on the basis of race, color or national origin (and 49 CFR Part 21); (b) Title IX of the Education Amendments of 1972, as amended (20 U.S.C. 1681-1683 and 1685-1686), which prohibits discrimination on the basis of sex; (c) Section 504 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794), and the Americans with Disabilities Act of 1990 (Pub. L. 101-336), as amended (42 U.S.C. 12101, *et seq.*), which prohibits discrimination on the basis of disabilities (and 49 CFR Part 27); (d) the Age Discrimination Act of 1975, as amended (42 U.S.C. 6101-6107), which prohibits discrimination on the basis of age; (e) the Civil Rights Restoration Act of 1987 (Pub. L. 100-259), which requires Federal-aid recipients and all subrecipients to prevent discrimination and ensure nondiscrimination in all of their programs and activities; (f) the Drug Abuse Office and Treatment Act of 1972 (Pub. L. 92-255), as amended, relating to nondiscrimination on the basis of drug abuse; (g) the comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970 (Pub. L. 91-616), as amended, relating to nondiscrimination on the basis of alcohol abuse or alcoholism; (h) Sections 523 and 527 of the Public Health Service Act of 1912, as amended (42 U.S.C. 290dd-3 and 290ee-3), relating to confidentiality of alcohol and drug abuse patient records; (i) Title VIII of the Civil Rights Act of 1968, as amended (42 U.S.C. 3601, *et seq.*), relating to nondiscrimination in the sale, rental or financing of housing; (j) any other nondiscrimination provisions in the specific statute(s) under which application for Federal assistance is being made; and (k) the requirements of any other nondiscrimination statute(s) which may apply to the application.

- **BUY AMERICA ACT 49 U.S.C 5323 (J) (APPLIES TO SUBRECIPIENTS AS WELL AS STATES):** Only steel, iron and manufactured products produced in the United States may be purchased with Federal funds unless the Secretary of Transportation determines that such domestic purchases would be inconsistent with the public interest, that such materials are not reasonably available and of a satisfactory quality, or that inclusion of domestic materials will increase the cost of the overall project contract by more than 25 percent. Clear justification for the purchase of non-domestic items must be in the form of a waiver request submitted to and approved by the Secretary of Transportation. **The Buy America Act does not apply to purchases under $5,000.**

- **Political Activity Act (Applies to Subrecipients as well as States):** The State will comply with provisions of the Hatch Act (5 U.S.C. 1501-1508) which limits the political activities of employees whose principal employment activities are funded in whole or in part with Federal funds.

- **Certification Regarding Federal Lobbying (Applies to Sunrecipients as well as States):** The authorized signatory certifies, to the best of his or her knowledge and belief, that:

  1. No Federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.

  2. If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, “Disclosure Form to Report Lobbying,” in accordance with its instructions.

  3. The undersigned shall require that the language of this certification be included in the award documents for all sub-award at all tiers (including subcontracts, subgrants, and contracts under grant, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.

  This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by section 1352, title 31, U.S. Code. Any person who fails to file the

required certification shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure.

- **Restrictions on State Lobbying (This Applies to Subrecipients as well as Sates):** None of the funds under this program will be used for any activity specifically designed to urge or influence a State or local legislator to favor or oppose the adoption of any specific legislative proposal pending before any State or local legislative body. Such activities include both direct and indirect (e.g., “grassroots”) lobbying activities, with one exception. This does not preclude a State official whose salary is supported with NHTSA funds from engaging in direct communications with State or local legislative officials, in accordance with customary State practice, even if such communications urge legislative officials to favor or oppose the adoption of a specific pending legislative proposal.

- **Certification Regarding Debarment and Suspension (This Applies to Subrecipients as well as States):**

  Instructions for Primary Certification

  1. By signing and submitting this proposal, the prospective primary participant is providing the certification set out below.

  2. The inability of a person to provide the certification required below will not necessarily result in denial of participation in this covered transaction. The prospective participant shall submit an explanation of why it cannot provide the certification set out below. The certification or explanation will be considered in connection with the department or agency's determination whether to enter into this transaction. However, failure of the prospective primary participant to furnish a certification or an explanation shall disqualify such person from participation in this transaction.

  3. The certification in this clause is a material representation of fact upon which reliance was placed when the department or agency determined to enter into this transaction. If it is later determined that the prospective primary participant knowingly rendered an erroneous certification, in addition to other remedies available to the Federal Government, the department or agency may terminate this transaction for cause or default.

  4. The prospective primary participant shall provide immediate written notice to the department or agency to which this proposal is submitted if at any time the prospective primary participant learns its certification was erroneous when submitted or has become erroneous by reason of changed circumstances.

  5. The terms *covered transaction, debarred, suspended, ineligible, lower tier covered transaction, participant, person, primary covered transaction, principal, proposal, and voluntarily excluded,* as used in this clause, have the meaning set out in the Definitions and coverage sections of 49 CFR Part 29. You may contact the department or agency to which this proposal is being submitted for assistance in obtaining a copy of those regulations.

  6. The prospective primary participant agrees by submitting this proposal that, should the proposed covered transaction be entered into, it shall not knowingly enter into any lower tier covered transaction with a person who is proposed for debarment under 48 CFR Part 9, subpart 9.4, debarred, suspended, declared ineligible, or voluntarily excluded from participation in this covered transaction, unless authorized by the department or agency entering into this transaction.

  7. The prospective primary participant further agrees by submitting this proposal that it will include the clause titled “Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion-Lower Tier Covered Transaction,” provided by the department or agency entering into this covered transaction, without modification, in all lower tier covered transactions and in all solicitations for lower tier covered transactions.



8. A participant in a covered transaction may rely upon a certification of a prospective participant in a lower tier covered transaction that it is not proposed for debarment under 48 CFR Part 9, subpart 9.4, debarred, suspended, ineligible, or voluntarily excluded from the covered transaction, unless it knows that the certification is erroneous. A participant may decide the method and frequency by which it determines the eligibility of its principals. Each participant may, but is not required to, check the list of Parties Excluded from Federal Procurement and Non-procurement Programs.

9. Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render in good faith the certification required by this clause. The knowledge and information of a participant is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.

10. Except for transactions authorized under paragraph 6 of these instructions, if a participant in a covered transaction knowingly enters into a lower tier covered transaction with a person who is proposed for debarment under 48 CFR Part 9, subpart 9.4, suspended, debarred, ineligible, or voluntarily excluded from participation in this transaction, in addition to other remedies available to the Federal Government, the department or agency may terminate this transaction for cause or default.

Certification Regarding Debarment, Suspension, and Other Responsibility Matters-Primary Covered Transactions

(1) The prospective primary participant certifies to the best of its knowledge and belief, that its principals:

(a) Are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded by any Federal department or agency;

(b) Have not within a three-year period preceding this proposal been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, State or local) transaction or contract under a public transaction; violation of Federal or State antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of record, making false statements, or receiving stolen property;

(c) Are not presently indicted for or otherwise criminally or civilly charged by a governmental entity (Federal, State or Local) with commission of any of the offenses enumerated in paragraph (1)(b) of this certification; and

(d) Have not within a three-year period preceding this application/proposal had one or more public transactions (Federal, State, or local) terminated for cause or default.

(2) Where the prospective primary participant is unable to certify to any of the Statements in this certification, such prospective participant shall attach an explanation to this proposal.

INSTRUCTIONS FOR LOWER TIER CERTIFICATION

1. By signing and submitting this proposal, the prospective lower tier participant is providing the certification set out below.

2. The certification in this clause is a material representation of fact upon which reliance was placed when this transaction was entered into. If it is later determined that the prospective lower tier participant knowingly rendered an erroneous certification, in addition to other remedies available to the Federal government, the department or agency with which this transaction originated may pursue available remedies, including suspension and/or debarment.

3. The prospective lower tier participant shall provide immediate written notice to the person to which this proposal is submitted if at any time the prospective lower tier participant learns that its certification was erroneous when submitted or has become erroneous by reason of changed circumstances.

4. The terms *covered transaction, debarred, suspended, ineligible, lower tier covered transaction, participant, person, primary covered transaction, principal, proposal, and voluntarily excluded,* as used in this clause, have the meanings set out in the Definition and Coverage sections of 49 CFR Part 29. You

may contact the person to whom this proposal is submitted for assistance in obtaining a copy of those regulations.

5. The prospective lower tier participant agrees by submitting this proposal that, should the proposed covered transaction be entered into, it shall not knowingly enter into any lower tier covered transaction with a person who is proposed for debarment under 48 CFR Part 9, subpart 9.4, debarred, suspended, declared ineligible, or voluntarily excluded from participation in this covered transaction, unless authorized by the department or agency with which this transaction originated.

6. The prospective lower tier participant further agrees by submitting this proposal that it will include the clause titled "Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion—Lower Tier Covered Transaction," without modification, in all lower tier covered transactions and in all solicitations for lower tier covered transactions. (See below)

7. A participant in a covered transaction may rely upon a certification of a prospective participant in a lower tier covered transaction that it is not proposed for debarment under 48 CFR Part 9, subpart 9.4, debarred, suspended, ineligible, or voluntarily excluded from the covered transaction, unless it knows that the certification is erroneous. A participant may decide the method and frequency by which it determines the eligibility of its principals. Each participant may, but is not required to, check the List of Parties Excluded from Federal Procurement and Non-procurement Programs.

8. Nothing contained in the foregoing shall be construed to require establishment of a system of records in order to render in good faith the certification required by this clause. The knowledge and information of a participant is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.

9. Except for transactions authorized under paragraph 5 of these instructions, if a participant in a covered transaction knowingly enters into a lower tier covered transaction with a person who is proposed for debarment under 48 CFR Part 9, subpart 9.4, suspended, debarred, ineligible, or voluntarily excluded from participation in this transaction, in addition to other remedies available to the Federal government, the department or agency with which this transaction originated may pursue available remedies, including suspension and/or debarment.

Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion—Lower Tier Covered Transactions:

1. The prospective lower tier participant certifies, by submission of this proposal, that neither it nor its principals is presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any Federal department or agency.

2. Where the prospective lower tier participant is unable to certify to any of the statements in this certification, such prospective participant shall attach an explanation to this proposal.

OGR Grant Conditions

INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM
TERMS AND CONDITIONS

In addition to the federal and state general grant conditions outlined above, the Office of Grants and Research (OGR) in the Executive Office of Public Safety and Security (EOPSS) has certain grant conditions that are essential to the administration of grant awards. Whether subrecipients are receiving funds from a federal or state grant, they must adhere to these conditions.

- **Federal *and* State Conditions** must be adhered to by subrecipients of federal grant funds.
- **Drug-Free Workplace Certification** for Departments Receiving Federal Grants for federal fiscal year 2014 available at http://www.mass.gov/osc/guidance-for-agencies/fiscal-year-updates/fy2014/fy2014-12.html
- **Time extensions**, while uncommon, may be granted at the option of OGR. They are not encouraged or guaranteed.
    - If a subrecipient needs additional time to complete the scope of work for the grant award, OGR may grant a time-only extension as long as the revised ISA containing the extension request is executed by both the subrecipient and OGR before the current end date of the ISA. No time extension can be granted if the revised ISA form is executed after the current ISA end date.
    - Requests for time extensions must to be made at least 30 days before the end date of the ISA.
- **Interdepartmental Service Agreement (ISA) spending** must adhere to the dates specified in the ISA. Spending occurring after the specified ISA end date may result in denial of those costs. The "child" department will be responsible for covering those costs with an account other than that funding the ISA. Subrecipients may not ask the Office of the Comptroller to extend an end date of the program code associated with the ISA without prior agreement by OGR. Should this occur, OGR will deny costs against the ISA. If the costs have already been accepted in MMARS, OGR will ask the "child" department to execute an expenditure correction transaction in MMARS to move those costs to another account belonging to the department.
- **Award amounts remaining at the end of the ISA** will be reverted back to OGR.
- **All goods must be received and all services rendered by the end date of the ISA.**
- **Each ISA has a defined accounts payable period.** All payments must be completed and disbursed by the end date of the specified accounts payable period.
- **An ISA that crosses a state fiscal year (June 30) into the next fiscal year, must observe the Commonwealth's policies on payment corrections or overpayments.** That is, any mistakes in coding must be corrected with an EX transaction before August 31. All payroll corrections must be made by the date in July specified in the Fiscal Year Open/Close guidance issued each year by the Office of the State Comptroller. Any overpayments must be corrected with an ER transaction before August 31. **If these actions are not taken by the times specified, the child department must move the charges to a non-OGR funded appropriation so that the funds can be returned to the federal government.**
- **Programmatic and financial reports** must be received in accordance with the requirements of the specific award. **OGR requires all Financial reports to be submitted along with a Warehouse Query detailing the expenditures made for that period.**
- **Procurement practices** specified by OSD must be followed. The subrecipient should ensure that its procurement practices conform to any specific federal guidelines found in the references in the federal conditions section above. Where there is a difference between the practices of the subrecipient agency/organization and a federal guideline, the more restrictive procedure applies.
- **Site visits and other monitoring** of subrecipients will be made by OGR periodically. All records, papers, and other documents of any kind related to the funded activity must be made promptly available upon request for inspection and copying to any person authorized by OGR.
- **Grant-related documents** must be retained for a period of six years from the close of the contract.
- **Evaluations** of a subrecipient's funded program by an outside evaluator during or at the conclusion of the project period, should be reported to OGR in writing and a copy of the evaluation should be provided.

INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM
TERMS AND CONDITIONS

- **Reporting alleged fraud, waste or abuse** to the Office of the State Auditor or Inspector General and/or to an applicable federal agency is the responsibility of the subrecipient. This includes any alleged violations, serious irregularities, sensitive issues or overt or covert acts involving the use of public funds in a manner not consistent with federal statutes, related laws and regulations, appropriate guidelines, or purposes of the grant.
- **Use of funds should begin** within 60 days of the start of the ISA, and if they are not, the subrecipient must report to OGR the steps taken to initiate the grant activities, the reasons for the delay, and the expected start of the use of the funds. If meaningful implementation steps have not begun after 60 days of the grant start date, OGR reserves the right to cancel the ISA.
- **Subcontractors** implementing activities with grant funds must adhere to the grant provisions in this document and should be approved by OGR prior to subrecipients executing subcontracts.
- **Instructional materials** created or produced with grant funds will be "work made for hire," as defined in United States copyright law, and EOPSS shall be considered the author. EOPSS shall be the sole owner of all rights pertaining to these materials, including copyrights and all rights to use, reproduce, or publish the materials, and subrecipients may not use, reproduce, or distribute such materials without prior written approval of OGR. If a project results in the production of **other original books, manuals, or copyrightable material**, unless otherwise provided in the contract documents, EOPSS reserves a royalty-free, non-exclusive and irrevocable license to reproduce, publish, translate or otherwise use, and authorize others to publish and use, such material. If paid with federal funds, the grant number must appear on the materials.
- **Audio visual or written materials** developed as part of the grant may be required to incorporate specific language or disclaimers (e.g., regarding the federal source of funding) and in some instances pre-approval from the federal funding agency as instructed by the OGR grants manager.

INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM

ATTACHMENT B - BUDGET

Check one: _X_ Initial ISA Budget

___ ISA Budget/Account Amendment. Maximum Obligation of ISA before this Amendment: $_____.

PRIOR MMARS DOCUMENT ID: _____ (for reference - if applicable)

CURRENT DOC ID: _____.

[See Instructions for Additional Guidance on completion. Insert as many additional lines as necessary.]

A Budget Fiscal Year	B Seller/Child Account	C Object Class	D Description	E Initial ISA Amount / or Amount Prior to Amendment	F Indicate Add or Reduce +/-	G Amendment Amount	H Enter "YES" if Amount is a prior FY budget reduction or a current FY "Carry-in" authorization for Federal ISA Funds	I New Amount After Amendment
2016	8000-4804	KK	**ALPR System**	$50,000.00				

FISCAL YEAR SUBTOTALS AND TOTAL MAXIMUM OBLIGATION FOR DURATION OF ISA	
FISCAL YEAR: _2016_____ SUBTOTAL (*or New Subtotal if Fiscal Year Subtotal being amended*	$ 50,000.00
FISCAL YEAR: ___ ____ SUBTOTAL (*or New Subtotal if Fiscal Year Subtotal being amended*	$
FISCAL YEAR: _____ SUBTOTAL (*or New Subtotal if Fiscal Year Subtotal being amended*	$
FISCAL YEAR: _____ SUBTOTAL (*or New Subtotal if Fiscal Year Subtotal being amended*	$
TOTAL MAXIMUM OBLIGATON FOR DURATION OF ISA (*or New Total Maximum Obligation if amended*)	$ 50,000.00

Additional Budget Specifications:

INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM

ATTACHMENT C – FEDERAL GRANT SELLER/CHILD ACCOUNT

[Complete ONLY if Buyer/Parent Account is a Federal Grant Account. Seller/Child Department must signoff in order to process document.]

__X__ NEW ISA ___ ISA AMENDMENT	BUDGET FISCAL YEAR: 2016
BUYER/PARENT DEPARTMENT: EPS	SELLER/CHILD DEPARTMENT: POL
CTR ONLY - REVENUE BUREAU WILL ASSIGN	
Revenue Budget	Revenue Source
BUYER/PARENT DEPARTMENT MUST COMPLETE ALL ITEMS BELOW	
CENTRAL BUDGET STRUCTURE (BGCN - BQ89)	
Appropriation Number: 80004804	Payroll Indicator : ___Yes __X__No
Budgetary Estimated Receipts $	BGCN Document Identification No.: ISAEPSFY16ALPRPOL16A
COST ACCOUNTING STRUCTURE (BGRG- BQ88)	
Total Maximum Obligation of ISA: $ 50,000.00	BGRG Document Identification No.: ISAEPSFY16ALPRPOL16A
MAJOR PROGRAM TABLE SET-UP	
Major Program (6 chars. or less) HSPGTS	Major Program Short Name (same as appropriation number): 80004804
Major Program Name: Highway Safety Program on GTS	
PROGRAM PERIOD TABLE SET-UP OR EXTENDED PROGRAM PERIOD	
Effective From Date:	Effective To Date:
Program Period:	
Program Period Name: Extended Program period	Program Period Short Name:
PROGRAM TABLE SET-UP	
Effective From Date: 02/01/2016	Effective To Date: 07/30/2016
Program Name: Automated License Plate Recognition	Program Short Name ALPR
Program Code: **(MUST START WITH "F" followed by up to 9 characters) F16ALPR**	Sub Account:

FUNDING PROFILE - FUNDING LINE		
Draw Name:	Customer ID	Payment System Code – **Check one option only**
EDCAPS:	VC7000000001	___**D**
ECHO:	VC7000000002	___**E**
LOCES:	VC7000000003	___**L**
SMARTLINK:	VC7000000004	___**S**
ASAP- OTHER:	VC7000000005	___**Y**
ASAP:	VC7000000006	___**Z**
GRANT- NON DRAW:	VC7000000007	__**X**__**No Code**

FUNDING IDENTIFICATION	
Federal Catalog Agency: (2 digit code) 20	Federal Catalog Suffix: (3 digit code) **600**
Letter of Credit No.:	

Authorized Signatory Seller/Child Department: _____ Date: _____ Name: _____

5269

INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM INSTRUCTIONS

The Interdepartmental Service Agreement (ISA) Form is issued by the Office of the Comptroller (CTR) pursuant to 815 CMR 6.00 for use by all Commonwealth Departments. The ISA Instructions are provided to assist both Buyer/Parent and Seller/Child Commonwealth Departments with the interpretation and completion of the ISA Form and are incorporated by reference into the ISA. The ISA Form is the "Contract" that documents the business agreement (joint venture) between two Commonwealth departments within the Executive, Judicial and Legislative Branches of government. A Department must be recognized as a Department in the State Accounting System (hereinafter referred to as "MMARS") in order to transfer or receive funding under an ISA. The ISA must comply with funding language in any appropriation act funding the ISA, as well as all applicable general and special state or federal laws, regulations. The Buyer/Parent and Seller/Child are responsible for reviewing and complying with the applicable CTR policies (including but not limited to the ISA, electronic signature and state finance law policies) located at the CTR Knowledge Center under Procurement and Contracts and also at the CTR Website at: Comptroller Policies. While reasonable efforts have been made to assure the accuracy of the legal requirements for ISAs, Departments should consult with their legal counsel to ensure compliance with all legal requirements related to their performance under an ISA. PLEASE NOTE THAT NOT ALL APPLICABLE LAWS HAVE BEEN CITED IN THIS DOCUMENT. INSTRUCTIONS AND HYPERLINKS MAY BE ADDED OR CHANGED WITHOUT NOTICE, SO CHECK THIS DOCUMENT PERIODICALLY FOR UPDATES.

➔ MMARS DOCUMENT ID: Enter the state accounting system (MMARS) BGCN or BGCS or other authorized MMARS document number associated with this ISA. ISA related DOC ID Numbering must be done as described below. The Doc ID must be the Doc ID entered into MMARS and reflected on the supporting ISA paperwork. All ISA Doc IDs MUST START WITH "ISA", as follows:

EXAMPLE DOC ID Number: **ISA**EPS12345678SDF06A

First 3 Characters	Second 3 Characters	Next 8 Characters	Next 3 Characters	Next 2 Characters*	Last Character
ISA	Buyer/Parent Department Alpha	Buyer/Parent defined. May be numeric, alpha or combination	Seller/Child Department Alpha	Fiscal Year	A (initial document) B (1st Amendment) C (2nd Amendment)
ISA	EPS	12345678	SDF	06	A

➔ BUDGET FISCAL YEAR. Enter the Budget Fiscal Year of the ISA or ISA Amendment, as appropriate.

➔ REQUEST FOR RESPONSE REFERENCE NUMBER. If the Seller/Child responded to an RFR that was posted on Comm-PASS, enter the RFR Reference Number as posted. If an RFR was not used, indicate "N/A". Seller/Child Departments may respond to a Request for Response (RFR) or other solicitation of a Buyer/Parent Department. If the Seller/Child Department is selected as a contractor, the ISA Form must be used as the "contract" (instead of the applicable Commonwealth Terms and Conditions and Standard Contract Form and Instructions).

➔ BUYER/PARENT/SELLER/CHILD DEPARTMENT NAME: Enter the 3 Alpha MMARS Department Code. For Example "CTR" for the Office of the Comptroller.

➔ BUSINESS MAILING ADDRESS: Enter the address where all correspondence to the ISA Manager must be sent. Unless otherwise specified in the ISA, legal notice sent or received by the Department's ISA Manager (with confirmation of actual receipt) through the listed fax number(s) or electronic mail address for the ISA Manager will meet any requirements for written notice under the ISA.

➔ ISA MANAGER: Identify the authorized ISA Manager who will be responsible for managing the ISA. ISA Managers must be Department Head Authorized Signatories in order to execute the ISA and otherwise obligate the Department with the appropriate MMARS Security to support Department Head Signature Authorization.

➔ PHONE/FAX/E-MAIL ADDRESS: Identify the phone, fax number(s) and electronic mail (e-mail) address of the ISA Manager.

➔ PURPOSE OF ISA. Check off whether this is a new ISA or an ISA Amendment. For New ISAs, enter the total Maximum obligation for the duration of the ISA. If an ISA Amendment, check off any of the Amendments that are being made and complete any information in the blanks provided and the Attachments that are identified.

➔ BRIEF DESCRIPTION OF PERFORMANCE GOALS TO BE ACCOMPLISHED BY THIS ISA, OR IF AMENDMENT, IDENTIFY WHAT IS BEING AMENDED: Identify a brief description of the ISA, ISA name and performance to be accomplished under the ISA. If an ISA Amendment, identify what is being amended. Merely stating "see attached" or referencing attachments without a narrative description of performance is insufficient *and will result in ISA or Amendment being returned to MMARS Liaison of Buyer/Parent Department*. The description is used to specifically identify the ISA performance, match the ISA with attachments and determine if the appropriate process has been selected.

➔ INDICATE WHETHER SELLER/CHILD DEPARTMENT STATE EMPLOYEES (AA OBJECT CLASS) WILL BE FULLY OR PARTIALLY FUNDED UNDER THIS ISA. Justification for use of state employees and details of who will be working and work that will be performed must be included as part of ATTACHMENT A.

➔ ACCOUNT INFORMATION.

- Check the correct option for either a BGCN – non-subsidiarized (federal, capital, trust); BGCS – subsidiarized (budgetary); Other (CT, RPO or other document authorized by CTR); Non-Financial ISA (no funds are transferred from Buyer/Parent to Seller/Child with resources committed to ISA; or Amendment without Budget changes to ISA (used only for an Amendment if there are no changes to the budget and no changes to Attachments B and C (if applicable).
- Identify for each account under the ISA whether the account is "added", "deleted or "no change". **THIS SECTION MUST BE COMPLETED FOR AMENDMENTS EVEN IF THE ACCOUNT INFORMATION HAS NOT CHANGED.** Enter each ISA account, fund, major program code and program code for all funding under the ISA. Attachment B must be completed for all financial ISAs and ISA Amendments (with Budgetary or Account amendments). Attachment C must be completed for any financial ISAs or ISA Amendments with Budgetary or Account amendments involving federal or capital funds).

➔ ISA ANTICIPATED START DATE**.** Enter the anticipated start date, provided that the Seller/Child certifies that it will not incur any obligations related to this ISA prior to the date that this ISA is executed, NOR prior to the date that sufficient funding for the obligations under this ISA available in the Seller/Child account for expenditure.

Note - ISA Duration. ISAs can be executed for the duration that makes sense from a business perspective. Multi-Year ISAs are encouraged if it best supports the Buyer/Parent and Seller/Child business processes. Similar to other types of contracts, all ISAs are subject to appropriation or other available funding. Therefore, Departments can enter into a Multi-year ISA even if funding transactions have to be processed annually to support each fiscal year of the ISA. Buyer/Parent and Seller/Child Departments are responsible for ensuring that the funding is in place in the authorized Seller/Child account(s) to ensure that the Seller/Child Department can timely encumber funds and pay employees, contractors, grantees, etc. from the authorized ISA Seller/Child account(s)in accordance with the ISA Terms and Conditions.

➔ TERMINATION DATE OF THIS ISA: The Buyer/Parent Department must enter the date the ISA will terminate. An ISA must be signed for the full duration and amount in accordance with what is negotiated between the Buyer/Parent and Seller/Child Department. Amendments to extend the

INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM INSTRUCTIONS

termination date, such as renewals, must be made using the ISA Form and must be signed by authorized Department Head signatories (with appropriate MMARS Authorized Signatory Security roles) of both the Buyer/Parent and the Seller/Child Department contemporaneously with the need for the amendment but no later than the termination date (or as previously amended) in accordance with 815 CMR 6.00.

➔ AUTHORIZING SIGNATURE FOR BUYER/PARENT DEPARTMENT/DATE: The Authorized Buyer/Parent Department Signatory must, in their own handwriting, and in ink, sign AND enter the date the ISA is signed. **THE DATE IS AN INEXTRICABLE PART OF THE SIGNATURE AND MUST BE COMPLETED BY THE SIGNATORY AND MAY NOT BE PRE-FILLED OR ENTERED AFTER THE SIGNATURE BY ANOTHER PERSON.** Rubber stamps, typed or other images are not acceptable. See CTR policies on Electronic Signature and Department Head Signature Authorization for Department Head and Authorized Signatory certifications and responsibilities.

➔ NAME /TITLE: The Buyer/Parent and Seller/Child Department Authorized Signatory's name and title must appear legibly.
NOTE: Secretariat signoff is not required in order for CTR to process an ISA. However, Seller/Child and Buyer/Parent Departments are required to follow any internal secretariat procedures when obtaining authorization for an ISA (or for certain ISA transactions such as an inter-subsidiary transfer "TS") prior to submission to CTR. All ISAs are periodically reviewed by CTR to verify that the signatories are authorized by their Department Head to execute contracts. Departments are responsible for timely processing through secretariats to ensure timely funding as required under the Department Head certifications.

➔ **ATTACHMENT A – TERMS OF PERFORMANCE AND JUSTIFICATIONS.** ***Attachment A is required for all new ISAs and for all ISA Amendments.*** Departments must use this attachment and insert (type, or copy and paste) the required information in addition to other terms of performance negotiated by the parties under Section 9. Sections 1-8 are mandatory and must be answered in detail or the ISA will be returned to the Buyer/Parent Department MMARS Liaison. All information must be inserted into Attachment A using as many pages as necessary. If Amending the ISA, completion of Sections 1, 2 and 3 identifying what is being amended and the reasons for the amendments is required. For sections 4-9 enter only the amended language in the sections being amended.

➔ **ATTACHMENT B - ANTICIPATED BUDGET.** ***Attachment B is required for all New ISAs and for all ISA Amendments with budget and accounting transactions.*** Departments must use this form. Insert all required information and use as many additional lines and pages as necessary. This attachment must breakdown the specifics of the ISA funding, by fiscal year, Seller/Child account, object class, description and amount. For multi-year ISAs the Attachment must provide a subtotal each fiscal year of the ISA (which equals each fiscal year's anticipated maximum obligation). All ISAs must provide a total maximum obligation for the total duration of the ISA (which must equal the total of all fiscal year subtotals) and must match the "Total Maximum Obligation for Duration of ISA" on the executed ISA.

- Check "Initial ISA Budget" , or "ISA Amendment"
- Identify the MMARS Doc ID if the ISA is being amended.
- **Complete Columns A-E For New ISAs. Complete Columns A-I for Amendments.**
  - **Column "A" (Budget Fiscal Year).** Enter the fiscal year of the funding, or amendment. For Multi year ISAs Column A must list planned expenditures by each fiscal year of the ISA.
  - **Column "B" (Seller/Child Account).** Enter the number of each Seller/Child account listed on the ISA Form. For ISAs using multiple Seller/Child Accounts, Column B must list planned expenditures for each Seller/Child account.
  - **Column "C" (Object Class).** Enter the Object Class (subsidiary) as outlined in the CTR Expenditure Classification Handbook (for example, "AA" for Employee compensation, "EE" for Administrative Expenses, "HH" for Consultant Contracts, etc.). IF the line item is authorized for multiple fiscal years, enter a separate line-item for each fiscal year of the ISA in which the line-item is authorized, specifying the estimated amount of the authorized expenditure. Line-items break downs of estimated expenditures by Object Class are required even if the Buyer/Parent account is non-subsidiarized, since the Budget acts as the authorization for the ISA expenditures. For subsequent fiscal years, entering "Balance Forward Amount" for federal, bond and trust accounts is insufficient, since good project management practices presume that departments will be managing estimated expenditures over the life of a project with planned fiscal year obligations, rather than managing projects solely based upon remaining uncommitted estimated receipts or uncommitted balances.
  - **Column "D" (Description).** Enter a brief description of the type of authorized budget expenditure or category, (e.g., "Conference Materials", "Program Manager", "Health Evaluations" etc.)
  - **Column "E" (Initial ISA Amount/or Amount Prior to Amendment).** Enter the amount for the budget item authorized under the ISA for each fiscal year. If the ISA is being amended, enter the current amount for this line-item, prior to the amendment. The Amendment amount will be entered in Column G and the new total will be entered in Column I.
  - **Column "F" (+/-)** is only used if the ISA is being amended to add or reduce a budget line item. Enter "+" for budget addition or "-" for a budget reduction.
  - **Column "G" Amendment Amount** is only used if the ISA is being amended to add or reduce a budget line item. Enter the amount of the budget line being increased or decreased.
  - **Column "H" (Carry-In)** is only used if the ISA is being amended to reduce a prior year federal grants fund line item with uncommitted estimated receipts that are being re-authorized in the current or a future fiscal year. Enter "YES" in this column for each line item being amended (by object class and description) to reflect a reduction in the budget in a prior fiscal year line item, and for each line item being added (by object class and description) to reflect a reauthorization of the funds in the current or a future fiscal year.
  - **Column "I" New Amount After Amendment** is only used if the ISA is being amended to add or reduce a budget line item. Enter new ISA Amount after the adding or reduction of the line-item amount referenced in Column G.
- FISCAL YEAR SUBTOTALS AND TOTAL MAXIMUM OBLIGATION.
  - Fiscal Year Subtotals. For single fiscal year ISAs enter the fiscal year (e.g., "Fiscal Year 2007") and enter the subtotal of all "Current Amounts" (Column E) for that fiscal year. For Multi-year ISAs, enter each fiscal year of the ISA as a separate subtotal and enter the subtotal of all "Current Amounts" for each fiscal year.
  - Total Maximum Obligation for Duration of ISA. Enter the Total Maximum Obligation for the Duration ISA for all fiscal years (as identified on the executed ISA Form). For single fiscal year ISAs, this amount should be the same as the Fiscal Year Subtotal. For Multi-fiscal year ISAs, this amount should equal the total of all the listed fiscal year subtotals.

➔ **ATTACHMENT C – FEDERAL GRANT SELLER/CHILD ACCOUNT** (complete only if Buyer/Parent Account is a Federal Account). Please enter the following information on this form.

- Enter whether this is a "New" ISA or an ISA Amendment and enter the Budget fiscal year.
- Enter the Buyer/Parent and Seller/Child Departments, which must match the ISA.
- *Skip the Revenue Budget and Revenue Source which will be completed by CTR.*
- CENTRAL BUDGET STRUCTURE:
  - Appropriation Number. Enter the Appropriation Number assigned by ANF.

INTERDEPARTMENTAL SERVICE AGREEMENT (ISA) FORM INSTRUCTIONS

- Payroll Indicator. Enter a Payroll indicator of Yes or No.
- Estimated Budgetary Receipts. Enter the amount of the Estimated Budgetary Receipts (the amount estimated in the ISA or Amendment for the current state fiscal year).
- BGCN Document Identification No. Enter the MMARS Document Identification Number for the Central Expense Document (BGCN). The BGCN must be entered and submitted to PEND in MMARS. Providing a screen print of the BGCN aids CTR in the processing of the ISA and set up of the accounts or account changes.

✸ COST ACCOUNTING STRUCTURE.

- Total Maximum Obligation of ISA or ISA Amendment Amount. For New ISAs, enter the Total Maximum Obligation of the ISA for the full duration of the ISA. For ISA Amendments, enter the amount of the modification.
- BGRG Document Identification No. Enter the MMARS Document Identification Number for the Reimbursable Grant Budget Document (BGRG). The BGRG must be entered and submitted to PEND in MMARS. Providing a screen print of the BGRG aids CTR in the processing of the ISA and set up of the accounts or account changes.

✸ MAJOR PROGRAM TABLE SET-UP. This sets up the cost accounting hierarchy with groups of activities (programs) all part of one structure. For example – a major program could be wastewater management – WASTE. All documents (contracts, encumbrances, payments will reference this code.) All documents (contracts, encumbrances, payments will reference this code.)

- Major Program. Enter the 6 (or fewer) character Major Program Code assigned by the department.
- Major Program Name. Enter the full Major Program Name.
- Major Program Short Name. Enter the Major Program Short Name.

✸ PROGRAM PERIOD TABLE SET-UP OR EXTENDED PROGRAM PERIOD (EPP). Enter the Program Period or Extended Program Period (EPP) information. This establishes the effective period of the grant. Please note that end dates are "hard edited" by the system, thus please take into account the accounts payable period for grants when establishing this date. Multiple periods allow for easy periodic reporting aligned to federal reporting dates. However, a Buyer/Parent department may choose to use 1 reporting period – EPP – that encompasses all dates. The downside of this method is that specific periodic federal reporting by the system is not achieved.

- Enter the Program Effective From Date and Effective to Date.
- Enter the Program Period or Extended Program Period (EPP) information.
- Enter the Program Period Name, and Program Period Short Name.

✸ PROGRAM TABLE SET-UP.

- Enter Program Name. For example a program could be for "storm water discharge".
- Enter Program Short Name:
- Program Code. Enter the 10 (or fewer) characters. All Federal Program codes must begin with the letter "**F**". This is the second level of the cost accounting hierarchy. Programs are individual activities within a Major Program. Using the major program example, a program could be for storm water discharge – the program code would be "Fstormdis". All documents (Recurring Payment Order (RPO), payments will reference this code.)
- The sub account must be the sub account in the award letter or the draw on the federal grant will fail. If a sub-account changes, this code must change.

✸ FUNDING PROFILE - Funding Line. This must be filled out properly – indicating the federal payment system to be used. If the wrong payment system is indicated, the draws on the federal grant will fail. Enter a check next to appropriate Payment System Code.

✸ FUNDING IDENTIFICATION.

- Federal Catalog Agency Code. Enter the 2 digit Federal Catalog Agency code.
- Federal Catalog Suffix. Enter the 3 digit Federal Catalog Suffix code from your award letter or contact the appropriate agency. This must align to the grant award. The proper grant identification information is a federal reporting requirement.
- Letter of Credit No. Enter the Letter of Credit No. for this grant award.

COMPLETED ISAS SHOULD BE SUBMITTED FOR PROCESSING TO:

Office of the Comptroller, One Ashburton Place – 9th Floor, Attention: Accounts Payable Bureau, Contracts, Boston, MA 02108
CTR Helpline: **617-973-2468**

Access Control Systems

PO Box 7521
Milford, NH 03055

Invoice

Date	Invoice #
1/8/2016	ACS16-4281

Bill To

MA State Police Fusion Ctr
Trpr. Brian Egnitz
470 Worcester Road
Framingham, MA 01701

FEID 35-2353461
DUNS 05-3355991

P.O. No.	Terms	Project	Rep
2016ACSYSU07POL21...	Net 30	MA State Police Fusion Ctr	CRP

Description	Qty	Qlfy	Rate	Amount
Wanco Systems- Mini Remote Video Monitoring System: WVT3(A) 3 Lines x 8 characters, 14" default font size, Upgrade solar panel 255W, 3 x 12V batteries, 600 Ah total capacity, 45 amp charger, Telescoping tower with 360 degree rotation, Full size computer console, Orange powder-coat finish, 2" ball hitch, Hydraulic Tower Lift, 400W inverter. Includes 1 Axis P5624E Camera or current model, Mounted 3M LPR single camera system, cellular remote modem: Sierra Wireless GX450, 3 RJ45, 1 serial, GPS, antennas mounted to sign and shipping. Estimated run time: All equipment: 9 days winter, 30 days summer. LPR 30 days Fall/Winter, Autonomous Spring Summer	1		34,125.00	34,125.00

Please remit to above address.

Total	
Payments/Credits	
Balance Due	

Access Control Systems

PO Box 7521
Milford, NH 03055

Invoice

Date	Invoice #
1/8/2016	ACS16-4281

Bill To

MA State Police Fusion Ctr
Trpr. Brian Egnitz
470 Worcester Road
Framingham, MA 01701

FEID 35-2353461
DUNS 05-3355991

P.O. No.	Terms	Project	Rep
2016ACSYSU07POL21...	Net 30	MA State Police Fusion Ctr	CRP

Description	Qty	Qlfy	Rate	Amount
Wanco Systems- Speed Trailer: Full matrix display - 26" LED characters - 24"x 30" regulatory speed limit sign with changeable speed limit numbers - Approach- only K band radar, FCC approved - Two 85 watt solar panels - Three 12VDC AGM batteries, 600 Ah total capacity - Telescoping tower with 90-degree rotation - Locking control box - White powder-coat finish - 2" ball hitch - 45A Battery charger, Axle Bar Lock, 400W inverter. Includes: Customer specified Sierra Wireless GX450 Modem with 3-RJ45 and 1 Serial Connection and Antenna mounted to sign and mounting of (1) 3M Camera (provided by other) and shipping. Estimated run time: 6-10 days between battery and charge, seasonal performance	1		21,060.00	21,060.00

Please remit to above address.

Total	
Payments/Credits	
Balance Due	

Access Control Systems

PO Box 7521
Milford, NH 03055

Invoice

Date	Invoice #
1/8/2016	ACS16-4281

Bill To

MA State Police Fusion Ctr
Trpr. Brian Egnitz
470 Worcester Road
Framingham, MA 01701

FEID 35-2353461
DUNS 05-3355991

P.O. No.	Terms	Project	Rep
2016ACSYSU07POL21...	Net 30	MA State Police Fusion Ctr	CRP

Description	Qty	Qlfy	Rate	Amount
Wanco Systems- Custom Mast Trailer: As per picture w/ previous mount for 3M LPR, 500 W Solar/ 3 x 200Ah, AGM Batteries (600 total Ah), 400W Inverter, 45A Battery Charger, Sierra Wireless GX450. Includes mounting of 3M camera (provided by other) and shipping. Estimated run time: Autonomous all year round	2		18,557.50	37,115.00
Training Services- One Day at customer site with a Wanco Factory Technician to go over commissioning , system operations and basic maintenance. ** Training DOES NOT cover the 3M LPR system **. Training requires a minimum of 2 weeks advanced scheduling.	1		2,925.00	2,925.00
PURCHASED VIA PO# 2016ACSYSU07POL21948				

Please remit to above address.

Total	$95,225.00
Payments/Credits	$0.00
Balance Due	$95,225.00

Overdue payments will result in late fees of 1.5% monthly. For billing questions call (603) 249-9820. If your check is returned for non-sufficient funds, you expressly authorize your account to be electronically debited or bank drafted for the amount of the check plus any applicable fees. Payment by check is your acknowledgement and acceptance of this policy and its terms and conditions.

5275

LAW ENFORCEMENT EQUIPMENT, SUPPLIES, & SERVICES



SAFEWARE®

SAFEOPS



ACCESSORIES
- B-Square
- Blackinton
- Break-Free
- Hoppe's
- KleenBore
- M-PRO 7
- Smith & Warren
- Speedfeed

AERIAL DRONES
- Aeryon
- DJI
- FLIR

APPAREL
- 5.11 Tactical
- Arc'teryx
- Bulwark
- Elbeco
- Horace Small
- LION
- PROPPER
- Spiewak
- TRU-SPEC

BAGS, CASES & PACKS
- 5.11 Tactical
- BLACKHAWK!
- Crye Precision
- Hatch
- OK-1
- Pelican
- Plano
- R&B Fabrications
- Wolfpack Gear

BALLISTIC SHIELDS
- Hatch
- Paulson Mfg.
- PROTECH Tactical
- United Shield

BATONS
- ASP
- Monadnock

BODY ARMOR & HELMETS
- 3M
- ABA
- Angel Armor
- Armor Express
- Crye Precision
- Custom Armor Group
- FirstSpear
- HESCO
- PROPPER
- PROTECH Tactical
- Second Chance
- Team Wendy
- United Shield

BODY CAMERAS
- Kustom Signals
- HauteSpot Networks

BUNKERS & BARRICADES
- Mitigation Technologies
- Special Ops Bunker

COMMUNICATIONS
- Atlantic Signal
- Con-Space
- LRAD
- NowForce
- Peltor
- Tactical Electronics

CRIME SCENE INVESTIGATION
- DetectaChem
- EVI-PAQ
- Forensics Source
- FoxFury
- Identicator
- Lightning Powder
- Mistral Security
- NIK Public Safety
- ODV
- TacticID by B&W Tek

DECONTAMINATION
- Decon7
- DuPont
- Force1Decon
- Kappler
- Lakeland
- TrueTech

DUTY GEAR
- Bianchi
- BLACKHAWK!
- Boston Leather
- Gould & Goodrich
- Safariland
- Uncle Mike's

EOD
- ADS
- BAHIA 21
- Inert Products
- Lindon Defense
- Med-Eng
- Mistral Security
- Tactical Electronics
- TacticID by B&W Tek
- United Shield

EYEWEAR
- 3M
- Crossfire Safety
- Edge Eyewear
- ESS
- MSA
- Paulson Mfg.
- Pyramex Safety
- Radians
- Revision Military
- Smith Optics
- Wiley X

FIELD TESTING, DRUG & ALCOHOL
- DetectaChem
- Field Forensics
- Intoximeters
- Mistral Security
- TacticID by B&W Tek
- Thermo Fisher
- TrueTech

FIRE SUPPRESSION
- Cold Fire Tactical

FIRST AID & TRAUMA
- Combat Medical Systems
- H&H Medical
- North American Rescue
- Tactical Medical Solutions
- Z-Medica

FLASHLIGHTS & ILLUMINATION
- BLACKHAWK!
- Brite-Strike
- Cyalume
- Eflare
- FoxFury
- Nightstick by Bayco
- Pelican
- Streamlight
- SureFire

FOOTWEAR
- 5.11 Tactical
- Black Diamond
- BLACKHAWK!
- Danner
- HAIX
- Onguard Industries
- Timberland PRO
- Tingley Rubber

GLOVES & ACCESSORIES
- 5.11 Tactical
- Ansell
- Best Glove
- Hatch
- HexArmor
- Honeywell

HANDCUFFS & RESTRAINTS
- CTS Thompson
- Hiatt
- Monadnock

HAZARDOUS ENVIRONMENT APPAREL
- Blauer
- DuPont
- Kappler
- Kimberly-Clark
- Lakeland
- LION
- Radiation Shield Technologies

HAZARDOUS ENVIRONMENT MONITORING
- ADVNT Biotechnologies
- Biosystems
- Bruker Detection Corp.
- BW Technologies
- Chemring
- Draeger
- GFG Instrumentation
- Honeywell
- MSA
- Proengin
- RAE Systems
- Response Biomedical/ RAMP
- Scott Safety

HEAD PROTECTION
- CMC Rescue
- Custom Armor Group
- Hatch
- Revision Military
- Team Wendy
- United Shield

HEARING PROTECTION
- Howard Leight
- MSA
- Peltor

HYDRATION & COOLING
- CamelBak
- TechNiche

K-9
- Castle's K-9
- Vohne Liche Kennels

KNIVES
- Benchmade

LESS LETHAL
- Combined Systems
- Defense Technology
- FNH
- Royal Arms
- Sage Control Ordnance

LICENSE PLATE RECOGNITION
- 3M
- Cintel
- Vigilant Solutions

OPTICS, THERMAL & NIGHT VISION
- Aimpoint
- Argus
- ATN
- Bushnell
- Dueck Defense
- FLIR/Armasight
- Fraser Optics
- Holosun
- ITT Night Vision
- L3-EOTech
- Morovision
- Night Optics USA
- Vortex Optics
- Wilcox

RESPIRATORY
- 3M
- Avon Protection
- Draeger
- Honeywell
- MSA
- North
- Scott Safety

RIOT CONTROL
- Argus
- Armadillo Merino
- Cold Fire Tactical
- Damascus
- DMS
- FirstSpear
- Hatch
- Mehler Law Enforcement
- Original S.W.A.T.
- Yaffy

ROBOTS
- ICOR Technology
- Mistral Security
- Northrop Grumman
- RoboteX
- QinetiQ

SECURITY
- ADANI Systems
- CEIA
- Garrett
- Rapiscan Systems

TOOLS & TACTICAL ENTRY EQUIPMENT
- Armadillo Tactical Gear
- BLACKHAWK!
- Broco
- HURST Jaws Of Life
- J&N Tactical
- Mistral Security
- Osen-Hunter
- Wilcox

TRAFFIC SAFETY & SPEED DETECTION
- Bone Safety Signs
- Eflare
- Harris Industries
- JBC Safety
- Kustom Signals
- ML Kishigo
- MPH Industries
- Stalker Radar
- Wanco

TRAINING EQUIPMENT
- Monadnock
- UTM

TRAINING SERVICES
- Blackthorne Services Group
- Safariland
- Survival Edge Tactical Systems

VEHICLES
- ICS
- LDV
- Lenco
- Nomad
- Polaris

VIDEO & SURVEILLANCE
- AgileMesh
- Camero
- Kustom Signals
- Tactical Electronics

WEAPON ACCESSORIES
- Badger Ordnance
- FirstSpear
- SureFire
- TAB Gear

WEAPON SECURITY
- Auto Vault











TABLE OF CONTENTS

5278

HEAD PROTECTION 6
COMMUNICATIONS 7
RESPIRATORY 8
BODY ARMOR 10
BALLISTICS 10
ACTIVE SHOOTER 11
PUBLIC ORDER 12
- FR BASE LAYER 12
- FR OUTER GARMENT 13
- SCORPION BODY ARMOR 14
- SCORPION BODY ARMOR/VESTS 15
- HEAD PROTECTION 16
- HAND & FOOT PROTECTION 17
- RESPIRATORY PROTECTION 18
- SHIELDS/BATON 19
- FIRE SUPPRESSION 20
- LESS THAN LETHAL 20
- IDENTIFICATION 21
- ACCESSORIES 21

FIRST AID & TRAUMA 22
EXPLOSIVE MITIGATION 24
ROBOTS 26
DRUG DETECTION 27
NIGHT VISION 28
THERMAL IMAGING 28
FLASHLIGHTS & ILLUMINATION 29
VIDEO & SURVEILLANCE 30
TACTICAL ENTRY 31
TRAINING SERVICES 32
K9 32
BODY CAMERA 33
SPEED DETECTION 33
VEHICLES 34
GAS DETECTION 34
RADIATION DETECTION 35
PPE 35
DECONTAMINATION 37
HEARING 38
APPAREL 38
FOOT PROTECTION 39
DUTY GEAR 40

FOR MORE INFORMATION OR TO PLACE AN ORDER:

800.331.6707 | info@safewareinc.com | www.safewareinc.com

UNITED SHIELD ACH/MICH MIL BALLISTIC HELMET

The new US Military design featuring a low profile compact helmet with minimum target area and weight.



- Weight: 2.6-2.8 lbs.
- Features an advanced 7 comfort pad system
- Offers improved head stability with a 4-point adjustable harness, suede covered chip cup and nape strap
- Ballistic performance to NIJ 0106.01 and HP White 0401.01
- Shock absorption - US Army ACH Spec for impact
- Hemi-Anvil, 10ft/sec with less than 150 G's force transmitted to head
- Fragmentation performance to US ACH Mil-Spec

UNITED SHIELD SPEC OPS DELTA GEN II

Made from advanced Aramid composites and provides lightweight robust protection from ballistic and fragmentation projectiles as well as other low energy threats.



- Weight: 2.7 lbs.
- NEW carbon fiber Universal NVG mount with guaranteed no-rattle fit
- NEW USI Rapid Adjustment Dial BOA® retention system with 2-way adjustments
- NEW 4D Combat Pad ultra comfort system with phase change technology
- Industry leading ballistic proprietary thermoplastic aramid composite shell
- Removable suede split chin strap to allow for laundry, replacement or use of gas mask extender
- 4-point adjustment harness, picatinny rails, helmet VELCRO® brand fastener kit and bungees
- NIJ 0106.01 Level IIIA, HP White 0401.01B Level IIIA and exceeds US MIL-SPEC for ACH helmet for 2, 4, 16, 64, 17 grain fragments

REVISION MILITARY BATLSKIN VIPER™ P4 HELMET

The Viper P4 head protection system is the most advanced combat helmet, weighing up to 24% lighter than the legacy U.S. Army ACH system - pushing the boundaries of obtainable weight reduction while maintaining superior ballistic and fragmentation protection.



- Stops NIJ IIIA level threats
- Available with Revision's MSS Liner System for enhanced comfort and stability
- Every helmet meets U.S. Army's strict performance, protection and quality standards
- Foundation for all Batlskin modular protection system components and accessories
- Available in 3 cuts (full, mid and high) and 4 sizes (S-XL)

UNITED SHIELD PASGT BALLISTIC HELMET

The PASGT helmet is manufactured with state of the art advanced high strength multi-layered Aramid composites laminated under heat and pressure.

- Excellent bullet resistance
- Minimal deformation at a weight of approximately 3 lbs.
- Offers improved head stability with a 4-point adjustable harness, suede covered chip cup and nape strap
- Ballistic performance to NIJ 0106.01 and HP White 0401.01B
- Wider cut around ears and collar cut to reduce interference from other equipment



TEAM WENDY EXFIL® BALLISTIC HELMET

With a ballistic rating of NIJ Level III-A, it exceeds current ACH Blunt Impact Protection requirements and offers optimal comfort, fit and stability.

- Hybrid composite shell for increased strength and a unique geometry for ideal fit
- Boltless CAM FIT™ retention utilizes a Boa® Fit System with Cam Lock sliders for one-handed adjustment. Left Eye Dominant (LED) option also available.
- Zorbium® foam liner provides customizable comfort while protecting against blunt impact, and allows for an overhead communications headband
- Lanyard compatible Wilcox® shroud secures any standard NVG mount
- Complete system weight of 2.6 lbs. (size 1) and 2.75 lbs. (size 2) includes the helmet shell, accessory rails, impact liner and retention system





LRAD® 100X

Self-contained, hand-held portable voice broadcast system for on-scene and tactical communications.

- Powerful, intelligible communication up to 600 meters
- 20-30 decibels louder than bullhorns and vehicle P.A. systems
- Focused, directional sound pattern for target-ed communication
- Create instant acoustic standoff perimeter
- 8-hour rechargeable battery
- Simple operator interface
- Water resistant



LRAD® 500X-RE

Compact long range communication system designed for mounting on tripods, larger vehicles and boats.

- Fixed or portable mounting
- Powerful, intelligible communication up to 2,000 meters
- Voice boost for extended coverage
- Creates instant acoustic standoff perimeter
- Rugged, military tested construction
- All-weather use
- Low power requirements: 60W w/voice, 260W w/ tone
- Simple operator interface



LRAD® 500X-MMT

Fully self-contained helicopter mounted, air-to-ground communication system featuring rugged mount with fu pan-and-tilt range of motion.

- Powerful, intelligible communication up to 2,000 meters
- Quickly installed and removed from helicopter
- Self-powered for 6+ hours of continuous operation when fully charged
- Supplemental type certificates not required
- Simple operator interface



LRAD® 100X MAG-HS KIT

Rapidly deployable, self-contained voice broadcast system with high-strength magnet mount and wireless operation capability.

- Wireless control up to 300 meters and a high strength, easy on/off magnetic mount system
- Up to 6X louder than systems of comparable size and weight
- Focused, directional sound pattern for targeted communication with unparalleled clarity
- Create instant acoustic standoff perimeter
- High-strength neodymium mount system
- Wireless system batteries operates up to 8 hours
- 8-hour rechargeable battery
- Simple operator interface
- Water resistant



LRAD® 360XT SOLAR W/ SATELLITE CONTROL

Mobile, self-contained mass notification system on wheels. Broadcasts highly intelligible voice messages and warning sirens with uniform 360° area coverage.

- Integrated with a fully self-contained, ruggedized trailer and features lockable electronics and equipment enclosures containing the amplifier modules and battery pneumatic systems
- Battery bank can be charged using the built-in AC powered battery charger or optional solar panel
- Standard configuration of a 3 stack 360X emitter provides a 1,000 meters radius of clear communication coverage



LRAD® 360XL-MID MOBILE KIT

Rapidly deployable, fully self-contained mass notification and incident management communication system.

- 360° uniform sound coverage
- Powerful, highly intelligible voice communications over 2.0 km2
- Complete mass notification kit (emitter head, power amplifier, control module, push-to-talk microphone)
- Lightweight and compact form factor
- Low power consumption for hours of continuous operation
- Industry-leading voice clarity and intelligibility



LRAD® 450XL

Low profile, lighter weight and designed for temporary or fixed mounting on tripods, vehicles, and small boats. Generates the audio output of systems almost twice its size and weight.

- Powerful, intelligible communication up to 1,700 meters
- Voice boost for extended coverage
- Safely communicate beyond standoff distances to determine intent
- Clear, long-range directional communication
- All-weather use
- Creates isntant acoustic standoff perimeter

LRAD

AVON FM54™ AIR PURIFYING RESPIRATOR

Provides maximum level of protection to the face, eyes, and respiratory tract from CBRN, riot agents, TICs, and toxic industrial materials while maintaining extreme user flexiblity as mission profiles change.

- Functions in both negative and positive pressure modes (APR, SCBA, CCBA, and PAPR)
- Panoramic single lens visor
- Electronic communication port for integrated voice projection and radio communication
- 4 sizes to accommodate all operators
- Low profile brow for superior helmet compatibility
- Interchangeable silicone nosecups for custom fit
- Multiple modes
- Optional VPU provides ability to easily communicate while wearing mask



AVON C50™ MASK ASSEMBLY

Based on the U.S. M50/JSGPM (Joint Services General Purpose Mask) and sharing key technologies, provides maximum operational flexibility to counter multiple threat scenarios, including CBRN agents, TICs and TIMs.

- Offers high protection, outstanding field of vision and superior comfort
- The innovative design features optimize the user's time in the operational area

FOR A NON-CBRN OPTION, ASK ABOUT AVON'S PC50



AVON ST53™ SCBA

Combines Avon's FM53 mask technology with an advanced modular breathing apparatus to provide positive pressure SCBA and/or PAPR capability for specialist operations.

- Utilizes black anodised lightweight components
- Enables a fast response to changing operational conditions in one complete modular system
- A switch between negative (filter) and positive (SCBA) pressure is achieved at the flick of an easy to locate lever on the front of the mask
- Can attach a short or long duration compressed air cylinder and enter a location on filter mode, assess the situation and change to SCBA mode if the need arises



MSA G1 SCBA

Designed solely with your safety and comfort in mind. The G1 SCBA offers integrated and enhanced solutions to exceed your needs today as well as years into the future.

- Facepiece is lightweight and compact (no electronics needed)
- Control module provides dual color LCD and analog displays
- Improved visibility through buddy lights and reflective material
- Heads up display (HUD) shows remaining cylinder pressure in 4 increments via colored LEDs
- Electronic communications are integrated into every unit
- G1 SCBA ergonomics
- Central power system for all electronics
- Available in easily-upgradeable threaded or quick-connect cylinder attachment
- Integrated technology for future expansion
- Customizable



MSA MILLENIUM CBRN GAS MASK

A Hycar version of the reliable military-style gas mask (MCU-2/P Mask, used by the Air Force in Desert Storm). The mask combines high performance, customized fit, comfort, cost efficiency and is ideal for law enforcement and emergency response personnel.

- Flexible, one piece polyurethane lens with wide field of vision, bonded to a durable super-soft Hycar rubber facepiece
- NIOSH approved for protection against CN and CS tear gas
- Effective against, but does not have approval for OC tear gas
- Effective against biological agents and chemical warfare agents
- Dual-canister mount to allow weapon firing from either shoulder
- Canister provides up to 8 hours service time against CN, CS and OC agents
- Drinking tube to allow fluid ingestion in contaminated atmospheres
- Standard equipment includes a speaking diaphragm for clear, short-range communications
- Features a nosecup to reduce lens fogging in low temperatures or high humidity conditions

MSA MILLENIUM CBRN CANISTER







3M™ SCOTT SAFETY AV-3000 W/ SURESEAL FACEPIECE

Combines superior fit with greater comfort and versatility. Holds NIOSH approvals across a wide variety of applications, including CBRN.

- Top down convertibility-single facepiece for APR, PAPR, supplied air and SCBA applications, including CBRN
- Reverse Reflex faceseal for improved comfort and fit
- Deep, low profile seal for easier interface with PPE
- Dual large mechanical voicemitters as well as extensive electronic options for improved communications for every workplace
- Available with Kevlar, Poly or Rubber head harness

3M™ SCOTT SAFETY 40MM CARTRIDGES AND CANISTERS



3M | SCOTT Fire & Safety

3M™ SCOTT SAFETY AIR-PAK™ X3 PRO

The Air-Pak™ X3 Pro SCBA is built on a proven foundation of redundant safety features to help ensure the security and comfort of today's firefighter.



- Easy to remove harness
- New harness materials offer greater resistance to chemical and water absorption to help minimize contamination
- Reflective webbing
- Natural articulation promotes greater range of motion to the firefighter, while transferring weight to the hips for a more balanced load
- Superior breathablity
- Electronic PAR (ePAR) provides wireless, bi-directional communication between the firefighter and incident command to improve fireground accountability and communications
- New buckle design provides firm hold
- Integrated drag rescue loop
- System integrity alarm provides visual and audible alert
- High flow alarm provides visual and audible alert
- No flow alarm provides visual and audible alert
- "Buddy" lights provide a 360° view of the firefighter's air pressure and PASS status

Honeywell

NORTH®

HONEYWELL OPTI-FIT™ TACTICAL GAS MASK

- Superior field of vision offers an unobstructed view
- Full facepiece constructed of soft silicone for excellent comfort, fit and durability
- Choice of headgear - 5-pt. strap or nylon mesh headnet
- Three-position canister mounting adaptable for various applications
- Anti-scratch coated polycarbonate lens
- Lens meets ANSI Z87.1 standard for impact and penetration resistance
- DIN-threaded 40 mm connectors
- Low breathing resistance
- NIOSH approved with the Model 1688 Canister to provide protection against choloracetophenone (CN), chlorobenzylidene malononitrile (CS) and includes a P100 filter for use against particulates such as pepper spray
- NIOSH approval number TC-14G 0264





HONEYWELL NORTH SAF-T-FIT® P100 PARTICULATE RESPIRATOR

NIOSH-approved P100 protection provides 99.97% particulate efficiency against oil and non-oil based particulates.

- Meets OSHA and EPA filtering facepiece requirements for lead abatement
- Full face seal for secure and comfort fit
- Durable and adjustable straps
- Exhalation valve expels warm air
- Molded cup design
- Incorporates humidity-resistant filter media
- Low breathing resistance
- Lightweight design
- Nose clip is color-coded for visible size recognition
- Latex free
- Multiple size options for wide range and improved fit

AIRIUS AND ARAURA LEVEL IIIA ALSO AVAILABLE



UNITED SHIELD AIRIUS LEVEL II VEST

The latest innovation in WEARABLE body armor.

- NIJ 0101.06 certified Level II armor
- Provides the areal density weight and thinness of leading polyethylene vests with the flexibility and softness of leading aramid vests
- Comes standard with SPA carrier with 'Dry Run' moisture management system to wick away mositure from the body
- The SPA features a 12-point adjustment system, hidden plate pockets, full side coverage, recessed closure system and optional tails
- Weight: 0.63 psf
- Thickness: .22'
- Performance: 9mm v50 - 1705 fps/.357 v50 - 1685 fps

UNITED SHIELD ARAURA LEVEL II VEST

- Weight: 0.99 psf
- Thickness: .25'
- Performance: 9mm v50 - 1729 fps/.357 v50 - 1663 fps

BALLISTICS



UNITED SHIELD LITE TACTICAL VEST

Blends the functionality of a tactical carrier with a lightweight design that's geared for high performance. Features an abrasion resistant outer fabric that provides exceptional durability for extreme situations.

- Sturdy 500D Cordura® nylon outershell exterior construction
- Top loading plate pockets
- Additional pocket for one size smaller rifle plate
- MOLLE compatible webbing on the front, back and sides
- Adjustable shoulder straps
- Adjustable cummerbund with hook/loop closure underneath the front flap
- Bungee lace cummerbund adjustment
- Flat Kanagroo magazine pockets on front flap
- "Man-Down" drag strap in the rear
- Internal straps for adjustable groin protector
- Accepts insertion of United Shield concealable panels



UNITED SHIELD GARRISON VEST

Providing high performance ballistic protection, integrated in a fully functional and versatile design to meet the strategic needs of your specific mission.

- Sturdy 500D Cordura® nylon outershell exterior construction
- Top loading plate pockets
- Additional pocket for one size smaller rifle plate
- MOLLE compatibility on front, back and sides
- Adjustable shoulder straps
- Adjustable cummerbund with hook/loop closure underneath the front flap
- Bungee lace cummerbund adjustment
- Flat Kangaroo magazine pockets on front flap
- "Man-Down" drag strap in the rear
- Internal straps for adjustable groin protector



UNITED SHIELD MOLLE CROSSOVER CARRIER

Ideal for law enforcement officers who have occasional equipment-carrying assignments. Can be easily converted into a ballistic protective vest by allowing insertion of United Shield ballistic panels.

- Durable 500D Cordura® nylon exterior fabric
- Spacer mesh interior fabric improves breathability
- Top loading internal front and back plate pockets
- MOLLE webbing compatibiilty in the front of the carrier
- Adjustable front to back side hook/loop closure
- Internal 4" adjustable elastic cummerbund sewn in the back



UNITED SHIELD DELTA +6H BALLISTIC PLATE

Level III+ stand alone single curve ballistic plate. Ergonomically designed using proven technology affording the wearers excellent stand alone protection against a range of high velocity threats.

- NIJ 0101.06 Certified
- 3.1 lbs. | 10" x 12"

DELTA LITE 6H ALSO AVAILABLE

UNITED SHIELD SIGMA 6H BALLISTIC PLATE

Level III+ stand alone multi-curve ballistic plate. Ergonomically designed using proven technology affording the wearers excellent stand alone protection against a range of high velocity threats.

- NIJ 0101.06 Certified
- 5.8 lbs. | 10" x 12"

SIGMA LITE 6H ALSO AVAILABLE

UNITED SHIELD ZETA 6H BALLISTIC PLATE

Level III+ stand alone single curve ballisitic plate. Ergonomically designed using proven technology affording the wearers excellent stand alone protection against a range of high velocity threats.

- NIJ 0101.06 Certified
- 7.6 lbs. | 10" x 12"

ZETA LITE 6H ALSO AVAILABLE



UNITED SHIELD UNIFORM SHIRT CARRIER

Specially designed to be worn over the dress shirt.

- Uniform shirt design
- Durable 600D Cordura® nylon exterior fabric
- Poly/cotton interior fabric
- Hook/loop shoulder adjustment
- Front adjustable side hook/loop closure
- Two front lower pockets with zipper closure
- Internal tablet pocket with zipper closure
- Front chest pockets with hook/loop closure
- Internal cell phone pocket
- Pen openings
- Shoulder mic tabs
- Bottom internal ballistic opening

ACTIVE SHOOTER

UNITED SHIELD LEVEL IV ACTIVE SHOOTER KIT

Includes:

- (1) PST SC650 helmet
- (2) Zeta 6h NIJ06 certified Stand Alone Ballistic Plates and (1) carrier option
- The Level IV plates are ergonomically designed to offer the user NIJ 0101.06 certified stand alone protection
- Bag included





BALACLAVA

- Fire retardant
- Designed to give a specified level of protection against accidental contact with flame and against certain forms of heat transfer
- One Size

DARK NAVY

EA — ARM 21305-15 (SZ)

ARMADILLO MERINO EPIC SOCK

- Over the calf sock
- Extra long so it can be folded down over the top of the boot
- Elastic arch support system
- Elastic above the ankle for a better fit
- Lightweight high-stretch padding up the shin and across the top of the foot
- Reinforced toe and heel
- Smooth toe seam
- 62% wool, 21% polyamide, 9% polypropylene, 8% elastic
- SM-XL

DARK NAVY

PR — ARM 11511-15-1 (SZ)

ARMADILLO MERINO COUGAR SHORT SLEEVE CREW SHIRT

- Crew neck with generous back length
- Seamless underarm for no chaffing and seamless shoulders designed for load carrying
- Extra strong tread in the stitching and a tag free neckline
- Regular fit
- 100% Merino Wool, Jersey Knit
- SM-4X

DARK NAVY

EA — ARM 21001-15-X

ARMADILLO MERINO JOHNNIES 2 LONG JOHN BOTTOMS

- Flattened seams for increased comfort
- Body hugging fit - comfortable under your uniform
- Tag free waist
- Flatlock stitching
- High stretch stitching
- 100% Merino Wool
- Jersey Knit
- SM-4X

DARK NAVY

EA — ARM 21352-15-(SZ)

ARMADILLO MERINO BOOT SOCK

- Over the calf
- 100% wool next-to-skin and elastic support system
- Reinforced toe and heel
- Smooth toe seam
- 65% Merino Wool, 38% Nylon, 11% Elastane
- SM-XL

DARK NAVY

PR — ARM 11606-15 (SZ)

ARMADILLO MERINO PANTHER LONG SLEEVE CREW NECK SHIRT

- Seamless underarm reducing chaffing
- Raglan sleeve with no seams on the shoulders
- Relaxed fit
- Tag free neckline
- Single needle stitching
- High stretch stitching
- 100% Merino Wool
- Jersey Knit
- SM-4X

DARK NAVY

EA — ARM 21011-15-(SZ)

FR PUBLIC ORDER PANT

- Stud fastening waist
- Zip around lower waist to match length of jacket zip
- Drawcord inside waistband
- Side leg pocket
- Knee darts
- Extra patch of outer cloth at knee
- Ankle tabs with stud adjustment
- 3 under studs penetrate only the outer cloth
- Combine with jacket

			DARK NAVY
EA	YAF	460	(SIZE/HEIGHT)

FR PUBLIC ORDER JACKET

- Flap covering
- Velcro fastening throat tab folds back to loop velcro
- Loop pull on front zip
- 6 cm jetted opening under chest flaps on each side
- Left side only zip fastening map pocket with mobile phone and notebook pocket inside
- 5 belt loops
- Back action pleats allowing 7 cm expansion on each side
- Combine with pant
- SM-3X (Short/Regular/Tall/XTall)
- 4X (Short/Regular/Tall/XTall/XXTall)
- 5X (Regular/Tall/XTall/XXTall)

	DARK NAVY
EA	YAF 771 (SIZE/HEIGHT)

PATROLLING SUSPENDERS

- Outside body: 500 D Nylon
- Nylon complies with US MILSPEC MilaCa43734D
- Webbing complies with US MILSPEC MilaWa17337 and MilaWaAA55301
- Mesh complies with US MILSPEC MilaCa8061

	BLACK
EA	FSL 12-0008

GEAR BELT

- Body is sewn with Type 13, 1-23/32" Nylon
- Climbing buckle (A.K.A. Cobra Buckle), 1.75"
- Nylon complies with US MILSPEC MilaCa43734D
- Webbing complies with US MILSPEC MilaWa17337 and MilaWaAA55301
- Mesh complies with US MILSPEC MilaCa8061

	BLACK
EA	FSL 15-0004





CHEST AND BACK PROTECTOR

- Lightweight, ergonomically designed chest and back protection
- Chest protection: From collar bones to waistline
- Back protection: From shoulder blades to waistline
- Outer shell: Super high impact ABS moulded shell. Ridged design gives excellent protection against impact while keeping weight to a minimum.
- Inner foam: Low-density impact absorbing polyethylene moulded foam reduces weight and allows circulation of air around the product
- Fastenings: 4 Velcro adjustable Nylon straps riveted to the body of the guard. One at each shoulder, two at the waist. Ensuring security and comfort.
- Guards should be worn beneath a compatible flame retardant coverall. The outer moulding offers limited flame spread in accordance with UL-94 HB.
- Certification: Meets the requirements of UK Home Office Centre for Applied Science and Technology Standard 20/07
- Sizes SM-LG

BLACK

PR — DMS CH/BCK (SZ)



SHOULDER AND UPPER ARM GUARDS

- Lightweight, ergonomically designed shoulder and upper arm protection
- Area of protection: The clavicle, the top and point of the shoulder and the upper arm to above the elbow
- Outer shell: Super high impact ABS moulded shell. Ridged design gives excellent protection against impact while keeping weight to a minimum.
- Inner foam: Low-density impact absorbing polyethylene moulded foam reduces weight and allows circulation of air around the product
- Fastenings: 2 cotton covered Velcro adjustable Nylon straps riveted to the body of the guard. One attaches around the shoulder strap of body armour, the other fastens around the upper arm.
- Guards should be worn beneath a compatible flame retardant coverall. The outer moulding offers limited flame spread in accordance with UL-94 HB.
- Certification: Tested and approved to UK Home Office Centre for Applied Science and Technology Standard 20/07 rated
- Sizes XS-XL

BLACK

PR — DMS SHP/ARM (SZ)



FOREARM AND ELBOW GUARDS

- Lightweight, ergonomically designed lower arm protection. Fits the curvature of the arm minimising pressure points at the wrist and elbow. Articulated elbow section ensures freedom of movement.
- Area of protection: The forearm from the wrist to above the elbow
- Outer shell: Super high impact ABS moulded shell. Ridged design gives excellent protection against impact while keeping weight to a minimum.
- Inner foam: Low-density impact absorbing polyehtylene moulded foam reduces weight and allows circulation of air around the product
- Fastenings: 3 cotton covered Velcro adjustable Nylon straps riveted to the body of the guard. Ensuring security and comfort.
- Guards should be worn beneath a compatible flame retardant coverall. The outer moulding offers limited flame spread in accordance with UL-94 HB.
- Certification: Tested and approved to UK Home Office Centre for Applied Science and Technology Standard 20/07 rated
- Sizes XS-XL

BLACK

PR — DMS FRM/040 (SZ)

FEMALE GROIN GUARD

- Lightweight, ergonomically designed female groin protection
- Area of protection: Groin and lower abdomen
- Outer shell: High impact lightweight polypropylene moulding contained within a washable polyester cover
- Inner foam: Low-density impact absorbing foam
- Fastenings: Fully adjustable 2" waist strap. 2 x 1" leg straps pass from the bottom of the guard, between the legs to fasten around the waist strap at the back
- Guards should be worn beneath a compatible flame retardant coverall
- Certification: Tested and approved to UK Home Office Centre for Applied Science and Technology Standard 20/07
- Sizes SM-MD

BLACK

EA — DMS FGG/100 (SZ)



MALE GROIN GUARD

- Lightweight, ergonomically designed male groin protection
- Area of protection: Groin and lower abdomen
- Outer shell: High impact lightweight polypropylene moulding contained within a washable polyester cover
- Inner foam: Low-density impact absorbing foam
- Fastenings: Fully adjustable 2" waist strap. 2 x 1" leg straps pass from the bottom of the guard, between the legs to fasten around the waist strap at the back
- Guards should be worn beneath a compatible flame retardant coverall
- Certification: Tested and approved to UK Home Office Centre for Applied Science and Technology Standard 20/07
- Sizes MD-LG

BLACK

EA — DMS MGG/100 (SZ)



THIGH GUARDS

- Lightweight, ergonomically designed thigh protection
- Area of protection: The front and side of the thighs from close to the hip to just above the knee
- Outer shell: Super high impact ABS moulded shell. Ridged design gives excellent protection against impact while keeping weight to a minimum.
- Inner foam: Low-density impact absorbing polyethylene moulded foam reduces weight and allows circulation of air around the product
- Fastenings: 2 cotton covered Velcro adjustable Nylon straps riveted to the body of the guard. One passes around the thigh, the other attaches to the waist belt. Ensuring security and comfort.
- Guards should be worn beneath a compatible flame retardant coverall. The outer moulding offers limited flame spread in accordance with UL-94 HB.
- Certification: Tested and approved to UK Home Office Centre for Applied Science and Technology Standard 20/07 rated
- Sizes XS-XL

BLACK

PR — DMS THG/050 (SZ)



SHIN AND KNEE PROTECTORS

- Lightweight, ergonomically designed lower leg protection. Fits the curvature of the leg minimising pressure points at the knee and ankle. Articulated knee section ensures freedom of movement.
- Area of protection: The knee and shin to the top of the instep
- Outer shell: Super high impact ABS moulded shell. Ridged design gives excellent protection against impact while keeping weight to a minimum.
- Inner foam: Low-density impact absorbing polyethylene moulded foam reduces weight and allows circulation of air around the product
- Fastenings: 3 cotton covered Velcro adjustable Nylon straps riveted to the body of the guard. Ensuring security and comfort.
- Guards should be worn beneath a compatible flame retardant coverall. The outer moulding offers limited flame spread in accordance with UL-94 HB.
- Certification: Tested and approved to UK Home Office Centre for Applied Science and Technology Standard 20/07 rated
- Sizes XS-XL

BLACK

PR — DMS SHN/100 (SZ)



METATARSAL PROTECTOR

- Lightweight, ergonomically designed instep/metatarsal protection
- Area of protection: The top of the foot from the bottom of the shin/knee guard to the toecap of the boot
- Outer shell: Super high impact ABS moulded shell. Ridged design gives excellent protection against impact while keeping weight to a minimum.
- Inner foam: Low-density impact absorbing polyethylene moulded foam reduces weight and allows circulation of air around the product
- Fastenings: A single Velcro fastening leather strap loops around the boot laces to hold firmly in position
- The outer moulding offers limited flame spread in accordance with UL-94 HB.
- Certification: Tested and approved to UK Home Office Centre for Applied Science and Technology Standard 20/07 rated
- Sizes XS-XL

BLACK

PR — DMS FTPM (SZ)

FORTRESS UNIVERSAL TACTICAL VEST

- Provides full protection to the front, back and sides
- Capable of accepting Level II and IIIA ballistic inserts
- Comes with a gusset sewn top-loading plate pocket that accepts 10 x 12 plates and a heavy-duty operator rescue drag handle
- 360° MOLLE webbing, and front gusset sewn map/tool pocket for quick mission access is fully adjustable in girth and length to fit multiple sizes
- Vest adjustments allows standardization of team equipment and has velcro on the front and rear to accept ID patches
- Accessories include neck, throat, bicep and groin armor
- Sizes SM-XL



NAVY

EA — USI FUTV-SZNV

ID PANELS

- Custom identification panels available for helmets and vests
- Customer can select background color and lettering color
- Vest ID panels will have a Velcro backer to apply to vest. Helmet ID panels will come with both sides of the Velcro attached with a glue backing for helmets.





CALL FOR PRICING/ADDITIONAL INFORMATION



FORTRESS UNIVERSAL PLATE CARRIER

- Provides full protection to the front, back and sides
- Capable of accepting Level II and IIIA ballistic inserts
- Comes with a gusset sewn bottom loading plate pocket that accepts 10 x 12 plates and a heavy-duty operator rescue drag handle
- 360° MOLLE webbing, and front gusset sewn map/tool pocket for quick mission access is fully adjustable in girth and length to fit multiple sizes
- Sizes SM-XL

NAVY

EA — USI FUPC-SZNV



017 SERIES PUBLIC ORDER HELMET

- Thermoplastic shell
- Energy absorbing expanded polystyrene line improves impact protection
- High comfort, flame retardant interior with removable cheek pads for easy cleaning, improved hygiene and longer service life
- Headbands, crown pads and sizing pads for easy fit to individual head shapes and sizes
- High-impact polycarbonate visor with option of anti-mist and anti-scratch coating for improved resistance to fogging and surface abrasion
- Replaceable heavy duty neck curtain - padded for extra comfort and optimum protection
- Four metal gauze audio inserts - resistant to liquid penetration
- Adjustable chinstrap with quick release buckle
- Comply fully with PAS 017: 1995 - the first technical performance standard to be dedicated to public order helmets offering a new higher standard of protection for police and prison officers exposed to front line hazards
- Sizes 00-5

	BLACK, NAVY BLUE
EA	ARG 017T/3 (SIZE/COLOR)



APH05 PUBLIC ORDER HELMET

- Choice of thermoplastic or GRP helmet shells incorporating optically correct, high impact resistant polycarbonate visor with optional anti-mist, anti-scratch coating
- Liquid resistant, metal gauze audio apertures enable local commands to be heard
- Compatible with range of CBRN respirators
- Replaceable neck protector and quick release chin strap with chin cup - accepts high dynamic load with minimum extension and helps to maintain helmet stability
- Range of sizes available to provide optimum fit, with combined impact and padded linings to maximize protection and comfort. Internal fitting accepts radio connection.
- Complies with testing requirements of Home Office Scientific Development Branch Standard 2004, incorporating new tests for impact attenuation of whole helmet and solvent resistance of visor
- Thermoplastic (Sizes 00-5)
- GRP (Sizes 00-6)

	THERMOPLASTIC (BLACK, NAVY BLUE)
EA	ARG APH05T/1 (SIZE/COLOR)

	GRP (BLACK, NAVY BLUE, RED, YELLOW, WHITE)
EA	ARG APH05G/1 (SIZE/COLOR)

RIOT CONTROL HEADSET SYSTEM

- Low profile, single sided headset
- Can be mounted inside riot helmet
- Has the ability to adjust the headset's positon close to his/her ear and provide a noise canceling microphone that would cancel crowd noise, focusing only on the clear transmission of the officer's voice
- Push-To-Talk provides the officer with ease of access to activate when needed yet provide a protective shroud to prevent accidental depression

	BLACK
EA	ATL RCH.ERC.47 (HEADSET SYSTEM)
EA	ATL RCH.P01.47 (PUSH TO TALK ASSEMBLY)
EA	RADIO INTERFACE CABLE



PUBLIC ORDER - HAND PROTECTION

AA50 PUBLIC ORDER GLOVE



- Lightweight
- Black leather
- Elasticated mid-length cuff. Gathered wrist with foam padded lining to prevent ingress of liquids. Compatible with commonly used forearm guards and coveralls.
- Outer material: 0.9-1 mm goatskin leather
- Inner lining: 365 gsm Polyester (Heat resistant to EN659:1996 Annex A)
- Intermediate lining: 0.5 mm Low Density Polyethylene Foam
- Thread: Aramid - flame retardant
- Impact protection: 7-8 mm foam rubber to back of hand & 4 mm foam to back of fingers/thumb
- Abrasion protection: Leather reinforcement to high wear areas of palm/fingers
- Blade cut protection: Aramid loaded reinforcement to palm, fingers and back of hand
- Certification: BS7971-6:2003 Type 2 Level 3
- Sizes 6-13

BLACK

PR — DMS AA50 (SZ)

RIOT ControlBY

- Waterproof aniline fireproof cowhide leather according to DIN/EN 407, level 4
- Anti-cut insert lining according to DIN/EN 388, level 5
- Hard shell knuckle and handback protectors
- Shock absorbing protectors (foam and jelly) on fingers, thumb and wrist
- Fireproof stitching thread and fireproof male and female velcro
- Roller buckle closure with leather strap at wrist for secure fit
- Sizes 5-13

BLACK

PR — MLE 13514SW (SZ)



PUBLIC ORDER - FOOT PROTECTION

HAIX® AIRPOWER XR2



- 8" boot
- Climate system
- Reinforced leather pull tab
- Water resistant sun reflect leather
- Rubber/PU outsole
- Anatomically formed TEXON fleece footbed
- Quality insole
- Composite toe cap
- Metal free puncture protection
- Sizes 5-15 (including 1/2 sizes) (Medium, Wide, Extra Wide)

BLACK

PR — HAI 605118 (SZ)

ORIGINAL S.W.A.T. PUBLIC ORDER BOOT



- 9' boot
- Certified to British Standards BS 7971 2016 Part 5 Footwear for protective clothing and equipment for use in violent situations
- Meets EN ISO 20345:2011 for safety boots
- Composite protective toe cap
- 2.2-2.4mm fire resistant full grain leather
- Waterproof membrane for water, liquid and blood borne pathogen resistance
- LENZI® non-metallic anti-penetration board
- 6mm Poron® XRDMA internal metatarsal protector
- 3M™ Defender fluorochemical finish to assist with fluid run off
- Nomex® flame and heat resistant laces
- Additional PORON® XRDMA in lateral ankle area
- Fire and slip resistant rubber outsole tested [redacted]°C
- Salamander Skin™ toe cap resists abrasion, fire, and liquid fuel
- Sizes: D: 4-15 and EEE: 7-16

BLACK

PR — OSB 114031 BLK (SZ)



AVON C50™ MASK ASSEMBLY

- Based on the U.S. M50/JSGPM and sharing key technologies
- Provides maximum operational flexibility to counter multiple threat scenarios, including CBRN agents, TICs and TIMs
- Offers high protection, outstanding field of vision and superior comfort
- The innovative design features optimize the user's time in the operational area
- Sizes SM-LG

	BLACK
EA	AVO 70501-18X



AVON FM53™ MASK ASSEMBLY

- A multi-role Respiratory Protective Equipment (RPE) System that has been developed specifically for specialist applications where the user needs to respond to ever changing operational conditions
- Provides protection against traditional chemical and biological warfare agents and select TIMs
- Offers both positive pressure SCBA, PAPR and negative pressure APR/capability
- All of the capabilities are available from one mask platform without the need to change components
- Right, left or twin port filter configurations available
- Sizes XS-LG

	BLACK
EA	AVO 72601-250-X



AVON OUTSERT ASSEMBLY

CLEAR OUTSERT

- Flexible polycarbonate outsert that simply attaches to 50 series masks to provide additional impact and scratch resistance in extreme environments.

EA	AVO 70501-156

SUNLIGHT OUTSERT

- Additional protection against high level UV light and flash flares. Constructed from flexible polycarbonate providing additional impact and scratch resistance.

EA	AVO 70501-157



MASK BAG

	BLACK
EA	SFW 44014



CBRNCF50 FILTER

- When combined with an appropriate chemical protective mask, the CBRNCF50 filter canister protects the face, eyes and gastrointestinal tract of the wearer against known chemical and biological agents in aerosol, liquid and vapor form

	BLACK
EA	AVO 72602-2



CTCF50 RIOT AGENT FILTER

- Low profile combination filter containing a pleated high-efficiency filter element
- Specifically designed for removal of riot control agents and tear gases including CS, CN and OC pepper spray
- Pack of 4

	BLACK
PK	AVO 72606-3



INTERLOCKING SHIELDS

- Lightweight personal protective shield
- Can be used individually or locked together to form a continuous barrier
- 4 mm thick clear Makralon Polycarbonate. Offers excellent resistance to impacts, thrown objects and liquids while giving the user an excellent field of vision ahead.
- Handles: Forearm hook and double D handle (optional locking folding handles). Aluminum handles with rubber hand grips. Bolted through the blade and backing plate for maximum strength and security

4'	CLEAR
EA	DMS SLD1200INT
6'	CLEAR
EA	DMS SLD1800INT

POLICE OR SHERIFF ID PANEL AVAILABLE

****ID PANEL IS AN OPTION, NOT STANDARD**

PUBLIC ORDER BATON

- One-piece, solid nylon with moulded rubber grip, retaining strap and locating ring
- 31 mm diameter black Nylon 6
- Grip: Moulded rubber textured grip gives excellent security and control
- Lanyard: 5 mm diameter plaited cord
- 24"

	BLACK
EA	DMS BAT610





SOLO SHIELD

- Lightweight (2.0 kg) personal protective shield
- Forearm loop allows the shield to be retained while leaving both hands free to use other equipment
- 4 mm thick clear Makralon Polycarbonate. Offers excellent resistance to impacts, thrown objects and liquids while giving the user an excellent field of vision ahead.
- Handles: Swivelling steel forearm loop and aluminum grab handle. Bolted through the blade and backing plate for maximum strength and security.
- Shield handles are mounted on a foam/aluminum backing plate which significantly reduces transmission of vibration to the forearm and through the handles
- 650 mm diameter x 4 mm thick

	CLEAR
EA	DMS RSHD

POLICE OR SHERIFF ID PANEL AVAILABLE

****ID PANEL IS AN OPTION, NOT STANDARD**

LEATHER BATON HOLDER

	BLACK
EA	BOS7701-1-BLK



PUBLIC ORDER - FIRE SUPPRESSION

AMEREX HALOTRON I "CLEAN AGENT" EXTINGUISHER



- 9 second discharge
- 6-8 foot range
- 10 H x 3.5 W x 2.63 D
- Stored pressure design
- Dependable drawn steel cylinders
- Durable high gloss polyester powder pain
- All metal valve construction
- Temperature range (-40°F to 120°F)
- EPA approved "Clean Agent" for Class A, E and C hazards
- Low GWP
- Low ODP
- Leaves no residue
- User friendly
- 1.4 LBS

	RED
EA	AMX A384T

LEATHER CARRIER

	BLACK
EA	BOS 7702-1-BLK

COLD FIRE™ TACTICAL CANS

- An environmentally friendly fire extinguishing agent that puts out any fire faster, safer, with less water, less damage to property and less risk to personnel
- Completely 'green' and non-toxic
- Instantly cools everything it touches
- Cools 21x faster than water and works to remove heat, therefore preventing re-igniton
- Encapsulates and breaks down hydrocarbons
- Availablity: 12 oz. and 20 oz. Pistol Grip or Loop Handle Spray Cans, 2L and 6L CFT extinguishers, backpack and fleet kit



12OZ. LOOP HANDLE TACTICAL CAN	
EA	CFT CF302-12TL

20OZ. LOOP HANDLE TACTICAL CAN	
EA	CFT CF302-20TL

2 LITER KIT	
EA	CFT CF302-2LTRKIT

PUBLIC ORDER - LESS THAN LETHAL



COMBINED TACTICAL SYSTEMS AEROSOLS

- Advanced solutions with an array of formulations, sizes and delivery including stream, fog, gel, vapor and Omni-Stream™
- Pepper spray
- Crown management, high volume units
- Omni-Stream™ features a bag on valve (BOV) delivery system allowing the operator to hold the can at any orientation and get consistent stream performance



COMBINED TACTICAL SYSTEMS FLASH BANGS AND STING BALL GRENADES

- Flash Bangs are an ATF controlled Class-C explosive device
- Sting-Ball Grenades are explosive "rubber-ball" style grenades that upon initiation eject rubber balls into a radius surrounding the device



COMBINED TACTICAL SYSTEMS 40MM LAUNCHER

- Multi-Launcher 6.2" Cyl Collapsible Stock
- Lightweight and versatile
- Manufactured using 4140 hardened steel, 6061-T6 mil-spec anodized aluminum and DuPont super tough glass filled nylon



SAGE HAND THROWN MUNITIONS

- 40MM Munitions
- 37MM Rifled Munitions
- 37MM Smooth Bore Munitions

SAGE CHASSIS STOCK SYSTEMS

Each SAGE Enhanced Battle Rifle Chassis System is precison CNC machined from a solid billet of high strength aircraft grade aluminum and is finished with mil-spec hard anodizing. The system increases accuracy and reliablity, reduces perceived recoil, provides ambidextrous sling mounts and multiple Picatinny rails for mounting optics and accessories.





V-LITE™

- 0.8 oz.
- A versatile personal lighting/identification marker
- A simple and intuitive alternative to chemical light sticks
- One button to cycle through the preset functions
- Fully encapsulated to ruggedize the electronics, the flexible silicone body not only protects the good stuff inside but also conforms to curved surfaces
- Mounting is made simple with the V-Lite™ sleeve, providing the operator with a velcro-backed attachment system
- An unnoticeable addition to your helmet during routine operations and low-profile enough to reduce snag hazards during airborne operations
- Modes available: On/Off, Blink/Off, On/Blink/Off, Low/High/Off
- One Size

RED, WHITE, BLUE, ORANGE, GREEN, INFRARED

EA — S&S VL-COLOR01XV



LEATHER WATER BOTTLE CARRIER

BLACK

EA — BOS 7703-1-BLK



VTAC® BROKOS HARNESS

- An ideal tactical load bearing solution
- Complements the 5.11® Brokos belt
- Fully adjustable padded shoulder straps
- MOLLE/5.11 SlickStick® shoulder webbing
- Adaptable rear yoke
- 500D Nylon and aerospace mesh
- Low profile adjustment buckle
- Patch tabs at front and rear
- Removable loop ID panel on back
- One size

BLACK

EA — 511 56105 019



EQUIPMENT BAG

- 80 liter storage
- 6 external zipper pockets
- Protective helmet storage pocket
- Heavy duty bottom
- Cordura nylon with reinforced seams and shoulder straps (backpack or shoulder)

BLACK

EA — DMS 80 LTR



VTAC® BROKOS BELT

- Highly versatile load bearing belt
- Wrap-around MOLLE/5.11 SlickStick® web platform
- Polymer inserts for an ergonomic shape
- Durable, weather resistant 500D Nylon
- Aerospace mesh interior
- Lengths: SM-MD (26.5"), L-XL (33"), 2X-3X (42")

BLACK

EA — 511 58642 019 (SZ)

511 58642 019 2XL/3XL

HOOK & LOOP INNER DUTY BELT

- SM (26-30")
- MD (32-36")
- LG (38-42")
- XL (44-48")



BLACK

EA — BLK 44B7SZBK

CALL 800.331.6707
FOR A QUOTE TODAY!



H&H MEDICAL SWAT-T TOURNIQUET (ORANGE)

Allows a more rapid means to control extremity bleeding and allows application higher into the groin and axilla than other tourniquets.

- Ease of application
- Made with a bright safety orange color for easy identification and application
- Instructions for use are printed on the tourniquet along with the trademark pressure application measure showing just how much pressure to apply to reach occlusion



H&H MEDICAL H*VENT LAMINAR VENTED CHEST DRESSING

Designed to work to relieve pressure from an open chest wound due to air in the chest or bodily fluid.

- A unique multi-directional vented dressing (allows the fluids to "drain towards gravity")
- Helps prevent occlusion
- The unique dome membrane design creates a complete seal around the wound area
- Large vent openings on the H*VENT allows for visual monitoring of the wound
- Proven in internal testing to retain a seal during inhalation and to maintain a sustainable negative pressure (below ambient pressure) within the pleural space
- Lowest profile of any vented chest seal and easy to fold



H&H MEDICAL BLEEDING CONTROL BASIC KIT

Provides first responders with a compact and durable individual hemorrhage control kit to treat bleeding from penetrating and other traumatic injuries.

Kit includes:

- SWAT-T tourniquet
- H&H Mini Compression Bandage
- H&H PriMed Compressed Gauze roll
- Nitrile gloves



NORTH AMERICAN RESCUE COMBAT APPLICATION TOURNIQUET (C-A-T)

The C-A-T® utilizes a durable windlass system with a patented free-moving internal band providing true circumferential pressure to the extremity.

- New single routing buckle for faster application, decreased blood loss, effective slack removal, fewer windlass turns, and simplified training with single protocol application standards
- Includes reinforced windlass, stabilization plate, windlass clip and writeable windlass security strap
- Featuring NAR's signature Red Tip Technology® elliptical tab providing added visual clues during application

NORTH AMERICAN RESCUE



NORTH AMERICAN RESCUE RIGID GEN 7 TOURNIQUET CASES W/ SHIRT SHIELD

Designed to provide personnel with the capability of carrying the life-saving C-A-T® Tourniquet on their person by easily mounting it to their duty/patrol/pistol belt, where it is needed most.

- Includes a Shirt Shield complete with mounting hardware to protect your uniform shirt from undue wear caused by the friction from the windlass clip
- Blade-Tech TekLok Belt Attachment fits up to a 2.25" belt
- Injection molded nylon case to stand up to rugged LE/MIL usage



H&H MEDICAL TECC KIT

Designed to hold enough emergency products to respond to a mass casualty situation.

- Contains everything you need to treat the 3 most preventable causes of traumatic death: blood loss, airway occlusion and sucking chest wound
- Meets the basic requirements for Tactical Emergency Casualty Care



NORTH AMERICAN RESCUE M-FAK MINI FIRST AID KIT

Designed to be the most compact, multi-use IFAK for delivering immediate critical care for penetrating, blast or other traumatic injuries.

Kit includes:

- 1 x C-A-T® (Combat Application Tourniquet®) black
- 1 x 4" Flat ETD™
- 1 x S-rolled gauze (4.5" x 4.1 yd)
- 1 x HyFin® Vent Compact Chest Seal, twin pack
- 1 x pair Bear Claw® nitrile trauma gloves, LG
- Super compact, rugged nylon platform that allows attachment both vertically (MOLLE backing) and horizontally (3" belt loop)
- Clam shell configuration utilizes (2) main sleeves that open on both ends for easy access



NORTH AMERICAN RESCUE PATROL VEHICLE TRAUMA KIT

Desinged to provide personnel with an easily accessible, quick to deploy medical kit from your patrol vehicle.

- One side covers all your agency needs to administer basic first aid and community assistance
- Second side offers a first time combination of basic first aid and basic trauma medical items
- Exterior includes MOLLE-style system to accommodate extra equipment as needed





QUIKCLOT® BELT TRAUMA KIT®

A compact, lightweight, wearable holder that fits up to a 2" belt and can be rotated 90° to make room for other gear. Contents can treat up to one injury.

Includes:

- QuikClot Combat gauze® LE
- SWAT-T™ pressure dressing
- Nitrile gloves



QUIKCLOT® BLEEDING CONTROL BAG®

This bag is integral for responding to a range of bleeding situations. Its innovative design allows it to function in a stand-alone capacity or as part of an overall bleeding control program. Contents can treat up to 12 injuries.

Includes:

- QuikClot Combat gauze® LE
- QuikClot® EMS 4x4 dressings
- QuikClot® EMS rolled gauze
- Tourniquets, C-A-T™ , SOF™ TT-W
- Dressing, TacMed Control™ Wrap
- Nitrile gloves
- Shears, EMS-style



ADS XR150 X-RAY SOURCE

Provides the ultimate option in portability for high powered X-ray machines.

- Weighs less than 5 lbs.
- Penetrates up to 1/2" of steel
- Small size makes the unit easy to position in hard to reach places or to maneuver on a robot arm
- Performance - high penetrating capability, durable, lightweight packing, long battery life
- Simplicity - only one variable to control exposure
- Safety - extremely short exposure time and low leakage
- Spectrum - wide spectrum penetrates both high and low density material in same radiograph



ADS MITHIX PRO EOD HOOK AND LINE TEAM KITS

Designed for EOD, bomb squad, and special operations prodedures.

- High quality components
- Stainless steel hooks
- High-strength marine-grade pulleys
- Low-stretch high grade Kevlar rope and other essential tools made specifically for IED, remote movement and remote handling operations



ADS NEX-RAY®

Offers advanced, portable, lightweight x-ray image capture units designed to obtain accurate, near real-time radiographic imaging.

- Patented technology allows NeX-Ray® to dispense with the use of fragile and heavy glass plates integral to most flat panel imagers
- 2 models available (FPX and MMX)
- Can be operated with Windows XP, 7, or 8 laptops or with Android 4.2 (or later) mobile devices
- NeX-Ray® imagers can be operated in standalone, tethered remote, and wireless modes

ADS TITAN

(1) 12" main barrel
(2) Smooth bore extensions
(1) Rifled extenson
(1) Breech cap
(1) Breech plug
(1) Thread protector



NOW WITH TWO NEW CONFIGURABLE OPTIONS

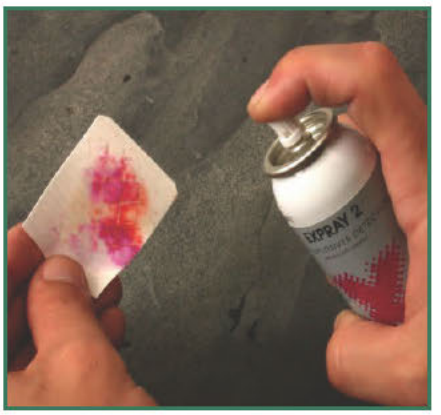
MISTRAL INC.
Member of Mistral Group



MISTRAL SECURITY EXPEN

Ampoule-based technology. Designed for military, EOD, and security personnel primarily for easy carrying and for situations that do not require multiple tests.

- Capabilities: Nitro Aromatic, Nitramines, Ammonium Nitrate, Peroxide, Acetic Anhydride, and much more



MISTRAL SECURITY EXPRAY®

A unique explosive aerosol test technology, Expray®, detects both trace and substance levels of explosives as well as homemade explosive (HME) precursors.

- Capabilities: Nitro Aromatic, Nitro Esters, Nitramines, Inorganic Nitrates and much more



MISTRAL SECURITY TOTAL CONTAINMENT VESSELS (ARC)

Provides full protection against blast and fragmentation with repeated detonation capability.

- Safely contain and transport explosive devices

TACTICAL ELECTRONICS
ELITE TACTICAL CAMERAS & EOD SOLUTIONS





TACTICAL ELECTRONICS 1ST LINE EOD TOOL KIT

Designed to provide EOD operators and bomb technicians with a versatile, lightweight kit that builds upon the capabilities of the Immediate Action Pouch without necessary or wasteful redundancy. Ideal for missions where the user has limited cargo or carry space and where the operator must take weight or dimensions into consideration.

- Small lightweight design
- Can be carried in a cargo pocket or stored in a small compartment
- Ideal for dismounted operations

TACTICAL ELECTRONICS WIRE ATTACK SPECIAL PIERCER PROBES (WASPP) KIT

Specifically designed to allow EOD operators to make non-invasive electrical measurements of wires.

- Includes 10 specialized "bed of nails" piercers with volt meter leads, 10 extensions and 1 roll up carry pouch



TACTICAL ELECTRONICS 2ND LINE EOD TOOL KIT

Customized to equip EOD and bomb technicians with the tools necessary to execute render safe procedures. Allows operators to customize the configuration based on each scenario.

- Comes complete with 6 individually populated tool kits: 1st Line, Immediate Action Pouch, RIP Kit, Detonator Diagnostic Kit, Manual Access Kit and Bit Kit
- All kits fit into one pack with extra room for additional supplies

QINETIQ TALON®

TALON robots are powerful, durable, lightweight tracked vehicles that are widely used for EOD, reconnaissance, communications, sensing, security, defense and rescue. They have all-weather, day/night and amphibious capabilities and can navigate virtually any terrain.

- IOP compliant
- Man-portable, instantly ready for operation
- Fast
- Configurable
- Intuitive
- Outstanding situational awareness: standard 4 color cameras, including night vision, thermal and zoom options
- Withstands repeated decontamination

QINETIQ DRAGON RUNNER® 10

The micro unmanned ground vehicle is lightweight, compact, multi-mission remote platform developed for supporting small unit dismounted operations. When fitted with the Light Weight Modular Arm, it has the ability to investigate and recover or neutralize a potential IED. Day and night sensors allow it to serve as the forward eyes of the team while also delivering remote sensors, emplacing counter-IED charges and more.

- Speed: 4 mph
- Max arm lift: 4.4 lbs.
- Front and rear cameras
- On-board microphone
- Controller: compatible with lightweight radio unit and Gen 2.5 hand controller
- Tough enough to be thrown and survive rough handling and adverse weather

DRAGON RUNNER® 20 ALSO AVAILABLE!"





QINETIQ North America

ICOR MINI-CALIBER®

The lightweight, modular Mini-CALIBER® is a man transport robot for SWAT and EOD operators. Developed for rapid tactical missions, the robot is simple to operate and quick to deploy, providing fast action for searching rooms, hallways, stairwells and confined spaces.

- Includes a manipulator arm on a rotating turret with a 10X zoom camera on the claw and a max arm lift of 15 lbs.
- CBRNE detectors and sensors can be mounted onto the deck of the robot chassis
- Handheld command control unit is portable and intuitive to use
- Clear images are transmitted to the 5.8" LCD daylight readable screen over a wireless RF system

ICOR TECHNOLOGY



ALSO AVAILABLE:



Caliber® T5



Caliber® MK4



MK3 Caliber®



TacticID By. B&W TEK





B&W TEK TACTICID® - GP

A field-ready handheld spectral analysis instrument designed for non-contact forensic analysis. Utilizes proven Raman spectroscopy, allowing users to get real-time actionable identification of unknown chemicals, narcotics, pharmaceutical drugs, explosives and many other substances while reducing operational uncertainty and response time.

- Customized libraries
- Critical component mixture ID
- Indirect contact analysis
- Wi-Fi connectivity
- Touch screen quick notes
- Color-coded result screens
- TacticOne Response™ (24/7/365 emergency support and spectral analysis)

B&W TEK TACTICID® - N

Handheld Raman analyzer for narcotic and pharmaceutical drug identification.

- Comes standard with a comprehensive library of over 1,000 substances
- Critical component mixture ID
- Indirect contact analysis
- Wi-Fi connectivity
- Touch screen quick notes
- Color-coded results screen
- TacticOne Response™ (24/7/365 emergency support and spectral analysis)

MISTRAL SECURITY PDT

A series of individual, presumptive reagent drug tests that help law enforcement officers, drug enforcement agencies and military CID units quickly and easily identify controlled substances while in the field.

- Options: Heroin, LSD, marijuana, cocaine, bath salts and much more



MISTRAL SECURITY PENTEST

An ampoule-based technology that detects trace amounts of drugs as well as bulk amounts.

- Multi-use
- Will not destroy evidence
- Options include: D4D (general screening), Coca, Cannabis, Herosol, LSD, Meth/X, Opiates, and more



MISTRAL INC.
Member of Mistral Group

MISTRAL SECURITY FENTANYL PDT

The only fentanyl test that can distinguish fentanyl from other drugs like meth or amphetamines.

NIGHT VISION



ARMASIGHT PVS7 GEN 3P NIGHT VISION GOGGLES

The most widely recognized and dependable U.S. Military night vision goggle system available.

- Compact, rugged design
- Waterproof
- Ergonomic, simple, easy to operate controls
- Built-in infrared illuminator and flood lens
- Equipped with Automatic Brightness Control (ABC)
- Head or helmet mountable for hands-free usage

AIMPOINT® MICRO T-2

Electronic red dot sighting technology.

- Advanced optical lenses
- Cutting edge lens coatings
- Lightweight sight for extreme conditions
- Excellent night vision compatability

NIGHTOPS TACTICAL PVS-14

A widely recognized monocular night vision device, battle tested by the U.S. Military.

- L-3 Gen 3 Unfilmed technology
- 40 hour runtime
- 1X magnification



THERMAL IMAGING



FLIR BREACH® PTQ136

Thermal imaging monocular. Spots th total darkness.

- Weighing only 7.4 oz. (can be concealed in a pocket or mounted to a helmet with its mini-rail feature)
- On-board recording
- Exceptional vision
- 7 palettes for fast detection of suspects or evidence, day or night
- Digital compass and inclinometer



FLIR THERMOSIGHT® PRO SERII

Thermal imaging weapon sight.

- Exceptional vision
- Built using the new FLIR Boson 1
- Bright, high definition FLCOS display for absolute clarity
- Completely digital for better detection, classification and recovery, day or night
- Powerful and compact hardware is protected by a robust body
- On-board video recording, image capture and storage
- Multiple color palettes
- Digital compass and inclinometer

PELICAN™



PELICAN 7600 TACTICAL FLASHLIGHT WITH WAND KIT

- Performance surpassing 900 lumens
- 3 LED colors (white, red, and green)
- Provides high, strobe, medium and low modes
- Full time battery level indication
- USB rechargeable lithium ion battery
- Type III hard anodized finish
- Ingress protected IPX8 submersible



PELICAN 7100 TACTICAL FLASHLIGHT

Compact/high performance flashlight.

- 5" long
- 700 lumens of light output
- High, strobe, medium and low modes
- Full time battery level indication
- USB Lithium Ion rechargeable
- Ingress protected IPX8 submersible

PELICAN 9490 REMOTE AREA LIGHT

- Up to 6,000 lumens (calculated)
- Up to 24 hours of run time
- Intelligent control (allows for various light output levels)
- Maintenace free LED array with 50,000 hour life expectancy
- Full time battery level indication with low level flashing indicator
- 6' deployable mast with 340° rotation
- Multiple deployment positions
- Quick release/ Hot swappable battery design with 12 volt power supply
- Convenient shoulder strap



STREAMLIGHT

STREAMLIGHT PROTAC HL® USB FLASHLIGHT

USB rechargeable, 850 lumen tactical flashlight.



- Choice of three user selectable programs
- Multi-fuel capability
- Durable, anodized aluminum construction
- Water resistant sliding metal sleeve protects USB port
- Multi-function, push-button tail switch for one-handed operation
- LED technology impervious to shock with a 50,000 hour lifetime
- Anti-roll head
- IPX4 water resistant
- 1m impact resistance tested

STREAMLIGHT TLR-1® GUN LIGHT

Rail-mounted tactical weapon light.



- 300 lumens
- 2.5 hours regulated run time
- 12,000 candela peak beam intensity
- Rail grip clamp system securely attaches/detaches quickly and safely with no tools
- Powered by two 3-volt CR123 lithium batteries
- Mounts directly to handguns with Glock-style rails and to all MIL-STD-1913 (Picatinny) rails
- Machined aluminum sealed construction with black anodized finish
- IPX7 rated design, waterproof to 1m for 30 minutes

STREAMLIGHT TLR-7® GUN LIGHT

Small and mighty 500 lumen tactial weapon light.



- Runs 1.5 hours
- 4,300 candela
- Custom optic produces a concentrated beam with optimum peripheral illumination
- Uses one CR123A lithium battery
- Safe off feature prevents accidental activation
- Rail grip clamp system securely attaches/ detaches quickly and safely with no tools
- Durable, anodized machined aluminum construction
- IPX7 waterproof to 1m for 30 minutes



SUREFIRE X300U-A

1,000 lumens LED handgun light.

- Custom TIR lens creates smooth, far-reaching light with a larger center spot beam
- Integral ambidextrous momentary-and constant-on switching
- Attaches securely to both universal and picatinny accessory rails
- High-strength aerospace aluminum body, mil-spec hard anodized for extreme durability

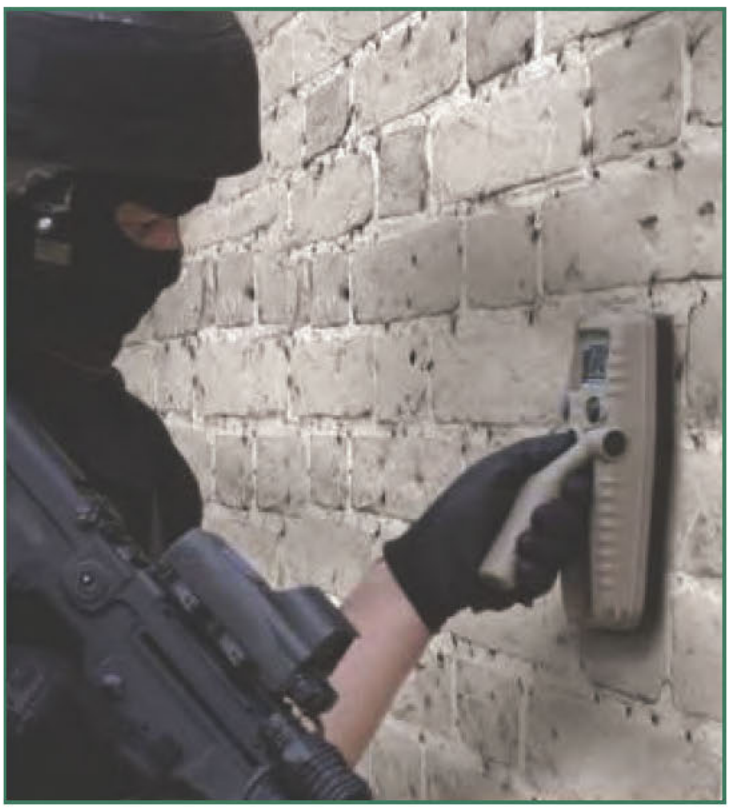


SUREFIRE M600DF-BK

1,500 lumen dual fuel rechargeable LED scout light.

SUREFIRE®

- Virtually indestructible ultra-high-output LED generates 1,200 lumens of blinding light with SF123A batteries and 1,500 lumens with included SF18650A rechargeable lithium ion battery charger kit
- TIR lens shapes versatile beam with enough reach and surround light for close-to longer-range operations
- Mil-Spec hard anodized aluminum body, tempered window and O-ring seals make light rugged, durable, and combat ready
- Activation via Z68 momentary/contant-on push button switching with protective shroud



CAMERO
Step into the known

CAMERO XAVER™ 100

Handheld, tactical through-wall detection system. Provides instant critical situational awareness and target acquisition data.

- Potential uses include: Tactical entry/assault, hostage recovery, search and rescue, breaching and force protection
- Reliable detection of moving and static people behind most common wall materials
- 1d imaging information
- Simple user interface and operation requiring no advanced training

CAMERO XAVER™ 400

Compact, tactical through-wall imaging system. Allows for quick location of people hidden by walls and barriers, enabling tactical teams to step into the known and obtain mission-critical information.

- Compact, light and easy to operate
- Ready to go at the push of a button
- Simple user interface with tracking capabilities for intuitive interpretation
- Simultaneous detection of static and moving objects
- Provides information about room dimensions and major infrastructure elements





CMC RESCUE PERSONAL RAPPEL KIT

Lightweight, durable and low profile. Provides everything needed for rappel access or escape for one tactical officer.

Kit includes:

- Black storage bag
- Stealth rope bag
- 8 Link
- Tactical rappel harness
- Black variable anchor strap
- Large edge guard
- Kong Trapezium Quick-Link
- CMC Lifeline - 75' of black 3/8"
- Prusik cord - 5' of blue 7 mm
- Tubular webbing - 20' of black
- (5) black ProTech™ Screw-Lock carabiners



CMC RESCUE TACTICAL TEAM RAPPEL KIT

Provides rope, harnesses, and hardware for two tactical officers moving in vertical environments, where keeping a low profile is a must.

Kit includes:

- Black storage bag
- #2 black rope bag
- Heavy Rescue Organizer™
- (2) 8 Link
- Black variable anchor strap
- (2) tactical rappel harnesses
- Kong Trapezium Quick-Link
- CMC Lifeline - 150' of black 7/16"
- Tubular webbing - 40' (2 z 12') of black
- Large edge guard
- Prusik cord - 10' (2 x 5') of blue 7 mm
- (7) black ProTech™ Screw-Lock carabiners

TACTICAL ELECTRONICS CORE POLE CAMERA

Extend your vision and tactical inspections.

- High-Definition 1280x720p monochrome video
- Longwave infrared (LWIR) thermal imager
- 4 High-intensity white and LED illumination
- Telescopic pole with locking sections
- Lightweight high density graphite pole
- Omni-directional microphone
- Attaches to POLE Grip, or CORE Grip
- Wireless video transmission - 5 GHz
- AES encryption
- WPA2-PSK authentication
- Graphical LCD for status information
- Hardwire video option
- Backlit push buttons
- MicroSD card video recording (32GB)





TACTICAL ELECTRONICS CORE K-9 CAMERA

Transmits real-time HD video back to the handler.

- High-Definition 1280x720p color video
- Longwave infrared (LWIR) thermal imager
- Adjustable high-intensity IR LED illumination
- Push-to-talk two-way audio
- Wireless video transmission - 2.4 GHz
- AES encryption
- Graphical LCD for status information
- Backlit push buttons
- MicroSD card video recording (32GB)

5.11 BREACHING EQUIPMENT

The Heavy Breaching Kit includes four 5.11 breaching tools desgined to defeat any portal quickly and effectively, along with a steel-reinforced, backpack-style Heavy Kit Bag that keeps your breaching tools organized and ready to roll.

- Size: 37" high
- Includes: MultiBreacher, MultiPry, MiniRam, and EdgeBender, Heavy Kit Bag
- Minimizes breach team exposure time
- Durable steel-framed carry pack
- Padded yoke straps
- 400 lb. quick-release buckles
- Removable hood with hook and loop brand closure



TACTICAL ELECTRONICS CORE UNDER DOOR CAMERA

Gain covert visual inspection into rooms behind closed doors.

- 0.26" insertion panel thickness
- Adjustable high-intensity IR LED illumination
- Attaches to POLE Grip or CORE Grip
- Lightweight high density graphite POLE Grip
- Color eyepiece - AMOLED display (CORE Grip)
- Wireless video transmission - 5 GHz
- AES encryption
- WPA2-PSK authentication
- Graphical LCD for status information
- Hardwire video option
- Backlit push buttons
- MicroSD card video recording (32GB)

TACTICAL ELECTRONICS CORE MONITOR

Presents high-definition video from all CORE cameras over an AES encrypted 5 GHz wireless channel.

- Receives high-definition 1280x720p color video on a 5.0" IPS LCD
- Secure pairing with multiple CORE cameras
- Capacitive touchscreen for setup/ configuration
- 1mm Corning Gorilla Glass screen
- Remote camera control for view selection and illumination/dimming
- WPA2-PSK authentication
- Hardwire video option
- Backlit push buttons







BSG CBRNE

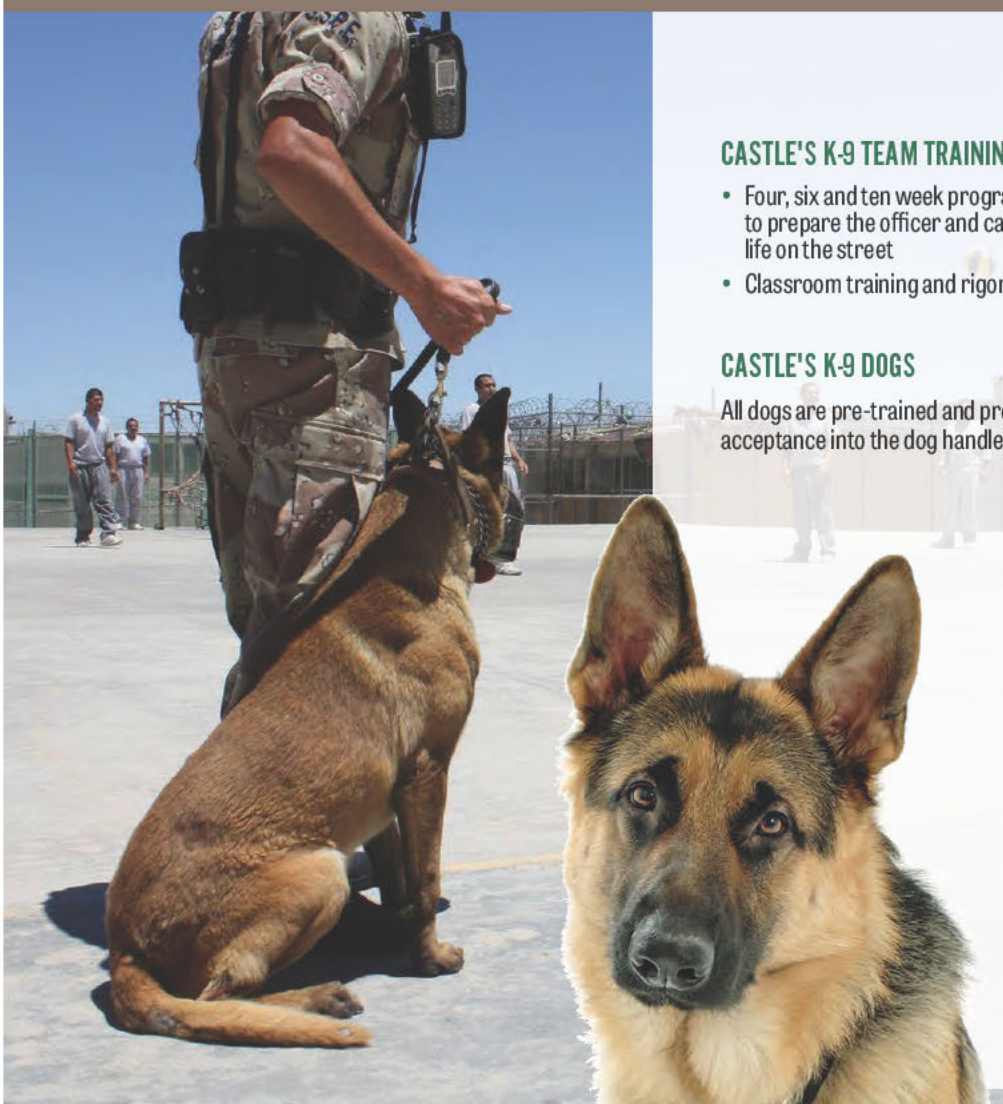
BLACKTHORNE SERVICES GROUP

Provides expertise in CBRNe and related matters. BSG can also branch out to other areas of expertise through their strategic alliances to provide a single point for coordinated consultation on an even larger subject matter.

Training programs include:

- PPE for first responders
- First 100 minutes of RDD, Biological, Chemicals and Explosives response
- Hazardous materials/WMD training
- Illicit and drug lab recognition
- Hazmat rapid intervention teams/fast teams
- Much more!

K9



CASTLE'S K-9 TEAM TRAINING

- Four, six and ten week programs are designed to prepare the officer and canine for everyday life on the street
- Classroom training and rigorous field training

CASTLE'S K-9 DOGS

All dogs are pre-trained and pre-tested before acceptance into the dog handler bonding process

VOHNE LICHE KENNELS

- Selection tested canines
- Narcotic or Explosive trained
- Single or dual purpose

BODY CAMERA

5306

KUSTOM SIGNALS VANTAGE BODY CAMERA

- Flexible data storage solutions (use our cloud or use yours, it is up to you!)
- 30 years of video for law enforcement
- One piece-no cable
- Glove friendly
- Configurable (use only the features you want)
- Rugged design
- IP64 compliant
- 480SD-1080HD capable (and all in between)
- 32GB internal storage
- 120° field of view
- Bookmark button (to mark important events on tape)
- Magnetic mount
- Audio mute

KUSTOM SIGNALS, INC.®



SPEED DETECTION



KUSTOM SIGNALS SMART 650

Speed monitoring awareness radar trailer.

- Kustom Directional RADAR
- 12' high intensity amber LED display
- Flashing overspeed violater alert
- Optional overspeed alerts including 'SLOW', red/blue lightbar, and white LED strobe
- Optional traffic statistics
- 5 year warranty



KUSTOM SIGNALS SMART 850

Speed monitoring awareness radar trailer.

- Kustom Directional RADAR
- 18" high intensity amber LED display
- Flashing overspeed violator alert
- Optional overspeed alerts including "SLOW DOWN", red/blue lightbar, and white LED strobe
- Optional traffic statistics
- Optional solar
- 5 year warranty



KUSTOM SIGNALS VARIABLE MESSAGE SIGN WITH HOMELAND TRAILER

Designed for static and dynamic messages, VMS trailers can be quickly and easily put into place.

- Kustom Directional RADAR
- Amber LED lights provide outstanding visibility
- Hydraulic sign lift
- 4x 2-ton screw leveling jacks
- Removable tongue and 2" ball hitch
- 80W solar panel
- Up to 39 day run time with 6 batteries
- Wi-Fi modem for local wireless programming

3M AUTOMATIC LICENSE PLATE RECOGNITION (ALPR)

3M

ALPR is widely recognized as an effective tool to combat criminal activity, enhance productivity and improve officer safety. Fixed and mobile ALPR systems can help identify certain people and situations:

- Stolen vehicles
- Wanted felons
- Amber alerts
- Sexual predators
- DUI surveillance
- Drug enforcement
- Campus security





GOVERNMENT SECURITY SOLUTIONS

CINTEL ALPR CAMERA

Manufacturer of a full suite of rapidly deployable fixed and mobile ALPR cameras and surveillance products.

CINTEL
Safe. Secure. Simple.





LENCO BEARCAT®

LENCO ARMORED VEHICLES
Protecting Our Nation's Defenders™

Can be used as a SWAT or Military Counter Attack and Rescue vehicle and is often used in hostile Urban Environments.

LDV MOBILE COMMAND CENTERS

LDV

Offers used and new mobile command centers, SWAT trucks and many other specialty vehicle solutions.

GAS DETECTION







MSA ALTAIR® 5X MULTI-GAS DETECTOR

The Altair® 5X is designed with XCell Sensor Technology for faster response and calibration times. XCell Sensors offer superior stability, accuracy and repeatability.

- Easy to use in all applications
- Bluetooth wireless connectivity
- A rugged polycarbonate housing provides unsurpassed durability
- MotionAlert sensor
- InstantAlert feature
- Altair Connect App available on Google Play
- Configurable to meet your needs

MSA
The Safety Company

RAE MULTIRAE WIRELESS, PORTABLE MULTIGAS MONITOR

With the flexibility of up to six gas sensors and the convenience of wireless portability, this multi-gas monitor is versatile and customizable, while delivering real-time access to instrument readings and alarm status from any location. Choose from 25 sensor options including LEL, PID, NDIR, and exotics that can be easily changed in the field. With five built-in alarms, including man down, and wireless connectivity to your command center, MultiRAE delivers vital information for fast incident response.

- Optional integrated wireless
- Dust-tight and waterproof (IP65-rated)
- Onboard gas libraries include 190 VOCs and 55 combustible gases
- Continuous data logging-6 months for 5 sensors 24/7

RAE GAMMARAE II R

A gamma radiation detector and full-range dosimeter in a single instrument. Designed specifically to meet the needs of first responders.

- Two types of sensors for excellent response in high and low dose rate ranges
- Waterproof to IP-67 standards
- Certified for use in Class I, Division 1 hazardous environments
- Top-mounted, invertible display
- Two AA alkaline batteries last up to 600 hours

Honeywell
RAE® SYSTEMS



KROMEK D3S ID

A wearable RIID that gives you the power to make the right decisions about nuclear threats in seconds. A powerful combination of two of Kromek's leading technologies: the non-3He compact thermal neutron detector and its world leading gamma detector, delivering the performance of a RIID in a small, but powerful device, the size of a PRD.

- One of the fastest and most accurate isotope ID devices on the market
- Discreet, wearable, lightweight
- Rapid, visible, audible and tactile alarm settings
- Identifies 17 extra isotopes, 4X faster
- Extensively tested and characterised in multiple DNDO and DARPA programs
- Quick, simple and intuitive to use, no need for specialist training or knowledge
- Built around your operational needs



FLIR®
The World's Sixth Sense®

FLIR IDENTIFINDER® R200

Spectroscopic Personal Radiation Detector (SPRD). Ideal for routine traffic stops or high visibility events and in mass transit or critical infrastructure entry control points.

- Wearable, weighs less than 0.9 lbs.
- Gamma only (R200-G) and gamma/neutron (R200-GN)
- Fully compliant with ANSI N42.32 and N42.48 standards, nuclide identification (≤ 7.5% resolution)
- IP67 and MIL-STD 810G rated enclosure, 1.5m drop-tested on all six sides
- Single-hand operation with 3-button control
- Common user interface with other FLIR raditation detectors
- No consumables or user maintenance



IDENTIFINDER® R300 ALSO AVAILABLE

FLIR IDENTIFINDER® R400

All-Purpose Radionuclide Identification Device (RID)

- Handheld radiation detection and identification
- Intuitive and lightweight (< 3.2 lbs.)
- 3-button interface simplifies operation in high stress situations
- Over 20,000 deployed globally

PPE

DUPONT™ TYCHEM® 2000 SFR

Chemical and secondary flame protection in a lightweight garment. Intended to be worn overy primary flame resistant garments. Also provides an effective barrier against a range of inorganic acids and bases as well as industrial cleaning chemicals and particles.

- Respirator-fit hood lined with Pro-Shield® 6 SFR fabric
- Covered, braided elastic at hood
- Nylon zipper with large metal pull
- Chin flap with double-sided adhesive tape
- Storm flap covers zipper which can be sealed by the wearer with double-sided adhesive strip to prevent intrusion at zipper
- Covered, braided elastic openings at wrist and ankle for tighter fit
- Taped seams

DUPONT®





DUPONT™ TYCHEM® 6000 TF611T

Made of a proprietary barrier film laminated to a Tyvek® substrate. The fabric provides at least 30 minutes of protection against over 180 challenge chemicals including chemical warfare agents and toxic industrial chemicals.

- Strong, durable and lightweight
- Hooded coverall with Elastomeric interface hood for tight fit around respirator
- Rear entry design keeps closure away from direct contact with frontal chemical exposure
- Double storm flap covers zipper which can be secured by the wearer with snaps and hook and loop closure to prevent intrusion at zipper
- Attached dissipative socks with boot flaps
- Attached inner gloves (to be used with appropriate outer gloves)
- Elastic wrist for an optimum fit
- Taped seams provide strong chemical resistance against heavy liquid splashes. A sewn seam is covered with a strip of compatible chemical resistant material through heat sealing

BLAUER RC3® ENSEMBLE

Designed to protect wearers against a broad range of CBRNe threats including liquid and vapor chemicals, radiological and biological particulates, and liquid chemical splash during physically demanding tactical entries, confined space rescue, and US&R missions.

- NFPA 1994 Class 3-R (2018 ed.) certification
- NFPA 1994 Class 4-R (2018 ed.) certification
- NFPA 1992 (2018 ed.) certification
- Breathable GORE CHEMPAK fabric
- Streamlined pattern provides a more tactical fit on the user and better equipment integration
- Durable fabric and seams prevent accidental contamination and provide user confidence
- Ten year shelf life
- Machine washable for multiple uses if not grossly contaminated





Kappler
Know What You're Getting Into.®

KAPPLER DURACHEM® 500

Certified NFPA 1994 protection for both CBRN and Hazmat.

- Includes dual certification to NFPA 1994 for both Class 1 and Class 2
- Provides tactical CBRN protection in non-encapsulating suit
- Rubber gasket fits securely around respirator (eliminates need for taping)
- Rear entry design enhances frontal splash protection





KAPPLER LANTEX® 100

Certified to NFPA 1999 for fentanyl response.

- NFPA 1999 certified Lantex® 100 meets IAB and CDC/NIOSH guidelines for fentanyl protection
- Fabric and seams pass ASTM F1671 blood and viral penetration test
- Breathable protective fabric provides enhanced comfort
- Unique rear entry garment design allows safer doffing, helps prevent cross-contamination
- Soft, flexible rubber gasket around face opening provides secure fit around respirator
- Finger loop features ensures sleeves extend over gloves





LION ERS

LION ready for action

The ERS (Extended Response Suit) protects against lower levels of vapor and liquid concentrations that may be encountered in the Warm Zone when deployed with the proper ensemble. This one piece, front entry suit is breathable for deployment over an extended period of time.

- Durable GORE® CHEMPAK® Selectively Permeable Fabric provides the wearer with protection against TIC's, TIM's, and CWA's below IDLH concentration levels while peforming technical and tactical operations
- Certified to (Warm Zone Operations), NFPA 1994, Class 3 (Toxic Industrial Chemical and Warfare Agent Protection) and NFPA 1992 (Liquid Splash)
- Certifed with variety of face pieces
- Increased mission time and performance due to the breathable selectively permeable membrane
- 24 hour / 3 wash wear life
- Sleek, one-piece, lighweight design with attached hood that easily compacts for storage
- Front-entry design for ease of donning/doffing
- GORE® G9492 inner glove
- Molded face seal that does not require tape and is certified for use with multiple CBRN respirators and masks
- Tapered legs with elasticated cuffs and attached booties for increased funtionality and mobility
- 4 adjustable belt loops to securely wear a duty belt or a PAPR and allow for easy doffing during decontamination

LION MT94™

The MT94™ (Multi-Threat) CBRN ensemble offers first responders advanced protection when facing some of the world's worst chemical and biological threats.

- Limited Hot Zone protection - certified to NFPA 1994, Class 2 and NFPA 1992 for hot zone operations
- GORE® CHEMPAK® Ultra Barrier Fabric provides durable protection against TIC's and CWA's above IDLH concentration levels while also providing improved mobility during tactical and technical operations
- Streamlined design combines durability, mobility and comfort
- Usable for multiple wears and washings, if not exposed or contaminated
- Rugged construction allows you to perform in the most challenging of circumstances
- Certified for use with GORE® G9492™ glove system using GORE® CHEMPAK® Ultra Barrier Fabric



PIP NOMEX HOOD

This NFPA straight cut full face hood is made of 20% Nomex and 80% Lenzing FR, fire resistant 2 ply knit fabrics that are certiifed to NFPA 1971-2007 standard for structural fire fighting.

- 20" in total length with a back gusset that allows it to lay flat around the neck
- Tunneled elastic face opening - 1/2" elastic is encased in fabric to ensure snug and durable fit
- Flatlock seams add strength and extra comfort



APPLICATIONS

- Incident command
- Privacy/scene/evidence protection
- Long-term operations
- Rehab
- Dive rescue

BENEFITS

- 1 person automatic deployment
- Compact storage
- All-weather use
- Pre-installed LED lighting
- Customizable





ZUMRO®
Fast. Simple. Proven.

#1 IN THE INDUSTRY ★

OTHER SIZES & OPTIONS AVAILABLE
PLEASE CALL FOR AN ON-SITE DEMO!



PELTOR®



3M™ PELTOR™ COMTAC™ HEADSETS

Designed to provide warfighters the options needed for successful field hearing protection and combat communications.

- 2-way tactical headset
- Level-dependent surround sound for "talk through"
- Ambidextrous noise-canceling boom mic
- Adjustable sizing

3M™ PELTOR™ TACTICAL 6-S HEADSET

Designed to perceive and localize weak sounds while offering hearing protection in high-noise environments.

- NRR: 19dB
- Small, compact and foldable
- Slim earcup profile
- External earcup microphones help provide situational awareness





ATLANTIC SIGNAL GLADIATOR H TACTICAL HEADSET

Allows an operator to engage and disengage hearing pro at-will while having no impact whatsoever on his ability to RX and TX.

- Earplugs provide up to 23 NRR
- Allows the operator to receive radio communications through his/her facial bones, leaving both ears free to maintain 360° of situational and directional awareness
- Audio transducers are positioned in front of the ears
- Communication systems are customizable

ATLANTIC SIGNAL COMBAT PUSH TO TALK

- Front mounted PTT switch as a secondary actuation switch
- Side mounted switch is quiet and shrouded
- Water resistant

atlantic signal

SAFEWARE IS A PROUD DISTRIBUTOR OF THESE LEADING UNIFORM MANUFACTURERS!

5.11

elbeco

SPIEWAK since 1904

TRU-SPEC





TIMBERLAND PRO® VALOR™ DUTY BOOT

Soft-toe waterproof boots feature outsoles that grip any terrain and lightweight insoles for athletic performance.

- Uppers are black smooth leather and 1200-denier ballistic nylon
- Waterproof membrane
- Mesh lining with antimicrobial treatment for odor control and comfortable feet
- Scotchgard™ protector by 3M for stain resistance
- Bloodborne pathogen-resistant membrane
- Dynamic anti-fatigue technology absorbs shock and returns energy at key zones of the foot for all-day comfort
- Rounded driving moc heel
- Wall-climb toe grip
- Non-marking Timberland PRO® rubber lug outsole is slip-, oil-, and abrasion-resistant



5.11 TACTICAL® A.T.A.C 8" SHIELD CSA/ASTM BOOT

Offers unbeatable puncture, moisture and toe protection for superior safety in the harshest environments. The ATAC Shield Boot keeps you mobile, secure and comfortable at all times.

- Waterproof/breathable BPR membrane
- Side zip functionality
- 5.11 Shock Mitigation System®
- Antibacterial and moisture-wicking lining
- Cushioned insole
- Oil and slip resistant, no-squeak outsole
- Semi-rigid heel and toe reinforcement
- Full grain leather and rugged nylon construction



DANNER ACADIA BOOTS

Made in the USA, the Acadia® features Danner's famous stitchdown construction, providing a more stable platform underfoot and superior durability.

- 8" black
- Waterproof breathable GORE-TEX® lining and a combination upper of 1000 Denier nylon and full-grain leather
- Vibram® Kletterlift outsole provides superior shock absorption and great traction on both wet and dry surfaces

PROPPER® SERIES 100® 8" WATERPROOF SIDE ZIP BOOT

- Polishable full grain leather (black only) with 1000D nylon upper
- Durable, coated, speed lace hardware with 550 paracord lacing
- Fast-rope compatible arch design resists wear from ladders and fast-roping
- Ortholite® sock liner for comfort
- Washable open cell foam inserts contour to your foot for weight distribution and arch support
- Oil- and slip- resistant upper outsole for excellent traction and impact absorption
- Open cell air mesh foam provides full foot air circulation for maximum comfort
- Anti-microbial breathable lining prevents odor and extends the life of the boot
- Triple stitching for durability NATO speed lacing system
- YKK side zipper with zipper guard





HAIX GSG9-S

Developed for and with SRT Teams.

- 8" black
- Waterproof leather
- Footwear liner which will never pull out or wrinkle up over time
- Lightweight foam injected into the sole to provide exceptional shock absorption and superior heat/cold insulation
- Two-zone lacing system

SAFEWARE OFFERS AN EXTENSIVE OFFERING OF DUTY GEAR

GOULD™ &GOODRICH
A PASSION FOR PROTECTION

Including badges, belts, holsters, flashlight holders, magazine cases, radio holders, handcuff holders and much more.



Analysis of Read Data from Massachusetts State Police

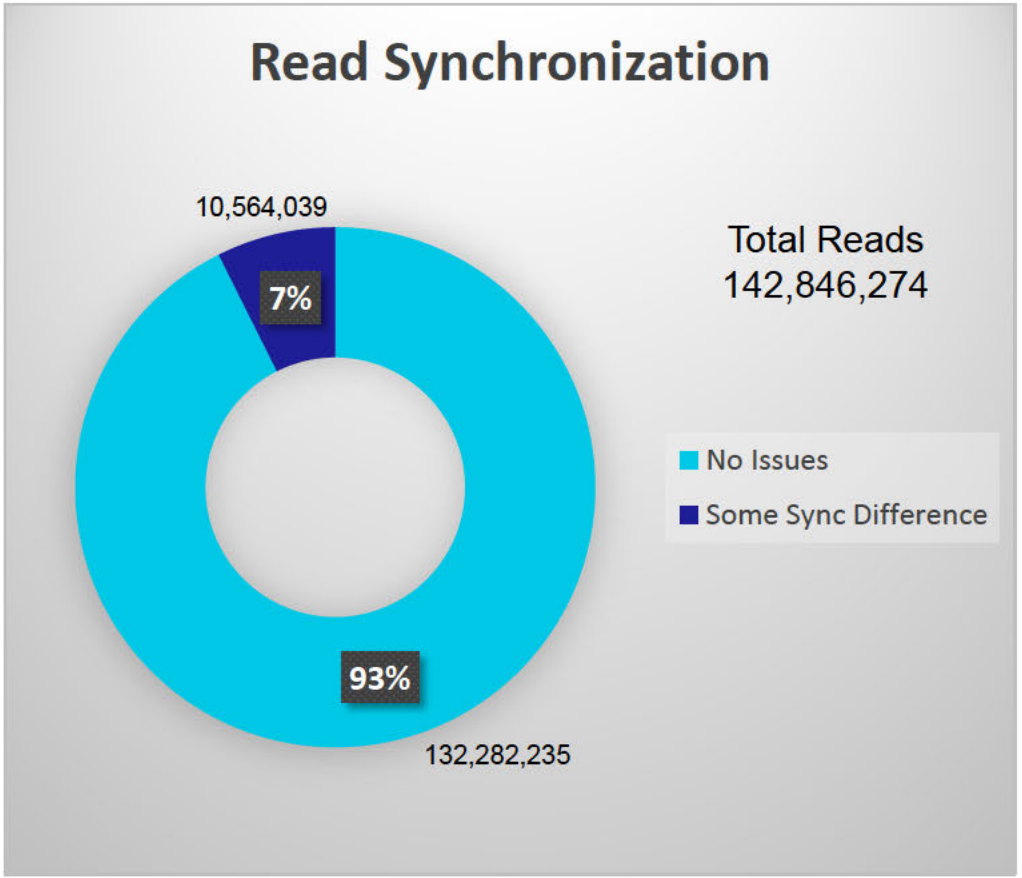
30 November 2020



Confidential

Read Synchronization

- System Scenario:
  - Database
    - Microsoft SQL Server
    - Contains approximately 142 million reads
    - One-year retention period
  - Software
    - BOSS 3
    - First installed: summer 2013
    - Last software update: spring 2018
    - Last annual support agreement: 2018
- This first chart shows the percentage of reads where the camera time is difference than the synchronize time in BOSS. There are a number of reasons for the deviation including but not limited to communication lag, BOSS server is unavailable, network traffic, and the SQL database is unavailable.
- Further analysis will focus on the 7% data.

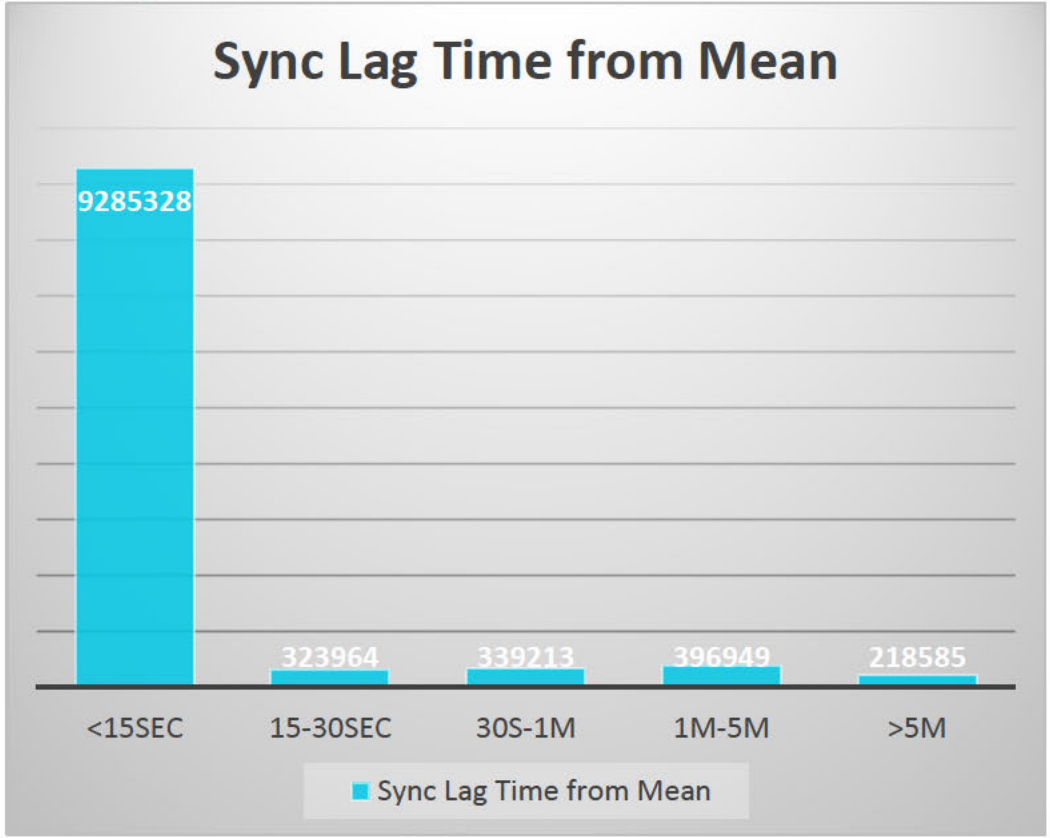


Confidential

Reads with Time Difference

This data represents the 7% data from the total reads where some time difference was identified 5316

- The mean is the average time when the read synchronized that BOSS synchronized with other cameras. This number is important because it gives context to the BOSS service's behavior and thereby accounting for issues with the server.
- Of the 10.5 million reads where the synchronization time is different, 87.9% of that data synchronized within 15 seconds on the mean.
- Of the reads, 94.17% of the data synchronized within a minute of the mean.
- In conclusion, only **0.43%** of the total reads are potentially misaligned with the synchronization. Therefore, we conclude that 99.57% is considered within acceptable synchronization.



Confidential

Summary

There are a number of reasons why the camera time can drift from the BOSS synchronization time. Most of these reasons do not affect the integrity of the read data. These include, but not limited to:

- Communication lags with the network
- BOSS server interruptions
- Bulk cached reads synchronizing all at once
- Database interruptions
- Aged hardware

For these instances, the time captured and recorded by the camera are accurate.

The purpose of the analysis to find signatures in the database that show anomalies that would be considered outside normal interruptions between the camera and the BOSS server. We narrowed the focus by evaluating a subset of reads that exhibit any synchronization time difference. This subset is approximately 7% of the total reads in the system, or 10.5M reads. Within that subset, we calculated an average for each read's sync time (sync mean time) to determine an acceptable deviation between the camera time and BOSS sync time. This was done to account for most BOSS server issues.

Of the subset analysis, approximately 9.95M reads were within one minute of the sync mean time. The remaining 615k reads would be considered potentially misaligned with the synchronization and would need to be evaluated further. This accounts for approximately **0.43%** of the total reads currently in the system. We believe upon initial further analysis that many of these are isolated to specific cameras or camera configurations.

Confidential

PIPS TECHNOLOGY

A NEOLOGY Business

www.pipstechnology.com

Home Office

National ANPR Standards for Policing and Law Enforcement

November 2020

Version: 2.1

1. Executive Summary

These standards articulate the requirements with which the police and other Law Enforcement Agencies (LEA), as detailed at Annex A must comply to access the National ANPR Capability (NAC). These standards do not cover the use of Automatic Number Plate Recognition (ANPR) for any purpose that is not law enforcement and will identify the purposes for which this document shall be applicable. Data from the NAC may not be used for other purposes, however in appropriate circumstances a camera may provide data to both the NAC and organisations other than those listed at Annex A to be managed independently.

This document includes a description of the legal basis for ANPR as well as the applicability of these standards. The standards comprise three main sections: Data Standards, Infrastructure Standards and Data Access and Management Standards. Audit standards and technical requirements are covered in other documents.

Data Standards comprise the security requirements that must be met for the NAC as well as the composition requirements for read data.

Infrastructure Standards cover the end-to-end infrastructure requirements for the NAC, including infrastructure development, cameras, networks, databases, infrastructure access and performance and legal requirements.

Data Access and Management Standards include the management of data within the NAC, including collection, storage, transfer and deletion of data. This section also provides guidance on FOI and Data Protection Act (DPA) enquiries.

The Annexes to this document include password requirements, guidance on investigation categories, the approval process for accessing ANPR data and a list of approved organisations that may access ANPR.

2. Contents

1. Executive Summary 2

Definitions 5

3. Introduction 8

4. Background 9

5. ANPR Legislation 10

6. Applicability 12

7. Part 1: Data Standards 13

7.1. Data Standards Overview 13

7.2. Data Security 13

8. Part 2: Infrastructure Standards 16

9. Part 3: Data Access and Management Standards 28

Annex A: Approved Organisations 38

Annex B: Investigation Categories 40

Major Investigations 40

Serious Investigations 41

Priority and Volume Investigations 43

Annex C: Data Access Requirements 45

Appendix A: Password Requirements 47

Document Revisions

Version 1.1 draft	July 2020	Change ref from CAST to DSTL in 8.14 Clarification at 9.8 re Command and Control Update of links within text
Version 2.0	September 2020	Published with amendments as above
Version 2.1	November 2020	Footnote added re data deletion (para 9.5.1)

Definitions

Acronym	Description
ANPR	Automatic Number Plate Recognition
ANPR system	A collection of cameras, readers components linking to NAS
Audit Standards	National Standards for Compliance and Audit of Law Enforcement ANPR
CCTV	Closed Circuit Television
CAMERA	The device used to capture an ANPR read
CAPTURE RECORD	The record of a vehicle recorded by NAS for a vehicle passing an ANPR camera including the ANPR READ, associated images and meta data.
COMMUNICATIONS LINKS	The connections between the camera, any local infrastructure and the NAS
CONTROLLER	The competent authority which alone or jointly with others determines the means and purposes of the processing of personal data. Part 3 data Protection Act 2018
CCA	Crime and Courts Act 2013
CPIA	Criminal Procedure and Investigations Act 1996 and the CPIA Code of Practice
DPA	Data Protection Act 2018
FOI	Freedom of Information Act 2000
GDPR	General Data Protection Regulation
GSCP	Government Security Classifications Policy – (formerly the Government Protective Marking Scheme (GPMS)
GPS	Global Positioning System
HIT	The report of a match of a vehicle registration mark (VRM) READ with a VRM that is included on a vehicle of interest list (VOI)
ICO Code	ICO Code of Practice for Surveillance Camera Systems

ISO	Information Security Officer – The member of staff with responsibility for ensuring compliance with requirements for IT security
ITHC	IT Health Check – The process for ensuring that security provisions for IT are appropriate and in compliance with requirements that are current at the time of the check.
JCA	Joint Controller Arrangements under provisions of the Data Protection Act 2018-
JPEG	Joint Photographic Expert Group image format
LEA	Law Enforcement Agency – Includes police forces and other agencies undertaking law enforcement activities. For the purpose of this document, LEAs shall only include those organisations listed at Annex A.
MIDAS	Motor Insurance Bureau (MIB) data of uninsured vehicles
MOPI	Code of Practice for the Management of Police Information
NAC	National ANPR Capability includes: • the NAS which is a single national system consisting of the functionality to enable use for operational response, investigation and intelligence purposes and a single national store of data, and, • the National ANPR Infrastructure (NAI) which is a network of ANPR cameras, communications links, firewalls and other related supporting components, that are the responsibility of LEA, that connect to the NAS.
NAI	A network of ANPR cameras, communications links, firewalls and other related supporting components
NAS	National ANPR Service
NASP	National ANPR Standards for Policing first version published in 2013 and replaced by NASPLE recognising the applicability to all law enforcement agencies that access the NAS
NASPLE	National ANPR Standards for Policing and Law Enforcement.
National VOI List	Nationally circulated lists that include stolen vehicles, vehicles requiring an operational response and vehicles within Schengen circulations
NAPS	National Accreditor for Police Systems – Responsible for confirming that police IT systems are in accordance with security requirements and authorising connection to national systems.
Network Connections	The IT links between components of the NAC

NPCC	National Police Chiefs' Council
NPCC Vetting Policy	The NPCC standards for vetting of staff for access to police information
PERSONAL DATA	Means any information relating to an identified or identifiable living individual. 'identifiable living individual' means a living individual who can be identified directly or indirectly, in particular by reference to_ a) an identifier such as name, an identification number, location data or an online identifier, or b) One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual Data Protection Act 2018
PNC	Police National Computer
READ	The interpretation of a VRM by an ANPR system
RIPA	Regulation of Investigatory Powers Act 2000
RIPSA	Regulation of Investigatory Powers (Scotland) Act 2000
Schengen	The Schengen Information System will enable the authorities of signatory countries to have access to reports on persons and objects for the purpose of border checks and controls and other police and customs checks
SMS	A Standards format for text messaging
TSpec	The document prescribing the technical specifications for data within the National ANPR Service (NAS) to comply with the requirements of NASPLE.
VOI	The details of a vehicle that are of interest to law enforcement for operational response or investigation purposes that is included on a list to enable it to be READ and for authorised staff to receive a report of that READ.
VRM	Vehicle Registration Mark

3. Introduction

The Home Office issues these standards in support of the management and use of the National ANPR Service (NAS). ANPR is used by the police and other law enforcement agencies (hereafter referred to as LEAs) for law enforcement purposes. LEAs should use these policy standards to shape technical standards, standard operating procedures and audit standards.

This document covers the use of ANPR within the NAC and will identify for which uses this document shall be applicable. The use of ANPR within the NAC otherwise than in accordance with this document is not permitted.

This document is divided into 3 sections:

- Part 1 – Data Standards, which define the compliance requirements for ANPR Data
- Part 2 – Infrastructure Standards, which define the compliance requirements for ANPR infrastructure
- Part 3 – Data Access and Management Standards, which define the access requirements for LEAs and other organisations that are associated with ANPR data for law enforcement purposes.

4. Background

ANPR technology is used to help detect, deter and disrupt criminality at a local, force, regional and national level. This includes tackling traveling criminals, Organised Crime Groups and terrorists. ANPR provides lines of enquiry and evidence in the investigation of crime and is used by LEAs throughout England, Wales, Scotland and Northern Ireland.

There exists a National Law Enforcement ANPR capability (NAC) which enables LEAs to benefit from operational use of ANPR. The NAC comprises:

- The NAS. This is a single national system comprising standardised functionality to enable use for operational response, investigation and intelligence purposes as well as a single national store of data;
- The National ANPR Infrastructure (NAI), which is a network of ANPR cameras, communications links, firewalls and other related supporting components. Any element of this network that is connected to the NAS shall be the responsibility of the LEA that manages that connection.

4.1 Technical Specifications

Technical specifications for the NAC are detailed within a technical specification document (TSpec). LEAs are required to conform to the requirements of that document.

5. ANPR Legislation

ANPR operates under a complex framework of legislation of general application, including the General Data Protection Regulation (GDPR), the DPA, the Surveillance Camera Code and Common Law.

The National Law Enforcement ANPR capability (NAC) is subject to the Information Commissioner's Office regulatory provisions and regulatory oversight by the Surveillance Camera Commissioner (SCC).[1]

5.1. ANPR Data: Legal Basis

ANPR data from police forces is police information within the meaning of The Code of Practice on the Management of Police Information 2005 (MoPI) made under the Police Act 1996 and Police Act 1997. It may be shared between LEAs in accordance with the provisions of that Code or any other document which applies similar standards in its place, including the National Crime Agency's (NCA) Statement of Information Management Practice (SIMP).

Access to and the retention and management of ANPR data obtained by LEAs must be compatible and consistent with their relevant legal obligations, which include: The Data Protection Legislation (i.e. the General Data Protection Regulations (GDPR) and the Data Protection Act 2018 (DPA));

- ICO Code of Practice for Surveillance Camera Systems (ICO Code);
- College of Policing Approved Professional Practice – Information Management. (MOPI);
- Part 2 of the Protection of Freedoms Act 2012 (PoFA);
- The Surveillance Camera Code issued under Part 2 of PoFA.
- Criminal Procedure and Investigations Act 1996 and Code of Practice issued under Part II of that Act (CPIA);

[1] Section 29(6) of the PoFA includes ANPR as one of a number of surveillance camera systems under the regulatory oversight of the SCC and its associated Home Office code of practice. Relevant authorities (as defined by Section 33 (s33) of PoFA) in England and Wales (including the police) must have regard to the code which provides guidance on the appropriate and effective use of surveillance camera systems, and therefore ANPR

5.2. Use of ANPR for Law Enforcement Purposes

ANPR infrastructure may only be deployed law enforcement purposes as defined in Part 3 of the DPA ; or on grounds of national security. Law Enforcement is defined by the DPA as “the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security”. The Joint Controller Arrangements (JCA).

The JCA details the responsibilities of controllers for compliance with the DPA. The National Police Chiefs’ Council (NPCC) ANPR lead is designated as the lead controller within the JCA for the NAS.

Joint Controllers have determined within the JCA that they will conform to consistent policy and procedures for the elements of the NAC for which their own LEA is responsible and for which they are controller.

5.3. ANPR Audit

The Home Office has also issued a separate document entitled “National Standards for Compliance and Audit of Law Enforcement ANPR” (Audit Standards). This document sets out the requirements for compliance and audit by all LEAs and of the national components of the NAC.

6. Applicability

These standards apply to any NAC operated by LEAs in the UK that connect to or receive data from the NAS.

Where, under an agreement, LEAs receive data from components that are under the ownership or control of other organisations it is the responsibility of the receiving LEA to ensure compliance with the NASPLE.

ANPR cameras that are used solely for speed enforcement are outside the scope of these standards.

ANPR systems that are not operated by LEAs and do not submit data to the NAS are similarly outside the scope of these standards.

6.1. Approved Organisations

An LEA may only connect to, or receive data from, the NAS following approval of the NPCC policing lead for ANPR within the NPCC Crime Operations Committee (NPCC policing lead for ANPR) - an "Approved Organisation".

For an organisation to be designated as an "Approved Organisation" it must be involved in and can lawfully process data for one or more of the following activities:

- National security and counter terrorism
- Law enforcement
    - The prevention and detection of crime
    - The apprehension and prosecution of offenders

In granting access, the NPCC policing lead for ANPR must be satisfied that it is necessary and proportionate for the organisation to be approved.

Approved Organisations must ensure that their organisation complies with the requirements of NASPLE and Compliance and Audit Standards.

References to LEAs within NASPLE includes only "Approved Organisations" unless indicated otherwise. Approved Organisations are listed in Annex A.

In addition to the above purposes LEAs may use the NAS for operational purposes relevant to individual and public safety. E.g Missing persons.

7. Part 1: Data Standards

7.1. Data Standards Overview

Part 1 prescribes the standards with which data must comply for it to be accepted into the NAS.

7.2. Data Security

LEAs have a duty to protect ANPR data to ensure its integrity and to maintain its value for law enforcement purposes. ANPR 'read' data must therefore be attributed a protective marking of OFFICIAL, in accordance with the Government Security Classifications Policy (GSCP).

When in the NAS database, other material could be accessed such that personal details of persons associated with the ANPR READ data may be identified. Once ANPR READ data is available within the NAS, it is personal data in the context of the DPA.

All ANPR data in the NAS, should therefore be managed in accordance with DPA principles and handled as OFFICIAL - SENSITIVE data, in accordance with the GSCP.

Whilst in the custody of, or being transmitted to or from a LEA, ANPR data should be handled in accordance with Part 2 and Part 3 of NASPLE.

Access to data within ANPR systems must be in accordance with Part 3 of NASPLE.

7.3. ANPR Read Records

7.3.1. Composition

An ANPR READ places a VRM at a specific location and time. It is obtained by a camera as part of an automatic number plate reading system. The data components of a record must not be entered manually into the NAS unless for the purposes of correcting a mis-read VRM on the system or by an administrator for testing the connectivity of a camera.

The READs must include VRM, time, location of read and camera identifier and be consistent with the requirements of section 7.4.

7.4. Core Data

7.4.1. Vehicle Registration Mark (Mandatory)

ANPR data must accurately represent VRMs of all vehicles with correctly represented EU and Schengen Community number plates. Systems must accurately record the VRM for vehicles passing within the field of view for each camera. The capture and read rates must be in accordance with the type of camera defined at Section 8.9.

7.4.2. Vehicle Registration Mark – Not Read (Mandatory where functionality is in place)

Where a CAMERA has the capability to record images of vehicles passing within the field of view where no VRM is identified by the system, information will be recorded in the VRM field in accordance with current TSpec.

7.4.3. Time (Mandatory)

System audit provisions must provide evidence of synchronisation at least once every 10 minutes using standard time source techniques in accordance with current TSpec.

Components of ANPR systems must automatically adjust the display of the time to daylight saving time during the period when this is in-force.

7.4.4. Location (Mandatory)

ANPR data must place a read in a location, accurate to within 10 metres. In addition, all fixed-site ANPR cameras must have their GPS co-ordinates accurately recorded to within 5 metres.

7.4.5. Supporting Imagery

In order to assist with assessment of the accuracy of individual read records, ANPR data may include images:

- Plate patch – showing the number plate only, to allow comparison of the visual image with the textual representation interpreted (Mandatory for systems under ownership or control of a LEA)
- Overview Image – showing the vehicle to allow identification of the make, model and colour of the vehicle within the read zone (Optional)
- 'Geo Tagging' - if an accurate GPS Geo Location is available, then this detail may be added to images (Optional)

Should any image be found to exceed prescribed limits for image size, cameras submitting the images must be revised to ensure images obtained are within the limits prescribed within a maximum of 7 days.

All images must be linked to the corresponding read record.

All images recorded must be forwarded to the NAS. Where no overview image has been recorded, the read record must include a reference to identify that no image is recorded.

7.4.6. Record Retention and Deletion

All read records received by LEAs including any associated images must be supplied to the NAS.

All records must be managed and subsequently deleted in accordance Section 9.5.

7.4.7. Camera Performance Evaluation

Camera Performance evaluation, as detailed in Section 8.14 of all components within LEA ANPR systems must be conducted to ensure compliance with the Data Standards. Where performance falls below the Data Standards then this must be corrected and reassessed to confirm that performance conforms to data standards, within 30 days of that issue being identified.

If camera performance issues are not resolved within 30 days of identification, then the feed of data from those cameras must cease until corrected.

8. Part 2: Infrastructure Standards

8.1. Infrastructure Standards Overview

Part 2 prescribes the standards for the components of the NAC, including the operability standards required that are to be used by LEAs connected to the NAS.

8.2. Accreditation

To preserve the integrity of the NAC, all components of infrastructure that connect to the NAS must be assessed to ensure that they do not pose a threat to the NAC and are suitably for handling data up to GSC OFFICIAL level.

8.3. LEA Domain

The assessment of risk to an LEA domain rests with the controller for each LEA, which will normally be discharged by the Information Security Officer (ISO) for that LEA. The level of risk posed should be determined through completion of a Risk Analysis Document and an IT health check (ITHC). Review of compliance with the risk analysis outcomes and the conduct of an ITHC is to be completed annually.

8.4. ANPR Network

The National Accreditor for Police Systems (NAPS) needs to be assured that the local LEA Infrastructure poses no threat to NAC. The NAPS will liaise with the LEA ISO to assess the level of risk posed, as documented through the LEA corporate information risk management and ITHC process.

The NAPS will approve the components of local infrastructure for connection to the ANPR Network. This will be confirmed by the completion of the Code of Connection.

8.5. ANPR Infrastructure Development

A consistent and standardised approach must be applied to infrastructure development within the NAC.

8.5.1. Strategic Assessments

A strategic assessment should be carried out prior to the deployment of an ANPR camera. An assessment should also be carried out prior to receiving ANPR data for onward submission to the NAS, that is received from ANPR systems operated by organisations that are not defined as LEAs. These assessments must identify a need for ANPR at that location for law enforcement purposes.

Where a need is identified, consideration of whether the deployment, or the receipt of ANPR data is appropriate and proportionate. This requires an assessment of the

value for law enforcement purposes taking account of the impact on fundamental rights and freedoms of individuals. Consideration of the legitimate expectations of individual privacy is also required. Strategic assessment should consider:

- National Security and Counter Terrorism,
- Serious, Organised and Major Crime
- Local Crime,
- Community Confidence and Reassurance, Crime Prevention and Reduction.

8.5.2. Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA), which may include consultations with relevant stakeholders, is required for all planned new infrastructure.

The DPIA must include:

- A description of the proposed development
- An assessment of the risks to the fundamental rights and freedoms of individuals – the data subjects.
- Measures to mitigate those risks
- Confirmation of safeguards and security measures to ensure protection of personal data and compliance with the DPA.
- Details of any stakeholder consultation

8.5.3. Information Commissioner's Office Consultation

The NAC may result in high risk to the rights and freedoms of individuals and prior consultation with the Information Commissioner's Office (ICO) may be required before the deployment of any new ANPR infrastructure. When a DPIA identifies a large increase in the number of deployed ANPR infrastructure or where significant privacy risks are identified the ICO should be consulted. (Section 64 DPA)

8.5.4. Strategic Assessment Reviews

LEAs must monitor the continued requirement for a camera to be maintained at a location, or for an LEA to receive data from ANPR systems operated by other organisations. Should the justification for deployment at that location cease, the device must be removed, and the receipt of data must be terminated.

The locations of all cameras and the need to receive data from systems operated by other organisations must be reviewed annually, considering requirements for infrastructure development to ensure that camera deployment or receipt of data remains appropriate and proportionate.

8.6. Vehicle-Mounted Systems

Vehicle-mounted ANPR may only be deployed where any of the following circumstances arise:

- For the purposes of monitoring hits against a list of VOI with the intention that an operational response to the hit will take place, either by staff within the vehicle containing the ANPR system or by others deployed in support of that vehicle for the purpose of providing a response.
- Deployed at locations identified following completion of infrastructure development assessment prior to the deployment of other camera at the location.
- Deployed as a result of Operational tasking processes within an LEA where it has been determined that it is proportionate for short-term deployment of ANPR;
    - In response to identified criminal activity
    - In response to identified community problems
- To support assessment of a location for future more permanent camera deployment in accordance with the infrastructure development procedure
- In support of immediate operational response following report of a crime or incident.

8.7. System Standards

The performance standards for camera shown below are most easily met for vehicles travelling towards a camera, and it is recommended that unless unavoidable, for example in some dual-lane deployments, that this configuration is used in all cases.

8.7.1. Static ANPR Systems

A static ANPR system has been built for the primary purpose of 'capturing' and 'reading' VRMs and is located in a fixed position, with no intention of the system being moved. Except in extreme weather conditions the performance standards for these systems must be achieved at all times. Systems must capture 98% of all VRM that are visible to the human eye[2] and accurately read 95% of captured VRM.

8.7.2. Moveable ANPR Systems

A moveable ANPR system has been built for the primary purpose of 'capturing' and 'reading' VRMs, is located in a fixed position on a temporary basis and may be

[2] 'Visible to the Human eye' should be determined from the viewpoint of the camera within the ANPR system. A number plate visible to a 'human eye' at that location should also be visible by the ANPR system.

moved. Except in extreme weather conditions the performance standards for these systems must be achieved at all times. Systems must capture 98% of all VRM that are visible to the human eye and accurately read 95% of captured VRM.

8.7.3. Multi-Lane ANPR Systems

A Multi-Lane ANPR system has the capability to read VRM for vehicles travelling in multiple lanes of the highway using a single camera. Except in extreme weather conditions the performance standards for these systems must be achieved at all times. For vehicles travelling towards the camera, systems must capture 98% of all VRM that are visible to the human eye and accurately read 95% of captured VRM.

For vehicles travelling away from the camera, the system must capture 90% of all VRM that are visible to the human eye and accurately read 95% of captured VRM.

8.7.4. CCTV Integrated ANPR Systems

A CCTV Integrated ANPR system may operate both as a CCTV camera and as an ANPR camera. The camera should be optimised[3] for the purposes of ANPR when being deployed as a camera. Integrated systems must only provide data to the NAS when in ANPR mode. Except in extreme weather conditions the performance standards for these systems must be achieved at all times when deployed in ANPR mode. CCTV systems may not be optimised to capture ANPR reads therefore systems must capture 85% of all VRM that are visible to the human eye and accurately read 95% of captured VRM.

8.7.5. Mobile ANPR Systems

A mobile ANPR system has been built for the primary purpose of 'capturing' and 'reading' VRMs. These include vehicle-mounted ANPR systems and other portable systems deployed on a temporary basis. Any equipment procured after the publication of version 1 of National ANPR Standards for Policing (NASP) (May 2013) must be live-linked to the NAS.

To achieve the optimum performance requirements, mobile equipment should be capable of night-time and low-light operation. Except in extreme weather conditions the performance standards for these systems must be achieved at all times.

Systems must capture 98% of all VRM that are visible to the human eye and accurately read 95% of captured VRM unless deployed in a moving vehicle, when the system must capture 80% of all VRM that are visible to the human eye and accurately read 95% of captured VRM.

[3] The optimum configuration of CCTV systems differs when used for general CCTV surveillance to when operated as an ANPR reader. It needs to be configured for ANPR use to ensure maximum possible data accuracy

8.7.6. Covert Systems

It is recognised that circumstances may arise where moveable or purpose-built, covert systems are deployed in support of an investigation in circumstances where it is not possible to establish a live-link to the NAS. Deployments of this type that are authorised within provisions of the RIPA or RIPSA are the only circumstances where equipment procured after the publication of version 1 of NASP (May 2013) may not have the capability to live-link to the NAS.

Unless unachievable due the nature of the deployment or in extreme weather conditions, the performance standards for these systems must be achieved at all times. Systems must capture 98% of al VRM that are visible to the human eye and accurately read 95% of captured VRM.

8.8. Camera Access Settings

Unless a camera is designated a 'Restricted Access' camera, all cameras that submit data to NAS must be attributed the settings of 'Open Access', such that all data received from that camera is visible to all users with appropriate permissions to access the data.

With appropriate authority, a camera may be designated a 'Restricted Access' camera. Designation of a camera for 'Restricted Access' may only be authorised by a senior manager. A 'Restricted Access' camera may or may not be covert and the designation of a device for 'Restricted Access' may require authorisation within the provisions of the RIPA or RIPSA.

A record of all authorisations for restricted access must be retained for the duration of the restriction and a period of 2 years thereafter.

8.9. System Capability and Resilience

8.9.1. Image Capture

All cameras under the ownership or control of LEAs must have the capability to capture and record supporting imagery in accordance with section 7.4.5.

There may be circumstances where the shared collection equipment that is owned and managed by a non-LEA organisation is being used that are not enabled for the recording of imagery. In these circumstance, these cameras may be connected to the NAS subject to the standards for ANPR Infrastructure Development.

Supporting Images are important to assist with the accuracy of individual capture records and therefore, where data is received from other a non-LEA organisation without supporting images, provision for upgrading of the system to enable the provision of images should be established.

8.9.2. Schengen Information Systems (SIS)

All ANPR systems must be capable of reading plates that form part of the SCHENGEN community.

8.9.3. Data Storage

The NAS must not allow any data loss.

8.9.4. Local System Resilience

All local ANPR systems must transfer data to the NAS on receipt in local systems from a camera and also have the capacity to retain ANPR reads and their related images for a minimum of 3 and a maximum of 7 days from the time of the ANPR read.

This will provide resilience should the local infrastructure connections, the NAS or communications to the NAS become unavailable and will prevent the loss of data. In the event of a failure to send read records and associated images to the NAS local systems must have the capability to re-send that data.

If for any reason reads from a camera are submitted to the local system more than 7 days after initial capture the reads may be retained on the local system for 24 hours to prevent loss of data, should connection to the NAS become unavailable.

8.9.5. Local system connection and data transfer

Local ANPR systems must not enable connection to or the transfer of data to ANPR systems operated by other LEA for the purposes of searching of data or monitoring of VOI lists.

During the period of any loss of connection to NAS local functionality may provide for basic search of a full or partial VRM and for alerting against the most recent VOI lists received from NAS.

LEAs must not share VOI lists, even in circumstances of NAS unavailability; however, LEAs may share information and intelligence relating to those VOI lists using established intelligence management procedures.

8.9.6. Local system data deletion

Data held on local systems must be deleted within the next 24 hours after the period of 7 days following the time of the read. Where a read is submitted to the local components of NAC more than 7 days after the time of the read by a camera it may be retained for no more than 48 hours in local systems and then deleted within the subsequent 24 hours.

8.9.7. Extended unavailability of NAS

In the unlikely event that connections to the NAS are unavailable for more than 7 days, then deletion of data in accordance with the above provisions may be suspended until such time as connection is restored. This may only be done with specific authority of the controller for the LEA collecting the data and a full written record of the granting of that authority is required.

8.9.8. Mobile ANPR Systems Data Transfer

All ANPR data held on mobile ANPR units that have been unable to transmit their data in real time must be transferred to the NAS within a maximum period of 48 hours from the time of capture except in circumstances where the camera is unable to connect to the local system.

8.9.9. Support and Maintenance

ANPR systems should be commissioned only with an appropriate level of support and maintenance to safeguard against component failure and assist with business change. Local provisions must be in place to ensure that, in the event of any failure of a component of infrastructure that provides communications to the NAS, to prevent loss of data. Reinstatement must be within a period consistent with the ability to retain data locally for that failed component and subject to a maximum period of 72 hours from the time that the component failed.

8.10. System Connectivity

8.10.1. Local ANPR Infrastructure Connectivity to LEA networks

Local ANPR Infrastructure must connect to the LEA network infrastructure to allow user access to the NAS and to support connections to the Police National Computer (PNC) and the NAS.

The security of all infrastructure connections must be managed via an organisation maintained and managed firewall in accordance with that organisation's own policy and the Community Code of Connection and NPCC/Police Scotland Community Security Policy.

8.11. National Databases

NAS must have the capacity to check against the following national databases, as a minimum; PNC; Includes 'Fast Track' 'Extract', 'Schengen' and 'MMC' data.

8.11.1. Response Times

In order to ensure compliance with DPA principles in the circulation of VOI, Real-time matching performance standards must be achieved in 95% of all reads.

The following table summarises maximum response times within the NAC:

System Type	Read to alarm	Number plate read by a camera to delivery to NAS	NAS process to delivery at a LEA for visibility by staff
Static ANPR system	4 sec	2 sec	2 sec
Moveable ANPR system	4 sec	2 sec	2 sec
Multi-Lane ANPR System	4 sec	2 sec	2 sec
CCTV Integrated ANPR system	4 sec	2 sec	2 sec
Mobile ANPR system	6 sec	4 sec	2 sec

8.11.2. Real-Time Data Delivery

In order to ensure operational capability and to support compliance with DPA, local LEA ANPR infrastructure must clearly display the current state of connectivity to the NAS and/or any time when data is not being sent to the NAS. In the event of a communications or systems failure, the LEA infrastructure must buffer that read data and deliver it to the NAS once the communications or failed systems have been restored. The real-time delivery of data is a priority and the delivery of any buffered data should take place in addition to delivery of real-time data.

8.11.3. Search and Export of Data

The NAS must provide for the identification and export of data to enable identification using criteria defined in TSpec.:

The ability to export ANPR data shall be limited to defined users.

In appropriate circumstances a message may be sent to authorised users by means of SMS text. Where SMS is used the information provided will be limited to the VRM, time and location of the read and the name of the list containing the VOI.

Bulk data, including images, required for investigative purposes that is stored under provisions of the Criminal Procedure and Investigation Act 1996 (CPIA) may be exported to an external LEA defined storage area and managed in accordance with local policy.

The NAS must provide for user defined privileges for use of data export functions and data may only be exported by users with those privileges.

8.11.4. Security

The NAC must provide for adequate security measures, including access control, to protect against unauthorised access to the system and data held within it. LEAs must ensure compliance with NAC requirements and are accountable for the security of all components of the NAC that are within their control. LEAs must ensure that individual user privileges are consistent with the requirements of their role and individual level of vetting.

Audit trails must be maintained to record all significant actions taken, including:

- User login,
- Successful and failed database searches, and;
- the addition to, and deletion of data from lists of VOI.

There must be provision within the NAS for users to record the reasons and any required authorisation for their actions. Access to audit trails must also be auditable and restricted to users who require this access as part of their role, as defined within policy.

The security of all LEA components of the NAC must be managed via an LEA. The LEA shall maintain and manage a firewall in accordance with the LEA's own policy, the Community Code of Connection and Community Security Policy. The requirements of the national network connections and GSC as confirmed by the appropriate governance authority in each case.

8.12. Databases

8.12.1. National Database

LEAs that receive VOI lists and updates from a national VOI list shall ensure that this list is loaded on their mobile system at the first opportunity following receipt of that list or update.

8.12.2. Third Party Databases

Where data is provided by a third party (e.g. the MIDAS File as provided from the Motor Insurance database), then there must be measures/procedures to ensure that the data is handled consistent with these standards. The criteria that must be addressed through these procedures include:

- Provisions must be in place to ensure that only the most up-to-date data set is in use.
- Version control and file naming systems must be in place
- Distribution methods must be in accordance with GSC security requirements.

8.13. Lists of Vehicles of Interest

8.13.1. Vehicle of Interest List Purpose

Lists of Vehicles of Interest (VOI) may be maintained by LEAs to support intelligence development, operations and investigations. The contents of a list of VOI will depend upon the purpose of that list, the format for which is detailed in TSpec.

8.13.2. Vehicle of Interest List Information and Access Controls

VOI Lists used for monitoring purposes and that do not require an operational response may include the details defined within the Tspec. When a VOI List is used to support operational response, sufficient information to ensure an appropriate response must be included.

LEA may maintain a VOI list for operational response purposes; however, these lists should only be used in circumstances that do not meet the need to include the information on the PNC. Access permissions for those lists must be restricted to ensure that data access is proportionate in each case.

Special Categories of Data and Criminal Convictions Data as defined by Schedule 1 of the DPA and Articles 9.1 and 10 of GDPR should only be included within a VOI list when it is essential to the purpose of circulation. The LEA circulating the list must ensure that the content and provisions for the access to any such list are appropriate at all times.

8.13.3. Vehicle of Interest List Resilience

The NAS will make lists of VOI available to LEA in order that they can be loaded onto management servers and mobile systems should the live-link to NAS become unavailable.

LEAs must not load VOI lists received from NAS onto any other systems and must establish procedures to ensure that VOI lists loaded onto the management server or mobile systems are current versions of those lists.

8.13.4. Actions required for a Vehicle of Interest List

Any LEA publishing a list of VOI onto NAS will determine access controls for that list. Lists will only be accessible to LEAs where it is proportionate for that accessibility. Where one LEA subscribes to the VOI Lists of another LEA, there is an obligation to monitor the list, assess a 'hit' against the list and respond subject to local resource availability and operational demands.

Logs of the loading of any VOI list onto a mobile system shall be maintained as required by Section 9.10.

8.13.5. Vehicle of Interest List Accuracy

The LEA supplying a VOI list to the NAS must ensure that information within the list is accurate, of current relevance, and is in a format that conforms to the requirements detailed within TSpec. All lists that are supplied must be reviewed on a regular basis by the LEA supplying the list.

8.13.6. Vehicle of Interest List Deletion

A list that is received from an LEA will be deleted from the NAS no later than 28 days after the last date of revision by the LEA that supplied the list.

8.13.7. Vehicle of Interest List Extraction

LEAs will not extract data from a list of VOI for the purposes of creating a composite list from a number of such lists, to be held outside the NAS.

8.14. Performance Evaluation

Performance testing must be consistent with current guidance provided by the Defence Science and Technology Laboratory (DSTL). (DSTL Guidance)

8.14.1. Installation of ANPR Infrastructure

Unless the exceptions for covert systems apply, on installation of any component of ANPR Infrastructure compliance with performance standards detailed within NASPLE must be confirmed and recorded.

Compliance with performance standards is required for both initial installation or on re-installation or re-deployment of any ANPR camera or other component.

8.14.2. Capture Rate Assessment

Any assessment of ‘capture’ rate must be based on not less than 250 consecutive vehicles (or a minimum period of 2 hours) displaying a VRM visible to the human eye passing within the field of view for a camera and in the case of a multi-lane system this applies to each lane covered by that system.

8.14.3. READ Rate Assessment

The READ rate for each type of system must be determined for not less than 250 consecutive ‘captured’ Vehicles displaying a VRM visible to the human eye.

Performance must be assessed for daylight and night time conditions. It is advisable to assess for a range of conditions including; bright daylight (dawn); bright daylight (dusk); overcast daylight and night time.

8.14.4. Performance Evaluation Schedules

The performance of all ANPR systems must be regularly reviewed to ensure conformance with the data standards defined in this document. NAS functionality should be used to monitor continued compliance with required 'capture' rates.

Compliance with the READ rate for a camera should be reviewed at least annually with a sample of not less than 250 consecutive reads. Provisions for performance evaluation must be defined in LEA policy and procedures.

In addition to the annual assessments, the performance standards for all cameras that do not have the capability to provide supporting imagery must be evaluated at no less than 6 monthly intervals. Assessments for this additional assessment shall include a sample of east 50 vehicles passing consecutively within the field of view.

8.14.5. Performance Evaluation of Covert Cameras

Where covert installation of ANPR infrastructure has been authorised within the provisions of RIPA or RIPSA, and the purpose of the installation may be compromised as a result of testing, the testing need not be completed.

8.14.6. Performance Evaluation Logs

A log for all performance evaluation activities must be retained in a form to enable the record of reviews for each component within ANPR systems to be identified and retrieved when required.

9. Part 3: Data Access and Management Standards

9.1. Data Access and Management Standards Overview

Part 3 prescribes the standards required for access to and management of ANPR data within the NAS.

The obligations that arise under the DPA are different depending on the reason for processing of data. It is the responsibility of the controller for the LEA that is processing the data to ensure compliance with relevant parts of the DPA in each case.

9.2. Data Management

9.2.1. Policy

All LEAs that connect to, or have access to, the NAS must have an up to date written policy in place for the access, management and use of ANPR data, including provisions for audit, which must be consistent with Compliance and Audit Standards.

Access to ANPR data must be proportionate to the circumstances of that access and taking account of the impact on the fundamental rights and freedoms of individuals.

9.2.2. Data Access Management

Authorised members of LEAs may access and use data within the NAS to the extent that is compliant with the DPA in the circumstances of each case, without reference to a controller unless otherwise required within the terms of NASPLE.

9.2.3. Shared Collection Equipment

9.2.3.1. Data provision by non-LEAs

NAS may receive data via an LEA from ANPR systems not directly within the control of the LEA in circumstances where it is using shared collection equipment that is owned and managed by a non-LEA organisation.

In these circumstances, the controller for the LEA that initially receives the data and the organisation owning the collection equipment are both controllers who will store data in separate databases that they manage independently. LEA controllers for data received under any such arrangement may manage the data and allow access to the data without reference to the owner, or any other user of the shared collection equipment.

9.2.3.2. Data received directly into NAS

NAS may receive data directly from ANPR systems not within the control of an LEA in circumstances where data is submitted to the NAS using shared collection equipment that is owned and managed by a non-LEA organisation, without the data first being received by a LEA.

The NPCC policing lead for ANPR as controller for data received under any such arrangement may manage the data and allow access to the data without reference to the owner, or any other user, of the shared collection equipment

9.2.3.3. Management of data provided by non-LEAs

In circumstances where a non-LEA has provided data to the NAS, the NPCC policing lead for ANPR and the organisation owning the collection equipment are both controllers who will store data in separate databases that they manage independently.

The NPCC policing lead for ANPR as controller for data received under any such arrangement may manage the data and allow access to the data without reference to the owner, or any other user, of the shared collection equipment.

9.2.3.4. Compliance Agreement

The LEA that receives data from a non-LEA organisation for submission into NAS, or the NPCC policing lead for ANPR in respect of data submitted directly to NAS, must ensure that a formal written-agreement is in place with the owner of the camera and other components of the ANPR infrastructure detailing appropriate arrangements to enable compliance with NASPLE.

9.2.4. Data Extraction from NAS

Where an LEA accesses data within the NAS they are controller for any data extracted from the NAS as a result of that access. Management of all data that is extracted must be in accordance with the provisions within NASPLE and any reports or other documents that include data from NAS must be marked in accordance with the requirements of the Government Security Classifications (GSC). Personal data must only be processed in accordance with the DPA.

9.3. Organisational and User Access to ANPR Data

9.3.1. ANPR Password Policy

Password requirements for access to NAS is based on national Cyber Security Centre guidelines and is applicable to all roles within LEA, third party contractors and suppliers and staff responsible for NAS service management.

Staff will be allocated individual accounts that may only be accessed using a password in a format approved by the national Accreditor to requirements detailed in Appendix A

9.3.2. ANPR Account Management

Staff who are approved to access NAS as both a user and for administrative purposes must be allocated separate accounts such that these functions cannot be achieved using a single log in account. Accounts must be reviewed, suspended or terminated in the following circumstances:

- An account must be suspended if it is not accessed for a period of 90 days. The need for access must be reviewed within the subsequent 7 days. The account may then be reactivated or deleted as appropriate,
- Access permissions must be reviewed within 7 days of a person changing role within an LEA.
- An account must be terminated within a maximum of 48 hours of a person leaving an LEA or partner agency.

9.3.3. Provisions for Data access

Any access to data must be for national security, counter terrorism, investigation and enforcement purposes as defined in Annex B or for the purpose of audit.

Staff within an LEA may be granted access to the extent relevant to their role, in accordance with local LEA policy in an LEA. LEA policy must be consistent with the purposes and standards within this document and the specific requirements at Annex C.

9.3.4. Data Access provision when NAS is unavailable

Data held within the local components of the NAC (Section 8.9) may only be accessed by authorised staff in circumstances where the NAS or communications to the NAS have become unavailable.

9.3.5. Vetting Requirements for access to ANPR data

Staff accessing the NAC are required to have successfully completed vetting to the standards as detailed below unless in exceptional circumstances with express written approval of the NPCC Policing lead for ANPR, as lead controller, approves any vetting process as equivalent to the required standard.

9.3.5.1. Police

Staff within a police service LEA authorised to access ANPR data must have successfully completed Recruitment Vetting (RV) to NPCC vetting standards.

9.3.5.2. Non - Police LEA

Staff within an Approved Organisation that is a non-police LEA authorised to access ANPR data must have current vetting clearance to national non-police personnel vetting (NPPV) Level 2.

9.3.5.3. Partner Agencies

Controllers may allow access to non-police staff in partner agency (e.g. local authority controllers) subject to have them having current vetting clearance to NPPV Level 2, to the extent necessary for their role.

9.3.5.4. Police Service Administration, Monitoring and Audit

Police LEA staff conducting activity in respect of administration, monitoring and audit of the NAS will have a current security clearance to SC level and NPPV to Management Vetting standard.

9.3.5.5. Non-Police LEA Administration, Monitoring and Audit

Non-police LEA staff conducting activity in respect of administration; monitoring and audit of the NAS will have a current security clearance to SC level and NPPV Level 3.

9.3.5.6. National Audit

Staff appointed to any National Audit role must have a minimum current security clearance to Developed Vetting (DV) level and NPPV Level 3.

9.3.5.7. National Administration and Processor Companies

Staff within NAS supplier companies or the Home Office that have access to the NAS for management or administrative purposes will have a current security clearance to SC level and NPPV Level 3.

9.3.6. Authorisation Requirements for access to NAS Data

Where an authorisation for access is required, staff providing that authorisation must ensure that access is proportionate in each case taking account of the DPA and associated principles and that access is in the interest of justice.

9.3.6.1. Authorisation of Staff Access

Each LEA will designate a senior manager who is accountable for the authorisation of staff who may access ANPR data.

9.3.6.2. Role Based Access and Training

Personnel will only be granted access to ANPR data to an extent that is necessary and proportionate to their role. LEAs must ensure that authorised staffs have

completed any required training and are fully aware of the provisions within NASPLE. Authorised staff will have individual access accounts and permissions.

9.3.6.3. Records of Authorised Staff

LEAs will maintain a list of authorised staff and ensure that a persons' authorisation is revised or cancelled as appropriate when they change role or leave the organisation.

9.4. Disclosure and Evidential Use of Data

Data held within or obtained from the NAS may not be used or disclosed for any purposes except those as authorised within NASPLE.

9.4.1. Disclosure schedules

Where ANPR data obtained is retained as material within the meaning of the CPIA (or similar procedures in Scotland), in preparation of disclosure schedules, information relating to ANPR methodology, tactics and camera locations will be recorded on the Schedule of Sensitive Material and may be disclosed to prosecution authorities.

9.4.2. Restrictions on personnel in disclosure of ANPR and in production of evidential materials

Statements of evidence in respect of data within the NAS may only be provided by staff authorised within LEAs to provide ANPR evidence with current access permissions within NAS for that purpose. Subject to the following authorised staff may provide a statement of evidence for any data held within the NAS.

9.4.3. Provisions to safeguard the location of ANPR infrastructure

The order to safeguard the national ANPR infrastructure, apart from data obtained from a Mobile ANPR system, the precise location for an ANPR read obtained from a camera will not be disclosed during an investigation, nor included in evidence unless the controller with responsibility for the camera that recorded the data has been consulted and provided written consent for that disclosure or for evidence to be provided. The following principles apply:

9.4.3.1. Evidential Use of Data

Evidence of an ANPR read will only be included where it is of specific relevance to an investigation and is of material value to any judicial proceedings.

9.4.3.2. Disclosing of Camera Locations in Evidence

Apart from data obtained from a Mobile ANPR system the production of a map or otherwise disclosing the precise location of the camera that recorded an ANPR read is not permitted during any stage of an investigative or prosecution process, unless

specifically authorised by the data controller for the LEA with responsibility for the camera that recorded that data.

9.4.3.3. Information to be included in evidential disclosure

The location of a read will be described in the following decreasing order of preference;

1. The general area of the location (e.g. Town, District, Metropolitan Borough)
2. The postcode (following consultation with the controller with responsibility for the camera that recorded the data, in circumstances where this will identify the precise location of the camera)
3. The name of the road (following consultation with the controller with responsibility for the camera that recorded the data, in circumstances where this will identify the precise location of the camera)
4. The precise location (following consultation with the controller with responsibility for the camera that recorded the data)

9.4.3.4. Disclosure of ANPR data for non-evidential purposes

Unless permitted within section 9.6 of this document, core ANPR read data and any supporting imagery as defined by section 7.4.5., is not to be transferred to other systems, nor disclosed to any third party, including staff from an organisation that is not listed at Annex A, Data may only be disclosed to the data subject in accordance with procedures for dealing with FOI and DPA enquiries in accordance with section 9.12. Data may be shared with an organisation that is not listed at Annex A with the express written authority of the controller with responsibility for the camera that recorded that data.

9.4.3.5. Disclosure to non-Approved Organisations

Where an LEA has an active role in collaboration with another LEA which is not listed at Annex A in the conduct of an investigation, and circumstances consistent with the provisions of Schedule 2 DPA apply, the results of a search of ANPR data may be disclosed to that other LEA with a requirement that it is not further disclosed without the express written authority of the controller for the 'Approved Organisation' collaborating in the investigation.

9.4.3.6. Controller Representations re Disclosure of Camera Locations

In addition to the above, the controller that owns or controls the camera that captures 'read' data will be provided with a specific opportunity to make representation to any court that is to consider an order for information to be disclosed regarding the location of a camera.

9.4.3.7. Recording of Disclosure

In all circumstances where data is disclosed a record must be maintained to include the identity of those disclosing and receiving the data and the reason for and any authorisation of that disclosure.

9.5. Retention and Deletion

9.5.1. Record Retention and Deletion

ANPR READ records must be deleted 12 months[4] after their initial capture, unless retained under provisions of CPIA or similar provisions in Scotland. Retained data may only be accessed in connection with the investigation subject to that retention after a period of 12 months following initial capture.

Records may also be retained for longer than 12 months following a review that identifies a continuing policing purpose for those items of data under provisions of MOPI. These records must be retained and managed in accordance with those provisions. LEAs must establish procedures for the management and review of any data held under these provisions including arrangements for deletion as required.

9.6. Storage of ANPR Data otherwise than in NAS

Data must not be stored outside the NAS except where held in buffer storage in accordance with section 8.9.5 unless for the purpose of retention in accordance with section 9.5.1 or in accordance with section 9.8 below where those requirements cannot be met within the NAS, or it has been extracted as a result of a court order or other lawful authority for the provision of the data.

9.7. Record Amendment

Records that are identified as incorrect for any reason must either be corrected or deleted at the time that they are found to be incorrect.

9.8. Record Deletion from Third Party Systems

ANPR data must be deleted from any computer-based system within 7 days of entry of that data, where an LEA has established any link between the NAS and any other computer-based system for the purposes of:

- Monitoring and the initiation of an operational response to any hit against a list of vehicles of interest or

[4] Read metadata is deleted on day 366 after initial capture. Associated images are deleted the following day. Data may only be accessed up to 12 months after initial capture (Annex C) unless in circumstances of 9.5.1 above.

- More advanced research and analysis purposes in relation to an investigation.
- Entries are included in command and control records

An exception exists for deletion after 7 days when a review has been conducted of the data that it is proposed to be retained which has identified the items of data where a continued policing purpose remains that can only be satisfied by the continued processing of the data within the system external to the NAS.

In this case provisions of MOPI (or similar provisions in Scotland) apply and the relevant items of data may be retained and managed in accordance with those provisions; or

An exception also exists for deletion after 7 days when a review has been conducted into the data that it is proposed to be retained which has confirmed that the items of data are relevant to an investigation. In this case the relevant items of data may be retained, managed and deleted in accordance with the requirements of CPIA.

9.9. Transfer to local systems for basic user access

Data may not be transferred to any local systems external to those required for connection to NAS facilitate basic user access to ANPR data.

9.10. Records of Data Processing, Access and Disclosure

9.10.1. NAS Logging

A log of all automated processing operations will be maintained within NAS to include records of access by administrators and authorised users, data capture, alterations and any search of data or records within NAS. Logs of administrator or user access must include details of the identity of the user together with the justification, date and time of that access and a record of any authorisation relevant to that access.

9.10.2. Mobile Systems Logging

A log recording the details of all lists of VOI that have been loaded onto mobile systems as authorised by section 8.9.8 will be maintained by the LEA that loaded the log onto the mobile systems.

9.10.3. Logging of Access on systems external to NAS

In addition, LEAs are required to maintain a record of any access by their staff to ANPR data, in any external system, to include records of access by administrators and authorised users, data capture, alterations and any search of data or records within NAS. Logs of administrator or user access must include details of the identity of the user together with the justification, date and time of that access and a record of any authorisation relevant to that access in a readily retrievable form.

9.10.4. Logging of Escalation of Investigation Category

LEAs are required to maintain a record of any escalation of an investigation to the category 'Major Investigation' or 'Serious Investigation', including details of the reason for escalation, in a readily retrievable form.

9.10.5. Logging of data Disclosures

Unless disclosure is in accordance with the provisions of the CPIA or similar provisions in Scotland, LEAs will maintain records of all disclosure of ANPR data including the justification, data and time of the disclosure, the identity of the person disclosing the data and the identity of the recipient of the data.

9.10.6. Use of Logs in Disciplinary Proceedings

Logs within NAS and those recorded by an LEA may be used for the purposes of self-monitoring by the controller or the processor, the conduct of internal disciplinary proceedings, in ensuring the integrity and security of personal data and for the purposes of criminal proceedings.

9.10.7. Disclosure of Logs to ICO, SCC and Home Office

Records within NAS and any local records must be made available to the Information Commissioner, the Surveillance Camera Commissioner and the Home Office on request for audit and monitoring purposes.

9.11. Management and Audit of NAS

Audit must be conducted in accordance with National Standards for Compliance and Audit of Law Enforcement ANPR by staff with appropriate security clearance.

LEAs will support all controllers for NAS in the audit and management of NAS.

LEAs will support the national auditor in the monitoring and audit of access to the NAS and will provide relevant information on request.

LEAs will audit the access to NAS by their staff in accordance with Audit Standards and maintain a record of all audits that are undertaken. Details of such audits will be made available to the Information Commissioner, the Surveillance Camera Commissioner and the national auditors on request.

9.12. Freedom of Information Act and Data Protection Act Enquiries

All requests for Information regarding the NAS made to a public authority under the provisions of the Freedom of Information Act 2000 (FOI) will be referred to the relevant controller for consideration and will be managed according to the JCA.

All requests in relation to data held on NAS, made under provision of the DPA, will be referred to the controller for consideration and will be managed according to the

JCA. This includes any subject access requests and requests for erasure or restriction on processing.

Annex A: Approved Organisations

List of Approved Organisations
Avon and Somerset Constabulary
Bedfordshire Police
Border Force
British Transport Police
Cambridgeshire Constabulary
Cheshire Constabulary
City of London Police
Civil Nuclear Constabulary
Cleveland Police
Cumbria Constabulary
Department for Work and Pensions (DWP)
Derbyshire Constabulary
Devon and Cornwall Constabulary
Dorset Police
Driver and Vehicle Licensing Agency (DVLA)
Driver and Vehicle Standards Agency (DVSA)
Durham Constabulary
Dyfed-Powys Police
Environment Agency
Essex Police
Food Standards Agency
Gangmasters and Labour Abuse Authority
Gloucestershire Constabulary
Greater Manchester Police
Gwent Police
Hampshire Constabulary
Hertfordshire Constabulary
H M Revenue & Customs (HMRC)
Humberside Police
Immigration Enforcement
Intelligence Services
Kent Police

Lancashire Constabulary
Leicestershire Constabulary
Lincolnshire Police
Medicines and Healthcare Products Regulatory Agency (MHRA)
Merseyside Police
Metropolitan Police Service
Ministry of Defence Police
National Crime Agency (NCA)
NAFN Data and Intelligence Services facilitating Local Authority Trading Standards investigations
National Vehicle Crime Intelligence Service (NaVCIS)
Norfolk Constabulary
North Wales Police
North Yorkshire Police
Northamptonshire Police
Northumbria Police
Nottinghamshire Police
Police Service of Scotland
Police Service of Northern Ireland (PSNI)
Royal Air Force Police
Royal Military Police
Royal Navy Police
South Wales Police
South Yorkshire Police
Staffordshire Police
Suffolk Constabulary
Surrey Police
Sussex Police
Thames Valley Police
Thurrock National Investigation Service
Warwickshire Police
West Mercia Constabulary
West Midlands Police
West Yorkshire Police
Wiltshire Police

Annex B: Investigation Categories

Investigations within LEAs fall within three main categories, so that there is a consistency of understanding within LEAs as to which investigations should be included within each category. The main categories are:

- Major Investigations
- Serious Investigations
- Priority and Volume Investigations

A consideration of the category of the investigation informs effective management and decision making, including the scope for an investigation and determination of the resources that are to be deployed. These categories provide the framework to support a national policy for retention of, and access to ANPR data. The categorisation of an investigation should be determined taking account of the circumstances in each case, using the below framework as a guide.

Major Investigations

A key characteristic is that Major Investigations should be normally be led by a Nationally Registered Senior Investigating Officer (SIO) within a police force or similarly senior investigator in non-police LEAs.

Designated Major Investigations

Major Investigation Types
Murder
Attempted Murder
Manslaughter
Infanticide
Child Destruction
Kidnapping

Terrorist related crimes

Serious Investigations

Designated Serious Investigations

Serious Investigation Types
Arson
Abduction
Aggravated Burglary dwelling and non-dwelling
Arson High Value or life endangered
Blackmail
Drug Trafficking
Death by Dangerous Driving
Female Genital Mutilation
Fraud and Associated Offences (80hrs + investigation time)
Gross Indecency Child
Perverting Justice
Public order (racially motivated)
Rape
Robbery (Firearms or ABH or more serious injury caused)
Sexual Assault (children under 13)
Threats to Kill
Vulnerable Missing Person

Wounding (S18/20)
Response to incidents of significant public interest / public safety/ public security

Serious Investigation Escalation

Serious Investigations may, with the authority of a senior manager[5] be escalated to the category of Major Investigations.

Investigations that have been escalated to serious from the category of Priority and Volume Investigations may not be further escalated to the category of major Investigation.

Any authority to escalate to the higher category together with the reasons for the grant of that authority must be recorded. Any authority to escalate will take account of the following factors:

Serious Investigation Escalation Factors

Consideration	Examples
Community factors	• Likely to escalate into large scale disorder or critical incident • Has escalated from a previous offence • Sensitivity regarding individuals involved
Offence characteristics	• Aggravating factors of the offence • Vulnerability of victims/witnesses, • Has crossed force or national boundaries • Forms a previously undetected series

[5] an officer of at least superintendent rank in the police or the equivalent level of seniority in a non-police organisation

Offender Characteristics	• Organised crime • Terrorism links • Resistance to police operational strategies • Multiple offenders

Priority and Volume Investigations

Investigations not included within the above categories will be considered as within the remit of Priority and Volume Investigations. This will include investigations into street robbery, burglary and vehicle-related criminality and non-crime issues such as anti-social behaviour, vehicle excise enforcement, road traffic offences, safeguarding and missing persons.

Priority and Volume Investigations may with the authority of manager[6], be escalated to the category of Serious Investigations.

Any authority to escalate to the higher category together with the reasons for the grant of that authority must be recorded and will take account of the following factors:

Priority and Volume Investigations Escalation Factors

Consideration	Examples
Community	• **High risk of critical incident** • **Sensitivity regarding individuals involved**

[6] an officer of at least Inspector rank in the police or the equivalent level of seniority in a non-police organisation

Offence Characteristics	• Aggravating factors of the offence such as: • Hate crime • Weapons used • Injuries sustained • Vulnerability of victims/witnesses, • Priority issue identified within NIM business process. • Series of offences e.g. forensic links to the offender(s) • Complexity of the Investigation
Offender Characteristics	• Criminal history • Resistance to investigative strategies • Prolific offender • Multiple offenders

Annex C: Data Access Requirements

Age of data to be accessed (as required)	Purpose of access to data
	To monitor alarms or receive reports from matches against a list of Vehicles of Interest (VOI) from a NRD for operational response or intelligence purposes.
Real or near real time during the course of monitoring	By any member of staff authorised to access ANPR systems with no additional authority required.
	To research data for 'Priority and Volume Investigation' purposes.
Up to 90 days	By any member of staff in accordance with their authorisation to access ANPR systems.
Over 90 days	By any member of staff in accordance with their authorisation to access ANPR systems with written authority of an Inspector or equivalent staff grade; a) where there has been a significant delay in reporting the offence to be investigated, or; b) new information or evidence has become available, or; c) the investigation is being conducted diligently and expeditiously and is not yet completed.
	To research data for 'Serious Investigation' purposes.
Up to 1 year	By any member of staff in accordance with their authorisation to access ANPR systems.

	To research data for 'National Security', 'Counter Terrorism' or other 'Major Investigation' purposes.
Up to 1 year	By any member of staff in accordance with their authorisation to access ANPR systems.
	To prepare evidential material for information revealed during a previous search of ANPR data.
	By any member of staff in accordance with their authorisation to access ANPR systems with no additional authority required.
	To comply with a written request from the Crown Prosecution Service, the procurator fiscal or on the direction of a court.
	By any member of staff in accordance with their authorisation to access ANPR systems with no additional authority required.
	To research data as part of an investigation into alleged breach of the policing Code of Ethics
	By any member of staff in accordance with their authorisation to access ANPR systems with written authority of a superintendent or equivalent staff grade.

Appendix A: Password Requirements

Password Requirements

Introduction

Purpose

1. The security of NAS requires that users generate an appropriately complex password to protect the National ANPR Capability (NAC) and its data from unauthorised access. The NAS utilises a username and password-based identity and access control for all front-end users.
2. The NAS Password Policy is a procedural part of the information security measures intended to:
    - Protect the Confidentiality, Integrity and Availability of the NAC.
    - Preserve the privacy of all the data and information stored within the NAC environment, ensuring only authorised users are permitted access on a need to know basis.

Procedures

The Purpose of Passwords

3. Passwords are an essential security control to authenticate users and confirm identity and access rights. Passwords protect access to the ANPR data and information in conjunction with the physical and procedural measures of a secure site.
4. Visual recognition of people within a work area, and Photographic ID Cards for sites and buildings, are also an important security layer to protect the NAC.

Limitations

5. The security provided by a password system requires the passwords are known only to the user of the account to which it relates. Thus, a password is vulnerable to compromise whenever it is stored or written down. A user must not disclose their password to anyone including other users and administrators.

Password Requirements

Password creation requirements:

6. Passwords **must** be a minimum length of 8 characters with at least 2 non-alphanumeric characters (e.g. % & ?);
7. Passwords **must not** be stored in any insecure form, users must **disable** password saving in web browsers;
8. Passwords **must not** be based on the following:
   - Months of the year, days of the week or any aspect of dates with which they are personally associated (e.g. birthdays, anniversaries);
   - Family names, initials or car registration numbers;
   - Organisation names, identifiers or references;
9. Good quality passwords should:
   - Not be the same as any of the previous 10 passwords (this will be enforced via the operating system or security solution within NAC);
   - Be unique and only used within the NAC;
10. Password must be changed on suspicion of compromise;
11. Password creation requirements are common for all types of NAC access. If a user has more than one account. For example, a user administrator and system administrator account, different passwords are required for each account;

Expiry terms and Account Lockout

	No of Attempts	*Password expiry*
User/ Role	5	1yr

12. If a user has attempted to log in **5 times** unsuccessfully their account will be:

    a. **Locked out** and **ONLY** unlocked via two alternative processes for use depending upon the business processes of the LEA:
       i. Notify the local User Administrator or,
       ii. Notify the local LEA IT Service Desk.

Forgotten Password Process

13. If a user has forgotten password, A **"I forgot my password"** link is provided on the NAS logon homepage. The system will email a new temporary password to the email address associated with the NAS user account. This temporary password **must** be immediately changed upon first successful login. This will not circumvent the lockout procedure described above.



© Crown copyright 2020

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at www.gov.uk/government/publications and www.npcc.police.uk/anpr

Any enquiries regarding this publication should be sent to us at anpr@homeoffice.gov.uk .

GOV.UK

1. Home (https://www.gov.uk/)
2. Crime, justice and law (https://www.gov.uk/crime-justice-and-law)
3. National ANPR standards (https://www.gov.uk/government/publications/national-anpr-standards)

- Home Office (https://www.gov.uk/government/organisations/home-office)

Guidance

National standards for compliance and audit of law enforcement ANPR - September 2020 (accessible version)

Updated 19 November 2020

Contents

1. Purpose of Compliance and Audit
2. Applicability
3. Audit Governance and Roles
4. Data Standards Audit
5. Infrastructure Standards Audit
6. LEA Local System Audit
7. Vehicle of Interest (VOI) lists Audit
8. Data Access and Management Standards Audit
9. Glossary of Terms, Abbreviations and Definitions
10. Document revisions

Print this page



© Crown copyright 2020

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 (https://www.nationalarchives.gov.uk/doc/open-government-licence/version/3) or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at https://www.gov.uk/government/publications/national-anpr-standards/national-standards-for-compliance-and-audit-of-law-enforcement-anpr-july-2019

1. Purpose of Compliance and Audit

Consistent management of NAS is essential to ensure that data is accurate and to maximise the benefits for law enforcement purposes. Public confidence in the system is essential and robust standards with clear records of compliance with those standards is importance to ensure support for ANPR systems is maintained.

Audit is one part of a larger suite of security controls and measures which includes, governance, physical, personnel, technical and procedural controls. The NAS is designed to provide a security regime that supports and compliments the business and technical needs. It is important that business audit standards, policy and governance are also in place which requires a robust compliance audit regime to be in place.

2. Applicability

These Audit Standards apply to national law enforcement ANPR capability (NAC) operated by the police and other law enforcement agencies (hereinafter called LEA), throughout the UK, that connect to or receive data from the National ANPR Service (NAS).

Audit is conducted with reference to National Standards for Policing and Law Enforcement (NASPLE)

LEAs must ensure compliance by their agency with the requirements of all parts of NASPLE.

3. Audit Governance and Roles

The National Strategic lead as lead controller must ensure that audit standards are in place to provide for effective governance of NAS taking account of threats and risks.

Staff conducting audits must have current security clearance to levels as detailed in NASPLE Part 3.

Staff with user access permissions to NAS may not conduct audits.

LEA must ensure that audit of any access to NAS using administrative permissions is conducted by staff who do not themselves have administrative responsibility for NAS.

3.1 Governance model

The below governance model is in place for NAS:

The National ANPR Strategy Board supports the NPCC Strategic Lead.

The National ANPR Advisory Board advises the NPCC Strategic Lead.

The NAS Service Management reports to the NPCC Strategic Lead.

The National Accreditor reports to the NPCC Strategic Lead.

The National Auditor reports to the NPCC Strategic Lead.

The National Accreditor advises the Security and Data Management within Strategic Board.

5372

The National Auditor advises the Security and Data Management within Strategic Board.

The Security and Data Management within Strategic Board advises the NAS Service Management.

The National Auditor audits the activity of National System Providers and the National Administrator.

The National Auditor monitors the activity of local auditors.

The Service Desk oversees the National System Providers.

The National Administrator supports and advises the Local Administrators.

Local Auditors audit users.

4. Data Standards Audit

Accurate data is essential to ensure legislative compliance and to enable the benefits that can be obtained from ANPR to be optimised. The following elements of NASPLE Part 1 are included for audit.

4.1 Data Security

Every 6 months LEA to review a sample of reports that have been obtained by that LEA from NAS for compliance with the requirements of the Government Security.

Classification Policy (GSCP) requirements for OFFICIAL – SENSITIVE data. (NAS configuration should ensure that all reports are appropriately marked).

4.2 Time

LEAs must record evidence of the accuracy of time recording for all camera that submit data to their management server. Records confirmation of time accuracy must be reviewed at Least once every 7 days. A record of review and any maintenance conducted as a result of the review must be retained for a period of 2 years following the review.

4.3 Location

The accuracy of the recording of location for a read record from all camera with the exception of mobile camera must be confirmed on installation and thereafter reviewed at Least once every 6 months by the LEA manging that camera. A record of all reviews and any maintenance conducted as a result of the review must be retained for a period of 2 years following the review.

4.4 Reporting of Data Standards

Every 12 months LEA must provide the national auditor with a report to include details of the number of cameras operated by the LEA, the number tested during the preceding 12 months, information of the accuracy for recording time and location for each camera tested and details of any maintenance conducted following testing.

5. Infrastructure Standards Audit

5.1 ANPR Infrastructure Development

Compliance with NASPLE Part 2 is important to ensure that ANPR systems are developed and maintained in conformance with relevant legislation and that the benefits that can be obtained from the NAS are optimised. The following elements of NASPLE Part 2 are included for audit.

5.2 Static ANPR Systems

Evidence that the need for deployment is consistent with NASPLE Section 8.6 and performance consistent with NASPLE Section 8.7 on installation and that this has been monitored for each camera and that an annual review for deployment of each camera has been conducted. Evidence of performance evaluation as required by NASPLE Section 8.14 LEAs to retain records of all reviews for a period of 2 years.

5.3 Moveable ANPR Systems

Evidence that the need for deployment is consistent with NASPLE Section 8.6 and performance consistent with NASPLE Section 8.7 on installation and that this has been monitored for each camera. Evidence of performance evaluation as required by NASPLE Section 8.14. LEAs to retain records of all reviews for a period of 2 years.

5.4 Multi Lane ANPR Systems

Evidence that the need for deployment is consistent with NASPLE Section 8.6 and performance consistent with NASPLE Section 8.7 on installation and that this has been monitored for each camera and that an annual review for deployment of each camera has been conducted. Evidence of performance evaluation as required by NASPLE Section 8.14. LEAs to retain records of all reviews for a period of 2 years.

5.5 CCTV Integrated ANPR Systems

Evidence that the need for deployment is consistent with NASPLE Section 8.6 and performance consistent with NASPLE Section 8.7 on installation and that this has been monitored for each camera and that an annual review for deployment of each camera has been conducted. Evidence of performance evaluation as required by NASPLE Section 8.14. LEAs to retain records of all reviews for a period of 2 years.

5.6 Mobile ANPR Systems

Evidence that the need for deployment is consistent with NASPLE Section 8.6 and performance consistent with NASPLE Section 8.7. Evidence of performance evaluation as required by NASPLE Section 8.14. LEAs to retain records of all reviews for a period of 2 years.

5.7 Covert Systems

Audit of deployments of ANPR systems authorised within provisions of the Regulation of Investigatory Powers Act 2000 (RIPA) or the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) to be completed in accordance with arrangements for compliance and review of RIPA and RIPSA deployments as appropriate.

6. LEA Local System Audit

6.1 Local Systems

Audit of local data storage to be completed by the LEA every 6 months to confirm that the period of retention is consistent with NASPLE Part 2 and that data is not transferred or used in other systems except as authorised by NASPLE.

6.2 Mobile Systems Data Transfer

Review of records for transfer of data from Mobile ANPR Systems to be completed by the LEA every 7 days to confirm compliance with NASPLE Part 2. LEAs to retain records of all reviews for a period of 2 years.

6.3 Support and Maintenance

Records for failure of any component of infrastructure to be reviewed by the LEA every 7 days to support compliance with requirements for reinstatement of capability as detailed in NASPLE section 8.14.

7. Vehicle of Interest (VOI) lists Audit

Compliance with the requirement for deletion of lists from NAS 28 days after the latest date of revision to be reviewed by the LEA every 14 days.

Lists held on Mobile ANPR Systems to be reviewed by the LEA at Least once every 7 days to ensure that they remain the current version of any VOI list.

LEA to maintain a record for the review of all VOI lists and retain those records for a period of 2 years.

8. Data Access and Management Standards Audit

8.1 Policy

Annually, the local auditor to confirm that a current written policy is in place in accordance with NASPLE Part 3.

8.2 Audit of provisions for Data Access

The identity of the senior manager as required by NASPLE Section 9.3.6.1 to be confirmed by the local auditor annually

Evidence of the management of staff authorisations and permissions to be audited by the LEA for compliance with authorisation and removal procedures to include:

- annually 5% of all new staff authorisations that have been approved during the previous 12 months
- annually review a sample of staff authorisations where the privileges have changed during the previous 12 months
- all staff who have not accessed NAS for a period of 90 days within the 14 days immediately following the expiry of that period
- all accounts for staff that have left the LEA within 48 hours of them leaving an LEA to ensure that access permissions have been ceased

- annually all staff with administrative access to ensure that this remains appropriate and is not combined with user access permissions
- monthly to review records for all failed ‘log on’ attempts. A record of all reviews conducted to be retained for a period of 2 years

LEA audit to be conducted every 6 months to confirm the deletion of data in accordance with NASPLE with an annual review of 5% of all cases where data is retained beyond standard deletion times to ensure continued retention remains appropriate, both for NAS and other systems.

LEA to audit of instances of data access to ensure access is appropriate within terms of NASPLE with reference to the justification and authority where required as follows:

- LEAs must establish provisions for audit of ANPR data where the period for the search includes data that entered the NAS 90 days or less prior to the search, that is proportionate in each case taking account of their assessment of the potential risk of non-compliance with NASPLE and for the misuse of data. The audit to be completed quarterly[footnote 1]
- to audit 5% of searches across a sample covering 30 consecutive days since the previous audit where those searches cover data that was captured more than 90 days prior to the date of search. The audit to be completed quarterly
- all instances of access to data preserved under provisions of the Criminal Procedure and Investigations Act 1996 (CPIA)

As a minimum, the following elements of data access must be reviewed as part of the audit:

- that any search was properly authorised where required with evidence of authorisation recorded
- that the timescales for the search were appropriate in that they were no greater than was necessary and proportionate in the circumstances of the investigation
- that the reason, purpose and justification for the search was fully recorded within NAS

In respect of access to data preserved under provisions of the CPIA that any access was solely for the investigation for which it was preserved.

LEAs to audit 10% of records of the disclosure of data otherwise than in accordance with CPIA or similar procedures in Scotland in respect of the justification, the date and time of the disclosure and the identification of both the person disclosing and the recipient of the data. (NASPLE section 9.4.3.7)

LEAs are responsible for dealing with any non-compliance with standards that are identified during audit and must report all non-compliance and a copy of the audit report to the national auditor within 28 days of the non-compliance being identified.

All LEAs must maintain a record of audits that are conducted to include:

- a statement of the findings for all audit activity
- a report of the extent of non-compliance
- a report of action taken in relation to non-compliance

Records of audit will be retained for a period of 2 years and made available to the national auditor on request.

8.3 Audit of Changes to Read Records

LEAs to review a sample of changes to ‘read’ records every 6 months to confirm the validity of the change. Records of review to be retained for a period of 2 years.

8.4 Audit of Access by System Providers, National Administrators and Local Auditors

The National Auditor will audit access to NAS by system providers, national administrators and local auditors, reporting details of any audit that is conducted for the information of controllers to the extent determined by those post holders.

The National Auditor will conduct a NAS system audit every 6 months to confirm data is deleted in line with the requirements of NASPLE Part 2.

Audit of access to NAS by a user with ‘Super Administrator’ permissions will be conducted for each occasion that the system is accessed when those permissions are enabled for that user by the National Auditor.

9. Glossary of Terms, Abbreviations and Definitions

ANPR	Automatic Number Plate Recognition
ANPR system	A collection of cameras, readers components linking to NAS
CCTV	Closed Circuit Television
CAMERA	The device used to capture and ANPR read. CPIA Criminal Procedure and Investigations Act 1996
DPA	Data Protection Act 2018
GSC	Government Security Classifications – (formerly the Government Protective Marking Scheme (GPMS))
GPS	Global Positioning System
JPEG	Joint Photographic Expert Group image format
NAS	National ANPR Service
NAC	National Law Enforcement ANPR Capability
NPCC	National Police Chiefs’ Council

5377

NASPLE	National ANPR Standards for Policing and Law Enforcement
LEA	Law Enforcement Agency – Includes police forces and other agencies undertaking law enforcement activities
Read	The interpretation of a VRM by an ANPR system
Schengen	The Schengen Information System will enable the authorities of signatory countries to have access to reports on persons and objects for the purpose of border checks and controls and other police and customs checks
VRM	Vehicle Registration Mark

10. Document revisions

Version 2.0, September 2020: Update of links within text, Minor revision of section 7

---

1. In most cases a sample of 2% of all instances where the period included in the search extends for 90 days or less prior to the date of the search being conducted for a sample of 30 consecutive days in a period since the previous audit (quarterly) is likely to be appropriate. Depending upon the level of risk a lessor or greater sample may be appropriate. The rationale for determining the data sample should be documented in all cases

Print this page

Home Office

National ANPR Service

National ANPR Service
Technical Specifications

Version 3.0
June 2020

Definitions

Acronym	Description
ANPR	Automatic Number Plate Recognition
ANPR system	A collection of cameras, readers components linking to NAS
CCTV	Closed Circuit Television
CAMERA	The device used to capture an ANPR read
CAPTURE RECORD	The record of a vehicle recorded by NAS for a vehicle passing an ANPR camera including the ANPR READ, associated images and meta data.
COMMUNICATIONS LINKS	The connections between the camera, any local infrastructure and the NAS
CONTROLLER	The competent authority which alone or jointly with others determines the means and purposes of the processing of personal data. Part 3 data Protection Act 2018
CPIA	Criminal Procedure and Investigations Act 1996 and the CPIA Code of Practice
DPA	Data Protection Act 2018
FOI	Freedom of Information Act 2000
GDPR	General Data Protection Regulations
GSC	Government Security Classifications – (formerly the Government Protective Marking Scheme (GPMS)
GPS	Global Positioning System
HIT	The report of a match of a vehicle registration mark (VRM) READ with a VRM that is included on a vehicle of interest list (VOI)
ISO	Information Security Officer – The member of staff with responsibility for ensuring compliance with requirements for IT security
ITHC	IT Health Check – The process for ensuring that security provisions for IT are appropriate and in compliance with requirements that are current at the time of the check.
JCA	Joint Controller Agreement under provisions of the Data Protection Act 2018-
JPEG	Joint Photographic Expert Group image format

LEA	Law Enforcement Agency – Includes police forces and other agencies undertaking law enforcement activities. For the purpose of this document, LEAs shall only include those organisations listed at Annex A.
MIDAS	Motor Insurance Bureau (MIB) data of uninsured vehicles
MOPI	Code of Practice for the Management of Police Information
NAC	National ANPR Capability includes: • the NAS which is a single national system consisting of the functionality to enable use for operational response, investigation and intelligence purposes and a single national store of data, and, • the National ANPR Infrastructure (NAI) which is a network of ANPR cameras, communications links, firewalls and other related supporting components, that are the responsibility of LEA, that connect to the NAS.
NAI	A network of ANPR cameras, communications links, firewalls and other related supporting components
NAS	National ANPR Service
NASP	National ANPR Standards for Policing first version published in 2013 and replaced by NASPLE recognising the applicability to all law enforcement agencies that access the NAS
NASPLE	National ANPR Standards for Policing and Law Enforcement.
National VOI List	Nationally circulated lists that include stolen vehicles, vehicles requiring an operational response and vehicles within Schengen circulations
NAPS	National Accreditor for Police Systems – Responsible for confirming that police IT systems are in accordance with security requirements and authorising connection to national systems.
Network Connections	The IT links between components of the NAC
NPCC	National Police Chiefs' Council
NPCC Vetting Policy	The NPCC standards for vetting of staff for access to police information

PERSONAL DATA	Means any information relating to an identified or identifiable living individual. 'identifiable living individual' means a living individual who can be identified directly or indirectly, in particular by reference to_ a) an identifier such as name, an identification number, location data or an online identifier, or b) One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual Data Protection Act 2018
PNC	Police National Computer
READ	The interpretation of a VRM by an ANPR system
RIPA	Regulation of Investigatory Powers Act 2000
RIPSA	Regulation of Investigatory Powers (Scotland) Act 2000
Schengen	The Schengen Information System will enable the authorities of signatory countries to have access to reports on persons and objects for the purpose of border checks and controls and other police and customs checks
SMS	A Standards format for text messaging
VOI	The details of a vehicle that are of interest to law enforcement for operational response or investigation purposes that is included on a list to enable it to be READ and for authorised staff to receive a report of that READ.
VRM	Vehicle Registration Mark

1 Introduction

This document prescribes the technical specifications for data within the National ANPR Service (NAS). National ANPR Standards for Policing and Law Enforcement (NASPLE) set out the standards that are required for the National ANPR Capability (NAC) to ensure compliance with relevant legislation in the operation and use of law enforcement ANPR. The information within this document is intended to support compliance and consistency in the operation and management of NAS by the police and other law enforcement organisations (hereafter referred to as LEA).

2 ANPR Read Records

2.1 System Testing

The only number that may be entered into any component of the NAS for the purpose of testing connectivity is QQ111QQQ.

2.2 Core Data Components

2.2.1 Vehicle Registration Mark (VRM) (Mandatory)

Where a camera has the capability to record images of vehicles passing within the field of view where no VRM is identified by the system, 'QQQQQQQ'1 must be recorded within the VRM field.

The required format must conform to the Standard Coding Format UTF-8character set. The VRM must contain no spaces.

2.2.2 Time (Mandatory)

Recorded and synchronised using standard time source techniques to Greenwich Mean Time (GMT) plus 0 (+0) at least once every 10 minutes, with accuracy to stratum level 3.

The required format is 'dd/mm/yyyy hh:mm:ss', in 24 hour format.

2.2.3 Location (Mandatory)

ANPR data must place a read in a location, accurate to within 10 metres. This location should have been ascertained through a Global Positioning System (GPS) device. In addition, all fixed-site ANPR cameras must have their GPS co-ordinates accurately recorded to within 5 metres.

[1] Some ANPR cameras can detect the presence of a vehicle where no VRM is visible and the use of 'QQQQQQQ' ensures that these vehicles are traceable in the database with a format that will not be attributed to a genuine VRM.

The required format for recording a location is latitude and longitude in decimal degrees.

When a mobile ANPR system is unable to deliver an accurate GPS coordinate for a read, the GPS field must be populated with N0000000 E00000000.

2.2.4 Supporting imagery

Plate patch – showing the number plate only, (Mandatory for systems under ownership or control of an LEA).

A plate patch must be in JPEG format, 120x60 pixels and be no more than 3kB in size.

Overview – showing the vehicle in the context of the read zone (Optional).

An overview image must be in JPEG format, no more than 25kB in size.

Where images obtained by a camera exceed 3Kb for a plate patch or 25KB for an overview, these must be adjusted prior to forwarding to the NAS.

'Geo Tagging', if an accurate GPS Geo Location is available, then this detail may be added to images using Exif (Exchangeable image file format) (Optional

Other metadata

Column	Format	Mandatory	Details
Feed ID	Numeric	Yes	2 character code as used by the Police National Computer (PNC) Also known as 'Force ID'
Source ID	Numeric	Yes	Short integer (range 1 to 9999)
NRD ID	Numeric	Yes	Short integer (range 0 to 9999) (NRD ID zero (0) must be used to denote VRMs entered manually by an administrator of the ANPR system.)
Lane ID	Alphanumeric	No	Optional text description
'Alias' ID	Alphanumeric	No	Optional textual description that does not disclose the exact location of a NRD
Username	String	Yes	Username of operator using the ANPR system. When deployed in other circumstances, use 'Unattended'.
Preset ID	Integer	No	Short integer Default value is 0 Used to indicate direction of travel on multi-lane CCTV cameras.

3 Data storage and management

3.1 Data loss and resilience

The NAS must not allow any data loss and be configured to provide to provide resilient capability.

3.2 Local system retention and deletion

Local components of NAC must be configured to enable retention of any data received from a camera at more than 7 days for a maximum of 48 hours and for deletion of that data within the following 24 hours.

3.3 Mobile Data Transfer

Local capability must be in place to support transfer of data from mobile ANPR units to the NAS within 48 hours of capture by the camera within the mobile system.

4 National Databases

The NAS must have the technical capability to run the following national databases, as a minimum - PNC; Includes 'Fast Track' 'Extract', 'Schengen' and 'MMC' data.

PNC Extract File

The PNC Extract File is available to forces at least three times every 24 hours and should be loaded onto the mobile systems opportunity following receipt. All ANPR reads must match against the PNC Extract File should the live link to the PNC be unavailable.

5 Vehicle of Interest (VOI) Lists

VOI lists in NAS will be referenced to the LEA that creates and manages the list. In order to support the display of symbols within vehicle mounted systems the file name will be in accordance with the reference list at Annex A.

The following character mapping is to be used. All lists of VOI must conform to the following template, **(Mandatory elements shown in bold text)**:

NB: Entries in 'Standard Words' section must match **exactly** those in the template for uploading into NAS

Column	Description	Standard Words	Comment
1	**VRM**		No spaces, Alphanumeric characters only
2	MAKE		
3	MODEL		
4	COLOUR		
5	**ACTION**	Stop Assess No Alert	Action can include a requirement to STOP the vehicle and take action as described Or To assess in the context at the time the vehicle comes to notice to determine action. Or No Alert only to be used when a VOI list is submitted for monitoring purposes with no intention that any action is taken when the vehicle comes to notice
6	**WARNING MARKERS**	No Warning Known Warnings Present	Generally, PNC ACTion should be used if warning markers are present. For VOI lists, 'No Warning Known' is most applicable. If it is essential to use a VOI list and warning markers are present then 'Warnings Present' should be used with the agreed PNC abbreviation (max of 3) entered as the first words separated only by a space in the Information /Action field. (field 9)

Column	Description	Standard Words	Comment
7	**REASON**	Intel Serious Crime Cloned Low Crime Drugs Intel Sexual Intel Low Crime Offender management Impaired Driving Documents Disqualified Other No Insurance DO NOT USE No MOT – Do NOT USE No Tax – Do NOT USE No Keeper – Do NOT USE LEA P1 LEA P2 LEA P3 LEA P4 LEA P5 LEA P6	Only one reason code per entry No Insurance, No MOT, No Tax and No Keeper MUST NOT be used as a REASON to create a VOI list entry. If intelligence relates to one of these categories, then DOCUMENTS must be used. They are included in the template solely for the use of nationally populated lists to support NAS functionality.
8	INTEL 3X5X2		Enter grading without X or spaces
9	**INFORMATION/ ACTION**	Free Text – Maximum of 198 characters including spaces and punctuation. Carriage return must not be used	Brief free text sufficient to add extra value and detail for the person dealing with activation.
10	**LEA AND AREA**		Include Force Name/ Area (BCU/Division letter/ other LEA ref
11	**START DATE**	Provide date in format [dd/mm/yyyy]	
12	**WEED DATE**	Provide date in format [dd/mm/yyyy];	Entries will be weeded on date specified
13	PNC ID		
14	**GSC marking**	OFFICIAL (or) OFFICIAL-SENSITIVE	Only one marker to be used
15	CAD		
16	**CONTACT**	Provide details of 24hour point of contact for enquiries if vehicle stopped	

6 Real Time Matching

The NAS must provide real-time matching to PNC and other lists of VOI for all ANPR reads.

The system response time from a Vehicle Registration Mark (VRM) being captured by a camera to the hit notification response being delivered to a specific operator must not exceed 4 seconds for static, moveable, dual lane and CCTV Integrated systems, and 6 seconds for mobile ANPR systems.

To allow for this end-to-end performance requirement, the camera must deliver ANPR reads to the NAS within 2 seconds of capture for static, moveable, dual lane and CCTV ANPR Integrated systems and within 4 seconds of capture for mobile ANPR systems.

The NAS must process that read against the PNC and other VOI databases and deliver any resultant match notification to the operator within 2 seconds of receipt of the read by the NAS for all systems.

7 Real Time Delivery of Data

Local LEA ANPR infrastructure must clearly display the current state of connectivity to the NAS and/or any time when data is not being sent to the NAS. In the event of a communications or systems failure, the LEA infrastructure must buffer that read data and deliver it to the NAS once the communications or failed systems have been restored. The real-time delivery of data is a priority and the delivery of any buffered data should take place in addition to delivery of real-time data.

8 Search and Export of Data

The NAS must provide for the identification and export of data to enable identification using any of the following criteria:

- Vehicle Registration Mark (VRM);
- Date and time parameters;
- by camera identification;
- by location co-ordinates;
- by ‘geo plotting’
- direction of travel (desirable)

9 Interoperability

Systems must enable interoperability between LEAs and the NAS to allow:

- Real-time matching of reads against lists of VOI and the real-time delivery of hits
- Remote research in accordance with prevailing researching guidelines
- NAS read searching for national data searches and data mining in accordance with the NAS Business Rules, as defined within current NASPLE
- Distribution of lists of vehicles of interest to the NAS
- Transfer of data and all associated images between LEA ANPR Infrastructure and the NAS.

Annex A

Vehicle of Interest List (VOI) Naming Convention

In order to display the name of the organisation creating the VOI list within symbols in vehicle mounted systems, character mapping is required. A VOI list file name will begin with the organisations PNC ID followed by an underscore (for example 07_Cheshire VOI List); the agreed force abbreviation will be displayed in the bottom 'white' section of the VOI symbol (in this example CHESH would be displayed). The following character mapping is to be used:

Character at start of VOI File name followed by underscore	***Display in bottom white section of VOI symbol***
52	**A&S**
40	**BEDS**
93	**BTP**
35	**CAMBS**
07	**CHESH**
48	**COLP**
59	**CNC**
17	**CLEV**
03	**CMBRIA**
30	**DERBYS**
50	**D&C**
55	**DORSET**
94	**DVLA**
201	**DVSA**
11	**DURHAM**
63	**DPP**
42	**ESSEX**
53	**GLOS**
06	**GMP**
61	**GWENT**
44	**HANTS**
41	**HERTS**
88	**LEA**
16	**HUMB**
46	**KENT**
04	**LANCS**
33	**LEICS**
32	**LINCS**
05	**MERPOL**
02	**METPOL**
24	**MOD**
36	**NFOLK**
60	**NWP**
12	**NYP**
34	**NHANTS**
10	**NORPOL**
31	**NOTTS**
90	**PSOS**

98	**PSNI**
62	**SWP**
14	**SYP**
21	**STAFFS**
37	**SFFOLK**
45	**SURREY**
47	**SUSSEX**
43	**TVP**
23	**WARWCK**
22	**WMERCA**
20	**WMIDS**
13	**WYP**
54	**WILTS**
LEA	**LEA**
TUTELAGE	**TULAGE**
MIDASGOLD	**MIBGLD**
TRIVIUM	**TRVIUM**

© Crown copyright 2020

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at anpr@homeoffice.gov.uk



PIPS TECHNOLOGY™
DETECTION INNOVATION



PAGIS Administrator's Manual

Version 2.14

Updated 4/10/2020

NEOLOGY MOBILITY TECHNOLOGIES

Table of Contents

Table of Contents 2

NOTICES 4

Technical Support 4

Design Changes 4

Trademarks 4

Copyright 4

Version 4

INTRODUCTION 5

1.1 Dual Lens Color and Infrared Camera 5

1.1.1 Available Products 5

1.2 Using This Manual 6

SCREEN REFERENCE 7

2.1 The PAGIS Software Login Screen 7

2.1.1 Logging on with the Default Administrative Account 7

2.2 Main Screen - Live View 8

2.2.1 Getting Started in PAGIS 8

2.3 The PAGIS Navigation Buttons 9

2.3.1 Camera Control Buttons 9

2.3.2 GPS Indicators 10

2.3.3 Camera Firmware Update (Restricted Users) 10

2.3.4 Day/Night Mode 10

2.4 Begin Shift 11

2.4.1 Sync via USB Thumb drive (or Local Source) 11

2.4.2 Sync via Wireless Network 11

2.4.3 PAGIS Auto-Sync Settings 11

2.4.4 Begin Shift – Additional Information 11

2.5 End Shift 11

2.5.1 Sync to BOSS 11

2.6 Cam Mode Button 12

2.6.1 Camera Modes 12

2.7 Taking a Picture 12

2.8 Search Entry Screen 13

2.8.1 Searching Synchronized Hotlists for License Plates 13

2.8.2 Searching Locally Stored Reads and Hits 13

2.8.2.1 Searching for a Match 14

2.8.3 Wild Card Symbols 14

2.8.4 Manually Adding a Plate to PAGIS 15

2.8.4.1 ADD VLP Query 15

2.8.4.2 ADD VRM Report Screen 15

2.9 The Review Screen 16

2.9.1 Summary Review Section 16

2.9.2 Review Navigation Buttons 16

2.9.3 Reads 17

2.9.3.1 Reads Result Screen Navigation Buttons 17

2.9.3.2 Interactive Buttons – Reads Screen 17

2.9.4 Hits 18

2.9.4.1 Hit Screen Attributes 18

2.9.4.2 Hit Screen Function Buttons 19

2.9.4.3 Interactive Buttons – Hits Screen 19

2.9.4.4 Set Disposition – Additional Detail 19

2.9.4.5 Add Intel – Additional Detail 20

2.9.5 Misreads 20

2.9.5.1 Marking a Record as a Misread: 21

2.9.6 Audits 22

2.9.7 Targets 22

2.9.7.1 The Targets Screen 23

2.9.7.2 Targets Screen Navigation Buttons 23

2.9.8 Databases 24

2.9.8.1 Databases Screen Functions 24

2.9.8.2 Databases Screen Navigation Buttons 24

2.9.8.3 Databases Edit- “Manual Reports” 25

ADMIN SETTINGS 26

3.1 Sync Options Screen 26

3.1.1 Synchronization Types 26

3.1.1.1 Synchronization to Disk (Local Storage) 27

3.1.1.2 Synchronization with BOSS 27

3.1.1.3 Sync to “Instation” (Formerly BOF2 and BOF3) 28

3.1.2 Global Sync Options 29

3.2 PAGIS Privacy Settings (Local Data Retention) 30

3.3 Language 31

3.4 Location 31

3.5 Users 32

3.5.1 User Privileges ____ 32
3.6 Sound ____ 33
3.6.1 Configuration Buttons ____ 33
3.7 System ____ 34
3.8 Rules ____ 35
3.8.1 Rules – Additional Clarifications ____ 35
3.9 OCR ____ 36
3.10 External ____ 37
3.10.1 XML Datastream Ports ____ 37
3.11 Cameras ____ 38
3.11.1 Checking the Connection ____ 38
3.11.2 Troubleshooting Camera Connections ____ 38
3.11.3 Configuring the Cameras in PAGIS ____ 39
3.12 Cam Setup ____ 40
3.12.1 Cam Setup Navigation Buttons ____ 40
3.13 Configs (Camera View Modes) ____ 41
3.13.1 Configs Navigation Buttons ____ 41
3.13.2 Reviewing and Modifying Existing Modes ____ 42
3.13.3 Adding a New Camera Mode ____ 43
3.14 Info ____ 44
3.15 Camera Firmware Update, (Admin) ____ 44
PAGIS INSTALLATION GUIDE ____ 45
4.1 PAGIS System Requirements ____ 45
4.2 PAGIS Prerequisites ____ 45
4.2.2 PAGIS Software Installation (MDC) ____ 46
4.2.3 PAGIS Software Installation (Mobile Processor) ____ 47
TROUBLESHOOTING TIPS ____ 48
5.1 Troubleshooting & Tips ____ 48
5.1.1 PAGIS with NetMotion VPN ____ 48
5.1.2 Cisco VPN Client: ____ 48
5.1.3 Microsoft .NET 3.5 Installation ____ 48
5.1.4 Firewall Settings for Client-Server Installations ____ 48
PAGIS/BOSS3 CONFIGURATION ____ 49
6.1 Creating a New Device in BOSS3 ____ 49
6.2 Enabling a New Mobile System in BOSS3 ____ 49
6.3 Assigning Ownership to a Device in BOSS3 ____ 49
6.4 Assigning Hotlists to a Device in BOSS3 ____ 50
PAGIS/BOSS4 CONFIGURATION ____ 50
7.1 Creating a New Device in BOSS4 ____ 50
7.2 Enabling a New Mobile System in BOSS4 ____ 50
7.3 Assigning Ownership to a Device in BOSS4 ____ 51
7.4 Assigning Hotlists to a Device in BOSS4 ____ 51
APPENDIX A: THE GLOSSARY ____ 52
APPENDIX B: PAGIS SOFTWARE DATABASE FILE ____ 53
APPENDIX C: FAQ ____ 55
APPENDIX D: XML DATASTREAM ____ 60

NOTICES

The information within this manual is authorized for distribution to customers, authorized service center personnel, and distributors of Neology. Every effort has been made to supply correct information. However, Neology assumes neither responsibility for its use, nor for any infringements of patents or other rights of third parties, which may result from its use. No license is granted by the manufacturer under any patent or patent rights. Neology reserves the right to modify and update the equipment at any time without prior notice. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means to a third party without the prior consent of the copyright holder. The manufacturer's warranty will be invalidated if untrained personnel operate the equipment or if any attempt is made to service the equipment by unauthorized personnel.

This manual contains confidential and proprietary information and should not be redistributed except as needed for proper use and maintenance of the agency's Mobile ALPR system.

Technical Support

Service of this equipment by replacement of parts, on-site repair, routine maintenance inspection, and scheduled remote support session is available. Please contact PIPS Technology's ALPR Technical Support.
Phone: 833-PIPS-LPR (833-747-7577), Option 2
Support Team Email: Support@PIPSTechnology.com
For Customers in Europe, Middle East and Africa: Support@PIPSTechnology.co.uk
Web: www.pipstechnology.com
Fax: 858-391-0264
Corporate Office: 13520 Evening Creek Drive Suite 460. San Diego, CA 92128

Design Changes

Neology reserves the right to change the design of any product from time to time without notice and with no obligation to make corresponding changes in products previously manufactured.

Trademarks

PIPS Technology™ is a trademark of Neology Inc., and either registered or pending registrations in several jurisdictions. Windows, Windows 7, Windows 8, Window 10, and .NET are all trademarks of the Microsoft Corporation. Other trademarks and registered trademarks are the property of their respective owners.

Copyright

The Neology / PIPS Technology PAGIS Software is copyright of Neology. All rights reserved. This product contains confidential and trade secret information of Neology and is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portions of it, may result in civil and criminal penalties.

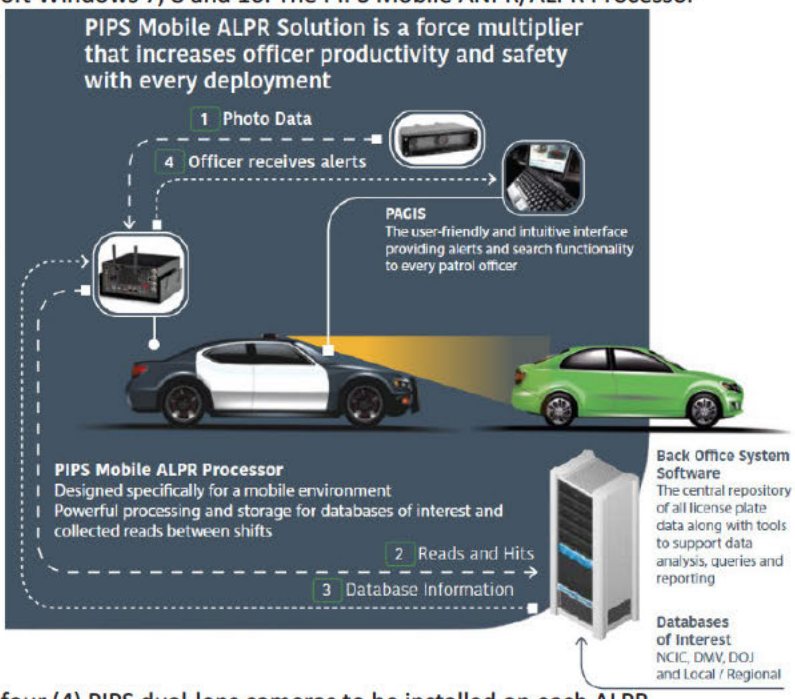
Version

This manual demonstrates the attributes of the Neology / PIPS Technology PAGIS Software Version 2.14 and was last updated in March 2020.

INTRODUCTION

PIPS Technology's Automated License Plate Recognition (ALPR) software solution called PAGIS utilizes dual-channel, dual-lens, cameras to "read" plates. Our software is optimized to run on the Mobile Processor itself or in conjunction with a mobile data computer (MDC). Our mobile software is compatible with Microsoft Windows 7, 8 and 10. The PIPS Mobile ANPR/ALPR Processor comes equipped with Microsoft Windows 7 Embedded.

The PAGIS Software processes the infrared plate image provided by any of the cameras and then interprets the plate number through Optical Character Recognition (OCR) via the mobile processor. The PAGIS application then searches for any matches of the plate with those listed in the databases, or "hotlists," distributed from the PIPS Back Office System Software (BOSS) or other external sources.



WARNING: To reduce the risks associated with impact, which if not avoided, could result in serious injury or death: Do Not interact with the ALPR system while driving in hazardous situations. The PIPS mobile camera series and License Plate Capture Software are not intended for use in hazardous environments, so that the User and/or others are not put at risk for personal injury and/or property damage.

1.1 Dual Lens Color and Infrared Camera

The PIPS Technology Mobile ALPR System allows for a maximum of four (4) PIPS dual-lens cameras to be installed on each ALPR vehicle provided that the vehicle supports the additional mounting equipment.

Each dual-lens mobile camera uses visible light to take color overview pictures of the vehicle and uses infrared (IR) illumination to capture the license plate's alphanumeric characters. IR illumination offers the best capture performance of reflective license plate characters for the following reasons:

- State issued license plates are designed to be highly reflective to IR light.
- Cameras using IR capture technology do not depend on the presence of visible light to function.
- Cameras using IR capture technology are not negatively impacted by the effects of headlights, solar glare, or total darkness.
- IR light penetrates rain and fog better than visible light.
- Due to these attributes, the system can be used 24 hours a day, seven days a week.

1.1.1 Available Products

Additional information about this and other PIPS Technology applications, cameras, and solutions are available on the PIPS web site: http://www.pipstechnology.com

1.2 Using This Manual

The section overview of this software manual is as follows:

Section 1: The Introduction and Basics

Section 2: PAGIS User's Section: Explains screen function and User Operations in the PAGIS Software

Section 3: Troubleshooting Tips

Section 4: Software Administrator's Guide: Explains how to install and configure the PAGIS Software

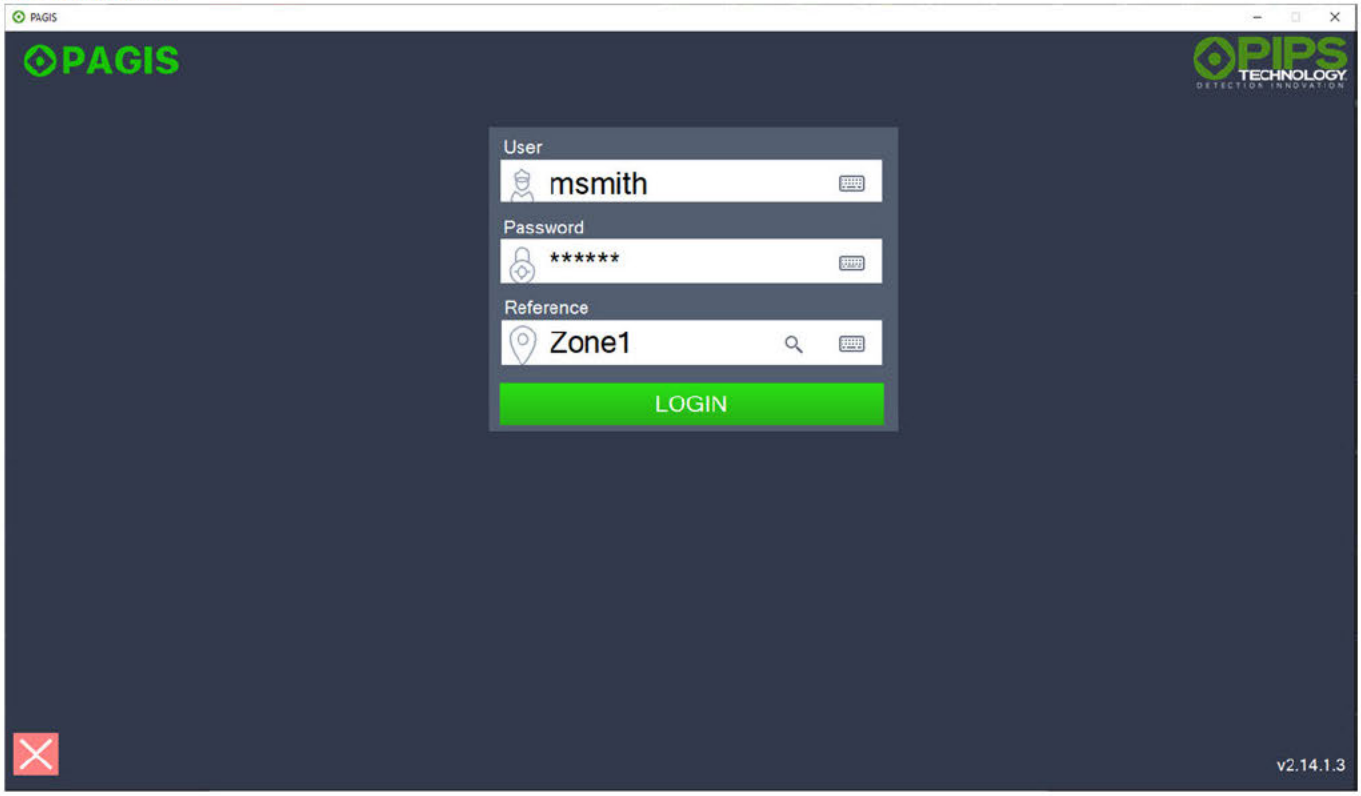
Section 5: Additional Information and Troubleshooting Tips

Section 6: Initial BOSS configuration for new PAGIS devices (MDCs)

Appendices: Additional features and details

SCREEN REFERENCE

This section guides the user through the PAGIS Software screens and the available options. Screens are grouped according to function. When a button is grayed out or missing, the option is not available, or no information has been accrued to activate it.



2.1 The PAGIS Software Login Screen

The PAGIS Software allows users with various access privileges to use the same MDC. For users with touch screen monitors, the Keypad button immediately to the right of any text box gives the user access to an on-screen keyboard for data entry.

User Field: The alphanumeric string assigned to identify the user. Usernames are not case sensitive.
Password Field: Password of the assigned user logging in. Passwords are case sensitive.
Reference Field: This is an optional field utilized to fit a number of use cases. A user can manually enter a reference at logon, leave the field blank, or select list of unique tags that will be associated with all data captured while logged in. If the Administrator has configured a default reference tags, that information will be displayed automatically. Otherwise, it will be blank.
Login Button: Submits the username and password to attempt a login.
Exit Button: By clicking the X icon in the lower left-hand corner, the user can exit/close the PAGIS Software.

2.1.1 Logging on with the Default Administrative Account

The PAGIS Software includes a default administrative account that can be used for the initial configuration. To do so, simply click the **Login** button with the User and Password fields blank.

NOTE: System Administrators are strongly encouraged to configure users for PAGIS just before, or soon after the installation and setup. PAGIS users accounts are created and maintained in BOSS. Once Users are established by the BOSS System Administrator, the default user account is automatically disabled. Best practices are to be certain at least one User account has administrative privileges.

2.2 Main Screen - Live View

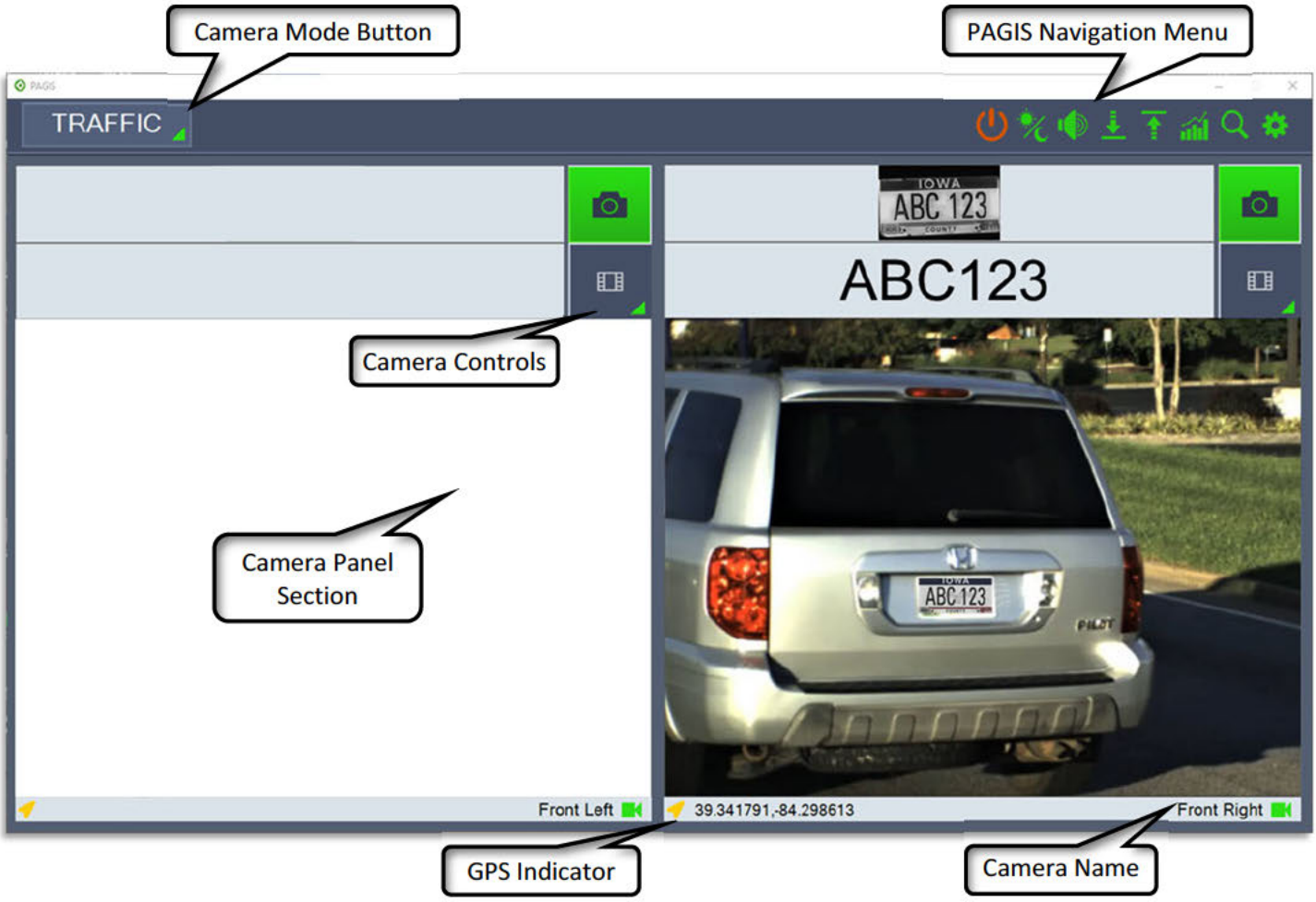
Upon a successful login, the user will see the Main screen (Live View). This is the default view and starting place of all PAGIS Software features. (NOTE: Access to features is based on user group rights established in BOSS.)

The Main Screen is also the place users will monitor read images and ALPR "hits". At the initial startup of the system it is normal to see only a blank/grey screen for a few seconds. Once a connection has been established with the mobile cameras, white boxes will be displayed showing the live-feed camera panels. At this point, the system is ready to capture reads/plates.

2.2.1 Getting Started in PAGIS

By default, PAGIS loads into a static view. This means live video will not automatically appear in the camera panels (white boxes) until a plate has be captured or the user selects one of the live feed options.

Once a plate is "seen" by a camera assigned to the current viewing mode (Traffic vs Parking), it will display the captured information in the corresponding camera panel. Each plate capture is also accompanied by a short "Beep" to audibly alert the user a read has taken place. (NOTE: If the user is in the Traffic Mode at the time a parking camera reads a plate, there will be a sound effect, but no plate image will be displayed on screen unless that plate is on a synchronized Hotlist or until the user switches to Parking Mode.)



2.3 The PAGIS Navigation Buttons

5400

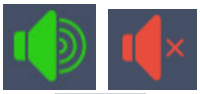
This section provides a quick reference guide to the available navigation buttons of the Live View screen.



The Camera Mode button is located in the upper left corner and is used to switch between the configured camera modes. Once configured, the name will change to a selected mode. The default values are “ALL”, “Traffic” and “Parking”.



The Logoff button is located in the upper right of the window. When selected, the user will be logged out of PAGIS and return to the login screen.



The Sound button is located to the right of the Logoff button. When selected, this button with toggle the PAGIS system sounds On and Off.



Day/Nite mode switches PAGIS between day & night mode screen skins.



The Begin Shift Synchronization button is located to the right of the Sound button. When selected, this will reach out to the BOSS server to download users, hotlists, and other system settings.



The End Shift Synchronization button is located to the right of the Begin Shift Button. When selected, this will upload any previously unsent reads, images, and audits to the BOSS server.



The Statistics/Review button is located to the right of the End Shift Button. When selected the user is able to review Databases/Hotlists, Reads, Targets, and other PAGIS information.



The Search button is located to the right of the Review Button. When selected the user can search his/her reads as well as manually add a license plate to a temporary hotlist.



The Admin/Settings button is located in the upper right corner of the screen. This button is only viewable to Admin level users and allows for system configuration changes and setup.



Firmware update icon will atomically appear when PAGIS detects a new firmware is available for the P720 mobile cameras. All user types are notified, but only Admins can apply the update.

2.3.1 Camera Control Buttons

The dual-lens cameras can capture both color and an infrared image. Formerly, there were a total of three buttons that allowed the user to view the IR and color feed as well as capture a picture directly from PAGIS. Now there is a toggle button to switch between color and IR views and a separate button to take a picture. These buttons are displayed on the main Live Screen as shown below:



The Camera View Selector button: This is the default state at login showing the Static View. (**NOTE**: PAGIS does not automatically display a life feed.)



Color View: by clicking on the Camera View Selector button once, the user will switch to the Color View Mode. This displays the current view of the color camera and will time out after 60 seconds.



IR View: by clicking on the Camera View Selector button twice, the user will switch to the Infrared (IR) View Mode. This displays the current view of the IR camera and will time out after 60 seconds.



The Take Pic button: Just above the Camera View Selector button is the “Take Pic” button. This button allows the user to quickly take a picture from the camera currently viewed.

2.3.2 GPS Indicators

GPS is stamped on each read and hit as capture events take place by the system. The signal strength and location indicators are located underneath the camera panels at the bottom of the Live Screen.

39.341788,-84.298518 Shows an example of the Location Indicator displaying the Lat/Long on the most recent read

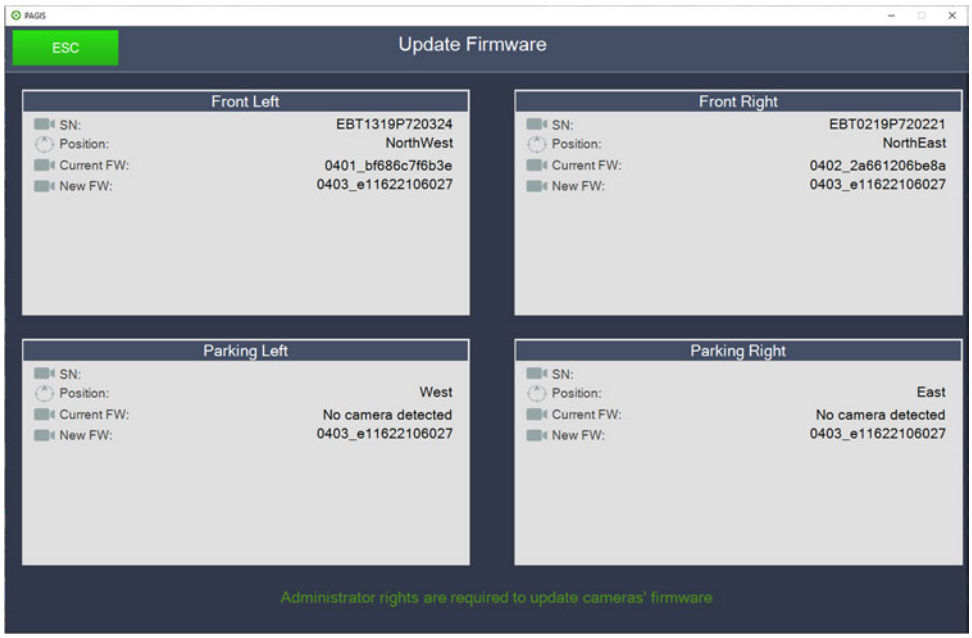
A green or yellow indicator shows a strong or medium strength GPS lock.

A red indicator shows there is no available GPS information.

2.3.3 Camera Firmware Update (Restricted Users)

Camera firmware update provides a means for PIPS to update the camera software to enhance and or correct camera performance. The frimware icon will only apper when update is avialable.

- The firmware update process only updates camera that are attached and function on the mobile processor.
- Restricted PAGIS users are only notified and displayed update information, only a PAGIS administrator can apply the FW update.

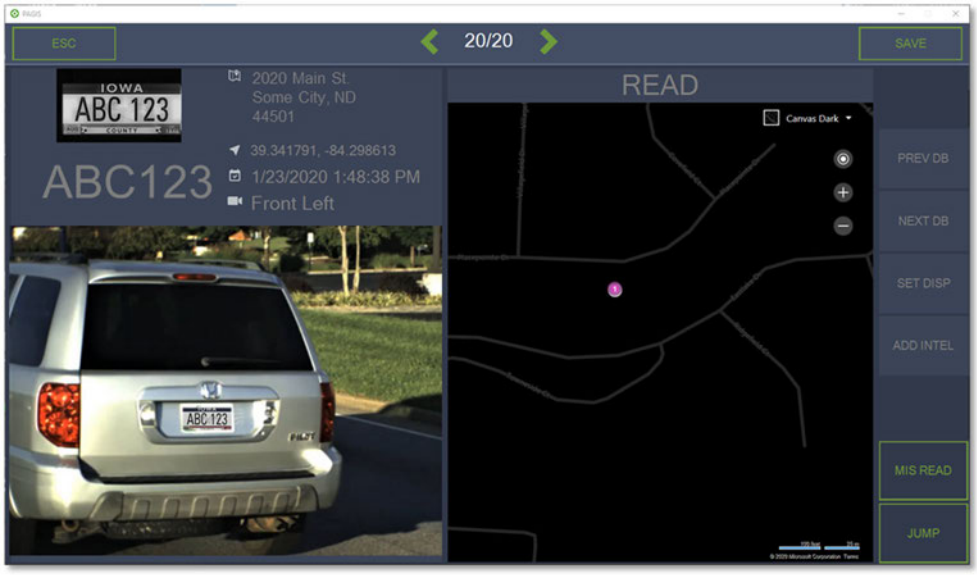


Firmware Updater Window List.

- Title “Camera Name”.
- Camera serial number.
- Position.
- Current FW version.
- New FW version available.

2.3.4 Day/Night Mode

Day/Night mode changes PAGIS user interface skins to a darker appearance to reduce illuminating the vehicle interior.



2.4 Begin Shift

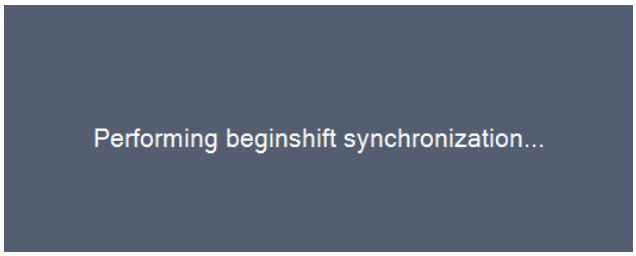
Begin Shift is thought of as the first step for all PAGIS users. From the Live View Screen, the PAGIS user must click the Begin Shift button twice. Once to select the function and once more to launch the Sync. With most agencies, this action utilizes a wireless network to import all the necessary data used during a shift (Hotlists, Dispositions, and Targets) directly from the BOSS Server. However, agencies can also configure their systems to perform this function via Thumb drive or a local source file.

2.4.1 Sync via USB Thumb drive (or Local Source)

Depending on the agency network, some alter the default PAGIS/BOSS configuration mode to use a USB Thumb drive or locally stored file on the MDC/Laptop instead of the wireless Sync. In order to synchronize effectively, the user must first confirm he/she has access to the source location before initiating Begin Shift. **NOTE**: All synchronizations using this method must be performed manually. To learn more about this process, refer to the "Client Tools" section of the BOSS Manual.

2.4.2 Sync via Wireless Network

Synchronizations over a wireless network provide the agency with additional automated features. Best practices recommend the user manually launch Begin Shift from the Live View Screen at the beginning of every patrol shift. However, it is possible for users to allow PAGIS to synchronize via its auto-sync settings. When a manual Begin Shift is launched, the Main View Screen removes the camera feeds and displays a status window of the Sync process. Once the Begin Shift operation is complete, PAGIS will return to the normal Main View Screen.





2.4.3 PAGIS Auto-Sync Settings

PAGIS auto-sync settings are best thought of as how PAGIS receives additional updates and maintains the downloaded ALPR data throughout the entire patrol shift. This prevents the need for the officer to manually perform Begin Shift functions multiple times a day. The auto-sync occurs every 30 seconds and receives data in small batches. The batches are not to exceed 1MB in size for every minute of download. In addition to receiving data, the auto-sync function also uploads a copy of data collected by PAGIS and sends it to BOSS for reporting/processing.

2.4.4 Begin Shift – Additional Information

By default, the synchronizations in PAGIS receive only what has been changed to the ALPR data since the last Sync. Meaning, if some plates have been removed from a Hotlist and others have been added, the system will only transfer that data instead of downloading the entire Hotlist each time the Begin Shift is launched. This helps to reduce the amount of data transferred over the agency's network. **NOTE**: Begin and End Shift synchronization, as well as all auto-sync features, are dependent upon stable communication to the BOSS server via an active data connection.

2.5 End Shift

End Shift in PAGIS is the process in which all the collected ALPR data (Reads, Hits, and Images) from the recent shift is uploaded to the BOSS server and cleared from the local cache. As with Begin Shift, the agency has two options. They can choose to Sync via USB Thumb drive or via wireless connection. Best practices recommend users perform an End Shift Sync at the end of every patrol.

2.5.1 Sync to BOSS

At the end of every shift, the accrued ALPR data should be exported to BOSS. Just like with Begin Shift, the user must click the button twice to launch it (once to select it and once more to execute the Sync). During the Sync, PAGIS uploads any Reads, Hits, and Images not already synchronized to BOSS and purges these items from the local cache on the MDC's hard drive. Completing an End Shift also removes any VLP entries manually added to PAGIS during the shift.

2.6 Cam Mode Button

Clicking the Cam Mode button in the upper left corner of the Live View Screen allows the user to cycle through the different camera modes configured by the PAGIS Administrator. Changing the camera mode changes which cameras are displayed on the Main Screen.

2.6.1 Camera Modes

By default, PAGIS provides "Parking" and "Traffic" as the two configuration modes. Users often switch these modes to suit their current use-case. For example, an officer in a parking lot will often switch the mode to "Parking" so s/he can see the parking cameras on the Live View Screen. They can then switch back to "Traffic" when monitoring city streets.

2.7 Taking a Picture

The PAGIS software has ability to quickly take a picture from one of the currently displayed ALPR cameras on the Live Screen. The user only needs to click on the Take Pic button.



To Take a Picture:

1. From the Live View Screen, press the Take Pic button from the desired camera
2. The image taken will be displayed
3. Enter a description of the picture in the text field at the bottom of the screen
4. Press Save to save the picture or Escape to cancel. Either action will return you to Live View.

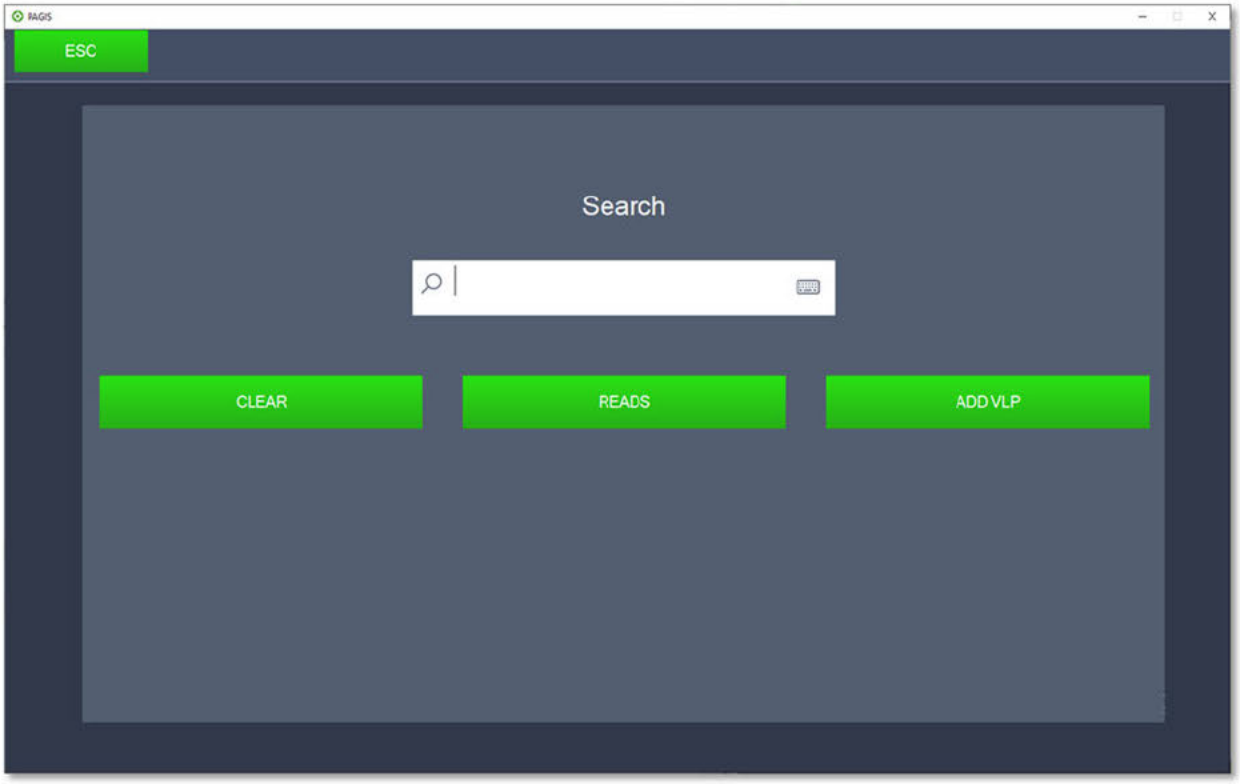
NOTE: The picture will Not be saved if a description/note is not entered in the text box.

To View the Saved Images:

1. Navigate to the Review menu in PAGIS
2. Select Audits
3. The user will be able to see a thumbnail of the image and the saved text/note
4. In order to review the saved images at a later time, the user will need to run the Audit Report from BOSS.

2.8 Search Entry Screen

Pressing the Search button icon from the Live View screen or SEARCH from the Databases window allows the user to search all manually entered plates as well as all BOSS synchronized databases (Hotlists) for license plate and target information. Users can also search all locally stored reads/images accrued since the last End Shift by clicking the Reads button instead of pressing the Enter key.



2.8.1 Searching Synchronized Hotlists for License Plates

By entering a vehicle license plate number (VLP) and pressing the Enter key or the ADD VLP button, the user can quickly search all the stored plate information locally collected as well as the information from all synchronized hotlists distributed from the BOSS server. **NOTE**: Hotlists can only be searched by entering complete VLPs. Wildcards and partial plate numbers will not return results.

Search Box: The text field used to enter the desired plate search via alphanumeric characters and/or wild card symbols.

Clear Button: Clears the contents of the search box.

Driver's License Info: The search field can also check the Hotlists for any DL information stored (Not available all countries).

Reads Button: This button searches for a match from all the reads/hits locally stored on the MDC/Laptop.

ADD VLP: Searches all locally stored hotlists for the plate and if there's no match, allows the user to add the plate to the "Manual Reports" alert list for use in the field. **NOTE**: All manual entries are cleared with each End Shift

ESC: The Escape button allows the user to exit to the Main/ Live View screen.

2.8.2 Searching Locally Stored Reads and Hits

As mentioned previously, this search function allows users to find reads and hits directly from their recent patrols using the search field and the Reads button. These searches pull only the reads and hits locally gathered/stored since the last time the user completed an End Shift. **NOTE**: The search results are specific to each Windows User Profile and do NOT pull images from the BOSS server.

2.8.2.1 Searching for a Match

5405

- From the Search field, users may enter a plate (or partial plate with wildcards) and then click the **READS** button.
- Results are displayed with the data gathered at the time the read was taken (See example below).
- Each result should display the infrared (IR) image of the plate as well as the color overlay of the vehicle for review.
- Each result shows the GPS data, Closest address point, Time and Date, and the Camera that read the plate.
- If there are multiple results, the user can cycle through them by clicking the left and right navigation arrows.



2.8.3 Wild Card Symbols

The use of wild card symbols in the Search box allows greater flexibility for the user, but may return a larger set of results.

- Wild card searches performed using the asterisk (*) designates an unknown number of characters.
- Wild card searches performed using the underscore (_) indicates a single missing or unknown character.
- Searches can be performed using one, both or no wild card symbols.

Example: The officer received an alert from Dispatch looking for a vehicle plate containing the letter J and the number 8 separated by one character. Because the officer doesn't know how many characters there are before or after the J and 8, he enters *J_8* in the search box to review all possible matches of J and 8 separated by only one digit.

2.8.4 Manually Adding a Plate to PAGIS

PAGIS allows users to manually add a plate of interest directly into the software as needed. Once saved, these entries are stored as part of the Manual Reports alert list and work just like any other Hotlist synchronized from the BOSS server.
NOTE: These additions are designed to be temporary and are cleared from the software with each End Shift.

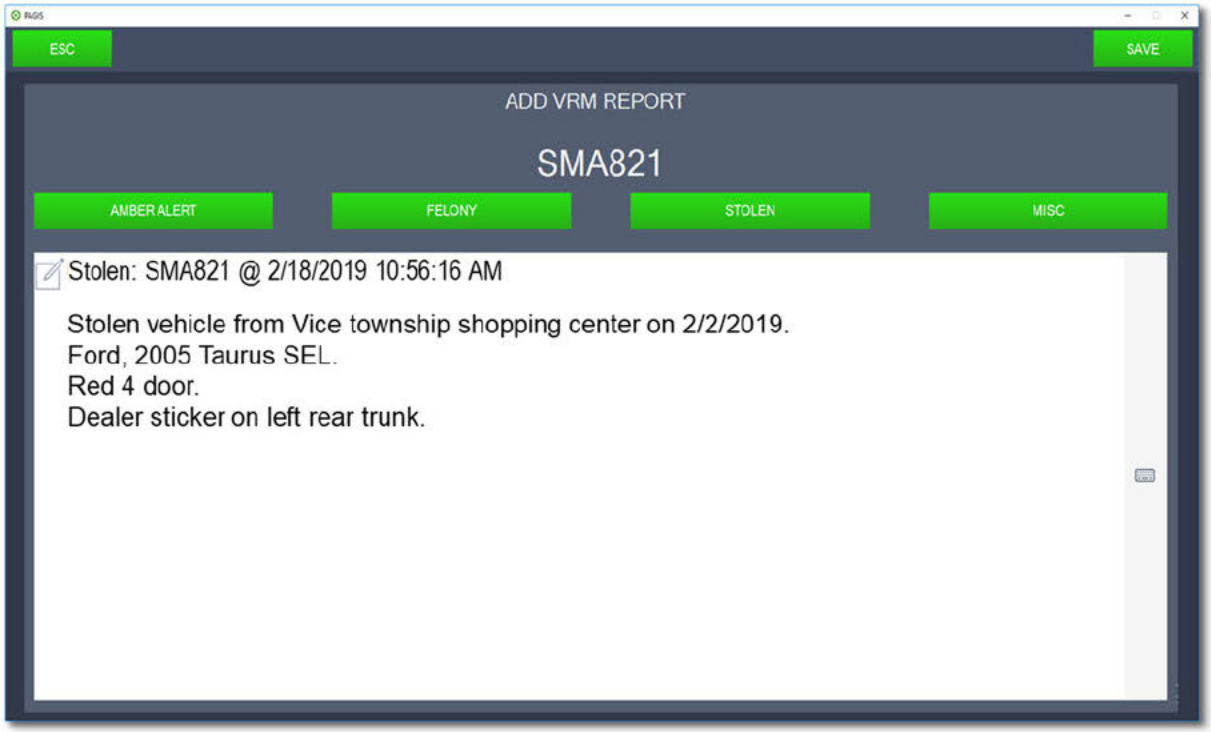
2.8.4.1 ADD VLP Query

Before an entry is added to the Manual Reports Hotlist in PAGIS, the software searches all stored databases for a match. If a match occurs, a message will display under the search box showing which Hotlist(s) it has been found in. If the VLP query does not return a match, the "ADD VRM REPORT" screen appears.



2.8.4.2 ADD VRM Report Screen

If the desired plate does not already reside in another Hotlist, the ADD VRM Report Screen becomes accessible to the user.



1. From the Search Entry Screen, enter the desired plate to add.
2. Click the ADD VLP button. If no match is found on any other hotlist, the "Add VRM Report" screen will appear.
3. Click to select the applicable alert type (AMBER ALERT , FELONY , STOLEN , or MISC)
4. Either leave the default information or add additional detail.
5. Click Save at the top right to add the plate to the Manual Entries Hotlist

2.9 The Review Screen

5407

PAGIS allows users to review all locally stored data from one easy location. Clicking the Review icon from the Main Screen launches Review. This screen is divided into the Summary View Chart and sub-section navigation buttons to the right.



2.9.1 Summary Review Section

The Summary View Chart is divided into five categories and allows a user to review the information collected during their shift at a glance.

Total Reads: Shows the total number of Reads/Hits synced to BOSS and the total number of reads captured during the shift.
Reads: Shows the total number of reads synced to BOSS and the total number of reads captured during the shift.
Hits: Shows the total number of hits synced to BOSS and the total number captured during the shift.
Misreads: Shows the total number of reads marked as a "misread" synced to BOSS and the total marked during the shift.
Audits: Shows the total number of audits synced to BOSS and the total number of audits during the shift.
Targets: Shows only the number of targets downloaded from BOSS.
(NOTE: The Sync value will always be zero for customers using Disk Sync mode/Client Tools.)

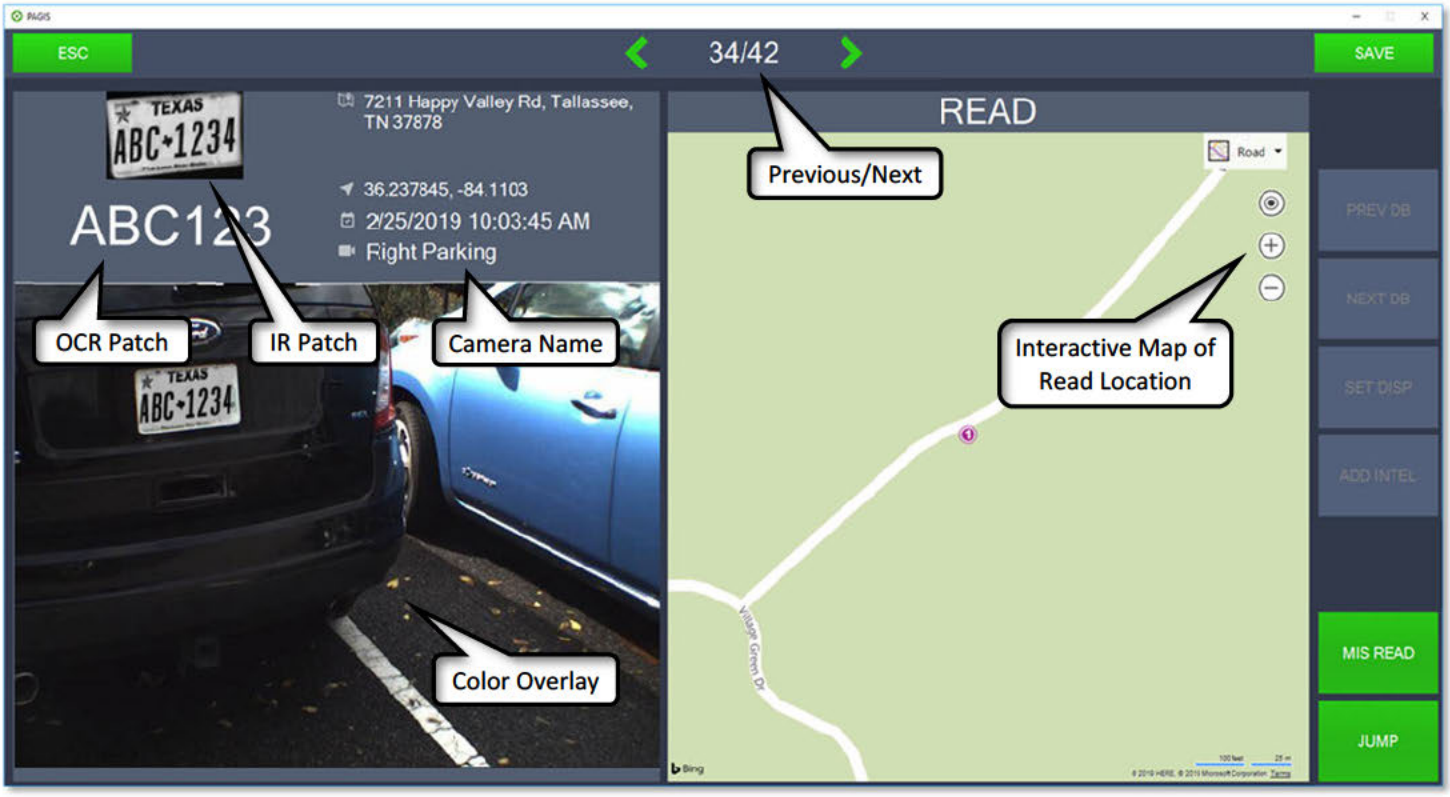
2.9.2 Review Navigation Buttons

The navigation buttons allow the user to review specific sets of information gathered during the shift.

Reads: Review all plate detections that have occurred since the last End Shift synchronization.
Hits: Review the hit alerts for Vehicle License Plate (VLP) reads that matched a Hotlist.
Misreads: Review reads and/or hits that have been manually flagged during the shift as misreads, where the plate number in the image does not match the OCR interpretation of the plate (e.g., a letter O misread as a Q or zero).
Audits: Review failed and successful logons, any manual data entered during the shift, pictures taken and all manual license plate searches.
Targets: Review targets that have been synchronized/downloaded from Boss.
Databases: Review all the Hotlists currently distributed to this PAGIS laptop/MDC.
Esc: Returns the user to the previous screen.

2.9.3 Reads

From the Main Screen, the user can review his or her accumulated Reads (those gathered since the last End Shift was completed) by clicking on the Review icon and then selecting the Reads Navigation button. The Read Review Screen is divided into two main sections. The left side displays the information gathered at the time of the read and the right side displays an interactive map of the GPS location.



NOTE: Buttons that are greyed out indicate options that are not available in the current view. For example, the Reads and Hits review screens share the same layout but different on-screen options.

2.9.3.1 Reads Result Screen Navigation Buttons



Read Count: The left number is the current record. The right number is the total available for review.

Next/Previous button: The arrows on either side of the read count allow the user to navigate back and forth to review reads/results.



MisRead button: When the button is green it indicates the record has NOT been edited as a Misread by a user. Once a Misread is saved, this button will turn grey and the record title will update.



Jump button: Allows the user to "jump" to a specific record without the need to navigate one record at a time using the Next/Previous buttons.



Save button: Apply any changes/edits and return to the Main Screen.



Escape button: Returns the user to the Main Screen.

2.9.3.2 Interactive Buttons – Reads Screen

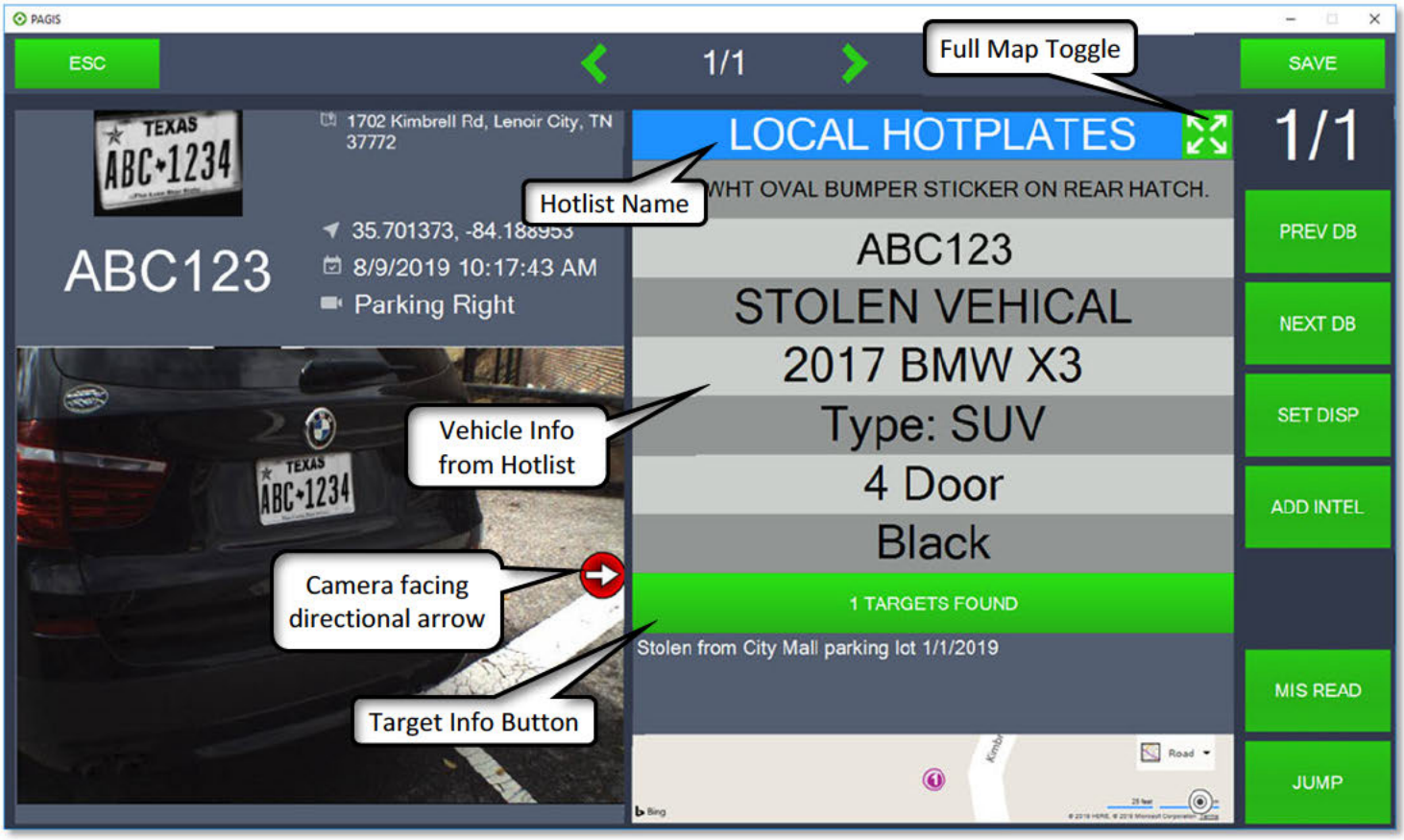
From the Reads Review, the user can interact with the following:

- IR Patch: The user can click on the IR "Patch" plate image to open a full-screen view.
- OCR Patch: The user can click on the OCR "Patch" image to edit the license plate number if necessary/Misread.
- Color OV Image: The user can click on the color image to open a full-screen view.
- Map: The user can manipulate the interactive map of the read location (Map Type, Scroll, and Zoom).

2.9.4 Hits

Users can manually access the Hits Section by first selecting the Review icon from the Live View Screen and then clicking the Hits Button. The Hits Screen is also divided into two main sections. The left side displays the information gathered from the ALPR equipment during the read. And the right side displays the information provided by the associated alert list.

NOTE: Each time a VLP matches a Database value (a license plate read by the system matches a Hotlist entry), PAGIS plays an audible tone and automatically displays the Hit Screen to alert the user.



2.9.4.1 Hit Screen Attributes

Hit Count and Navigation Buttons: Displays the total Hit count as well as the Next/Previous navigation buttons.

IR Patch Image: A thumbnail image of the license plate from the IR camera.

OCR Text: The character string the OCR engine generated from the current plate.

GPS Location: The GPS coordinates at the time of the hit. (If a GPS device is not attached, the Lat/Long is displayed as 0,0).

Date and Timestamp: The date and time when the read/hit was captured.

Overview Image: The overview image of the vehicle from the Color Camera. (**NOTE**: Color images require visible light)

Camera Name: The name of the camera that captured the read ("Right Parking" in the screenshot).

Hotlist Name: This is the name of the Hotlist or "Database" where the plate was matched.

Target Button: When available, this indicates a person of interest is associated with the Hit and opens the Targets Screen.

Vehicle Information: The area of grey bars will display the related vehicle information from the Hotlist. Any information added manually by the user will appear in the Text Box near the bottom of the screen.

Interactive Map: Shows the location the Hit took place. Users can access full-screen view by clicking the map or the toggle .

2.9.4.2 Hit Screen Function Buttons



The Hit Count Indicator: shows how many Hotlists the current Hit has registered against.



Previous DB button: This button moves the user to the previous Database/Hotlist that produced a Hit.



Next DB button: Pressing this button moves the user to the next Database/Hotlist that produced a Hit.



The Set Disposition button: prompts the user to report the disposition of the hit by selecting one of the approved codes assigned in BOSS by the Administrator.



The Add Intel button: allows the user to add additional information regarding the current Hit.



The Misread button: allows the user to flag the Hit as a misread.



The Jump button: Allows the user to "jump" to a specific Hit instead of navigating one at a time.

2.9.4.3 Interactive Buttons – Hits Screen

- IR Patch: The user can click on the IR "Patch" image to open a full-screen view.
- OCR Patch: The user can click on the OCR "Patch" image to edit the license plate number if necessary/Misread.
- Target Button: Shows associated person(s) of interest and opens the Targets Screen.
- Color OV Image: The user can click on the color image to open a full-screen view.
- Map: The user can manipulate the interactive map of the read location (Map Type, Scroll, and Zoom).

2.9.4.4 Set Disposition – Additional Detail

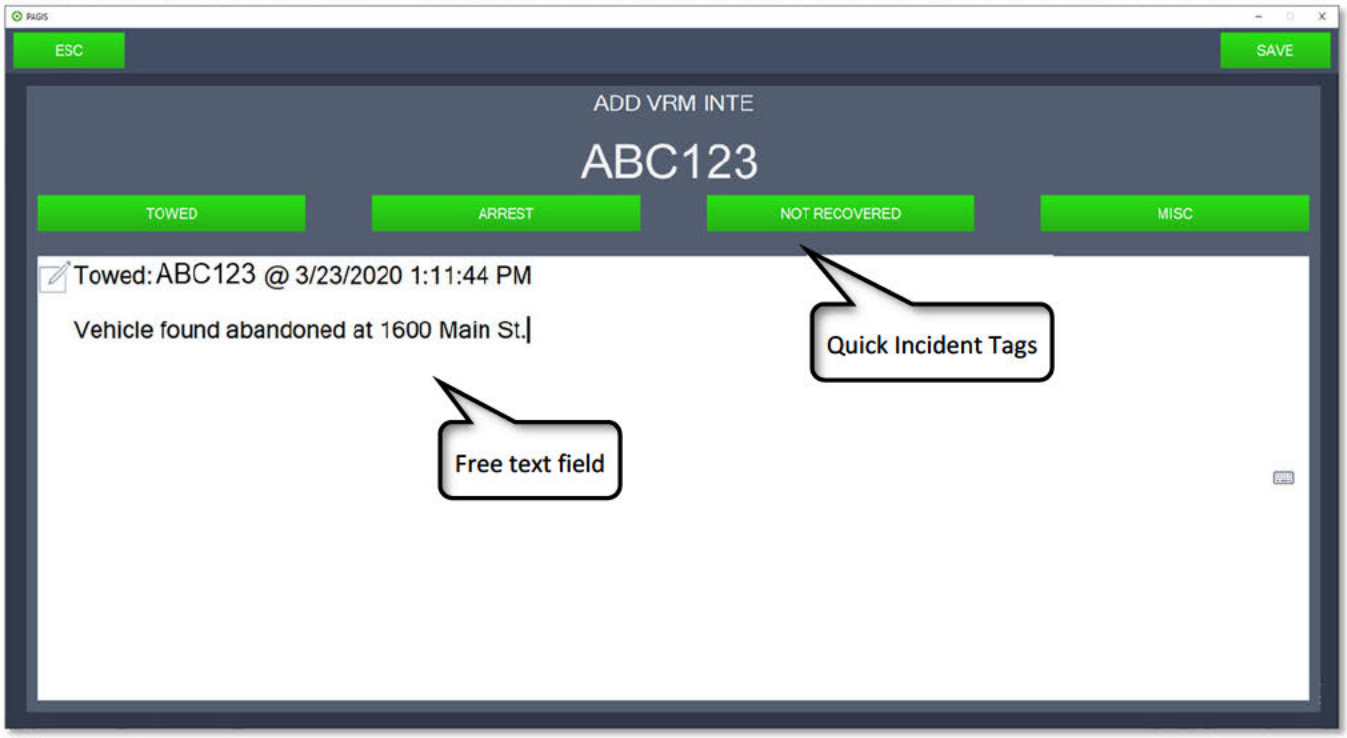


PAGIS allows for additional information to be added to a record in the form of a Disposition. Once Hits are flagged with a disposition code, the Agency is capable of running a "Reads Statistics by Disposition Report" in BOSS. Thus, providing valuable metrics and understanding to leadership in regard to their ALPR Enterprise.

When the "Set Disp" button is selected, the user is prompted to choose from a list of predefined values set by the Agency/BOSS Administrator. Once a disposition is selected and Saved, the disposition is reported to BOSS and will also show up in the Hits Review Screen text box in PAGIS on the next alert notification.

2.9.4.5 Add Intel – Additional Detail

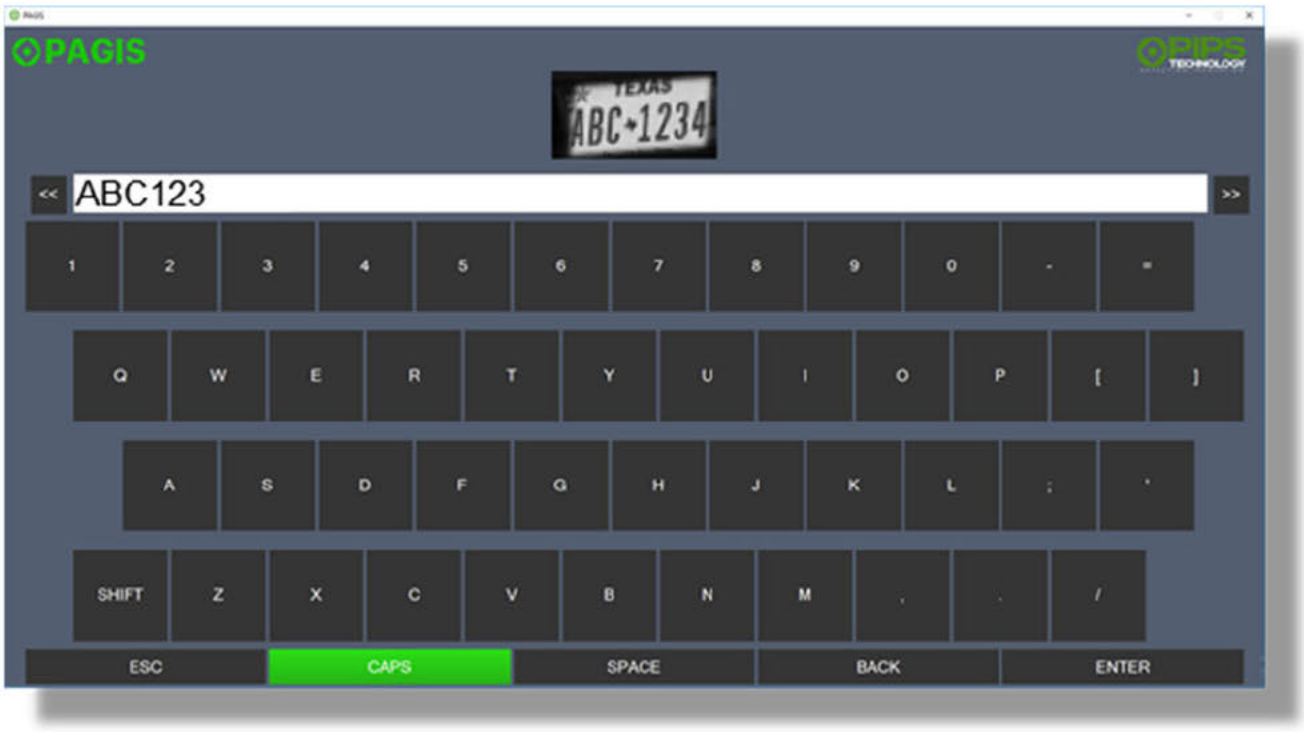
The Add Intel button launches the Intel screen. The user is prompted to assign one of four values: Towed, Arrest, Not Recovered, and Misc. by clicking the associated button at the top of the screen. The user may also enter additional detail regarding the license plate/vehicle. After clicking the Save button, the intel will now appear in the Hits Screen text box.



2.9.5 Misreads

PAGIS allows the user to mark Reads and Hits with incorrect OCR translations as a Misread. This is most commonly done by Agencies for Hits only as users typically don't have time to review every single Read from their shift. Once an errant Hit is corrected, the system updates the record to show it as a Misread and thus improves Agency Hit Reporting.

Correcting a plate read can be accomplished by clicking on the "OCR Patch" in either the Hits or Reads review screen. When the user clicks on the OCR Patch, the OCR Edit Screen opens and allows the user to update the Vehicle License Plate (VLP) data.



2.9.5.1 Marking a Record as a Misread:

The user can mark a record as a Misread from both Reads or Hits Review Screen. Each user can either simply flag the record as a Misread or update the OCR Patch information. **NOTE**: This ability is only available until the user has performed an End Shift function.

Manually Flagging a Read or Hit as a Misread:

1. Navigate to either the Reads or Hits Review Screen
2. Click on the Misread button on the Right
3. Click Save
4. Take note that the record title has now changed from “Read” to “Misread”

Updating the Read/Hit OCR Patch:

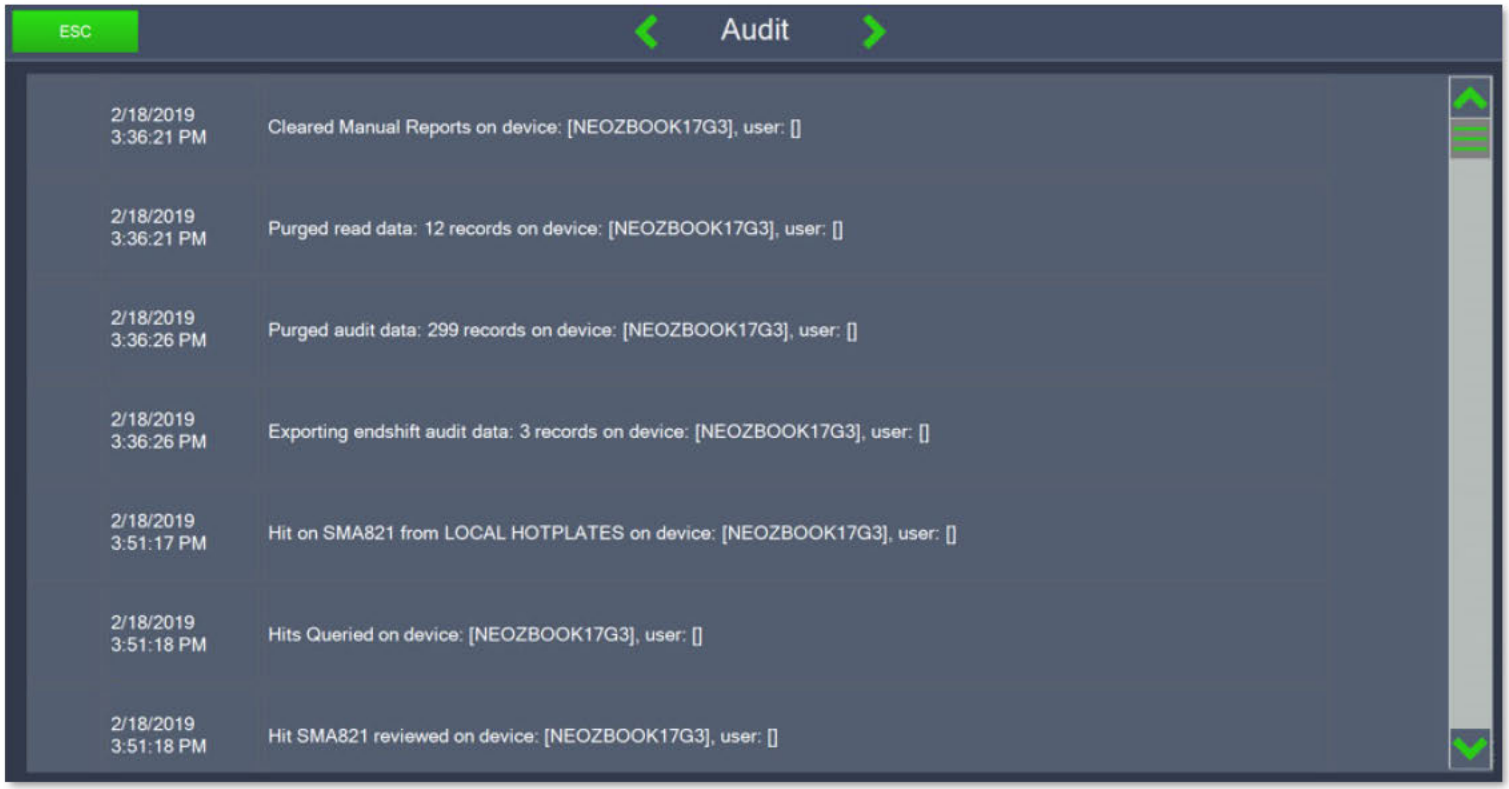
1. Navigate to either the Reads or Hits Review Screen
2. Click on the OCR Patch (Text just under the IR Plate Image)
3. Use the keyboard or on-screen keypad to update the Vehicle License Plate Number
4. Click the Enter Button to Save the changes (and exit back to the Review Screen)
5. When the user saves the changes to the OCR Patch, the record (Read/Hit) is automatically flagged as a Misread

2.9.6 Audits

5413

PAGIS logs both user and key system activity during each use of the software. The audit log captures various information like Read searches, synchronizations, hits, and user login attempts. The Audit Report is viewed in PAGIS by navigating to the Review section and selecting “AUDITS”.

NOTE: Performing an End Shift or syncing the database clears the current log.



2.9.7 Targets

PAGIS has the ability to display information regarding Persons of Interest in response to a Hit alert. Targets are created by BOSS/Hotlist Administrators, and typically provide detailed information about owners of a registered vehicles. When configured, Target data is always linked to unique VLP data (a specific License Plate). If PAGIS registers a Hit on a Plate with a target ID, the Target Information Button is displayed in the Hit Alert window and allows the user to access the Target Screen.



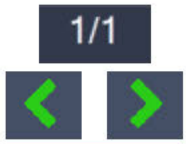
2.9.7.1 The Targets Screen

When a PAGIS user clicks the Target Information Button from a Hit Alert, the Targets Screen opens. This screen displays the information from the BOSS server about the Person(s) of Interest matched to the Hit (license plate).



2.9.7.2 Targets Screen Navigation Buttons

If a Hit alert has more than one Target associated with it, the PAGIS user can navigate all Target information with the buttons described below:



Target Count: The left number is the current record. The right number is the total available for review.

Next/Previous button: Arrows on either side of the target count allow the user to navigate back and forth to review the various targets.



Jump button: Allows the user to "jump" to a specific record without the need to navigate one record at a time using the Next/Previous buttons.

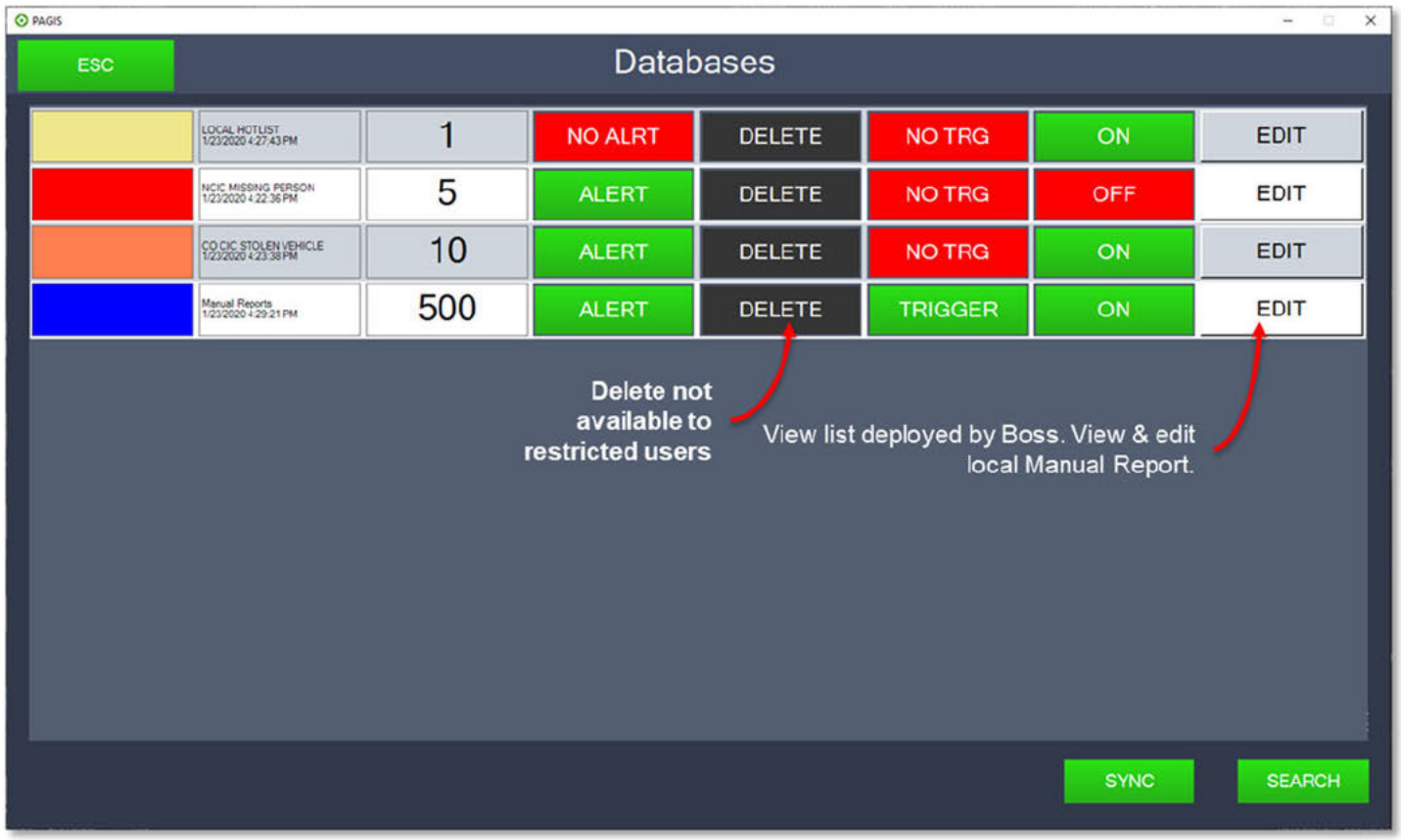


Close button: Returns the user to the previous screen.

2.9.8 Databases

Users can review Hotlists in PAGIS by navigating to the Review section and selecting "DATABASES" on the right. From the Databases Screen, users can toggle Hotlists functions On and Off based on their rights.

NOTE: User rights and Hotlist attributes are configured in BOSS.



2.9.8.1 Databases Screen Functions

Hotlist Color Code: The color attributed to each Hotlist by the BOSS Administrator.

Hotlist Name: The name of the Hotlist given by the BOSS Administrator. Also shows the time/date of the last synchronization.

Hotlist Priority: The priority of the Hotlist assigned by the BOSS Administrator. The lower the number between 1 and 999, the higher the priority. If a plate resides on multiple Hotlists, the list with the higher priority will be displayed first.

Alert Button: Toggles audible alerts On and Off for each Hotlist until the next synchronization.

Delete Button: Based on user rights, allows the user to temporarily delete a Hotlist from PAGIS until the next synchronization. To delete a hotlist, the user must click the button twice (it turns green and then deletes the list).

Trigger Button: Toggles external triggers On and Off. An example of an external trigger is a light bar.

On/Off Button: Disables and enables each Hotlist (each Hotlist is set to On by default).

Edit: View and edit localy created hotplates with a given hotlist, Hotlist/Hotplates deployed via BOSS can only be viewed.

NOTE: Hotlist settings altered in PAGIS will be reset to their default configuration during the next Sync or End Shift. The default configurations are assigned by the BOSS Server/Administrator.

2.9.8.2 Databases Screen Navigation Buttons

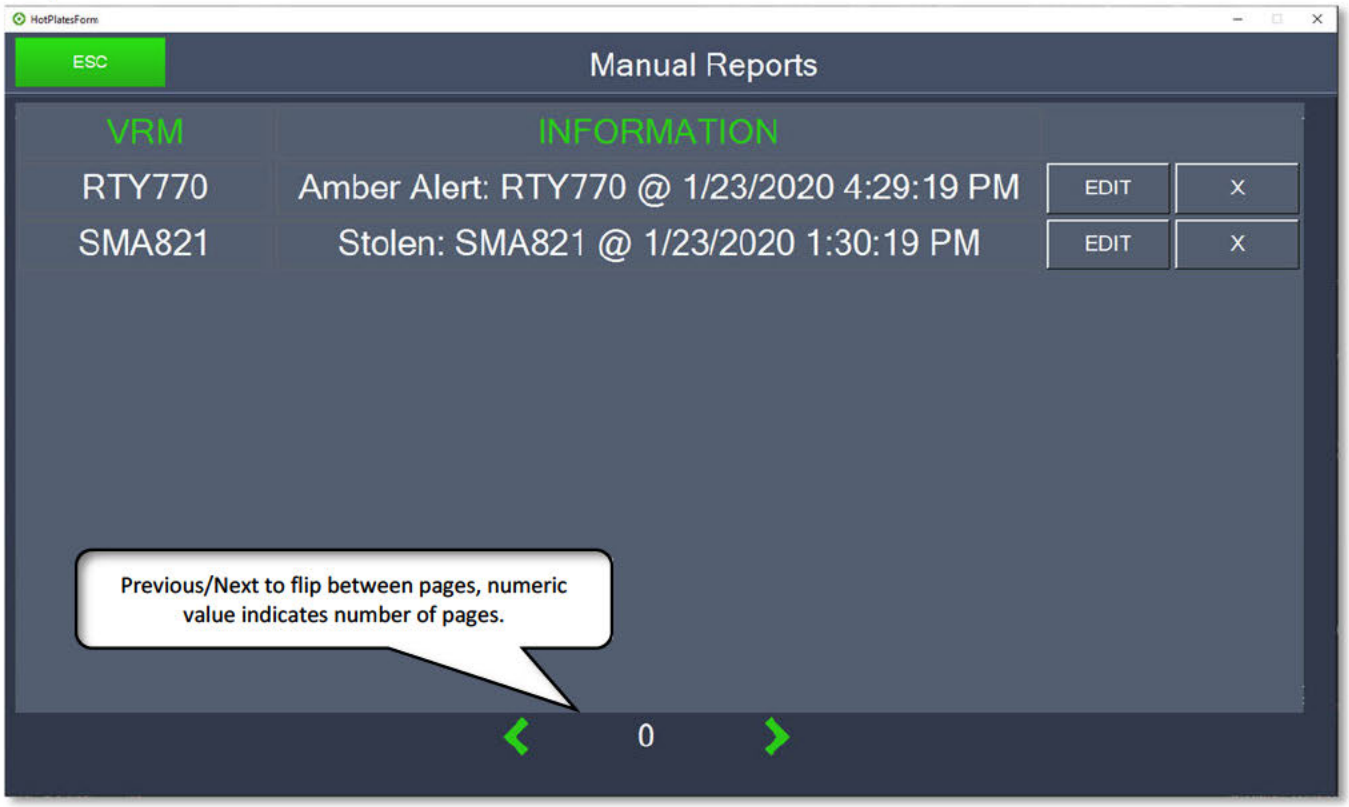
SYNC — **Sync button**: Synchronizes PAGIS with the BOSS server in order to update the Hotlists.

SEARCH — **Search button**: Open the Search Entry Screen (See section 2.8 for more information).

2.9.8.3 Databases Edit- “Manual Reports”

Editing Hotlist has two function based on origin of hotlist.

- Hotlist deployed to PAGIS via BOSS cannot be edited, only the hotplates list can be viewed. Editing/updates are indented to be managed via BOSS.
- Hotlist created in PAGIS, i.e. “Manual Reports” can be managed by PAGIS users, allowing for changes or deletion of the hotplates contained within the hotlist.



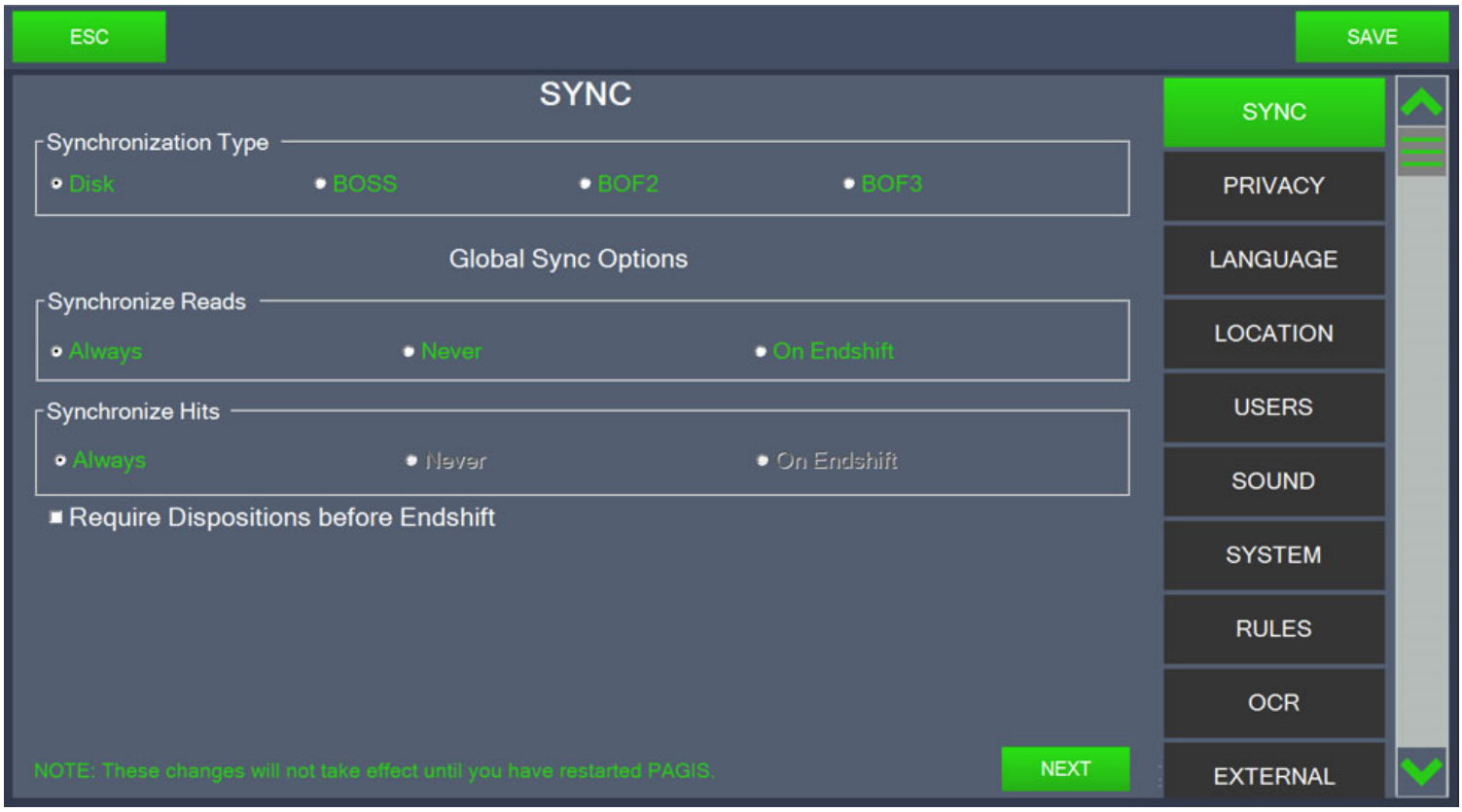
EDIT Button: Make changes to the indicustly hotplate information including licanse plate nuamber.
X Button: Remove indivualy hotlist from hotlist.
Previous/Next Button: Scroll thought lising of hotplates contaned within the hotlist. The numeric value indicates the number of pages.

ADMIN SETTINGS

The Settings Menu is the central location for configuring PAGIS Software functions endpoint by endpoint. Users with Admin level rights in PAGIS can see and click on the Settings Button from the Live View Screen. Launching Settings opens the menu to the Sync Options Screen by default. **NOTE**: Users without Admin level access will not see this icon on the Live View Screen.

3.1 Sync Options Screen

As mentioned previously in sections 2.4 and 2.5, PAGIS uses various sync options to store, update, and synchronize ALPR data to and from the BOSS server. On the Sync Screen, Administrators configure the synchronization method and options.
NOTE: Configuration changes will not take effect until they are saved and the PAGIS Software has been restarted.



3.1.1 Synchronization Types

- **Disk**: Uses local storage of Sync files in conjuction with a USB flashdrive to manually Sync to and from BOSS.
- **BOSS**: Uses a wireless data network to Sync files to and from the BOSS server.
- **BOF2**: Used predominantly in Europe (see regional guide for support).
- **BOF3**: Used predominantly in Europe (see regional guide for support).

3.1.1.1 Synchronization to Disk (Local Storage)

5418

Sync to Disk is a manual two-part process most commonly used with a USB Thumb drive. To use Begin Shift, the user accesses a centralized terminal (Ex. Patrol Room PC) to download the files from BOSS and then inserts the Thumb drive in the laptop to perform Begin Shift. At the end of the day, the user then Performs End Shift from the laptop/MDC connected to the Thumb drive and uploads those files to BOSS via the central terminal (See the "Client Tools" section of the BOSS Manual).
NOTE: From the Sync Menu, select "Disk" and click the Next button at the bottom to configure the drive location.

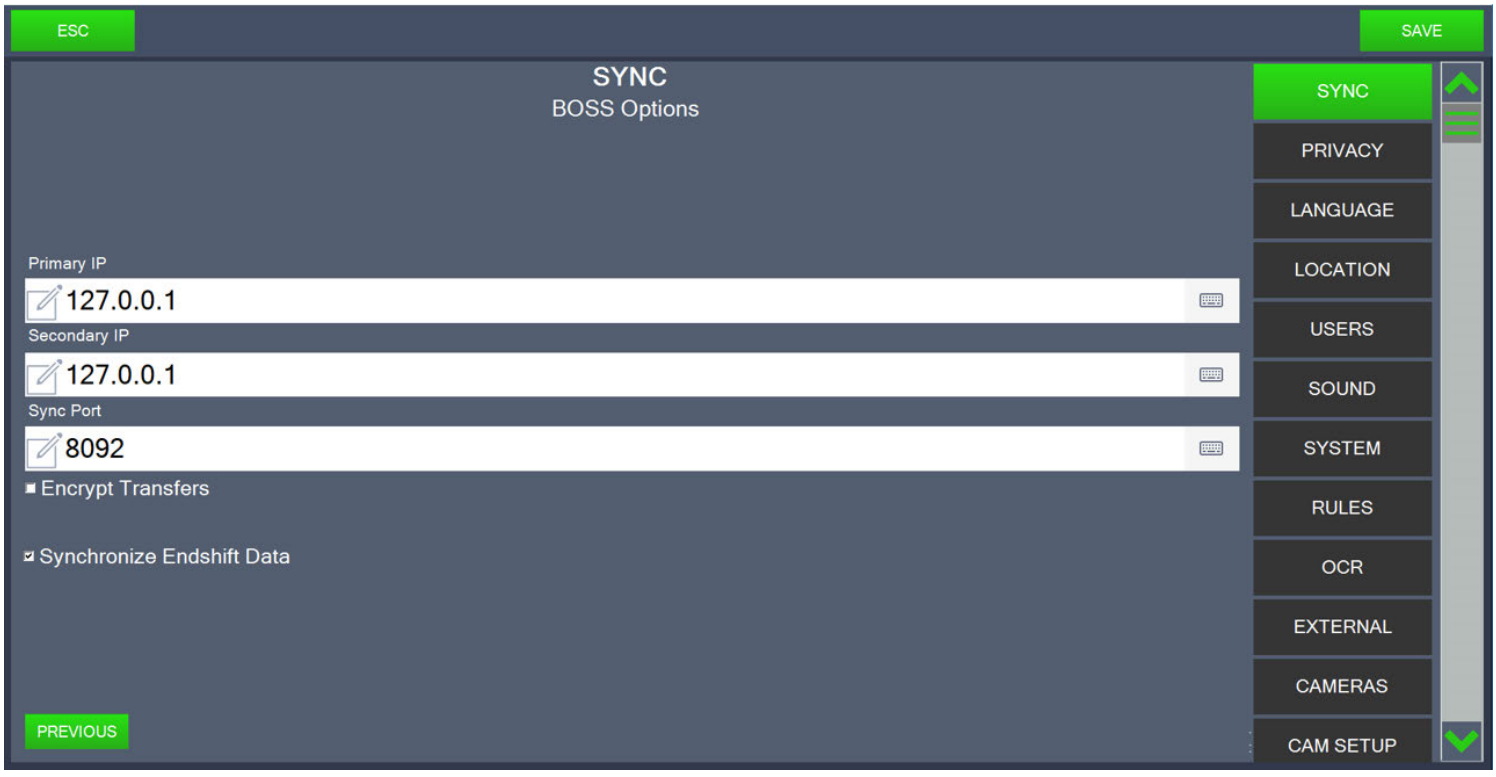


- **Delete Beginshift Data on Sync**: The sync folder on the Flash Drive is deleted once all Begin Shift data has been imported to PAGIS. This is on by default to help prevent false alerts.
- **Encrypt Endshift Data**: All uploaded End Shift data created in PAGIS is encrypted. This is off by default.
- **Copy Endshift Data on Sync**: If unchecked, no End Shift data will be transferred from PAGIS to the Drive location.
- **Keep Only Updated Databases**: Removes any Hotlists from PAGIS that were not updated during Begin Shift as "outdated". This is off by default.

Sync to Disk Setup:
In the text box, enter the drive path or letter to be used with Disk Sync. Folder name is not required as PAGIS creates the required folder(s). Once entered, select the desired options and then click the Previous button. Click Save to retain the settings.

3.1.1.2 Synchronization with BOSS

Sync to BOSS is a streamlined method for updating ALPR data to the field units and the server. Additionally, selecting this option enables the PAGIS auto-sync features that synchronize data throughout the shift without user involvement. However, this does require a stable data connection as well as some network configuration before it can be utilized.



Sync to BOSS Screen:

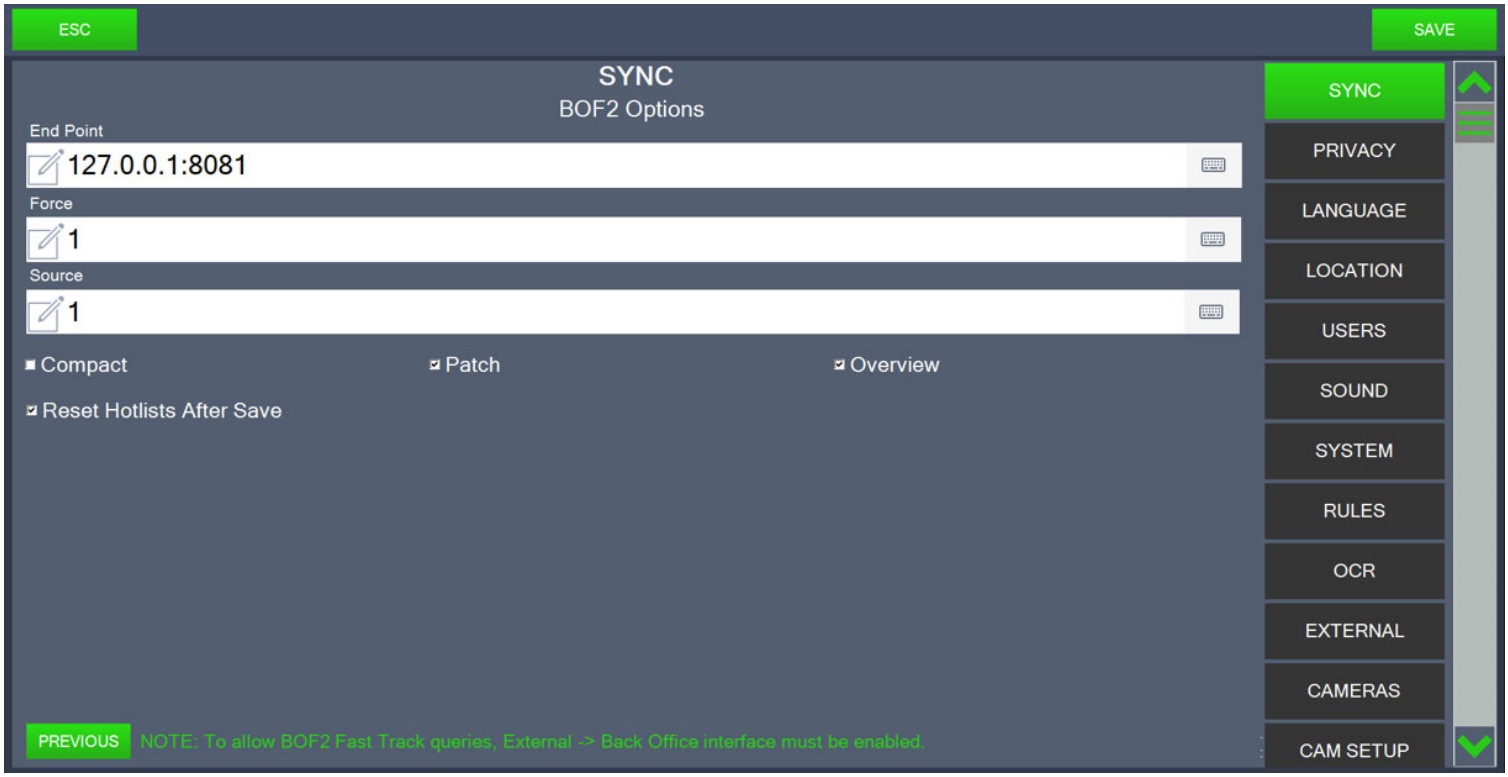
- **Primary IP**: The IP address of the BOSS server. This can also be the DNS name (**NOTE**: using DNS adds an additional failure point via the Domain Controllers and is not recommended as the best option).
- **Secondary IP**: Used for a secondary IP in cases where users switch from a cellular network to a Domain APN thus routing to BOSS from either an internal or external IP. This field can be left blank or with the primary IP as well.
- **Encrypt Transfers**: When enabled, data transfers to BOSS will be encrypted.
- **Synchronize Endshift Data**: On by default, this enables PAGIS to sync to BOSS when End Shift is performed by the user.

Sync to BOSS Prerequisites:
To establish the wireless sync to BOSS, the Agency Network Administrator will need to open TCP 8092 to the BOSS server as well as define the internal and/or external IP address(es).

Sync to BOSS Setup:
From the Sync Settings Menu, the Admin must select the BOSS option and click the Next button. Then s/he will update the Primary and Secondary IP fields as necessary and de/select any options. Once configured, click the Previous button and then click Save to retain the changes. (For more information on PAGIS Auto-Sync settings, refer to section 2.4.3)
NOTE: After synchronizing to BOSS, data is flagged in the database to prevent duplicate values on future synchronizations.

3.1.1.3 Sync to "Instation" (Formerly BOF2 and BOF3)

The Instation software was formerly known as BOF2 & BOF3 and was developed by Anite PLC. It is a web-based Back Office software suite used in European markets to provide similar features as the PIPS BOSS server and UI Client.
NOTE: These options are NOT used in the Domestic United States.

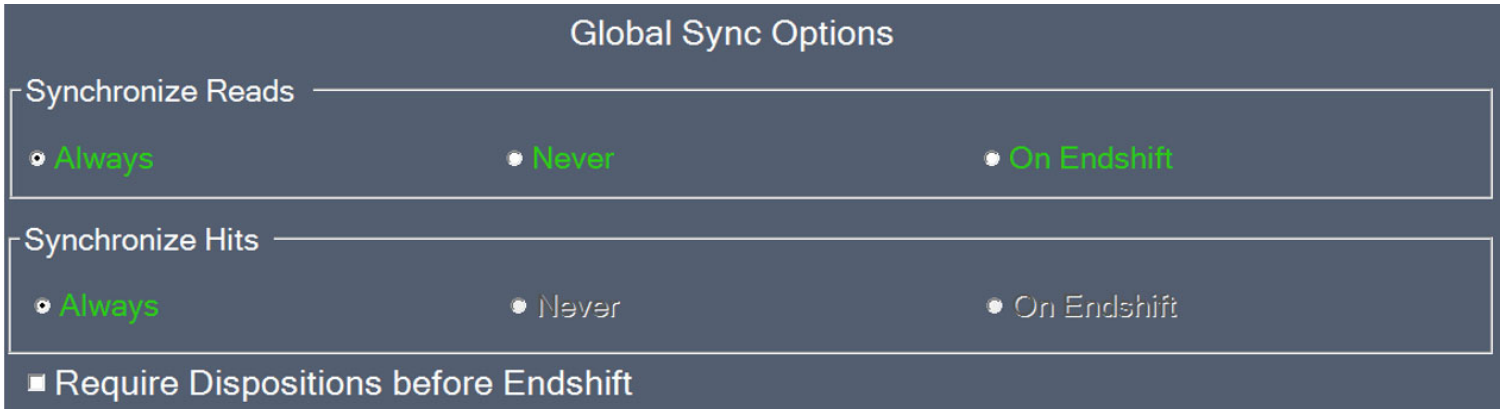


- **End Point**: The IP Address of the Instaion website. Format must be [IP Address:Port]
- **Force/Source**: Unique codes assigned to each police force.
- **Compact**: This option minimizes data transfer to Instation. Images will be deselected by default when in use.
- **Patch**: Refers to the image of the plate pulled from the read. This is on by default.
- **Overview**: Refers to the color overlay image from the read. This is on by default.
- **Reset Hotlists After Save**: When the software syncs to Instation, this will reset the hotlist tracking.

3.1.2 Global Sync Options

5420

Global Sync settings control how PAGIS synchronizes ALPR data during Begin and End Shift cycles and applies to both manually launched synchronizations as well as Auto-Sync functions. The two sections are Synchronize Reads and Synchronize Hits.



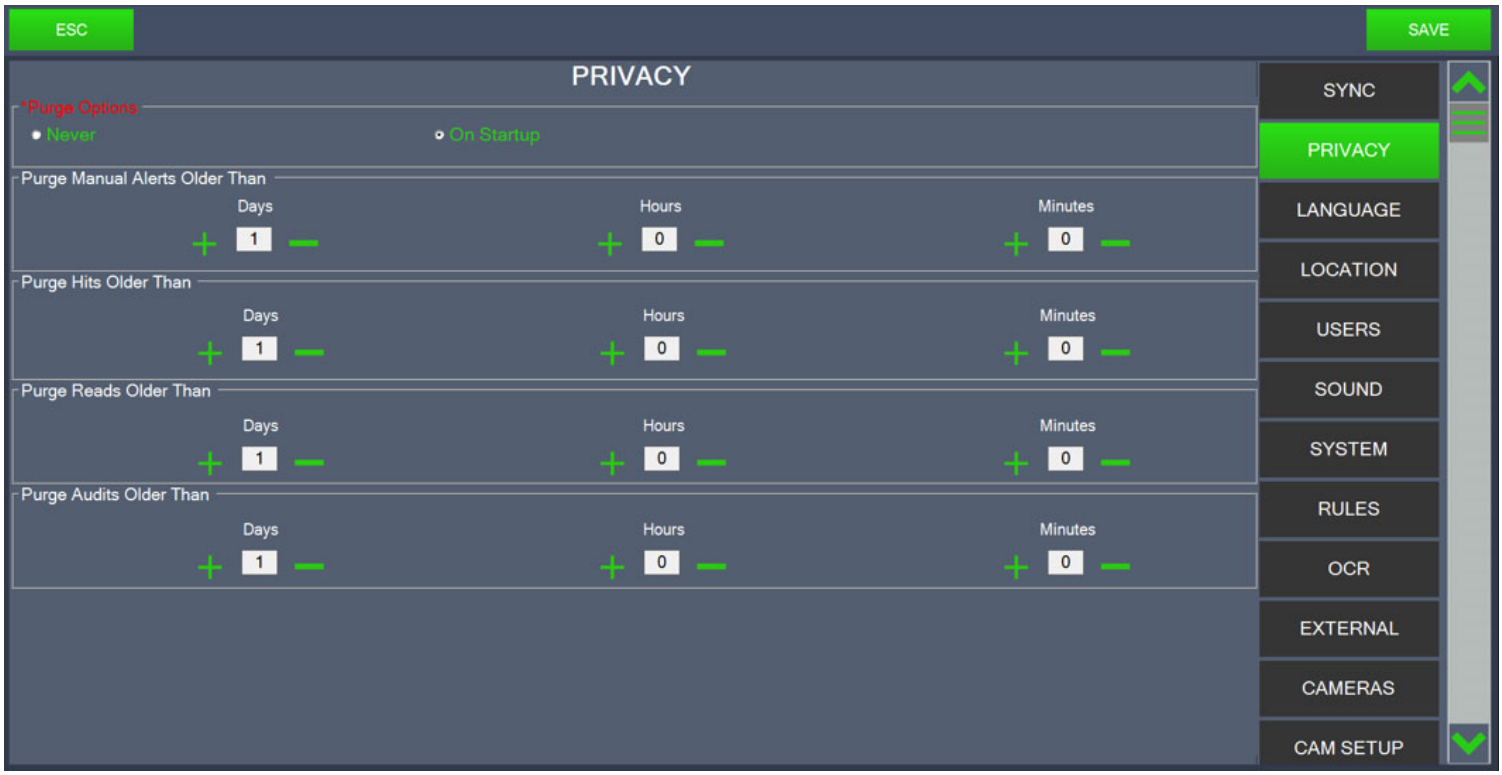
NOTE: All Hits are Reads, but not all Reads are Hits. A "hit" is a read that coincides with an Alert List. Due to this, the Options selected in the "Synchronize Reads" section dictate what options are available in the "Synchronize Hits" section. Unavailable options are greyed out.

- **Always**: Reads and Hits are synchronized to BOSS as close to real-time as the data network and PC processing allow.
- **Never:** The information gathered during the shift will be "sanitized" with each launch of End Shift. The corresponding data and images will NOT be sent to the BOSS server.
- **On End Shift**: Synchronization to BOSS will only occur when the user manually launches End Shift.
- **Require Dispositions before Endshift**: Requires the user to select a disposition code for each Hit registered in the PAGIS software since the last End Shift was completed before the Synchronization is processed.

3.2 PAGIS Privacy Settings (Local Data Retention)

5421

Although most commonly configured in BOSS, the PAGIS Software allows the Admin to configure the data retention settings for the local endpoint by minutes, hours, or days. This feature ensures the data captured/stored on the MDC is sanitized by the software itself (this is important for customers without BOSS). **NOTE**: To enable the Privacy settings, the Admin must select the "On Startup" purge option and then set at least one value in each row. Rows left with all Zero will not be sanitized or purged.



- **Never**: Selected by default, this option disables the PAGIS privacy settings and uses only those set in BOSS.
- **On Startup**: This option must be selected in order to enable the PAGIS privacy settings. Once enabled, PAGIS looks to purge/sanitize the system each time it's launched or restarted.
- **Purge Manual Alerts Older Than**: Controls how frequently all of the Databases/Hotlists in PAGIS are purged. The purge rate is calculated from the timestamp of the Hotlist. Once the retention value is surpassed, the Hotlist is deleted. Hotlists distributed from BOSS will be re-downloaded on the next Sync.
- **Purge Hits Older Than**: Controls how frequently all Hits in PAGIS are purged. The purge rate is calculated from the timestamp of read. Once the retention value is surpassed, the Hit is removed the next time PAGIS is restarted.
- **Purge Reads Older Than**: Controls how frequently all Reads in PAGIS are purged. The purge rate is calculated from the timestamp of read. Once the retention value is surpassed, the Read is removed the next time PAGIS is restarted.
- **Purge Audits Older Than**: Controls how frequently all Audits in PAGIS are purged. The purge rate is calculated from the timestamp of audit. Once the retention value is surpassed, the audit is removed the next time PAGIS is restarted.

NOTE: Once the hits, reads, databases, or audits have been purged, they can no loner be viewed in the PAGIS software.

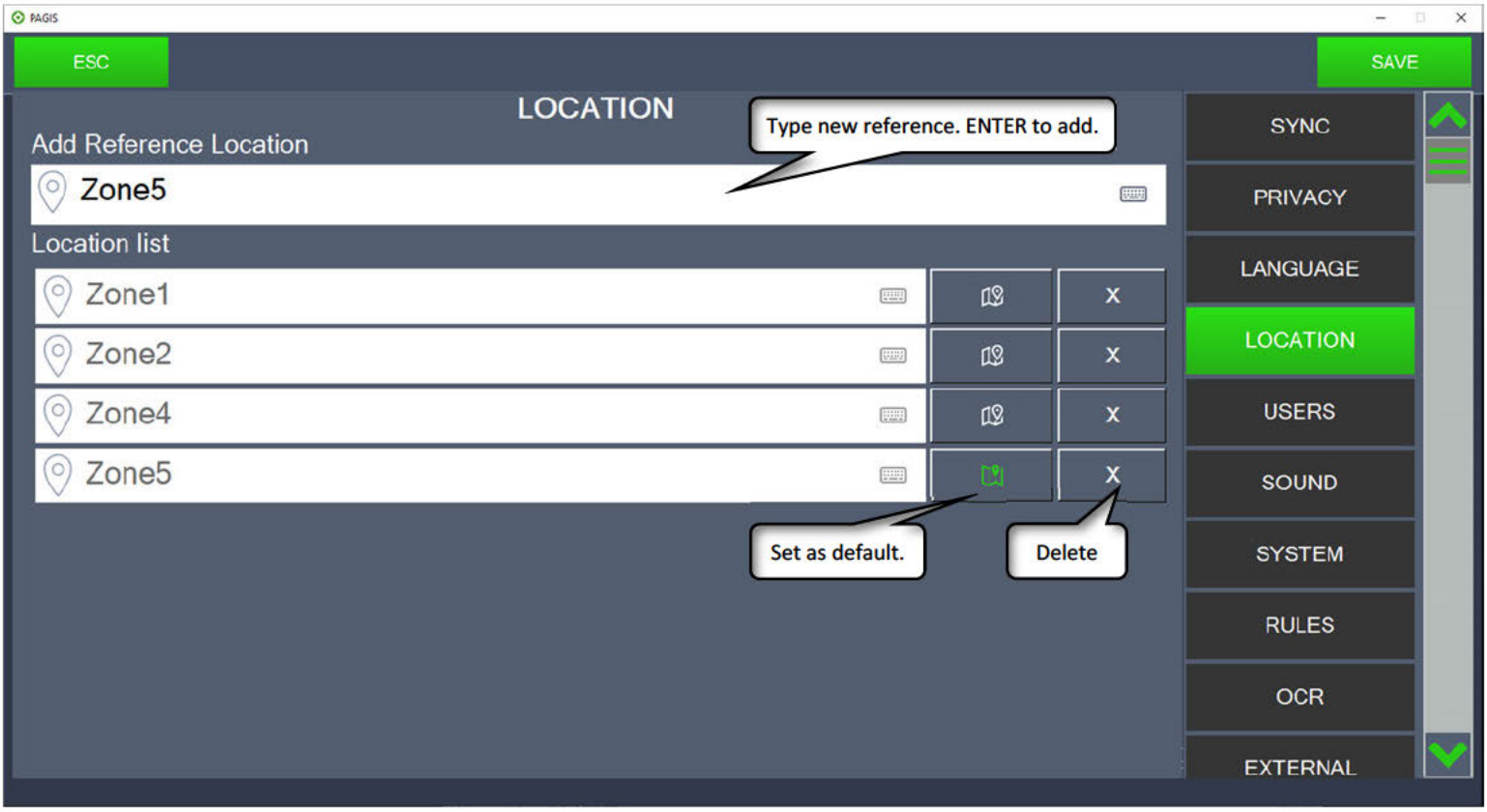
3.3 Language

5422

The Language screen allows the Admin to change the language assignment used in the PAGIS Software. Available languages are listed in the drop-down list and are added during the installation process.

3.4 Location

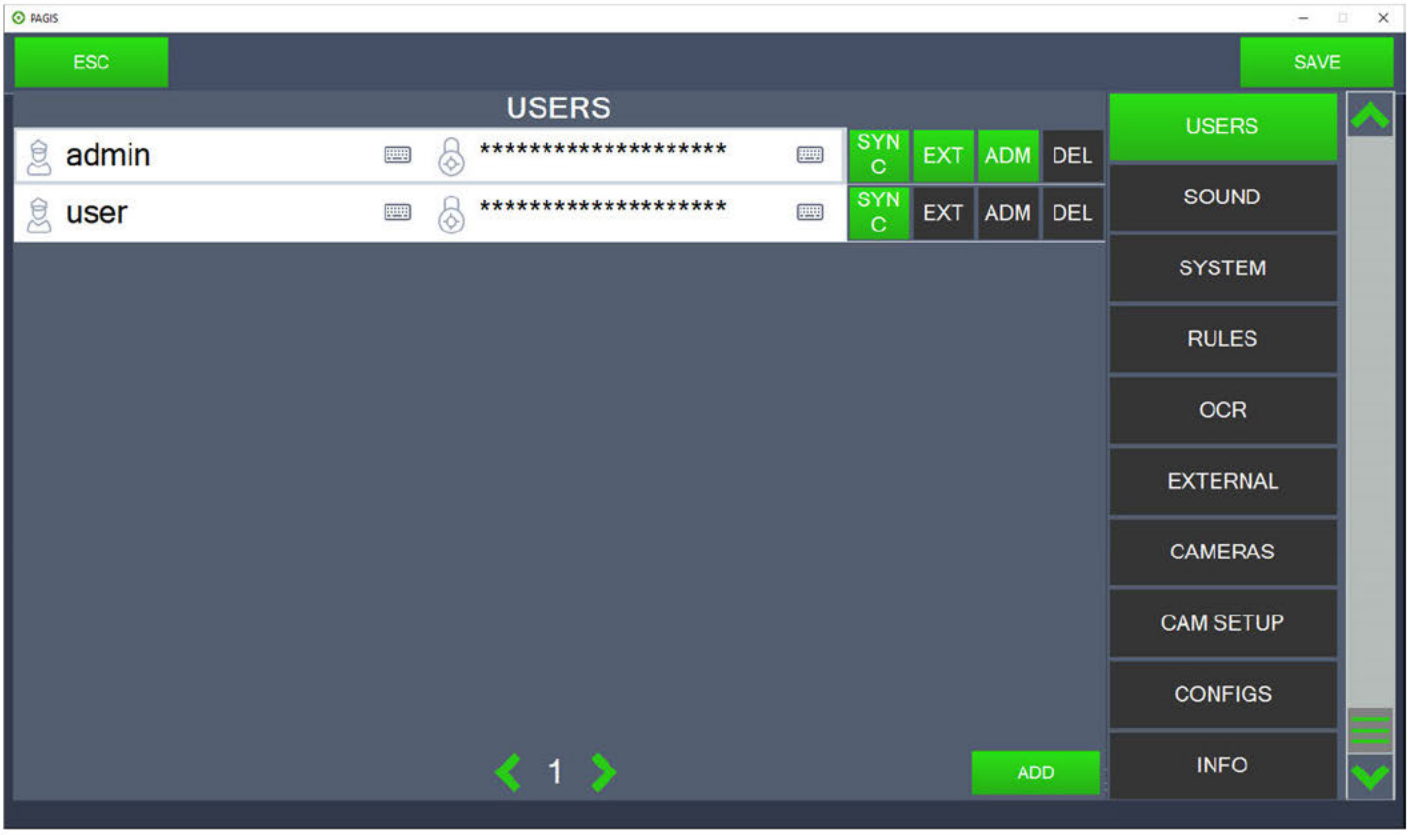
Updates to the location field will auto-fill the “Reference” section of the PAGIS Login Screen. These are often used to specify a patrol region (Examples: “North Patrol” or “A2”). Once designated all reads/hits will show this designation. Muiltiple “Referance” location can be added, the available list can then be selected from the login screen.



3.5 Users

5423

User accounts, credentials, and rights are generally administered from BOSS and then distributed to the MDC. However, PAGIS does allow for Administrators to add and delete users as well as set their privileges directly from PAGIS.



NOTE: Adding user directly in PAGIS should be limited to customers not utilizing a BOSS server. User accounts created directly in PAGIS by customers with BOSS will be overwritten/removed during the next sync.

Adding a User in PAGIS:

1. From the Admin Screen, select the Users Button on the Right
2. Click the Add Button ADD
3. Enter the case sensitive username in the Username Field (max of 15 alphanumeric characters)
4. Enter the case sensitive password in the Password Field (max of 15 alphanumeric characters)
5. Select the User's privileges
6. Click the Save Button SAVE

3.5.1 User Privileges

These are the "rights" the new user will have in the PAGIS software (When selected, each button turns green).

SYNC — **Sync:** Allows users to synchronize data.

EXT — **External**: Allows the user to access external databases.

ADM — **Admin**: Provides the user Admin rights and allows him/her to configure the PAGIS Software.

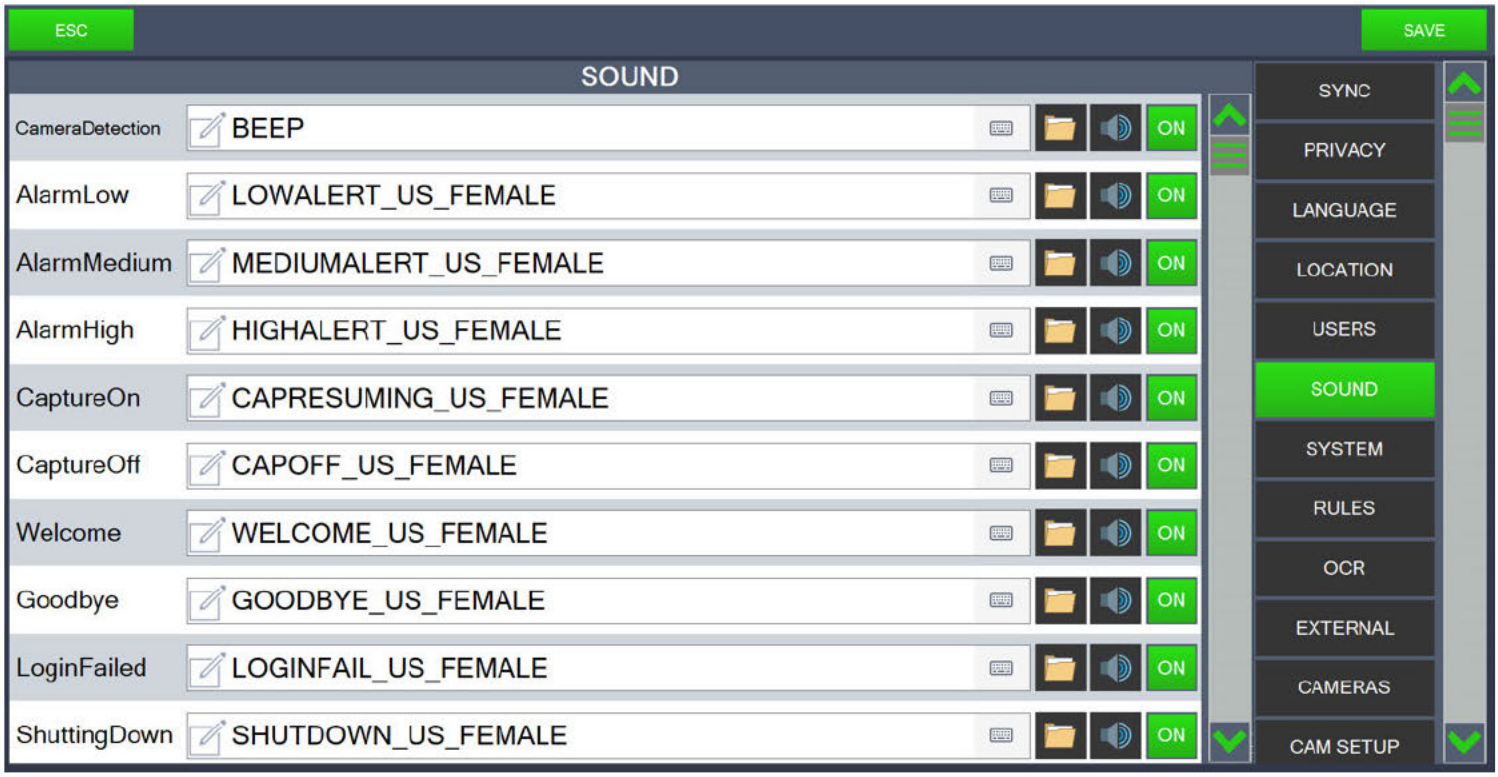
DEL — **Delete**: Allows the Admin to delete a User from the list. Click once to select and the save button to delete.

NOTE: Creating a new user in PAGIS automatically deactivates the default user account settings (Section 2.1.1).

3.6 Sound

5424

Sounds in PAGIS mirror the user or software activity (Ex. Login, Audible alert from a "Hit", and Logout) and are On by default. PAGIS Administrators can adjust the sounds from the available presets and/or load unique .wav files onto each MDC for custom use. **NOTE**: The default storage path is C:\Program Files (x86)\PIPS Technology, Inc\PAGIS2\sounds



3.6.1 Configuration Buttons

The sounds listed on the configuration screen can be altered or updated by PAGIS administrators using the buttons below. **NOTE**: Changes to any sounds must be saved before they can be played in PAGIS.



Click to browse to the sounds folder. This is used to select a new sound file.



Click to Test/Play the selected sound.



Shows the status of that sound. Click to turn each sound Off.

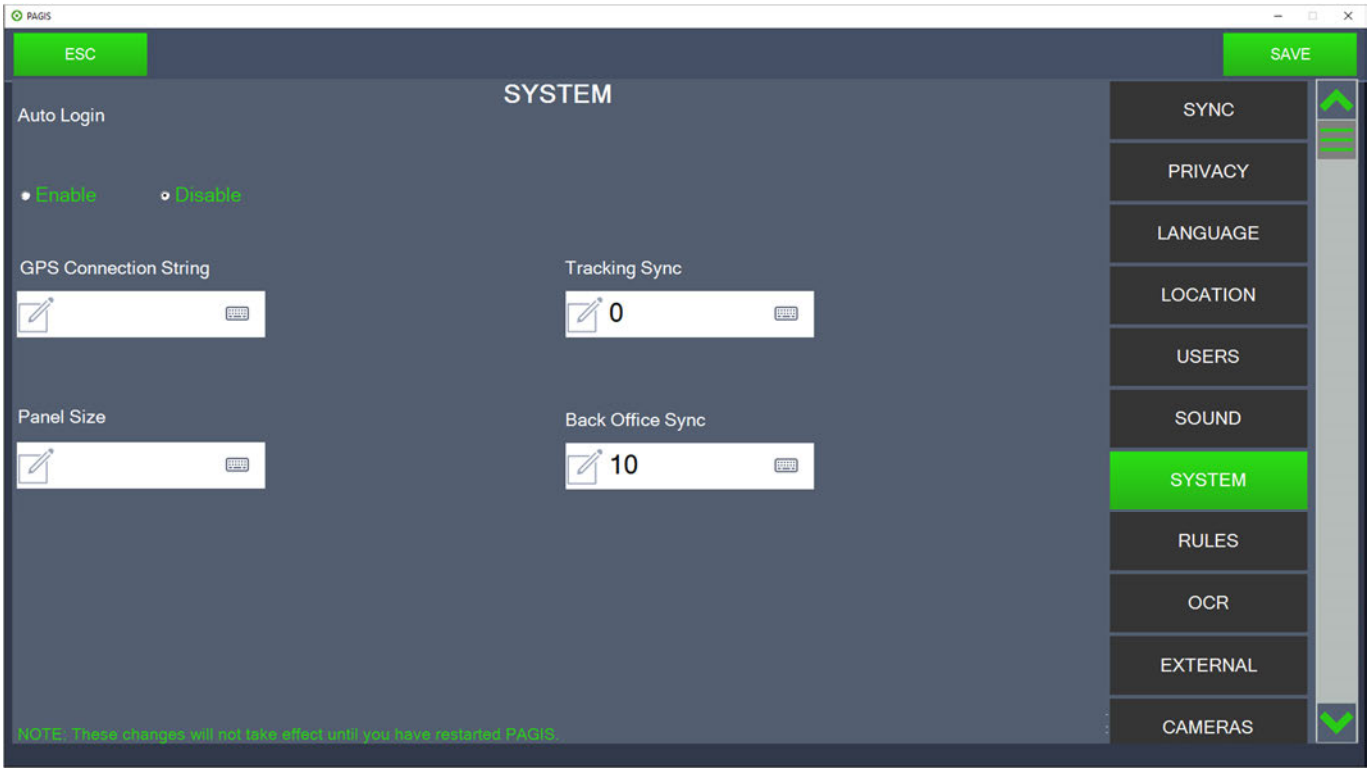


Shows the status of that sound. Click to turn each sound On.

3.7 System

5425

The System screen determines external system connections. The primary external connection is the GPS antenna. The GPS connection string will accept TCP/IP ports or COM port designations. This section also contains control of the PAGIS "Auto Login" feature (which is set to Off by default).

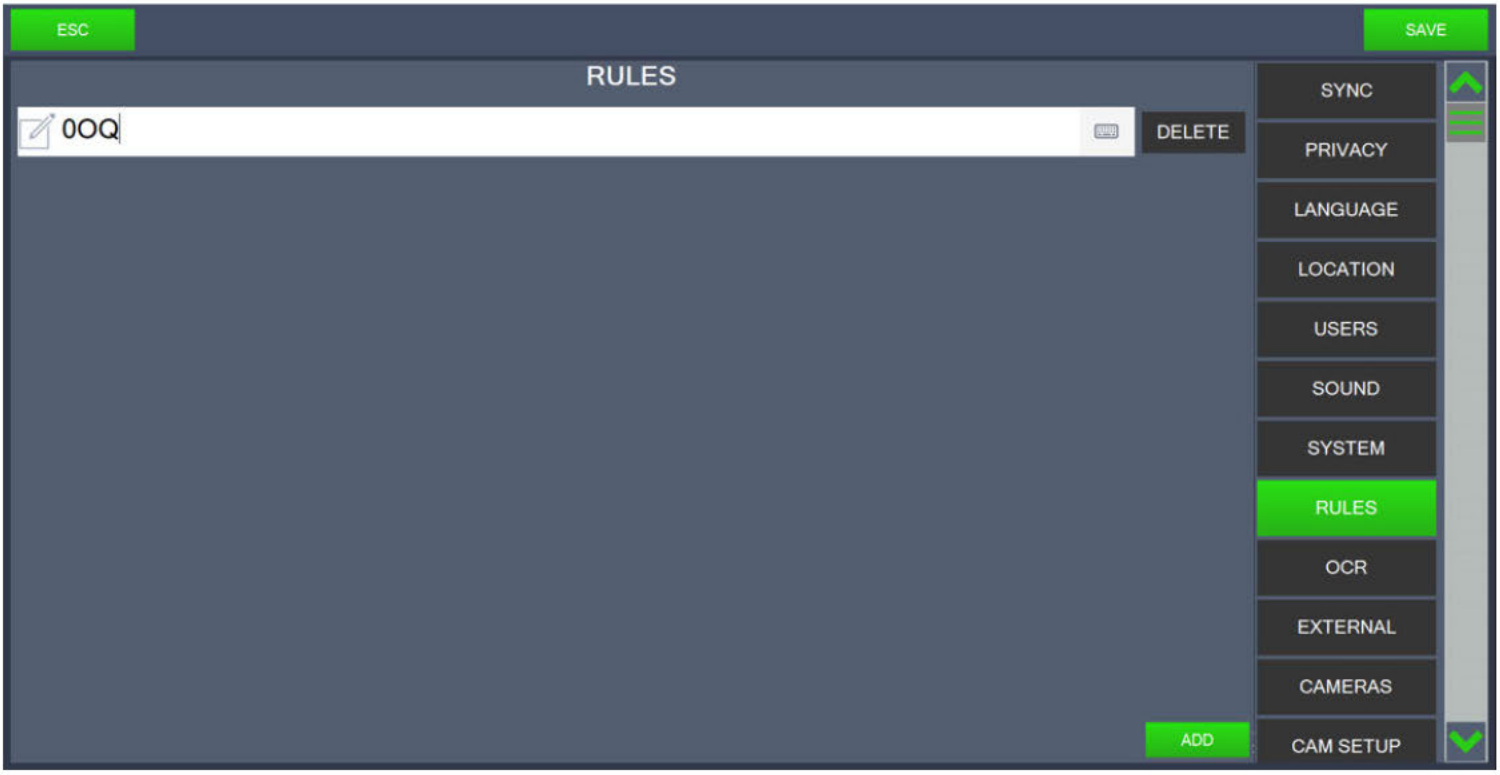


- **Auto Login**: Enabling this feature will ignore existing user account information and login to PAGIS as the Admin. This feature is recommended only for unattended use (Speed-Trailer applications and Covert Drop and Go deployments).
- **GPS Connection String**: This value is utilized by PAGIS to acquire the GPS feed from its source. The default is traditionally either blank (no entry) or 6.
- **Tracking Sync**: Controls the sync intervals in (Sec.) that PAGIS communicates with BOSS4 to update tracking status. Default off=Zero, values can range from 1-9999. BOSS4 Back Office Software requiered for this feature.
- **Panel Size**: Controls the resolution of the color image displayed on the Live View Screen. By default this is blank as PAGIS controls the aspect ratio. However a PAGIS Admin can assign custom resolutions in WxL format (720x1024) to assist with non-standard dispalys.
- **Back Office Sync**: This setting controls the sync timing that PAGIS sends data back to BOSS3/BOSS4, Timing is in (Sec.), default is 10sec, values can range from 0-9999.

NOTE: All changes must be saved and will not take effect until PAGIS is restarted.

3.8 Rules

Rules in PAGIS allow Administrators to force the software to process plate reads in specific ways. For example, in states that allow for both O and 0 (zero) on their license plates, a rule can be set to read any zero as an O and any O as a zero. This provides PAGIS greater flexibility to the standard OCR functions.



Adding a Rule to PAGIS:

1. Click the Add Button ADD
2. Enter the desired alphanumeric characters (Ex. 0 and O) into the text field
3. Click the Save Button SAVE at the top right of the screen

Deleting a Rule:

1. Locate the rule to be removed from PAGIS
2. Click the Delete Button DELETE to the right of the rule (It will turn green when selected)
3. Click the Save Button to complete the removal

3.8.1 Rules – Additional Clarifications

1. Rules are processed based on the first character entered. So in order to read any O as a zero, the Admin will need to add rule "O0". And in order to read any zero as an O, a second rule must be entered as "0O".
2. Rules are NOT designed to overhaul OCR function. Any consistently misread values should first be brought the attention of PIPS Support for review. And only those cases where further adjustments to the OCR software are impossible would rules be recommended.
3. Adding rules to PAGIS will make it less likely to miss a Hit Alert. However, it will increase the number of Hit Notifications that require the Officer to visually confirm the OCR read ("IR Patch") and the Hotlist Alert match.

3.9 OCR

The OCR Section in PAGIS provides Administrators some additional options on how they would like PAGIS to process plate reads.



- **JPEG Images**: On by default, this forces PAGIS to use compressed .JPG images instead of the full resolution Bitmap images each time a read is taken. This settings minimizes data storage requirements and preserves MDC drive space.
- **Inverse Plates**: Off by default, this setting is only used in States where plates with light color lettering over a dark background are prevalent. Enabling this option increases processing load and should remian disabled unless required.
- **Square Plates**: Off by default, this setting adjusts the read area plates that are square instead of retangular.
- **Disable Duplicate Read**: On by default, this setting helps PAGIS prevent duplicate plate reads. If a VLP is read by more than one camera within a short period, the duplicate read is ignored. This minimizes data storage requirements and improves overall system metrics related to numbers of Hits and Reads.

NOTE: Once changes are made, the Admin must click the Save Button SAVE button in the upper right corner to retain them.

3.10 External

The External Screen allows the Admin to connect PAGIS to an external database or device via XML Datastream. This feature is Off by default and any changes must be saved before they will be available.



Enabling the Datastream:

1. Click the Off Button OFF to toggle to On ON
2. Click the Save button in the upper right corner
3. Close and reopen PAGIS

NOTE: Enabling this feature will reduce the overall performance of the PAGIS Software.

3.10.1 XML Datastream Ports

Administrators will need to configure their external device or database to utilize two specific TCP ports:

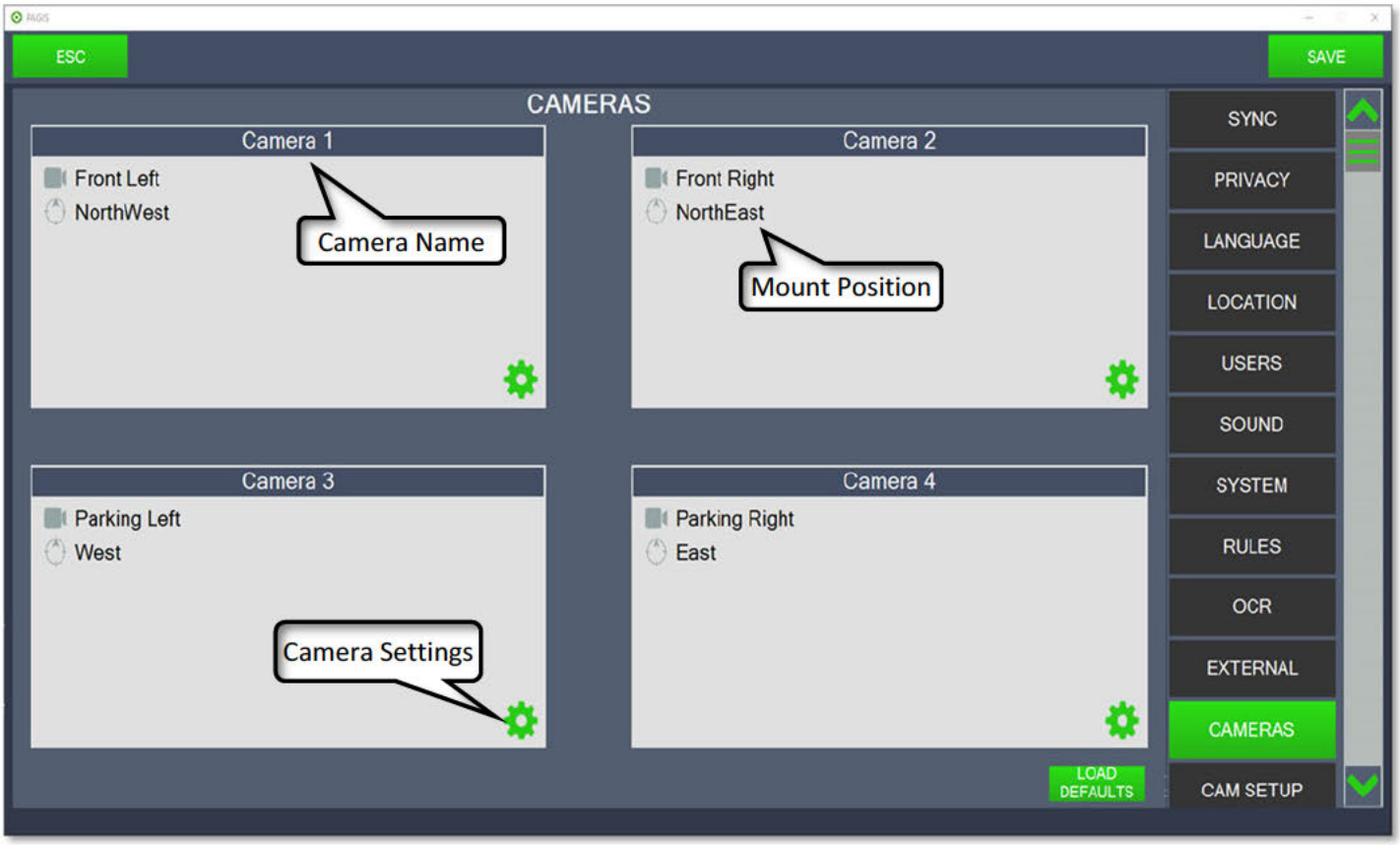
1. Query Port: TCP 7000
2. XML Datastream/Heartbeat: TCP 10100

NOTE: Greater detail on the XML Datastream can be found in Appendix D

3.11 Cameras

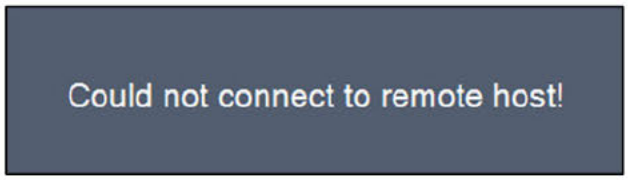
The Cameras Section provides the Administrator the means to add/delete, identify, and configure the ALPR cameras. Although the PAGIS Software comes preloaded with a default layout, best practices advise the Admin to fully review, and completely configure at least one MDC by hand in order to tailor the setup for the Agency's unique attributes.

IMPORTANT: The configuration steps completed here will dictate the available camera mode options in the Configs Section.



3.11.1 Checking the Connection

In order to configure the cameras, the PAGIS Software and the SX Processor (Black Box) must be able to communicate. If they cannot, the Administrator will receive the error message below as soon as he or she clicks on the Cameras Button CAMERAS indicating that PAGIS cannot "see" the cameras.



3.11.2 Troubleshooting Camera Connections

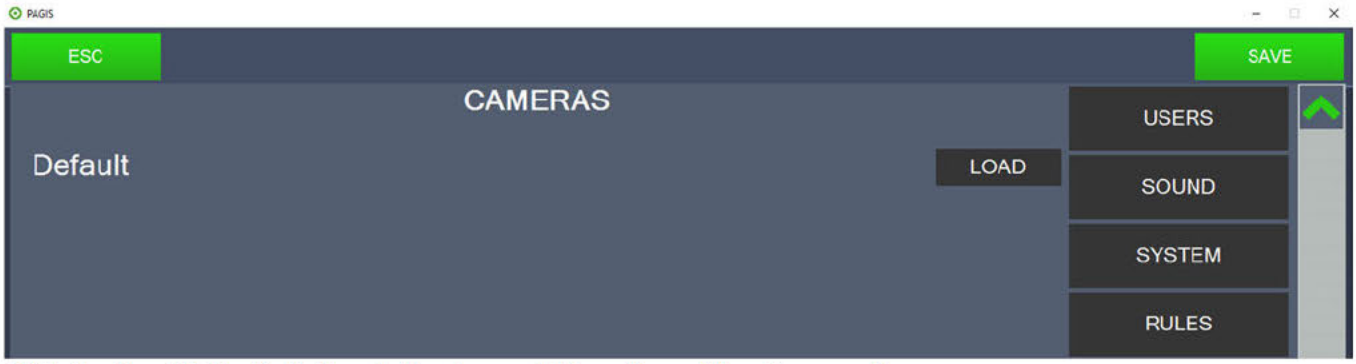
The most common troubleshooting steps have been included below for convenience. If these don't resovle the issue, please contact PIPS Support for additional assistance. **NOTE**: For more information see Appendix C – The Mobile FAQ

1. Start the vehicle and confirm power to the Processor. Confirm the SX switch, and any added in-line switch, is set to On.
2. Confirm the network adapter settings on the laptop match the proper Static IP scheme for the SX Processor in use.
3. Disable the local Windows Firewall, VPN software, and any real-time monitoring software one at a time.
4. Use a different network cable ensuring it's properly seating in NIC port on the SX as well as the MDC or Docking Station.
5. Docking Stations can also impede communication. Test by removing the laptop from thhe dock, directly connect the network cord to the laptop, and then reconfigure the network adapter settings as needed.

3.11.3 Configuring the Cameras in PAGIS

This section will assist with the general configuration of the cameras. Administrators can begin by selecting the Settings Icon to edit each of the existing cameras or by selecting the Load Defaults Button LOAD DEFAULTS. This manual will start with Load Defaults.

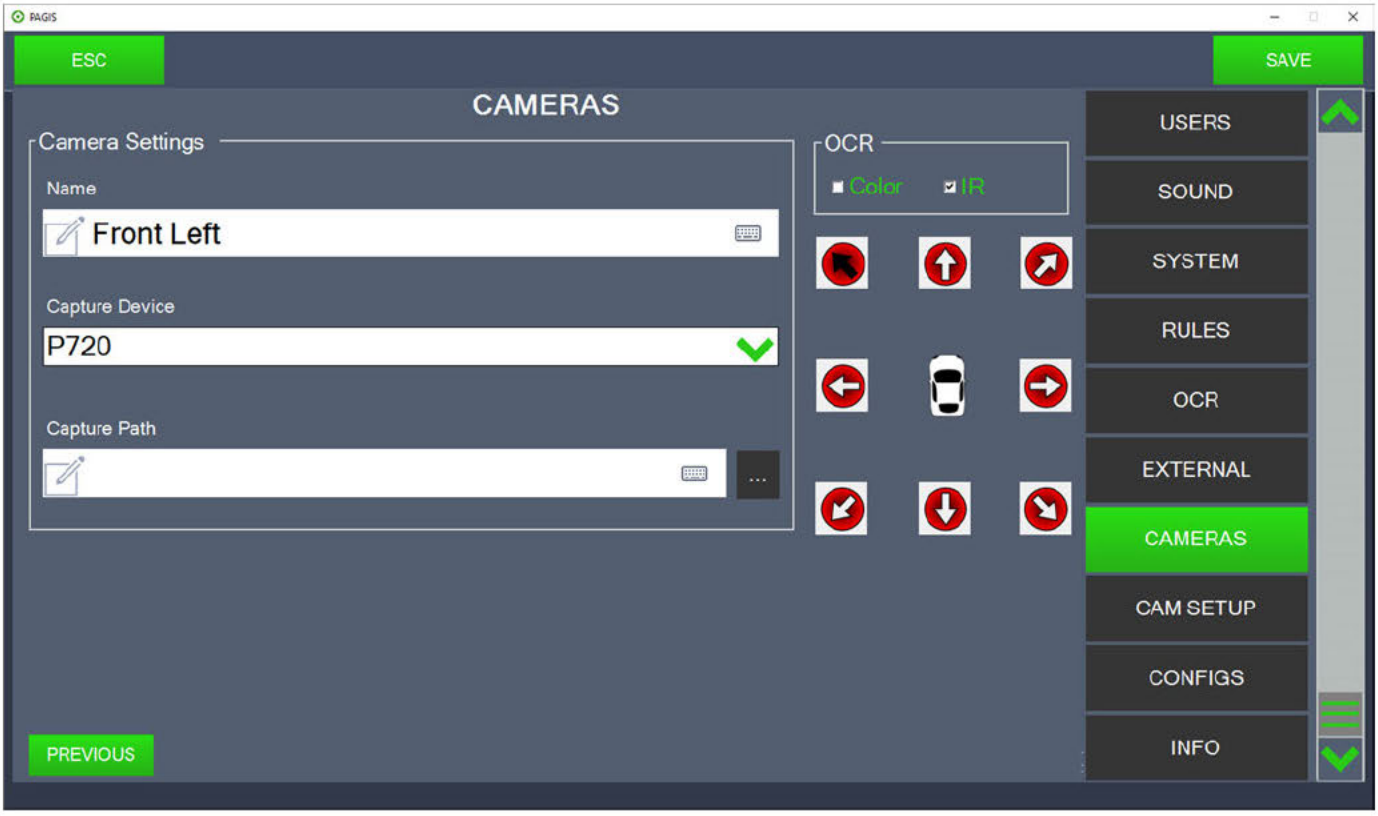
Gettings Started – Load Defaults:



1. Click the Load Defaults Button in the lower right portion of the Cameras Screen
2. Locate "Default" and click the Load Button LOAD
3. Once it's selected (and turned Green), click the Save Button (This returns the Admin to the Cameras Screen)
4. Click the Settings Icon to inspect and configure each camera one at a time

The Camera Settings (Edit) Screen:

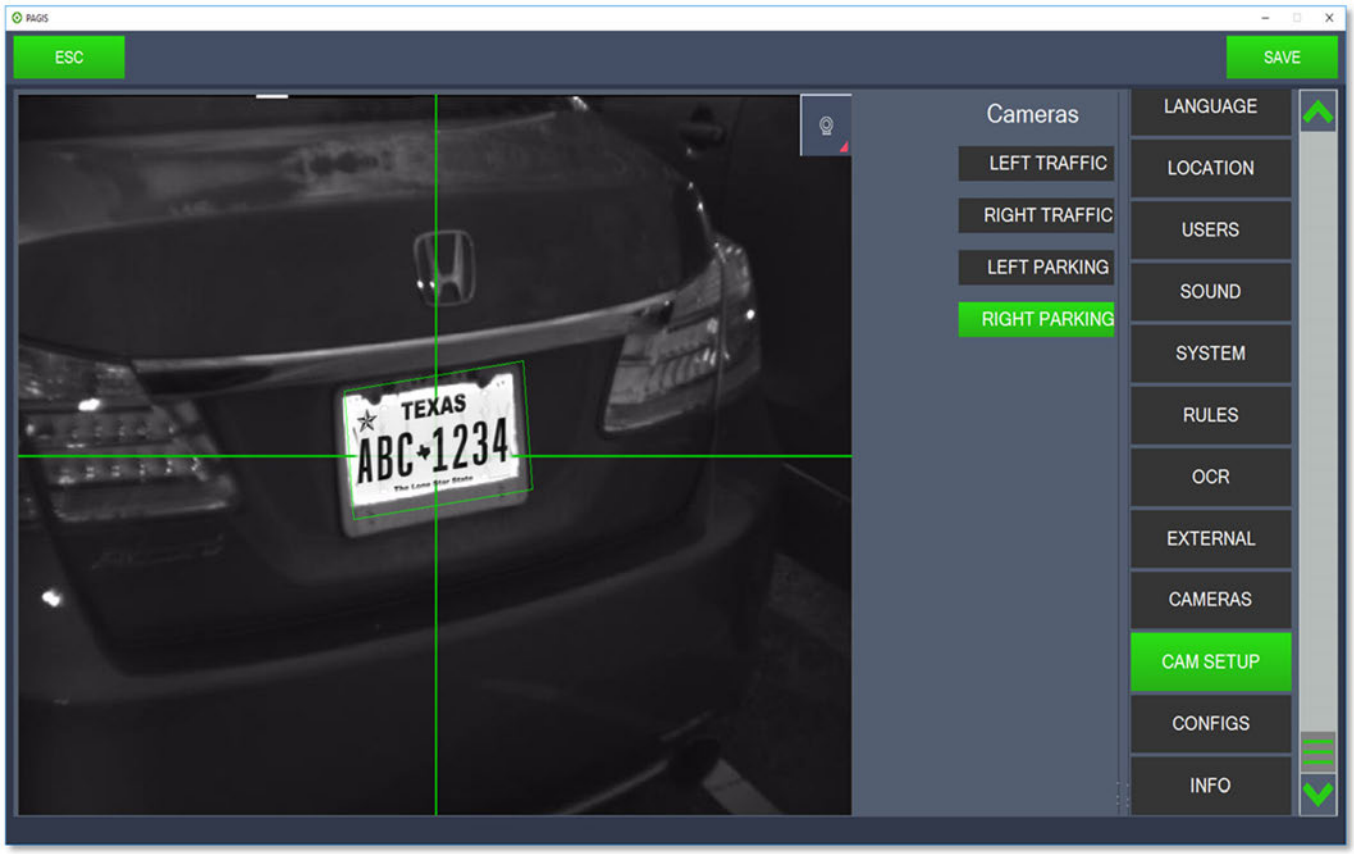
This provides the Admin a single screen to edit the name, confirm the capture device, assign camera position, and confirm OCR.



1. Confirm/Update the Camera Name **NOTE**: Use Camera Names with 11 characters or less to avoid various UI anomalies
2. Confirm the "Capture Device" field was auto-detected. If not, use the drop down to select the only Pxxx value on the list
3. Leave "Capture Path" blank (This is an optional field)
4. Select the camera mount position indicating the direction the camera is facing. The arrows turn black when selected
5. Ensure the OCR is set to IR. The color camera is used for OCR in only rare situations and will increase system load as well as the likelihood of false alerts. Use this setting with caution
6. Click the Save Button to retain the changes

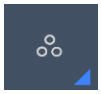
3.12 Cam Setup

The Cam Setup Screen presents Administrators with a live preview of the configured cameras. This section also allows the Admin to switch view modes from Color to IR to ensure the system is functioning properly. **NOTE**: This screen can also be utilized as a means to align newly mounted cameras when RDP access to the SX Processor is limited or unknown.



3.12.1 Cam Setup Navigation Buttons

The Admin may view the output of each camera by clicking on the camera name. When a camera is selected, the button will turn green to indicate it has been selected. In order to switch view modes, the Admin must use the following buttons:



Color View: The Color View Mode is the default view when the Admin first enters Cam Setup. This displays a live preview of the color camera.

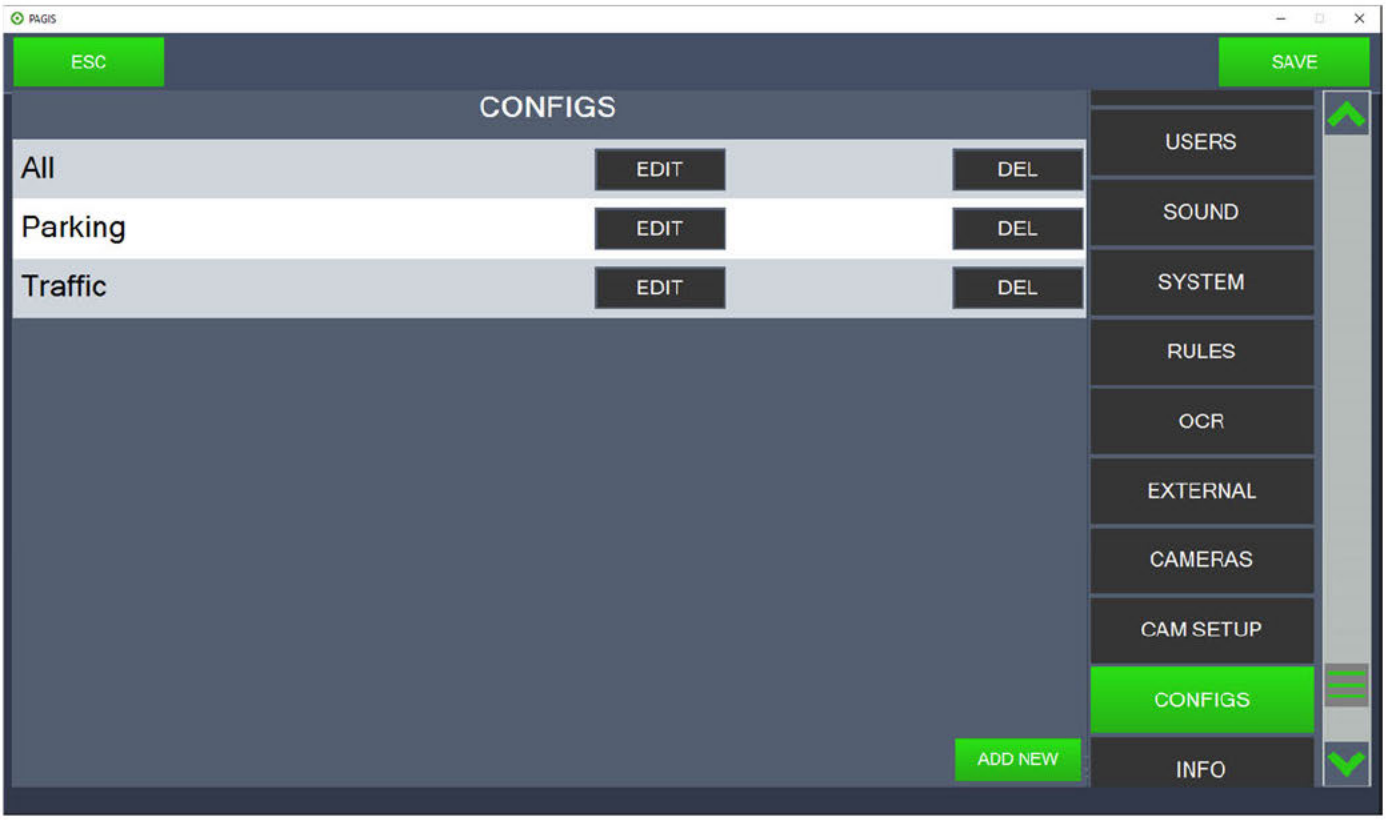


IR View: By clicking on the Camera View Selector button, the Admin will switch to the Infrared (IR) View Mode. This displays a live preview of the IR camera.

NOTE: Unlike the main Live View Screen, the camera feed shown on the Cam Setup page will not time out when in use. This feature makes it easier for the Administrator to review and align the mobile cameras.

3.13 Configs (Camera View Modes)

The Configs Screen allows the Admin to construct how the cameras will be displayed on the Live View Screen for the user. This section also allows agencies to create multiple viewing configurations to meet specific environmental needs or to add greater functionality to the software. By default, the Configs layout provides the agency with three camera modes, “ALL”, “Traffic” and “Parking”. All mode dipalys the front two cameras and rear two are activated, Traffic mode only displays the front two cameras and rear cameras are off, Parking mode only displays rear two cameras and front cameras are off.



3.13.1 Configs Navigation Buttons

To properly configure the camera modes used in PAGIS, the Admin will navigate this section with the following:



To delete a config/camera mode, click the DEL button to select it (turns Green) and then click Save



To review, edit, or modify a camera mode, click the EDIT button



To preserve changes or finalize a deletion, click the SAVE button

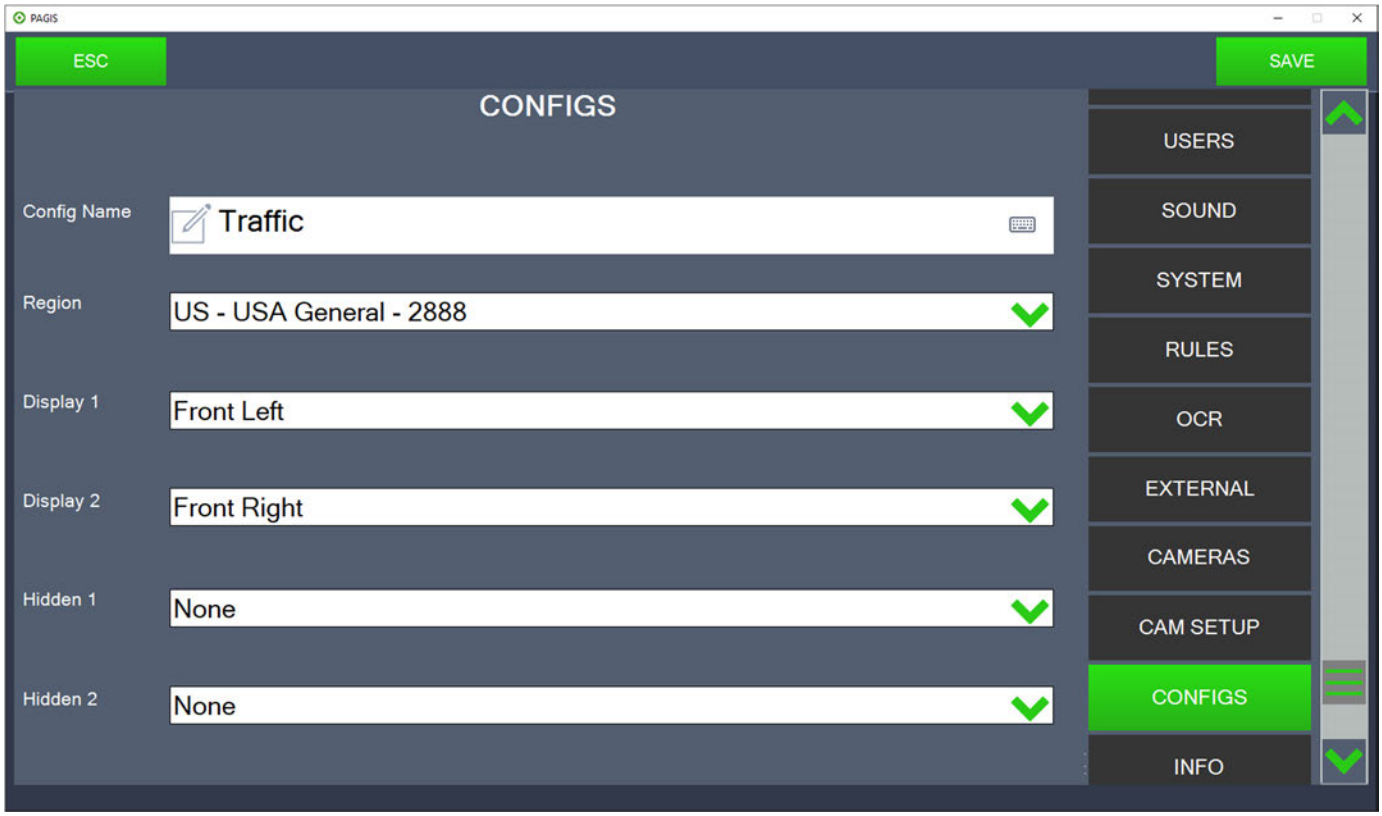


To add a new camera mode, click the ADD NEW button

NOTE: The number of Configs equals the number of Camera Modes available to the user from the Live View Screen. Each camera mode untilizes the Config name established in this section. Users cycle through the modes on the Live View Screen by clicking the Mode Selection Button in the upper left corner.

3.13.2 Reviewing and Modifying Existing Modes

When getting started, most Administrators will begin by simply modifying the existing camera modes or “configs”. The following example will demonstrate the standard configuration of a four-camera mobile unit.



1. Click the EDIT Button EDIT from the main Configs Screen to modify a mode
2. Review/Update the name of the Mode **NOTE**: The name should be intuitive for all users as this becomes the label of the mode selection button on the Live View Screen
3. Click the drop down arrow on the Region field to select the best local option (Adds additional accuracy to OCR)
4. Confirm the camera listed in the Display 1 field. This camera will be displayed on the left side of the Live View Screen
5. Confirm the camera listed in the Display 2 field. This camera will be displayed on the right side of the Live View Screen
6. Confirm the Hidden 1 field shows one of the other cameras not listed in the Display fields
7. Confirm the Hidden 2 field shows the last available camera not yet listed (Leave field as “NONE” for 3-cam systems)
8. Click the Save button to retain the changes
9. Click the Configs Button from the menu to access the other Mode(s)
10. Perform steps 1-8 for all Configs/Camera Modes available

NOTE: Cameras listed in the Hidden fields will function, perform OCR, and capture plate reads, but they will not be displayed to the user while in the named camera mode (unless a Hit is detected opening the Alert Screen). For ALPR units with more than two cameras, best practices dictate the Admin utilize these fields.

3.13.3 Adding a New Camera Mode

When the two default modes provided in the PAGIS software do not offer the agency all the functionality desired, the Administrator can use the Configs Screen to add additional camera modes. For example, if officers request a mode to view only the cameras on the left side of the vehicle while stopped on the side of the road, the PAGIS Adminstrator can build that functionality from this screen.



1. Enter a name for the new Mode (Ex. “Left Side”)
2. Click the drop down arrow on the Region field to select the best local option (Adds additional accuracy to OCR)
3. Confirm the camera listed in the Display 1 field. This camera will be displayed on the left side of the Live View Screen
4. Confirm the camera listed in the Display 2 field. This camera will be displayed on the right side of the Live View Screen
5. Confirm the Hidden 1 field shows one of the other cameras not listed in the Display fields
6. Confirm the Hidden 2 field shows the last available camera not yet listed (Leave field as “NONE” for 3-cam systems)
7. Click the Save button to retain the changes

3.14 Info

5435

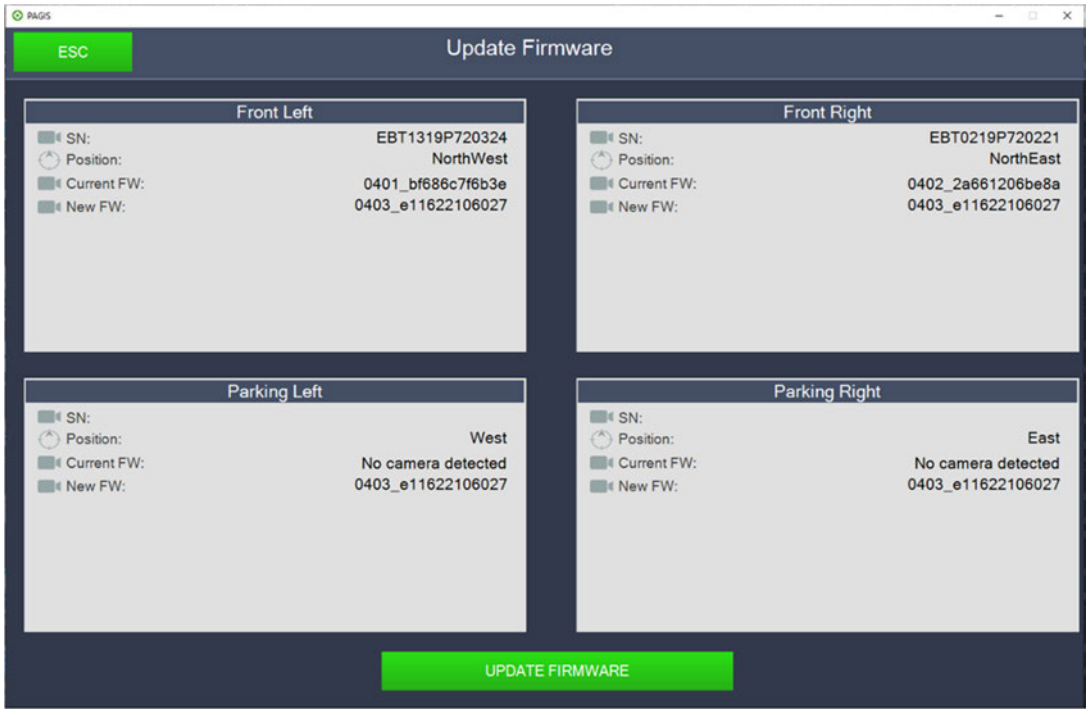
The Info screen displays additional information including the version number of the current installation. This information is helpful when contacting Technical Support.



3.15 Camera Firmware Update, (Admin)

Camera firmware update provides a means for PIPS to update the camera software to enhance and or correct camera performance. The frimware icon  will only apper when a update is avialable.

- The firmware update process only updates camera that are attached and function on the mobile processor.
- Administrator must log into PAGIS and apply the FW update. The update process takes around 4min and should not be interrupted or risk permanently damaging the cameras, PAGIS will return to normal opertaion after update.
- Once the "UPDATE FIRMWARE" button is clicked PAGIS will switch to full gray screen with message indicating "Camera Firmware is Updating", during this process you'll will notice small command windows opening on top of PAGIS, these windows represent the firmware being applied to each active camera so you may notice one or server depending. Once completed a message will appear "Firmware Updated Successfully" then PAGIS will return to normal operation.
- After FW completion and return to "Live View", its requiered to cycle thought the "Cam Mods" to refresh cameras.



Firmware Updater Window List.

- Title "Camera Name".
- Camera serial number.
- Position.
- Current FW version.
- New FW version available.

4.1 PAGIS System Requirements

The PAGIS Software requires the following minimum system requirements for the mobile data computer:

- Intel I3 CPU at 2.0 GHz or higher.
- Windows Operating System (Win7-Win10).
- Microsoft .NET Framework 3.5.
- 8 GB of RAM.
- At least 1 GB of free disk space.
- SVGA display with a minimum resolution of 800 x 600 pixels.
- Available 10/100 Ethernet port.
- Keyboard and mouse, or a touch screen monitor.
- Internet access needed for mapping and Firmware update.

4.2 PAGIS Prerequisites

Prerequisites:

1. Ability to install software.
2. Ability to configure the network adapter.
3. PAGIS 2.12 and above are only compatible with SX4 and SX4e Processors.

Network Adapter Settings:

The PIPS mobile processor operates based on a static IP and is preassigned the IP address of 192.168.200.201. When connecting laptop/MDC to the PIPS mobile processor your computer must be on the same IP network as the mobile processor, in fact the connecting compute must adopt one octet lower than the assigned IP of the PIPS processor in order for MDC installed PAGIS to connect to the mobile processor and receive data from the ALPR cameras. Below are the steps to configure your computer.

1. Navigate to Adapter Options in Windows and right click on the adapter and select properties.
2. Click to select IPv4 and click Properties
3. Click the radio button “Use the following IP Address” to set the Static IP address.
4. Enter 192.168.200.200 in “IP address” section.
5. Enter 255.255.255.0 in “Subnet mask” section.
6. Either leave the “Default gateway” blank or enter 192.168.200.201.
7. Click OK to save changes.

NOTE: The Mobile processor is pre-configured to relay its camera data connection to the .200 IP address, using alternative IP’s on Laptops will result in the software’s failure to communicate with the cameras.

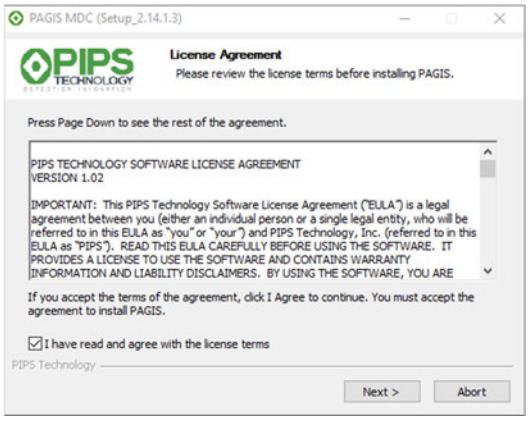
4.2.2 PAGIS Software Installation (MDC)

5437

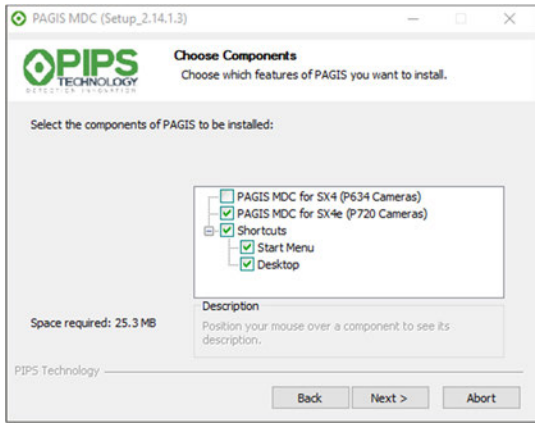
1. If PAGIS exist on your computer, it must be version 2.9 or 2.12 for installer to update. If your version of PAGIS is older it is recommended you “EndShift” any existing data, then uninstall PAGIS.
2. It is recommended you “EndShift” any existing data if upgrading a previous version of PAGIS.
3. Prior to software installation, take the time to figure out what version of PIPS mobile processor you have as the software installation requires you to select so it can properly configure the camera settings based on processor type. PAGIS version 2.14 supports processor versions SX4 & SX4e only, you can either look at the product tag located on the processor or look at the camera IO ports on the back of the processor, if the 4 camera IO ports are vertically arranged RJ45’s then it’s a SX4e, if they are vertically arranged circular shaped “LEMO” connectors then it’s a SX4. Horizonal arranged circular shaped “LEMO” connectors is a SX3 and is not compatible with PAGIS 2.14.
4. When upgrading to PAGIS V2.14.x.x also requires that the PIPS mobile processor be updated to same version in order to take advantage of Firmware update.



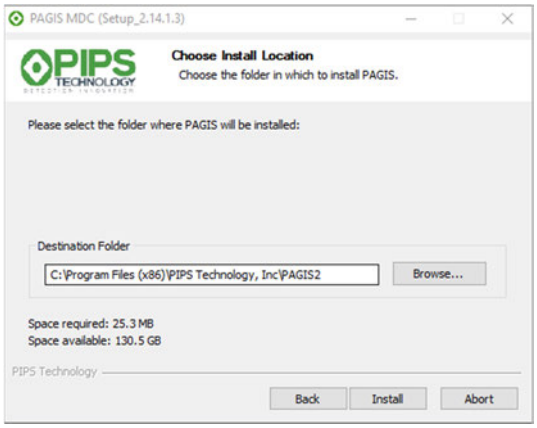
5. Place the PAGIS installer on your computer’s desktop, “PAGIS_Setup_MDC_2.14.x.x.exe”.
6. Right click the PAGIS installer executable and select “Run as administrator”.



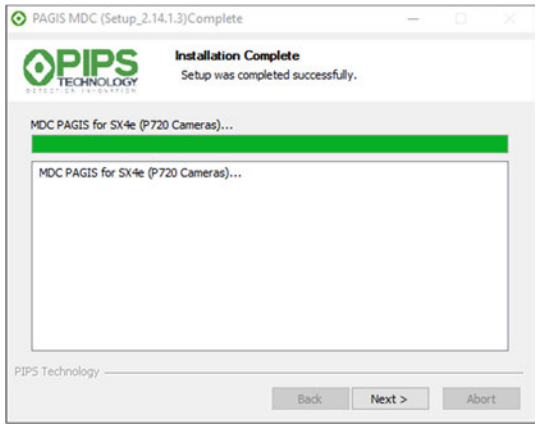
7. Check the license agreement box, then click Next.



8. Select the mobile processor type and alter “Shortcuts” if needed. Next to continue.



9. Confirm path if upgrading, click Install to proceed.



10. Installation Compete, Next to proceed.
11. Click Finish.
12. Click Yes to reboot if you would like to test PAGIS auto start at login if selected during installation, otherwise click No as its not required for PAGIS to run.

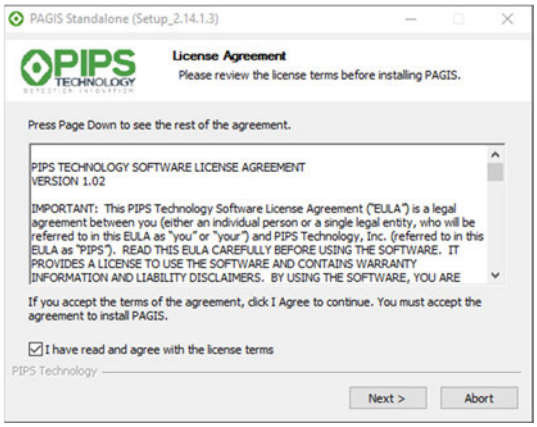
Note: See Appendix A for terminology definitions.

4.2.3 PAGIS Software Installation (Mobile Processor)

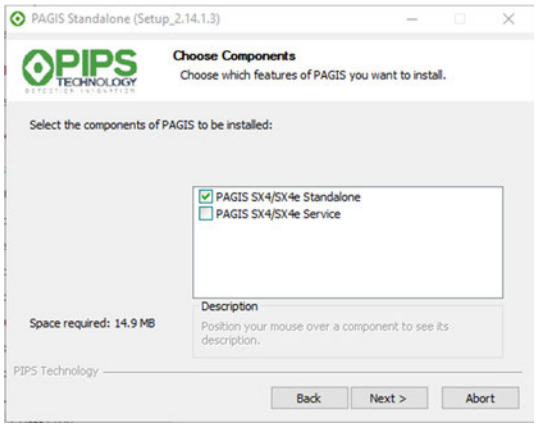
1. PAGIS v2.14.x.x updater is only compatible with PIPS mobile processors SX4 & SX4e.
2. The PAGIS updater only updates existing versions of PAGIS on mobile processor, version 2.9 and newer.
3. Update required for both “Standalone” & “Service/VPRelay” to support some of the newer features.
4. The processor must be in its respective mode to update that option as the folder path are hidden when not active, see “Change Mode” in SX4 or SX4e manual.



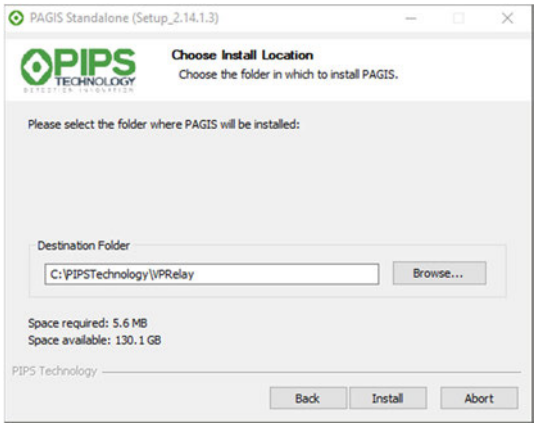
5. Remote desktop into processor or utilize attached monitor/keyboard.
6. Place the updater in C:\PIPSTechnology folder on the PIPS mobile processor.
7. Execute PAGIS Updater.



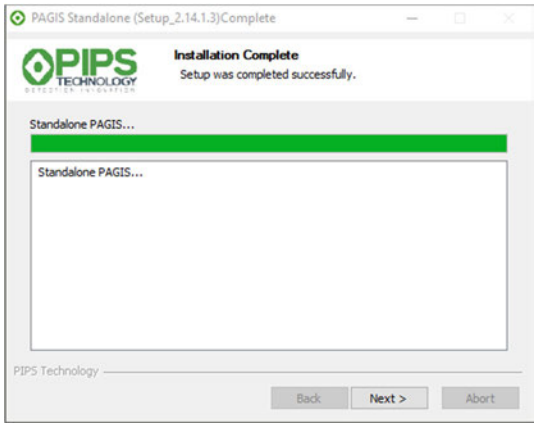
8. Check the license agreement box, then click Next.



9. Select option to update, next to continue.
   - Standalone= PAGIS login from Processor.
   - Service= PAGIS login from connected Laptop.



10. Change the default path presented by updater, see below.
    - For “Service” C:\PIPSTechnology\VPRelay.
    - For “Standalone” C:\PIPSTechnology\Standalone.



11. Installation Compete, Next to proceed.
12. Click Finish.
13. Click Yes to reboot.

Note: See Appendix A for terminology definitions.

TROUBLESHOOTING TIPS

This section provides some basic troubleshooting tips and information

5.1 Troubleshooting & Tips

- The first login to PAGIS after the new install of an unconfigured version does not require a username or password. Simply click Login to be granted Admin access to the software.
- A good means to test the communication from the MDC to BOSS is ping or telnet (over TCP 8092) through the command prompt.
- A good means to test the communication from the MDC to the SX Processor is ping or telnet (over TCP 9000) via command prompt.
- For many other troubleshooting tips, see Appendix C – Frequently Asked Questions

5.1.1 PAGIS with NetMotion VPN

Agencies utilizing NetMotion VPN software on the MDC will need to apply the following passthrough steps:

1. Login to the NetMotion server as administrator
2. Click Settings > Then select Client > Select Global Client Settings > Then select Passthrough List
3. Click the “Add…” button on the right > Select “Network Address”
4. Enter the following settings (as shown):
    A. IP address:192.168.200.0 (the zero is correct, it's an IP address “range”) Subnet Mask: 255.255.255.0.
    B. Keep all other settings default (as shown) and click OK.
5. The MDC must then disconnect from NetMotion and reconnect again for the settings to be applied locally.

5.1.2 Cisco VPN Client:

Make sure Stateful Firewall is unchecked and "Allow Local LAN".

5.1.3 Microsoft .NET 3.5 Installation

The PAGIS Software requires Microsoft .NET Framework 3.5 specifically. If the MDC doesn’t have .NET, it can be downloaded from the Microsoft website.

5.1.4 Firewall Settings for Client-Server Installations

For client-server installations, the Windows Firewall needs to allow the SX Processor and the MDC to communicate. If the MDC is maintained by a Network Administrator, he or she should be contacted before making changes to the firewall. The command prompt commands for the exceptions are below

Option 1: Allow Microsoft Windows Version 8 or newer to auto-detect the launch of the PAGIS.exe application and use the wizard to add the PAGIS.EXE to the exception list (making note of Public or Private Network settings as necessary).

Option 2: Add PAGIS to the exception list manually by browsing to the install path of PAGIS. The default is below for reference: C:\Program Files (x86)\PIPS Technology, Inc\PAGIS2\PAGIS.exe

Option 3: Add the communication ports manually:
TCP in/out 8092 = Pagis sync port to BOSS back office software.
TCP in/out 9000 = Mobile processor camera feed port.
TCP in/out 9001 = Mobile processor camera snapshot port.
TCP in/out 32023 = Mobile processor camera setup port.
TCP in/out 10000 = Mobile processor data capture port.
NOTE: XML Datastream uses TCP 10100 and TCP 7000

PAGIS/BOSS3 CONFIGURATION 5440

In order for the PAGIS software to function properly, the device must be built, enabled, and configured in BOSS3 before being deployed for service in the field.

6.1 Creating a New Device in BOSS3

Once network communication to BOSS3 has been established from the vehicle, the new device must be "built" or added to the Device List in BOSS3 before it can be used. The approved way to do this, is to simply perform a Begin Shift from the PAGIS software. **NOTE**: The computer name is what will be displayed in BOSS as device name.

1. At the PAGIS Live View Screen, click the Begin Shift button once to select it, and then click again to launch the sync.
2. If the laptop has previously been setup to communicate with BOSS and is already enabled, the sync transfer window should appear in the middle of the Live View Screen.
3. If this is a new/disabled device, a message indicating "HttpStatusCode" will be displayed.
4. This indicates the BOSS3 server has received the sync request but has rejected it due to device status.
5. Once the BOSS Admin has enabled the device, the Status Code error will not appear again, and syncs should complete as configured in BOSS3.

6.2 Enabling a New Mobile System in BOSS3

Installing PAGIS and configuring the network settings is only the first step in making the ALPR unit operational. Once PAGIS is configured to work with or on the SX Processor and the mobile cameras, it must then be enabled in BOSS3 before synchronizations can take place. **NOTE**: By default, every new device recognized by the BOSS3 server is disabled until the Admin enables it. This is done for security.

1. Log into the BOSS3 UI Client Software with Admin privileges.
2. Click the Admin button on the left to expand the options.
3. Click the Devices button. The new device should now be listed to the right.
4. Click the name of the Device to select it. (This will open the device details screen)
5. Click the Edit button at the bottom of the window.
6. Click the Enable button from the Edit window.
7. This will enable the device and return the Admin to the Device List.

NOTE: If desired, the Admin can re-enter the Edit window to assign an alternate name in BOSS3 for the new device. The Admin will need to update the "Description" field and then click the Save button. Agencies commonly use this field to signify the Unit number, Car name, or Patrol Shift. The "Name" field is the device/host name and cannot be edited in BOSS3.

NOTE: Once the Device is enabled the Admin needs to assign ownership and hotlist distribution.

6.3 Assigning Ownership to a Device in BOSS3

Every new device added to BOSS3 allows for Admin level access into PAGIS without the use of a username or password. In order to password protect the PAGIS software, the BOSS Administrator must assign "Owners" to the device in BOSS3.
NOTE: For more detail on Users, User Groups, Sites, and Roles, refer to the BOSS3 manual.

1. Login to the BOSS3 UI with Admin credentials.
2. Click the Admin button on the Left to expand the options.
3. Click Devices to review the list.
4. Click on the Device Name to open the device details screen.
5. Click on the Edit button.
6. Locate the "Owners" field. Click the Select button to the right.
7. Check the box(es) for the appropriate Site(s)/User Group(s). **NOTE**: This tells BOSS3 which sets of users will have rights to login to PAGIS from this specific device.
8. Notice the Select button has changed to a Save button. Click Save to retain changes.
9. Confirm the changes show in the Owners Field.
10. Click the Save button at the top left of the Edit window.

6.4 Assigning Hotlists to a Device in BOSS3

In order for the PAGIS users to receive alerts, one or more of the stored hotlists in BOSS3 must be distributed to the new device.
NOTE: For more information on building and configuring Hotlists, refer to the BOSS3 manual.

1. Login to the BOSS3 UI with Admin credentials.
2. Click the Admin button on the Left to expand the options.
3. Click the “Hotlists” button to review the list of configured alert lists.
4. Click the Hotlist Name to select the first alert list. This will open the Details screen.
5. Click the Edit button at the bottom of the window.
6. Locate the “Deployment” field. Then click the Select button to the right.
7. Check the box next to the name of the new device.
8. Notice the Select button has changed to a Save button. Click Save to retain the changes.
9. Confirm the changes show in the Deployment Field.
10. Click the Save button at the top left of the Edit window.
11. Perform these steps again for all remaining Hotlists necessary for this device.

PAGIS/BOSS4 CONFIGURATION

In order for the PAGIS software to function properly, the device must be built, enabled, and configured in BOSS4 before being deployed for service in the field.

7.1 Creating a New Device in BOSS4

Once network communication to BOSS4 has been established from the vehicle, the new device must be “built” or added to the Device List in BOSS4 before it can be used. The approved way to do this, is to simply perform a Begin Shift from the PAGIS software. **NOTE**: The computer name is what will be displayed in BOSS as device name.

1. At the PAGIS Live View Screen, click the Begin Shift button once to select it, and then click again to launch the sync.
2. If the computer has previously been setup to communicate with BOSS and is already enabled, the sync transfer window should appear in the middle of the Live View Screen.
3. If this is a new/disabled device, a message indicating “HttpStatusCode” will be displayed.
4. This indicates the BOSS4 server has received the sync request but has rejected it due to device status.
5. Once the BOSS Admin has enabled the device, the Status Code error will not appear again, and syncs should complete as configured in BOSS4.

7.2 Enabling a New Mobile System in BOSS4

Installing PAGIS and configuring the network settings is only the first step in making the ALPR unit operational. Once PAGIS is configured to work with or on the SX Processor and the mobile cameras, it must then be enabled in BOSS4 before synchronizations can take place. **NOTE**: By default, every new device recognized by the BOSS4 server is disabled until the Admin enables it. This is done for security.

1. Log into the BOSS4 URL with Admin privileges.
2. Navigate to the Resources pulldown menu.
3. Select Devices from the menu options. The new device should now be listed.
4. Click the name of the Device to select it. (This will open the device details windows on the left)
5. Click the Enable slide toggle to enable device, located in upper right of device edit window then click save.
6. This will enable the device, synchronization between BOSS4 and PAGIS is allowed.

NOTE: Once the Device is enabled the Admin needs to assign ownership and hotlist distribution.

7.3 Assigning Ownership to a Device in BOSS4

Every new device added to BOSS4 allows for Admin level access into PAGIS without the use of a username or password. In order to password protect the PAGIS software, the BOSS Administrator must assign “Owners” to the device in BOSS4.

NOTE: For more detail on Users, User Groups, Sites, and Roles, refer to the BOSS4 manual.

1. Login to the BOSS4 URL with Admin credentials.
2. Navigate to the Resources pulldown menu.
3. Select Devices from the menu options. The new device should now be listed.
4. Click the name of the Device to select it. (This will open the device details windows on the left)
5. Locate the “Owner” field. Click in the Owner filed, and a list of all available Groups will appear.
6. Select group by clicking on it, it will then automatically be added to owners, see list below “Owner”.
7. To add mode groups, repeat step 15.
8. Confirm the changes show in the Owner Field.
9. Click the Save button at the bottom right of the Edit window.

7.4 Assigning Hotlists to a Device in BOSS4

In order for the PAGIS users to receive alerts, one or more of the stored hotlists in BOSS4 must be distributed to the new device.

NOTE: For more information on building and configuring Hotlists, refer to the BOSS4 manual.

1. Login to the BOSS4 URL with Admin credentials.
2. Navigate to the System pulldown menu.
3. Select Hotlists from the menu options
4. Click the Hotlist Name to select the first alert list. This will open the Details screen.
5. Locate the “Deployment” field.
6. Check the box next to the name of the new device listed.
7. Click the Save button at the bottom right of the Edit window.
8. Perform these steps again for all remaining Hotlists necessary for this device.

APPENDIX A: THE GLOSSARY

5443

ALPR/ANPR	"Automatic License Plate Recognition/Automatic Number Plate Recognition".
BOSS	"Back Office System Software". This is the ALPR server.
GPS	"Global Positioning System".
GUI	"Graphical User Interface".
Hotlist	A database or list that contains vehicle license plates of interest ("alert list").
IR	Infrared light.
License Plate	Also called a tag or number plate.
MDC	"Mobile Data Computer". This is the tablet or laptop in the vehicle.
OCR	"Optical Character Recognition" (also referred to as a "cardet").
OS	"Operating System".
PAGIS	This is the License Plate Capture Software most commonly used in an ALPR vehicle.
Service	Operation mode of the PAGIS software. Service or "VPRelay" is used to refer to PAGIS instance that is running directly on the PIPS mobile processor without a GUI interface, this mode is intended to run in conjunction with MDC version of PAGIS installed on laptop connected via Ethernet.
Standalone	Operation mode of the PAGIS software. Standalone is used to refer to PAGIS instance that is running directly on the PIPS mobile processor with a GUI interface. Same a "Service"
SX	SX is a short notation referencing PIPS's mobile processor, commonly the SX is followed by the generation number of the processor, i.e. SX3, SX4 & SX4e.
UI	A "User Interface" is the means in which the user can access and navigate the software.
USB Flash Drive	Also called a thumb drive or memory stick.
VLP	"Vehicle License Plate".
VPN	"Virtually Protected Network".
VPRelay	Operation mode of the PAGIS software. VPRelay or "Service" is used to refer to PAGIS instance that is running directly on the PIPS mobile processor without a GUI interface, this mode is intended to run in conjunction with MDC versions of PAGIS installed on laptop connected via Ethernet.
Whitelist	Opposite of a standard BOSS Hotlist. This is a list of license plates that should not trigger an alert.

APPENDIX B: PAGIS SOFTWARE DATABASE FILE

This section is used to configure the PAGIS Software when it's not being used with the Back Office System Software (BOSS). Comma-separated value (CSV) format is the only format the PAGIS Software supports for importing data into the vehicles for the purpose of matching against the captured license plate data. PAGIS will support CSV files with any number of columns, called "fields", as long as the first field is the VLP (Vehicle License Plate). **NOTE**: The CSV format is standard ASCII.

Example CSV Files:

1. *ABC123, Red, Ford, Explorer, 1996, WANTED XYZ456, Blue, Audi, A4, 2001, MURDER*
2. *45ABC234, Vehicle wanted in associated with a kidnapping on 12/5/2005 995BD233, Vehicle reported stolen from Liz's Lounge at 6am on 12/1/2005*
3. *UIO223 ABC123*

General Function:

PAGIS calls/utilizes files in pairs. Each database in PAGIS is created using two files; a CSV file, and an INI configuration file. Without both of these files, the database will not load and PAGIS will not "see" it. Each CSV file/hotlist must have the exact same name as the INI configuration file. Example: Stolen.ini and Stolen.csv will work. Stolen.ini and Plates.csv will not.

Reading an INI Configuration File

Lines that appear in brackets [] are called "Headings". The labels that appear inside the headings, are called "values". Values will always contain an equal sign (=). If a line starts with a semicolon, it is considered to be a comment and is not read by the software. There is no limit to the number of comments in the INI file.

The [SETTINGS] Heading

The values in the Settings heading are: NumFiles, DbName, DbColor, Priority, Covert, Alarm, and NumFields.

- NumFiles: Determines how many database files the system should split the specified hotlist into. Generally, this value is set to 1. But for larger hotlists (200,000+ lines), a number of 2-5 may be more desirable.
- DbName: Tells the PAGIS Software what the displayed name of the hotlist should be.
- DbColor: Sets the display color of the hotlist. This is merely an esthetic setting and not a functional setting. The right-hand side of the equal sign is the HEX value representing the ARGB values for the color. If this value is unknown, the Admin should simply leave this line out of the file.
- Priority: Designates the priority of this hotlist in relation to other hotlists in the system. The highest priority database is 1 and the lowest is 999. **NOTE**: if a plate resides on multiple lists the higher priority will be alerted first.
- Covert: Determines whether standard PAGIS Software users are alerted when a hit is made from the database. Covert database can be used for hotlists that are included for information-gathering purposes rather than eliciting user intervention. The system can also be configured to notify via email or SMS message when a hit is made from a covert hotlist.
- Alarm: Sets the audible alert to be played in PAGIS when a hit is made from the hotlist. Values for Alarm are LOW, MED, HIGH
- NumFields: Indicates how many fields (columns) are in the CSV file. If this value is less than the actual number of fields in a file, then the additional fields are placed in the general information area. This value also determines the number of headings of the [Field x] present in the file. For example, if NumFields=2 then there will be two additional headings, [Field 0] and [Field 1]. **NOTE**: Adding "Creation =" will place the timestamp the hotlist was added to the Begin Shift file.

The [FIELD X] Heading

Under the Field heading, there are two configurable values, “Name” and “PAGIS”.

- Name: Tells the system what the name of this field is. If no name is specified, then no name given to the field. The format is Name = <field>
- PAGIS: Specifies how to display the field in the GUI/PAGIS Software.
    - If no value is defined, the field is placed as general information.
    - Values 1-5 represent special fields for the PAGIS Software that translate to the information being displayed in a box of its own when a hit is processed.
    - A value of 6 represents an ID number to cross reference the vehicle from the hotlist with a person from the wanted list.
    - A value of 7 is identical to leaving the value undefined.

Sample INI Configuration File

[Settings] NumFiles=1
DbName=Stolen Vehicles DbColor=ffffff00 Priority=5 Covert=False Alarm=MED NumFields=8
;PAGIS Values
;0 is VRM / VLP (Not User Definable, always Field 0)
;1 is Special Field 1
;2 is Special Field 2
;3 is Special Field 3
;4 is Special Field 4
;5 is Special Field 5
;6 is ID Number (PNC ID, Drivers License, Social Security Number, etc.)
;7 is General Info (Default for all undefined fields) [Field 0]
PAGIS=VRM

Sample INI Configuration File

[Field 0] Name=VRM
[Field 1] Name=Color
PAGIS=3 [Field 2]
Name=Make PAGIS=1
[Field 3] Name=Model
PAGIS=2 [Field 4]
Name=Action PAGIS=4
[Field 5] Name=Warning
PAGIS=5 [Field 6]
Name=PNCID PAGIS=6
[Field 7] Name=Intelligence PAGIS=7

APPENDIX C: FAQ

Q: **HOW DO I ENTER A SUPPORT CASE?**
A: We have a webform you can use here, you can email our Support Team at Support@PIPSTechnology.com, or you can call us on the phone Monday-Friday 8am to 4pm Central Time (9am-5pm Eastern) at (833) 747-7577 Option 2.

Q: **HOW DO WE CREATE USERS IN PAGIS?**
A: The agency BOSS Administrator creates all users, both for BOSS and for PAGIS. Once the user is created in BOSS, the Admin would click the user's name to select/edit the user. Then click the Advanced button and update the PAGIS specific password. Please note that the username and password fields are both case sensitive and the PAGIS users need to be added to a group with the Role that allows them to use PAGIS/LPCS.

If you have any further questions, please feel free to enter a request for support here.

Q: **WHERE DO USERS CHANGE THEIR LOGIN PASSWORD IN PAGIS?**
A: User passwords are created and updated in BOSS via the UI client software. For the majority of our customers using both the PAGIS Software and BOSS, any user accounts or passwords created in the PAGIS Software itself will be overwritten by the user information defined in BOSS during the next sync.

If you have any further questions, please feel free to enter a request for support here.

Q: **HOW DO WE REQUEST AN RMA REPAIR?**
A: To assist with this, please navigate here to review our RMA procedure as well as to download the request form. Please keep in mind that once submitted, all repairs are reviewed for age of equipment and warranty status before final processing takes place. Additionally, incomplete forms and those without much detail often result in processing delays.

If you have any further questions, please feel free to enter a request for support here.

Q: **WE GOT NEW MDC LAPTOPS IN THE PATROL CARS, HOW DO WE ADD THOSE DEVICES TO BOSS?**
Q: **HOW DO WE EDIT THE DEVICE NAMES IN BOSS?**
A: The initial device template/skeleton is automatically created in BOSS the first time the device attempts to Sync from the field. Devices should NEVER be created manually. For PAGIS laptops, this is done after PAGIS is installed and configured and Begin Shift is launched. However, if the agency would like to organize the device list by updating the "Device Name" field, those steps are below:
1. Login to the BOSS UI with Admin rights
2. Navigate to Admin > Devices
3. Click on a device name to select it > Click Edit
4. Update the name of the device in the "Description" field (Name field cannot be altered)
5. Click Save > This will take you back to the Device Summary List. The "Device Name" field should show the new name

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **WE HAVE A NEW MOBILE COMPUTER/MDC THAT'S NOT SYNCING WITH BOSS.**
Q: **WE KEEP SEEING AN HTTP_STATUS_CODE ERROR WHEN RUNNING BEGIN SHIFT.**
A: This error most commonly means that a new device in the field (laptop/tablet) can "see" the BOSS server, but that it hasn't been enabled yet to "talk" with it. Follow the general steps below to address this issue:
1. The agency BOSS Administrator will need to login to the BOSS UI client and Select Admin
2. Then select Devices and from there, left click on the device/computer name of that MDC to edit it
3. Once in the Edit screen, Enable the device. This will take you back to the Device List.
4. Click the name to edit the device again. Now assign users/Owners and save.
NOTE: The Select button becomes a Save button when selecting which Groups/Users should have access to login to this device
5. Once that is done, navigate to Admin > Hotlists
6. From here, click on each hotlist one at a time to distribute them to the new device being sure to Save the changes next to the Distribution field. Note again that the Select button becomes a Save button. And there's another Save button at the top left of

the edit window.
7. After this is complete, perform Begin Shift from the field unit/MDC and confirm there are no further errors. [5447]

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **NEW PAGIS USER CAN'T LOGIN BUT OTHERS CAN.**
Q: **USERS CAN LOGIN TO PAGIS WITH NO CREDENTIALS AT ALL.**
A: Entry or login to the PAGIS software in the field is partially controlled by the Device settings in BOSS. The users themselves must also be properly setup with an LPCS/PAGIS password. To check the current device settings/ access, perform the following steps:
1. Login to BOSS UI (with Administrator rights)
2. Select the Admin Section
3. Select Devices and then Select the Device in question by PC name
4. Once selected click on the Edit button near the bottom
5. Locate and inspect the "Owners" Field (this is a list of users/groups that have access to login to the device)
NOTE: If this field is blank, the device is in an open configuration mode allowing admin level access simply by clicking login (any credentials would also be accepted).
6. To update the device owners, click the "Select" button next to the Owners field (notice it changes to a Save button)
7. Check which Users/Groups of Users should be able to login to PAGIS from this device
8. Click the Save button next to the field
9. And then click Save in the upper left portion of the Edit window
10. Have a previous user or Admin login to PAGIS and perform Begin Shift to sync the new data
11. A PAGIS Admin can confirm by navigating to Admin, Admin, and then Users to review the list
12. Another test would be to have the new user attempt to login

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **WHEN USERS LOGIN TO PAGIS, THEY ONLY SEE A GREY SCREEN.**
Q: **CAMERAS AREN'T SHOWING UP IN PAGIS ANYMORE.**
SEE ALSO: "THE LINK LIGHTS ON OUR ALPR COMPUTER/MDC WON'T TURN ON OR FLASH"
A: Below are some basic troubleshooting steps you'll want to follow before creating a support ticket.
1. Doublecheck the physical power switch on the black box/Processor is On. In many vehicles, there is also an in-line switch in the front of the vehicle that needs to be switched On. When the units are properly powered and on, you should see lights and hear fans running.
2. Confirm that the network adapter settings on the laptop match the proper Static IP scheme for the SX Processor in use. The older scheme is 192.200… and the newer scheme is 192.168…. NOTE: the adapter status in Windows should say "unidentified network". If it says "cable unplugged" the laptop can't "see" the SX.
3. If the power and Static IP settings are good and things still aren't working, test further by disabling the three main software related culprits. Turn off/bypass the local Windows firewall, antivirus, and VPN software one at a time.
4. If you're still not able to see the camera feed after that, you may want to use a different network cable as those can get damaged over time and then confirm that the cord is properly plugged into the ports.
5. If the network cord from the SX Processor is routed through a docking station, then it's possible the dock is preventing the traffic. You should contact the dock's manufacturer for the most recent firmware. To test for this, remove the laptop from the dock, directly connect the network cord to the laptop, and then reconfigure the network adapter settings (remove the static settings from the dock's adapter/ and assign the static IP to the laptop's NIC adapter).

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.
Q: **THE LEFT FRONT CAMERA ON OUR ALPR VEHICLE IS NO LONGER SHOWING IN PAGIS**?
Q: **HOW DO WE TROUBLESHOOT MOBILE CAMERAS**?
A: Below are the main troubleshooting steps to test the camera(s) and cable(s) on a system where only one or two cameras are no longer displaying images.
Step 1: Confirm MDC/SX communication - steps shown in section "Cameras aren't showing up in PAGIS anymore."
Step 2: Access the SX Processor – RDP or directly connect a monitor, keyboard, and mouse to the SX. Contact PIPS Support for

help with RDP if the credentials are unknown to the agency.
Step 3: Confirm camera activity – Launch Tools. Then open P6Utility or Mobile Toolkit. Check the camera feeds/function by switching the Input menu to the camera(s) in question
Step 4: Unplug and Reattach the Camera Cables – Note, the cables DO NOT TWIST. The metal locking nut on the cable slides back about a millimeter and the cable comes straight out. Do this at the SX Processor and the Camera. You may need to remove the camera from the mount in order to unplug the cable successfully (most brackets use a #3.5 Hex/Allen Wrench)
Step 5: Swap Port on SX Processor – At the SX Processor, swap the camera cables from the non-working camera to a port with a working port (Take care to note the swap so the cables get back to their original ports). If the camera outage stays at the port site, the issue is most likely the capture card on the SX Processor and will require RMA (Example: working Left cam is swapped to port of non-working Right cam and no longer functions. AND the previous non-working Right cam starts working once it's plugged into the Left cam's port). If the fault/error stays with the camera regardless of SX port, continue to Step 6.
Step 6: Physically Swap Camera Locations – Once all other items are checked, move the camera itself to a working position in order to test the cable. (Example: physically move Left cam to the Right cam position on the top of the vehicle) Connect the cable at the new position and test feed in Tools > P6Utility/Mobile Toolkit. If the camera works at the new location, the issue is most likely a bad cable. If the camera still does not work, the issue is most likely a faulty camera in need of repair/RMA.

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **WE'RE NO LONGER GETTING GPS IN PAGIS.**
Q: **WE'RE NOT SEEING GPS DATA FROM SOME OF OUR FIELD UNITS IN BOSS.**
A: Below are the basic troubleshooting steps for checking the GPS of field units:
1. Login to PAGIS (as Admin)
2. Navigate to Admin section, then click the Admin button
3. Select "System" on the left pane
4. Confirm/Set the button at top to "Default"
5. Remove any value(s) stored in the GPS Connection String field. Leave '5' in the Computer String.
6. Click the Save button to retain changes made.
7. Close PAGIS fully and relaunch and log back in to test (Note: GPS will only show with test reads/hits)
8. For versions of PAGIS 2.9 and up, test with a GPS Connection String of 6 if the blank field doesn't work. Save the changes. Log out. Close the software and then relaunch to test.

Please be advised, that some GPS issues can be caused by local or domain firewall settings, antivirus software, or any other software package monitoring/transmitting network data. To test these, disable or bypass those software options on the MDC and retest.

If these initial troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **HOW DO I INSTALL THE PAGIS SOFTWARE?**
Q: **I JUST LOADED PAGIS ON A MACHINE AND IT CRASHES WITH A .DLL ERROR WHEN I TRY TO LAUNCH IT.**
A: The most common installation of PAGIS is Client/Server or "VPRelay Mode". The .dll error is caused by the installer not being run from the HDD and/or the wrong install option being selected (Example: SupeRex instead of MDC). The best practices for the installation are below. (Note, this does not cover MDC or PAGIS configuration, only the act of installation)
1. Always copy the installer over to the HDD/Desktop of the MDC. Never run it from a thumb-drive or network share
2. Regardless of how you're logged in to Windows, right click the installer and select "run as Admin" or "run with elevated privileges"
3. Continue through the message/error about OS compatibility
4. Click next on the wizard and then be sure to select the MDC option (to use with VPRelay)
5. After that, it's next, next, next, finish the reboot is not necessary

If these steps did not resolve the issue, please feel free to enter a request for support here.

Q: **USERS ARE GETTING HITS/ALERTS ON PREVIOUSLY RECOVERED STOLEN PLATES.**
Q: **USERS AREN'T GETTING HITS FROM KNOWN ACTIVE PLATES.**

Q: **THE HOTLISTS IN PAGIS DON'T SHOW TODAY'S DATE.**
Q: **THE HOTLISTS AREN'T SYNCING WITH BEGIN/END SHIFT.** 5449
A: Whether it's from data latency or just use over time, the local file structure can get some minor corruption and will need to be refreshed. The steps below show the best practices:
1. Login to Windows with Admin rights (ability to uninstall/delete software)
2. Login to PAGIS and perform an End Shift
3. When complete without error, Logout of PAGIS and then Exit/Close the program
NOTE: If the End Shift fails or displays an error, contact Support for additional assistance.
4. If there were no errors, locate the PAGIS icon on the desktop.
5. Right click on the icon and select "Open File Location" (This should open a window where the program was installed)
6. Scroll up and locate the folder labeled "data". Double-click it to open it
7. Select and delete everything in here EXCEPT for "Attributes.db"
8. Once that's complete, Login to the PAGIS software again
9. Perform a Begin Shift. This will pull down fresh data from the server
NOTE: Once complete, the files in the data subfolder as well as the Databases section of PAGIS should be restored.

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **IS PAGIS COMPATIBLE WITH OUR NEW WINDOWS 10 LAPTOPS?**
A: Although there's a warning about compatibility during the install of PAGIS on any Windows OS after XP, it is compatible with all them. However, we have seen errors occur when agencies copy and paste folder structures from previous installations. This of course is not recommended.

Q: **THE LINK LIGHTS ON OUR ALPR COMPUTER/MDC WON'T TURN ON OR FLASH.**
Q: **OUR WINDOWS 10 MDC WAS WORKING BUT HAS STOPPED COMMUNICATING TO THE SX PROCESSOR.**
A: There are many variables with troubleshooting any network connection. And the connection from the ALPR computer to the SX Processor is no different. The following troubleshooting list highlights the most common:
1. The physical network cord is bad/damaged.
A: Test with a different cable and confirm that it is plugged in fully

2. The network adapters are not configured or have incorrect static IPs
A: Confirm the Static IP scheme in use and properly configure the network adapters

3. Local and/or Domain Firewall rules have prevented the flow of communication
A: Disable or bypass these and test again

4. VPN, Anti-Spyware, Antivirus, or other monitoring software has blocked communication
A: Disable or bypass these one at a time and test after each to find the culprit(s)

5. Docking Station Firmware can be incompatible with some newer computers or become corrupt
A: Test by running the network cord straight to the MDC and then configuring the network adapters (NOTE: It would also be a good idea to contact station manufacturer to see what the latest firmware version is and upgrade as necessary)

6. The NIC Drivers have become corrupt
A: Update the specific Networking drivers in use on the MDC through the Device Manager in Windows

7. Turn off all power saving settings of the Ethernet Adapter in the device manager
A: Uncheck "Allow the computer to turn off this device to save power"

8. Check for Windows 10 update 1709 and 1803 as this update will not allow the NIC and Cellular Aircard to run simultaneously
A: Settings > Update and Security > Windows Update > "Update History" link – if there, see the steps in the FAQ

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **AS SOON AS WE DOCK OUR MDC, WE LOSE CONNECTION TO THE WIRELESS.**
Q: **OUR WINDOWS 10 LAPTOP LOSES CONNECTION TO THE INTERNET WHEN THE NETWORK CABLE IS PLUGGED IN.**
Q: **OUR MDC HAS MICROSOFT VERSION 1709 OR 1803 AND CAN'T CONNECT TO WIFI WHEN DOCKED.**
A: Microsoft Updates (1709 and 1803) prevent the Wireless connection as soon as a Network cable is plugged into the device. This also occurs for MDCs/laptops that are docked (where the Network cable from the SX Processor is run through the docking station). As of January 2019, the steps to correct this are below.
WIN10 version 1803
1. Open Regedit
2. Expand HKEY_LOCAL_MACHINE
3. Navigate to Software > Policies > Microsoft > WcmSvc > Local
4. Right click on Local > Hover over New > Select "DWORD (32-bit)"
5. Name the new value "fMinimizeConnections"
6. Right click the on the new name > select Modify > Set value data to 1 (leave base Hex) > Click OK
7. Reboot Windows and test

WIN10 version 1709 - Microsoft fixed this with Update KB 4284822. But if you still have issues, the registry steps are below:
1. Open Regedit
2. Navigate to HKEY_LOCAL_MACHINE > Software > Policies > Microsoft > WcmSvc > Local
3. Right click on Local > Hover over New > Select "DWORD (32-bit)"
4. Name the new value "fMinimizeConnections"
5. Right click the on the new name > select Modify > Set value data to 0 (leave base Hex) > Click OK
6. Then Navigate to HKEY_LOCAL_MACHINE\Software\Microsoft\Wcmsvc
7. Right click on Wcmsvc > Hover over New > Select DWORD (32-bit)
8. Name the value "IgnoreNonRoutableEthernet"
9. Right click on the new value > Modify > Set value data to 1 (leave base in Hex) > OK
10. Reboot Win10 and test

If the steps above did not resolve the issue, you may need to address this with Microsoft. Their support site is here.

APPENDIX D: XML DATASTREAM

Overview

The XML Datastream can be used to push the current data from a running PAGIS system to another application. The data available via the Datastream includes reads, hits and current images. The connection to the Datastream is a TCP/IP socket (default port: 10100). When initially connecting, an XML packet is passed to the PAGIS Software to subscribe to the Datastream. The data connection is configured as "push only" and doesn't allow receipt of additional external data. The current image stream is pushed periodically whereas reads and hits are passed as close to real-time as possible.

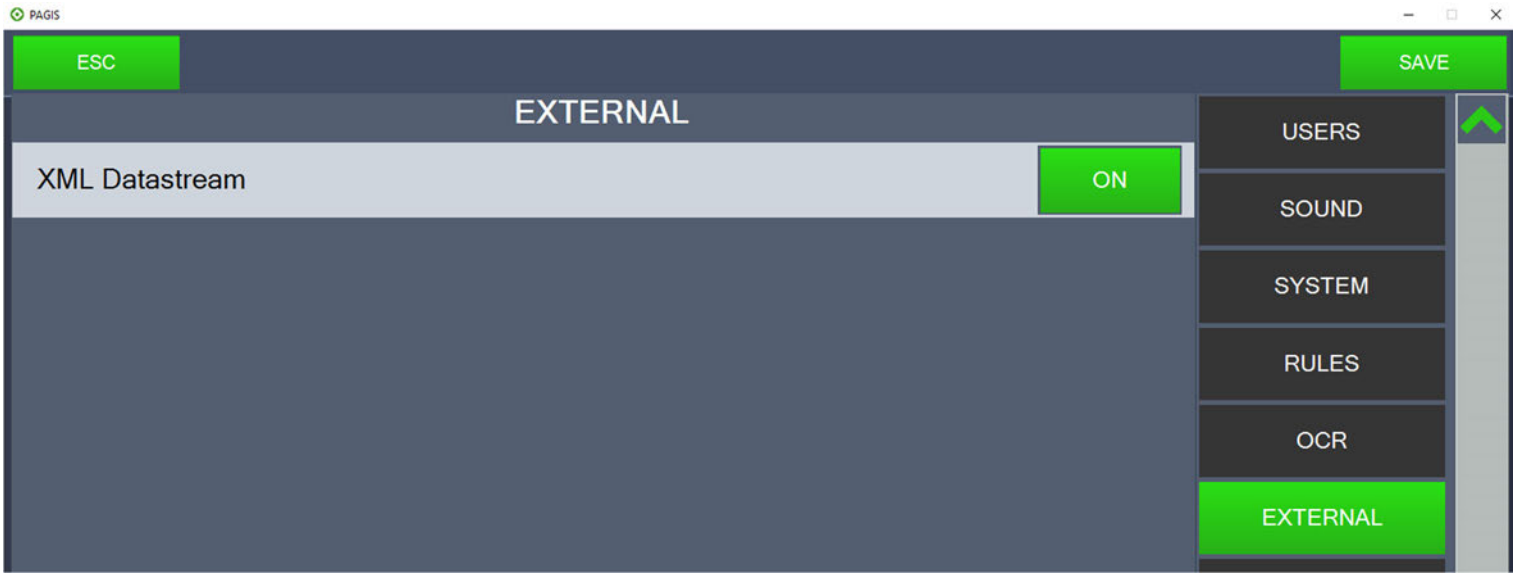
PAGIS Port

By default, the PAGIS.exe.config file has a key for defining the port number for the XML Datastream. The default value is 10100. This setting does not need to be changed unless the default port is unavailable.
The key has the following format:

```
<!--XML Datastream Settings/-->
<add key="XML.Datastream.Port" value="10100"/>
```

PAGIS Admin Setting

To utilize this feature, the XML Datastream needs to be enabled in PAGIS. To do this, navigate to Settings > Admin > External. The "XML Datastream" option should be turned on as shown in the image below and then saved.



XML Subscription

When initially connecting to PAGIS, the Datastream subscriber will receive only a Heartbeat XML packet (see example below) until PAGIS receives a subscription packet from the subscriber. The properly formed subscription packet defines the specific data that the subscriber wishes to receive.

Heartbeat XML Packet

The Heartbeat Packet is sent once every 10 seconds. The purpose of the heartbeat packet is to let the subscriber know that the communications channel is working between PAGIS and the subscriber. The timestamp is sent in the format of "`YYYY-MM-DDThh:mm:ss`".

Sample of the Subscription XML Packet

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-heartbeat>
  <timestamp>2011-10-13T09:41:56Z</timestamp>
</pips-datastream-heartbeat>
```

Subscription XML Packet

A properly formed subscription packet will have all of the data being requested from PAGIS. To receive a specific datatype, a tag must be added to the subscription to define the desired datatype. The valid entries for datatype are: Reads, Hits, and CurrentImage.

- Subscribing to Reads will send all plates that are detected by PAGIS regardless of whether or not it has an associated hit.
- Subscribing to Hits will send all plates detected by PAGIS that are on a hotlist and the associated Read data for that Hit.
- Subscribing to the CurrentImage Datastream offers two additional attributes that may be passed as well. The "camera" attribute can be set to determine which camera the image is coming from. If no value is passed for "camera" the value defaults to zero. The "milliseconds" attribute determines how long the system waits between sending the current image. The default value for milliseconds is 1000. If a value of zero is sent, the system will send a single snapshot.

Sample of the Subscription XML Packet

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-subscription>
  <datatype>Reads</datatype>
  <datatype>Hits</datatype>
  <datatype>HitTrigger</datatype>
  <datatype camera="0" milliseconds="1000">CurrentImage</datatype>
</pips-datastream-subscription>
```

HitTrigger

The HitTrigger packet is used to alert other systems that a hit has occurred on the PAGIS system. The packet is greatly simplified from the Reads/Hits XML packet and only contains the license plate text, timestamp and a description of the hit. The description will contain the name of the hotlist that originated the hit and may be used to send additional information.

Sample of the HitTrigger XML Packet

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-hittrigger>
  <timestamp>2011-10-13T09:41:56Z</timestamp>
  <vrm>SBX989</vrm>
  <hotList name='Alpha'>
    <field1><![CDATA[This is Alpha Field 1]]></field1>
    <field2><![CDATA[This is Alpha Field 2]]></field2>
    <field3><![CDATA[This is Alpha Field 3]]></field3>
    <field4><![CDATA[This is Alpha Field 4]]></field4>
    <field5><![CDATA[This is Alpha Field 5]]></field5>
  </hotList>
</pips-datastream-hittrigger>
```

Reads/Hits XML Packet

The Reads/Hits packet contains information about the plate that was detected. This information includes:

- Source – The device that detected the plate
- Camera – The camera on the device that detected the plate
- Read – The Information about the plate that was captured
- VRM – The plate translated to text
- Timestamp – When the read occurred
- GPS – The location coordinates where the read took place
- ImagesPatch – The image of plate in infrared (IR)
- Overview – The image of scene/car in Color
- Hits – The associated hotlist(s) data

Sample of the Current Image XML Packet

NOTE: The Current/Live Image XML Packet contains the current image from the camera. It is sent every 5 seconds.

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-currentimage>
  <timestamp>2011-10-13T09:41:56</timestamp>
  <data>(Image data here)</data>
</pips-datastream-currentimage>
```

Sample Read with Hits XML

```
<?xml version="1.0" encoding="utf-8"?>
<pips-datastream-reads>
  <reads>
    <source>
      <name>PAGIS_90210</name>
      <software name="PAGIS" version="2.6.8" />
      <camera name="Front Left">
        <read>
          <state>TN</state>
          <vrm>SBX989</vrm>
          <confidence>97.5</confidence>
          <timestamp>2011-09-30T09:30:10Z</timestamp>
          <username><![CDATA[shronski]]></username>
          <gps>
            <latitude>-87.4567</latitude>
            <longitude>98.7654</longitude>
          </gps>
          <images>
            <image name='Patch'>
              <type>IR</type>
              <data>

<![CDATA[/9j/4AAQSkZJRgABAQAAAQABA.....................................................................
.....................................................................................................
..... /9k=]]>
              </data>
            </image>
            <image name='Overview'>
              <type>Color</type>
              <data>

<![CDATA[/9j/4AAQSkZJRgABAQAAAQABAAD..................................................................
.....................................................................................................
.... //2Q==]]>
              </data>
            </image>
          </images>
          <misread>0</misread>
          <manual>0</manual>
          <hits>
            <hotList name='Alpha'>
              <field1><![CDATA[This is Alpha Field 1]]></field1>
              <field2><![CDATA[This is Alpha Field 2]]></field2>
              <field3><![CDATA[This is Alpha Field 3]]></field3>
              <field4><![CDATA[This is Alpha Field 4]]></field4>
              <field5><![CDATA[This is Alpha Field 5]]></field5>
            </hotList>
            <hotList name='Beta'>
              <field1><![CDATA[This is Beta Field 1]]></field1>
              <field2><![CDATA[This is Beta Field 2]]></field2>
              <field3><![CDATA[This is Beta Field 3]]></field3>
              <field4><![CDATA[This is Beta Field 4]]></field4>
              <field5><![CDATA[This is Beta Field 5]]></field5>
            </hotList>
          </hits>
        </read>
      </camera>
    </source>
  </reads>
</pips-datastream-reads>
```



PIPS TECHNOLOGY™

DETECTION INNOVATION



PAGIS User's Manual

Version 2.14

Updated 3/30/2020

NEOLOGY MOBILITY TECHNOLOGIES

Table of Contents

Table of Contents 2

NOTICES 3

Technical Support 3

Design Changes 3

Trademarks 3

Copyright 3

Version 3

INTRODUCTION 4

1.1 Dual Lens Color and Infrared Camera 4

1.1.1 Available Products 4

1.2 Using This Manual 5

SCREEN REFERENCE 6

2.1 The PAGIS Software Login Screen 6

2.1.1 Logging on with the Default Administrative Account 6

2.2 Main Screen - Live View 7

2.2.1 Getting Started in PAGIS 7

2.3 The PAGIS Navigation Buttons 8

2.3.1 Camera Control Buttons 8

2.3.2 GPS Indicators 9

2.3.3 Camera Firmware Update (Restricted Users) 9

2.3.4 Day/Night Mode 9

2.4 Begin Shift 10

2.4.1 Sync via USB Thumb drive (or Local Source) 10

2.4.2 Sync via Wireless Network 10

2.4.3 PAGIS Auto-Sync Settings 10

2.4.4 Begin Shift – Additional Information 10

2.5 End Shift 10

2.5.1 Sync to BOSS 10

2.6 Cam Mode Button 11

2.6.1 Camera Modes 11

2.7 Taking a Picture 11

2.8 Search Entry Screen 12

2.8.1 Searching Synchronized Hotlists for License Plates 12

2.8.2 Searching Locally Stored Reads and Hits 12

2.8.2.1 Searching for a Match 13

2.8.3 Wild Card Symbols 13

2.8.4 Manually Adding a Plate to PAGIS 14

2.8.4.1 ADD VLP Query 14

2.8.4.2 ADD VRM Report Screen 14

2.9 The Review Screen 15

2.9.1 Summary Review Section 15

2.9.2 Review Navigation Buttons 15

2.9.3 Reads 16

2.9.3.1 Reads Result Screen Navigation Buttons 16

2.9.3.2 Interactive Buttons – Reads Screen 16

2.9.4 Hits 17

2.9.4.1 Hit Screen Attributes 17

2.9.4.2 Hit Screen Function Buttons 18

2.9.4.3 Interactive Buttons – Hits Screen 18

2.9.4.4 Set Disposition – Additional Detail 18

2.9.4.5 Add Intel – Additional Detail 19

2.9.5 Misreads 19

2.9.5.1 Marking a Record as a Misread: 20

2.9.6 Audits 21

2.9.7 Targets 21

2.9.7.1 The Targets Screen 22

2.9.7.2 Targets Screen Navigation Buttons 22

2.9.8 Databases 23

2.9.8.1 Databases Screen Functions 23

2.9.8.2 Databases Screen Navigation Buttons 23

2.9.8.3 Databases Edit- “Manual Reports” 24

TROUBLESHOOTING TIPS 25

3.1 Troubleshooting & Tips 25

3.1.1 PAGIS with NetMotion VPN 25

3.1.2 Cisco VPN Client: 25

3.1.3 Microsoft .NET 3.5 Installation 25

3.1.4 Firewall Settings for Client-Server Installations 25

APPENDIX A: THE GLOSSARY 26

APPENDIX B: PAGIS SOFTWARE DATABASE FILE 27

APPENDIX C: FAQ 29

NOTICES

The information within this manual is authorized for distribution to customers, authorized service center personnel, and distributors of Neology. Every effort has been made to supply correct information. However, Neology assumes neither responsibility for its use, nor for any infringements of patents or other rights of third parties, which may result from its use. No license is granted by the manufacturer under any patent or patent rights. Neology reserves the right to modify and update the equipment at any time without prior notice. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means to a third party without the prior consent of the copyright holder. The manufacturer's warranty will be invalidated if untrained personnel operate the equipment or if any attempt is made to service the equipment by unauthorized personnel.

This manual contains confidential and proprietary information and should not be redistributed except as needed for proper use and maintenance of the agency's Mobile ALPR system.

Technical Support

Service of this equipment by replacement of parts, on-site repair, routine maintenance inspection, and scheduled remote support session is available. Please contact PIPS Technology's ALPR Technical Support.
Phone: 833-PIPS-LPR (833-747-7577), Option 2
Support Team Email: Support@PIPSTechnology.com
For Customers in Europe, Middle East and Africa: Support@PIPSTechnology.co.uk
Web: www.pipstechnology.com
Fax: 858-391-0264
Corporate Office: 13520 Evening Creek Drive Suite 460. San Diego, CA 92128

Design Changes

Neology reserves the right to change the design of any product from time to time without notice and with no obligation to make corresponding changes in products previously manufactured.

Trademarks

PIPS Technology™ is a trademark of Neology Inc., and either registered or pending registrations in several jurisdictions. Windows, Windows 7, Windows 8, Window 10, and .NET are all trademarks of the Microsoft Corporation. Other trademarks and registered trademarks are the property of their respective owners.

Copyright

The Neology / PIPS Technology PAGIS Software is copyright of Neology. All rights reserved. This product contains confidential and trade secret information of Neology and is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portions of it, may result in civil and criminal penalties.

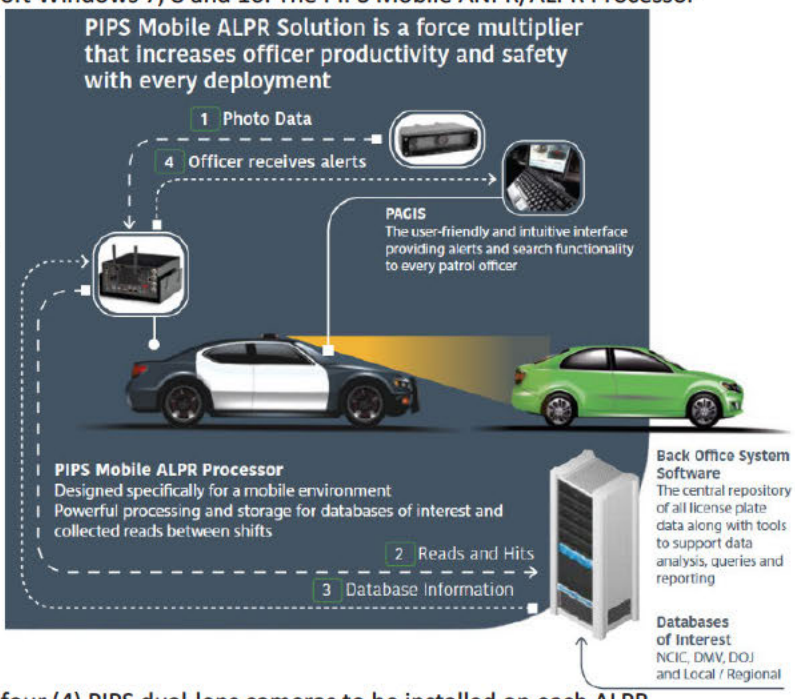
Version

This manual demonstrates the attributes of the Neology / PIPS Technology PAGIS Software Version 2.14 and was last updated in March 2020.

INTRODUCTION

PIPS Technology's Automated License Plate Recognition (ALPR) software solution called PAGIS utilizes dual-channel, dual-lens, cameras to "read" plates. Our software is optimized to run on the Mobile Processor itself or in conjunction with a mobile data computer (MDC). Our mobile software is compatible with Microsoft Windows 7, 8 and 10. The PIPS Mobile ANPR/ALPR Processor comes equipped with Microsoft Windows 7 Embedded.

The PAGIS Software processes the infrared plate image provided by any of the cameras and then interprets the plate number through Optical Character Recognition (OCR) via the mobile processor. The PAGIS application then searches for any matches of the plate with those listed in the databases, or "hotlists," distributed from the PIPS Back Office System Software (BOSS) or other external sources.



WARNING: To reduce the risks associated with impact, which if not avoided, could result in serious injury or death: Do Not interact with the ALPR system while driving in hazardous situations. The PIPS mobile camera series and License Plate Capture Software are not intended for use in hazardous environments, so that the User and/or others are not put at risk for personal injury and/or property damage.

1.1 Dual Lens Color and Infrared Camera

The PIPS Technology Mobile ALPR System allows for a maximum of four (4) PIPS dual-lens cameras to be installed on each ALPR vehicle provided that the vehicle supports the additional mounting equipment.

Each dual-lens mobile camera uses visible light to take color overview pictures of the vehicle and uses infrared (IR) illumination to capture the license plate's alphanumeric characters. IR illumination offers the best capture performance of reflective license plate characters for the following reasons:

- State issued license plates are designed to be highly reflective to IR light.
- Cameras using IR capture technology do not depend on the presence of visible light to function.
- Cameras using IR capture technology are not negatively impacted by the effects of headlights, solar glare, or total darkness.
- IR light penetrates rain and fog better than visible light.
- Due to these attributes, the system can be used 24 hours a day, seven days a week.

1.1.1 Available Products

Additional information about this and other PIPS Technology applications, cameras, and solutions are available on the PIPS web site: http://www.pipstechnology.com

1.2 Using This Manual

5458

The section overview of this software manual are as follows:

Section 1: The Introduction and Basics

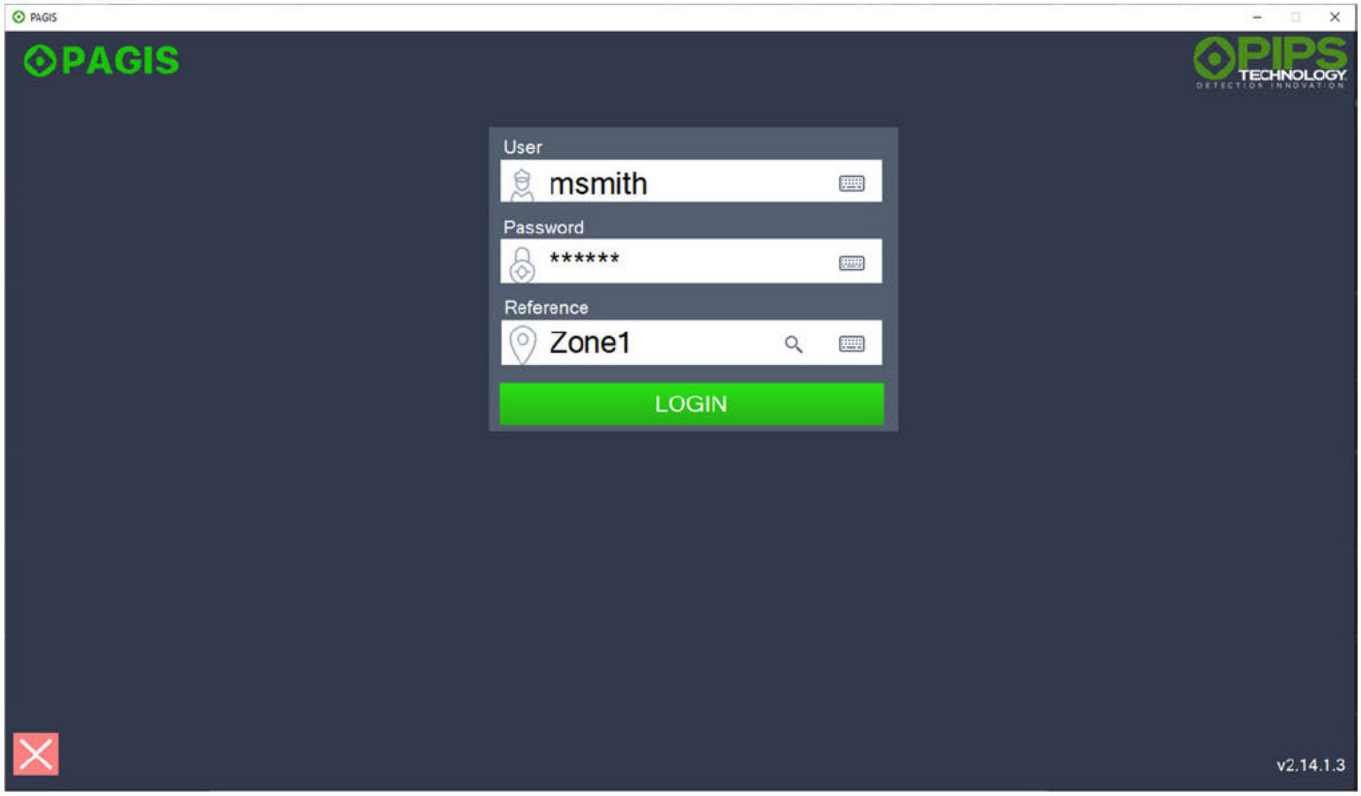
Section 2: PAGIS User's Section: Explains screen function and User Operations in the PAGIS Software

Section 3: Troubleshooting Tips

Appendices: Additional features and details

SCREEN REFERENCE

This section guides the user through the PAGIS Software screens and the available options. Screens are grouped according to function. When a button is grayed out or missing, the option is not available, or no information has been accrued to activate it.



2.1 The PAGIS Software Login Screen

The PAGIS Software allows users with various access privileges to use the same MDC. For users with touch screen monitors, the Keypad button immediately to the right of any text box gives the user access to an on-screen keyboard for data entry.

User Field: The alphanumeric string assigned to identify the user. Usernames are not case sensitive.
Password Field: Password of the assigned user logging in. Passwords are case sensitive.
Reference Field: This is an optional field utilized to fit a number of use cases. A user can manually enter a reference at logon, leave the field blank, or select list of unique tags that will be associated with all data captured while logged in. If the Administrator has configured a default reference tags, that information will be displayed automatically. Otherwise, it will be blank.
Login Button: Submits the username and password to attempt a login.
Exit Button: By clicking the X icon in the lower left-hand corner, the user can exit/close the PAGIS Software.

2.1.1 Logging on with the Default Administrative Account

The PAGIS Software includes a default administrative account that can be used for the initial configuration. To do so, simply click the **Login** button with the User and Password fields blank.

NOTE: System Administrators are strongly encouraged to configure users for PAGIS just before, or soon after the installation and setup. PAGIS users accounts are created and maintained in BOSS. Once Users are established by the BOSS System Administrator, the default user account is automatically disabled. Best practices are to be certain at least one User account has administrative privileges.

2.2 Main Screen - Live View

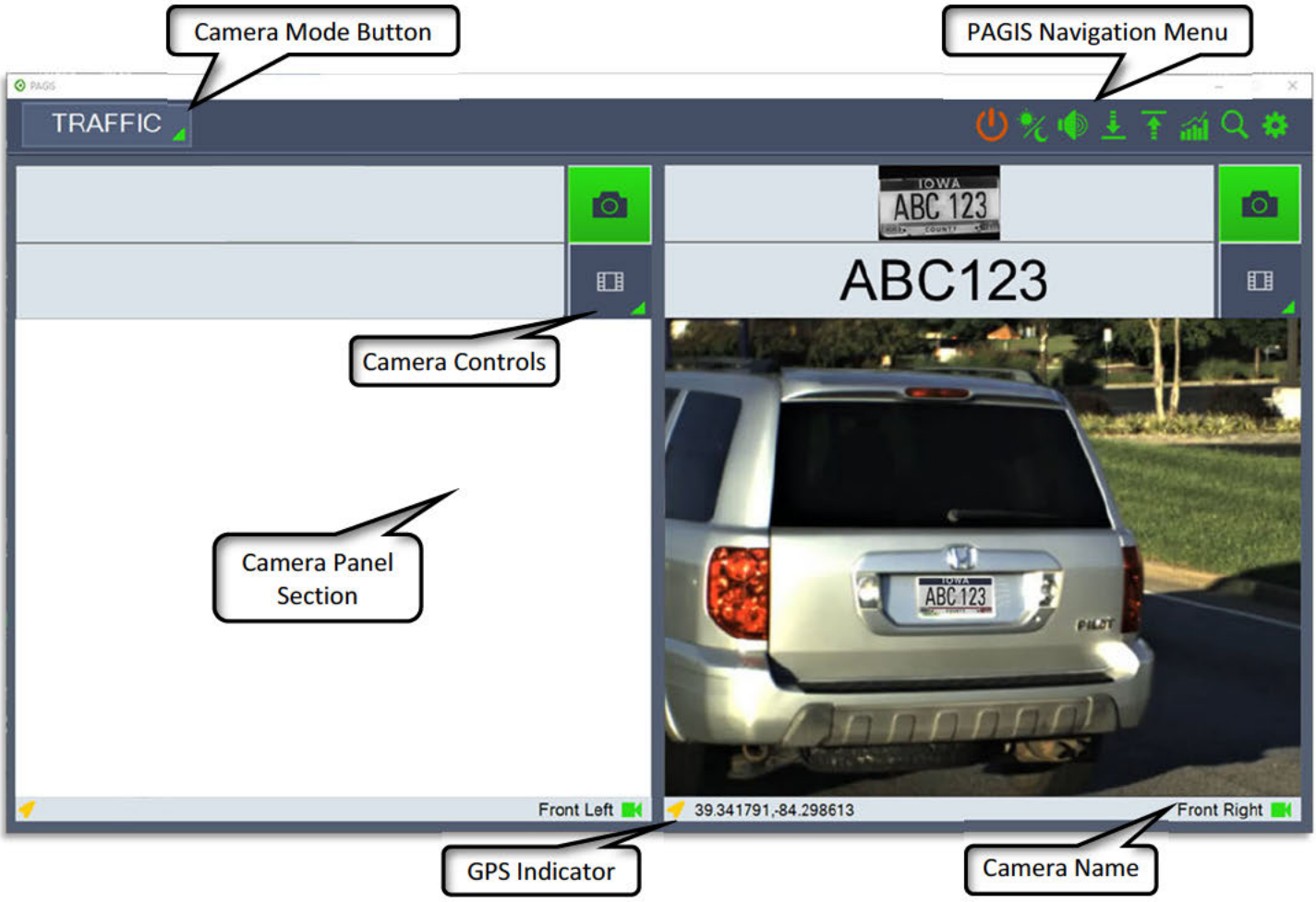
Upon a successful login, the user will see the Main screen (Live View). This is the default view and starting place of all PAGIS Software features. (NOTE: Access to features is based on user group rights established in BOSS.)

The Main Screen is also the place users will monitor read images and ALPR "hits". At the initial startup of the system it is normal to see only a blank/grey screen for a few seconds. Once a connection has been established with the mobile cameras, white boxes will be displayed showing the live-feed camera panels. At this point, the system is ready to capture reads/plates.

2.2.1 Getting Started in PAGIS

By default, PAGIS loads into a static view. This means live video will not automatically appear in the camera panels (white boxes) until a plate has be captured or the user selects one of the live feed options.

Once a plate is "seen" by a camera assigned to the current viewing mode (Traffic vs Parking), it will display the captured information in the corresponding camera panel. Each plate capture is also accompanied by a short "Beep" to audibly alert the user a read has taken place. (NOTE: If the user is in the Traffic Mode at the time a parking camera reads a plate, there will be a sound effect, but no plate image will be displayed on screen unless that plate is on a synchronized Hotlist or until the user switches to Parking Mode.)



2.3 The PAGIS Navigation Buttons

5461

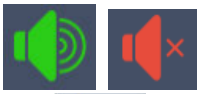
This section provides a quick reference guide to the available navigation buttons of the Live View screen.



The Camera Mode button is located in the upper left corner and is used to switch between the configured camera modes. Once configured, the name will change to a selected mode. The default values are “ALL”, “Traffic” and “Parking”.



The Logoff button is located in the upper right of the window. When selected, the user will be logged out of PAGIS and return to the login screen.



The Sound button is located to the right of the Logoff button. When selected, this button with toggle the PAGIS system sounds On and Off.



Day/Nite mode switches PAGIS between day & night mode screen skins.



The Begin Shift Synchronization button is located to the right of the Sound button. When selected, this will reach out to the BOSS server to download users, hotlists, and other system settings.



The End Shift Synchronization button is located to the right of the Begin Shift Button. When selected, this will upload any previously unsent reads, images, and audits to the BOSS server.



The Statistics/Review button is located to the right of the End Shift Button. When selected the user is able to review Databases/Hotlists, Reads, Targets, and other PAGIS information.



The Search button is located to the right of the Review Button. When selected the user can search his/her reads as well as manually add a license plate to a temporary hotlist.



The Admin/Settings button is located in the upper right corner of the screen. This button is only viewable to Admin level users and allows for system configuration changes and setup.



Firmware update icon will atomically appear when PAGIS detects a new firmware is available for the P720 mobile cameras. All user types are notified, but only Admins can apply the update.

2.3.1 Camera Control Buttons

The dual-lens cameras can capture both color and an infrared image. Formerly, there were a total of three buttons that allowed the user to view the IR and color feed as well as capture a picture directly from PAGIS. Now there is a toggle button to switch between color and IR views and a separate button to take a picture. These buttons are displayed on the main Live Screen as shown below:



The Camera View Selector button: This is the default state at login showing the Static View. (**NOTE**: PAGIS does not automatically display a life feed.)



Color View: by clicking on the Camera View Selector button once, the user will switch to the Color View Mode. This displays the current view of the color camera and will time out after 60 seconds.



IR View: by clicking on the Camera View Selector button twice, the user will switch to the Infrared (IR) View Mode. This displays the current view of the IR camera and will time out after 60 seconds.



The Take Pic button: Just above the Camera View Selector button is the “Take Pic” button. This button allows the user to quickly take a picture from the camera currently viewed.

2.3.2 GPS Indicators

GPS is stamped on each read and hit as capture events take place by the system. The signal strength and location indicators are located underneath the camera panels at the bottom of the Live Screen.

39.341788,-84.298518 Shows an example of the Location Indicator displaying the Lat/Long on the most recent read

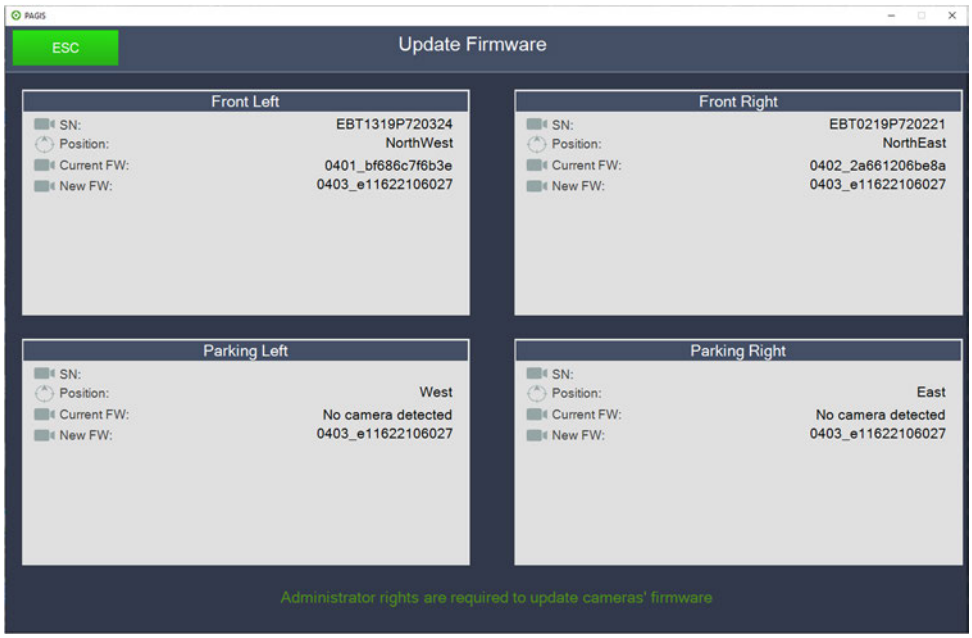
A green or yellow indicator shows a strong or medium strength GPS lock.

A red indicator shows there is no available GPS information.

2.3.3 Camera Firmware Update (Restricted Users)

Camera firmware update provides a means for PIPS to update the camera software to enhance and or correct camera performance. The frimware icon will only apper when update is avialable.

- The firmware update process only updates camera that are attached and function on the mobile processor.
- Restricted PAGIS users are only notified and displayed update information, only a PAGIS administrator can apply the FW update.

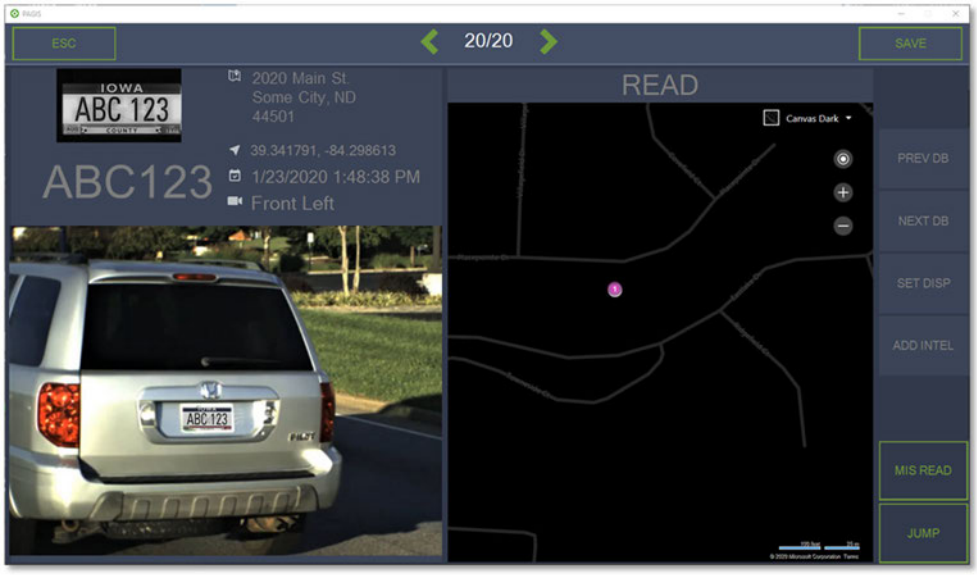


Firmware Updater Window List.

- Title “Camera Name”.
- Camera serial number.
- Position.
- Current FW version.
- New FW version available.

2.3.4 Day/Night Mode

Day/Night mode changes PAGIS user interface skins to a darker appearance to reduce illuminating the vehicle interior.



2.4 Begin Shift

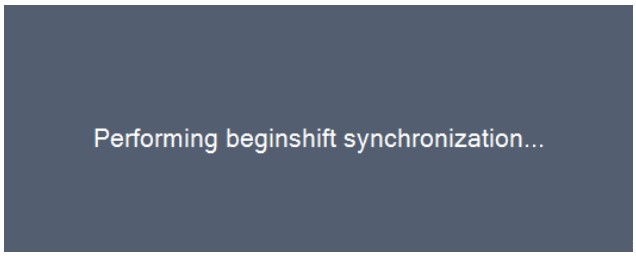
Begin Shift is thought of as the first step for all PAGIS users. From the Live View Screen, the PAGIS user must click the Begin Shift button twice. Once to select the function and once more to launch the Sync. With most agencies, this action utilizes a wireless network to import all the necessary data used during a shift (Hotlists, Dispositions, and Targets) directly from the BOSS Server. However, agencies can also configure their systems to perform this function via Thumb drive or a local source file.

2.4.1 Sync via USB Thumb drive (or Local Source)

Depending on the agency network, some alter the default PAGIS/BOSS configuration mode to use a USB Thumb drive or locally stored file on the MDC/Laptop instead of the wireless Sync. In order to synchronize effectively, the user must first confirm he/she has access to the source location before initiating Begin Shift. **NOTE**: All synchronizations using this method must be performed manually. To learn more about this process, refer to the "Client Tools" section of the BOSS Manual.

2.4.2 Sync via Wireless Network

Synchronizations over a wireless network provide the agency with additional automated features. Best practices recommend the user manually launch Begin Shift from the Live View Screen at the beginning of every patrol shift. However, it is possible for users to allow PAGIS to synchronize via its auto-sync settings. When a manual Begin Shift is launched, the Main View Screen removes the camera feeds and displays a status window of the Sync process. Once the Begin Shift operation is complete, PAGIS will return to the normal Main View Screen.





2.4.3 PAGIS Auto-Sync Settings

PAGIS auto-sync settings are best thought of as how PAGIS receives additional updates and maintains the downloaded ALPR data throughout the entire patrol shift. This prevents the need for the officer to manually perform Begin Shift functions multiple times a day. The auto-sync occurs every 30 seconds and receives data in small batches. The batches are not to exceed 1MB in size for every minute of download. In addition to receiving data, the auto-sync function also uploads a copy of data collected by PAGIS and sends it to BOSS for reporting/processing.

2.4.4 Begin Shift – Additional Information

By default, the synchronizations in PAGIS receive only what has been changed to the ALPR data since the last Sync. Meaning, if some plates have been removed from a Hotlist and others have been added, the system will only transfer that data instead of downloading the entire Hotlist each time the Begin Shift is launched. This helps to reduce the amount of data transferred over the agency's network. **NOTE**: Begin and End Shift synchronization, as well as all auto-sync features, are dependent upon stable communication to the BOSS server via an active data connection.

2.5 End Shift

End Shift in PAGIS is the process in which all the collected ALPR data (Reads, Hits, and Images) from the recent shift is uploaded to the BOSS server and cleared from the local cache. As with Begin Shift, the agency has two options. They can choose to Sync via USB Thumb drive or via wireless connection. Best practices recommend users perform an End Shift Sync at the end of every patrol.

2.5.1 Sync to BOSS

At the end of every shift, the accrued ALPR data should be exported to BOSS. Just like with Begin Shift, the user must click the button twice to launch it (once to select it and once more to execute the Sync). During the Sync, PAGIS uploads any Reads, Hits, and Images not already synchronized to BOSS and purges these items from the local cache on the MDC's hard drive. Completing an End Shift also removes any VLP entries manually added to PAGIS during the shift.

2.6 Cam Mode Button

Clicking the Cam Mode button in the upper left corner of the Live View Screen allows the user to cycle through the different camera modes configured by the PAGIS Administrator. Changing the camera mode changes which cameras are displayed on the Main Screen.

2.6.1 Camera Modes

By default, PAGIS provides "Parking" and "Traffic" as the two configuration modes. Users often switch these modes to suit their current use-case. For example, an officer in a parking lot will often switch the mode to "Parking" so s/he can see the parking cameras on the Live View Screen. They can then switch back to "Traffic" when monitoring city streets.

2.7 Taking a Picture

The PAGIS software has ability to quickly take a picture from one of the currently displayed ALPR cameras on the Live Screen. The user only needs to click on the Take Pic button.



To Take a Picture:

1. From the Live View Screen, press the Take Pic button from the desired camera
2. The image taken will be displayed
3. Enter a description of the picture in the text field at the bottom of the screen
4. Press Save to save the picture or Escape to cancel. Either action will return you to Live View.

NOTE: The picture will Not be saved if a description/note is not entered in the text box.

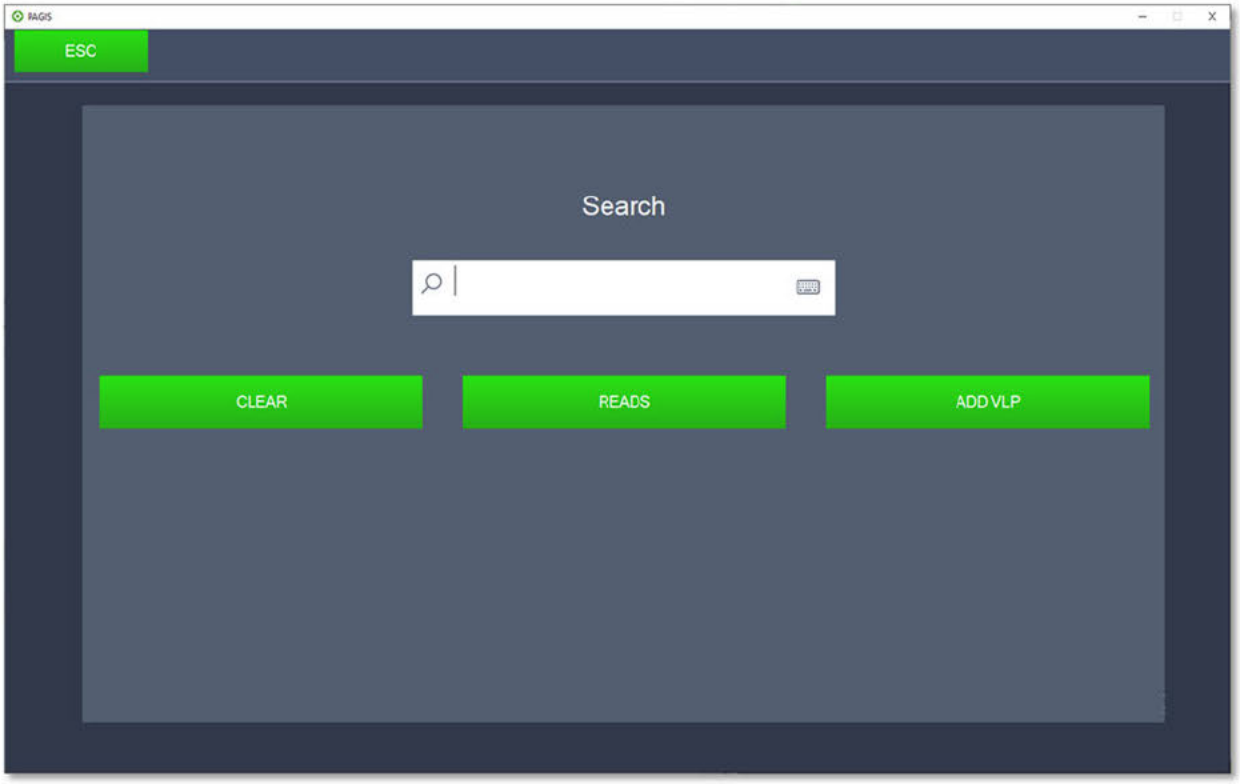
To View the Saved Images:

1. Navigate to the Review menu in PAGIS
2. Select Audits
3. The user will be able to see a thumbnail of the image and the saved text/note
4. In order to review the saved images at a later time, the user will need to run the Audit Report from BOSS.

2.8 Search Entry Screen

5465

Pressing the Search button icon from the Live View screen or SEARCH from the Databases window allows the user to search all manually entered plates as well as all BOSS synchronized databases (Hotlists) for license plate and target information. Users can also search all locally stored reads/images accrued since the last End Shift by clicking the Reads button instead of pressing the Enter key.



2.8.1 Searching Synchronized Hotlists for License Plates

By entering a vehicle license plate number (VLP) and pressing the Enter key or the ADD VLP button, the user can quickly search all the stored plate information locally collected as well as the information from all synchronized hotlists distributed from the BOSS server. **NOTE**: Hotlists can only be searched by entering complete VLPs. Wildcards and partial plate numbers will not return results.

Search Box: The text field used to enter the desired plate search via alphanumeric characters and/or wild card symbols.

Clear Button: Clears the contents of the search box.

Driver's License Info: The search field can also check the Hotlists for any DL information stored (Not available all countries).

Reads Button: This button searches for a match from all the reads/hits locally stored on the MDC/Laptop.

ADD VLP: Searches all locally stored hotlists for the plate and if there's no match, allows the user to add the plate to the "Manual Reports" alert list for use in the field. **NOTE**: All manual entries are cleared with each End Shift

ESC: The Escape button allows the user to exit to the Main/ Live View screen.

2.8.2 Searching Locally Stored Reads and Hits

As mentioned previously, this search function allows users to find reads and hits directly from their recent patrols using the search field and the Reads button. These searches pull only the reads and hits locally gathered/stored since the last time the user completed an End Shift. **NOTE**: The search results are specific to each Windows User Profile and do NOT pull images from the BOSS server.

2.8.2.1 Searching for a Match

5466

- From the Search field, users may enter a plate (or partial plate with wildcards) and then click the READS button.
- Results are displayed with the data gathered at the time the read was taken (See example below).
- Each result should display the infrared (IR) image of the plate as well as the color overlay of the vehicle for review.
- Each result shows the GPS data, Closest address point, Time and Date, and the Camera that read the plate.
- If there are multiple results, the user can cycle through them by clicking the left and right navigation arrows.



2.8.3 Wild Card Symbols

The use of wild card symbols in the Search box allows greater flexibility for the user, but may return a larger set of results.

- Wild card searches performed using the asterisk (*) designates an unknown number of characters.
- Wild card searches performed using the underscore (_) indicates a single missing or unknown character.
- Searches can be performed using one, both or no wild card symbols.

Example: The officer received an alert from Dispatch looking for a vehicle plate containing the letter J and the number 8 separated by one character. Because the officer doesn't know how many characters there are before or after the J and 8, he enters *J_8* in the search box to review all possible matches of J and 8 separated by only one digit.

2.8.4 Manually Adding a Plate to PAGIS

PAGIS allows users to manually add a plate of interest directly into the software as needed. Once saved, these entries are stored as part of the Manual Reports alert list and work just like any other Hotlist synchronized from the BOSS server.
NOTE: These additions are designed to be temporary and are cleared from the software with each End Shift.

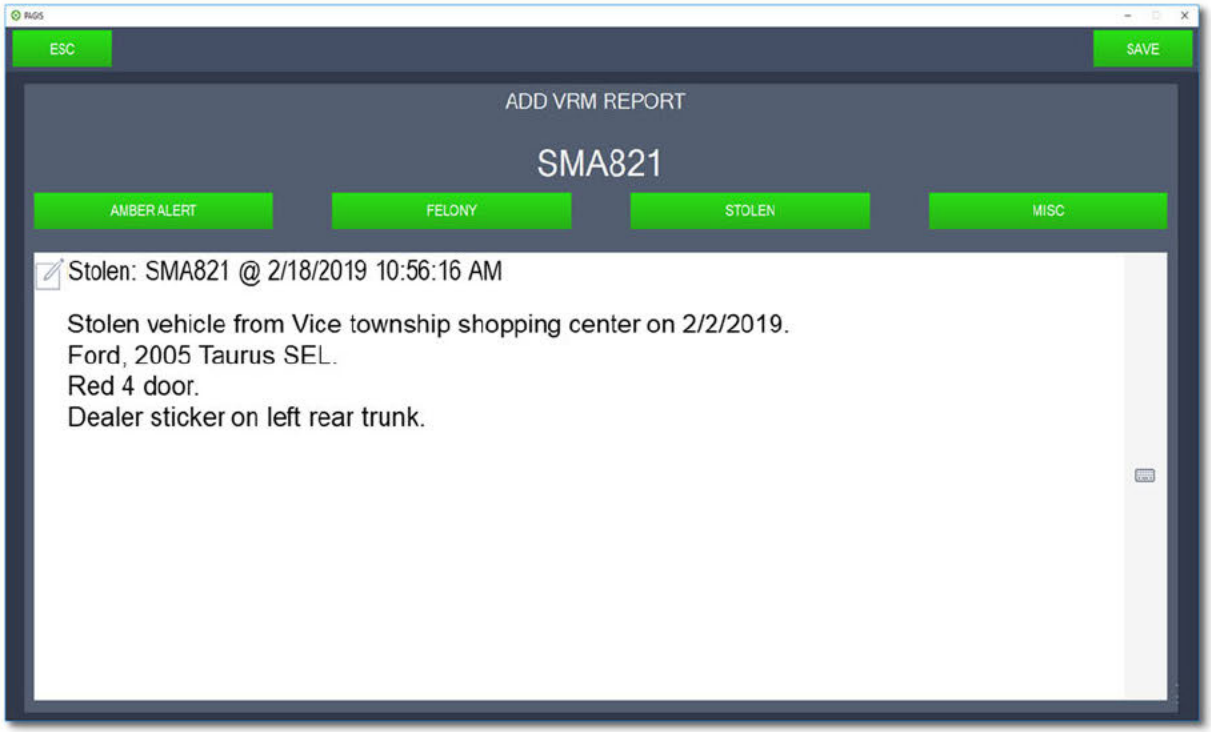
2.8.4.1 ADD VLP Query

Before an entry is added to the Manual Reports Hotlist in PAGIS, the software searches all stored databases for a match. If a match occurs, a message will display under the search box showing which Hotlist(s) it has been found in. If the VLP query does not return a match, the "ADD VRM REPORT" screen appears.



2.8.4.2 ADD VRM Report Screen

If the desired plate does not already reside in another Hotlist, the ADD VRM Report Screen becomes accessible to the user.



1. From the Search Entry Screen, enter the desired plate to add.
2. Click the ADD VLP button. If no match is found on any other hotlist, the "Add VRM Report" screen will appear.
3. Click to select the applicable alert type (AMBER ALERT , FELONY , STOLEN , or MISC)
4. Either leave the default information or add additional detail.
5. Click Save at the top right to add the plate to the Manual Entries Hotlist

2.9 The Review Screen

5468

PAGIS allows users to review all locally stored data from one easy location. Clicking the Review icon from the Main Screen launches Review. This screen is divided into the Summary View Chart and sub-section navigation buttons to the right.



2.9.1 Summary Review Section

The Summary View Chart is divided into five categories and allows a user to review the information collected during their shift at a glance.

Total Reads: Shows the total number of Reads/Hits synced to BOSS and the total number of reads captured during the shift.
Reads: Shows the total number of reads synced to BOSS and the total number of reads captured during the shift.
Hits: Shows the total number of hits synced to BOSS and the total number captured during the shift.
Misreads: Shows the total number of reads marked as a "misread" synced to BOSS and the total marked during the shift.
Audits: Shows the total number of audits synced to BOSS and the total number of audits during the shift.
Targets: Shows only the number of targets downloaded from BOSS.
(NOTE: The Sync value will always be zero for customers using Disk Sync mode/Client Tools.)

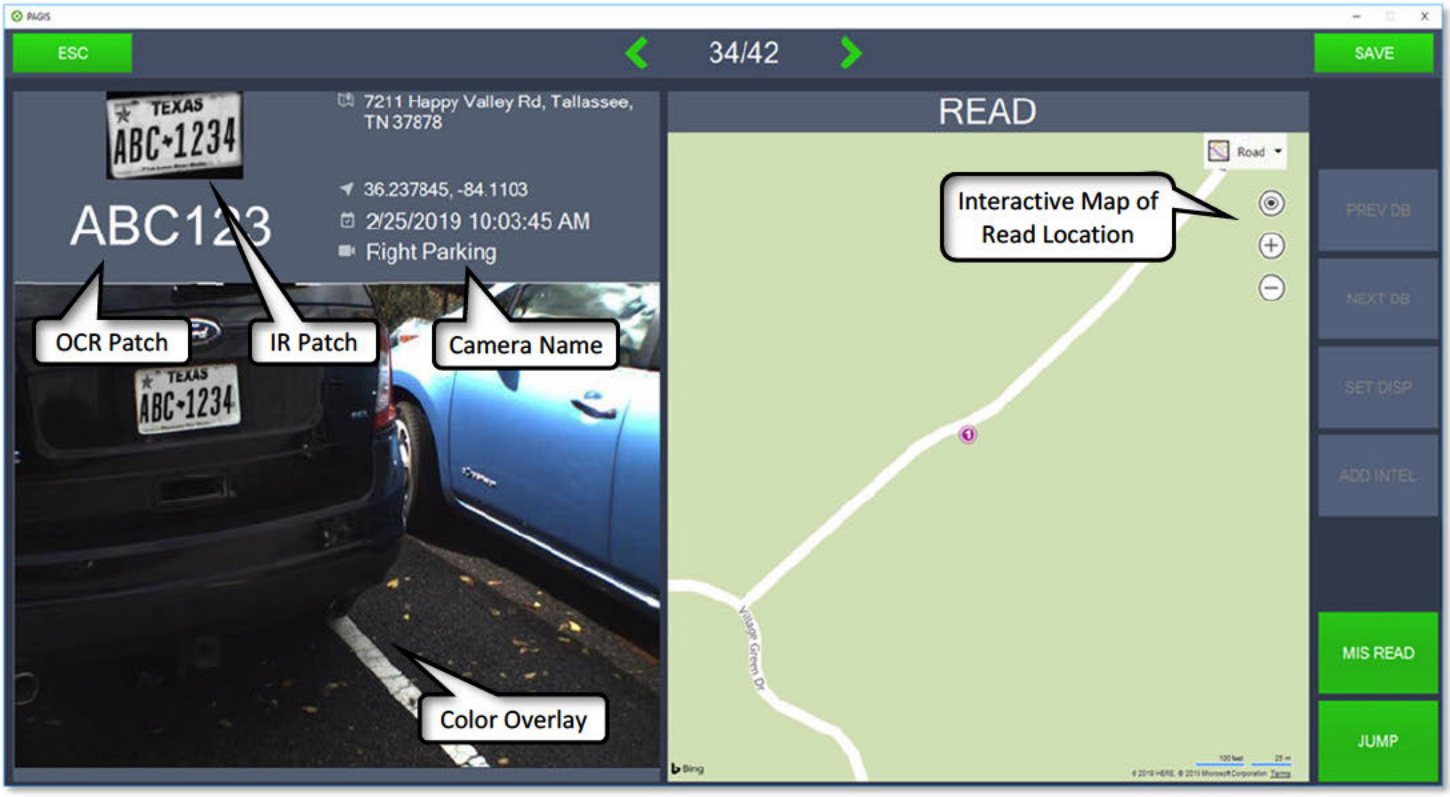
2.9.2 Review Navigation Buttons

The navigation buttons allow the user to review specific sets of information gathered during the shift.

Reads: Review all plate detections that have occurred since the last End Shift synchronization.
Hits: Review the hit alerts for Vehicle License Plate (VLP) reads that matched a Hotlist.
Misreads: Review reads and/or hits that have been manually flagged during the shift as misreads, where the plate number in the image does not match the OCR interpretation of the plate (e.g., a letter O misread as a Q or zero).
Audits: Review failed and successful logons, any manual data entered during the shift, pictures taken and all manual license plate searches.
Targets: Review targets that have been synchronized/downloaded from Boss.
Databases: Review all the Hotlists currently distributed to this PAGIS laptop/MDC.
Esc: Returns the user to the previous screen.

2.9.3 Reads

From the Main Screen, the user can review his or her accumulated Reads (those gathered since the last End Shift was completed) by clicking on the Review icon and then selecting the Reads Navigation button. The Read Review Screen is divided into two main sections. The left side displays the information gathered at the time of the read and the right side displays an interactive map of the GPS location.



NOTE: Buttons that are greyed out indicate options that are not available in the current view. For example, the Reads and Hits review screens share the same layout but different on-screen options.

2.9.3.1 Reads Result Screen Navigation Buttons



Read Count: The left number is the current record. The right number is the total available for review.

Next/Previous button: The arrows on either side of the read count allow the user to navigate back and forth to review reads/results.



MisRead button: When the button is green it indicates the record has NOT been edited as a Misread by a user. Once a Misread is saved, this button will turn grey and the record title will update.



Jump button: Allows the user to "jump" to a specific record without the need to navigate one record at a time using the Next/Previous buttons.



Save button: Apply any changes/edits and return to the Main Screen.



Escape button: Returns the user to the Main Screen.

2.9.3.2 Interactive Buttons – Reads Screen

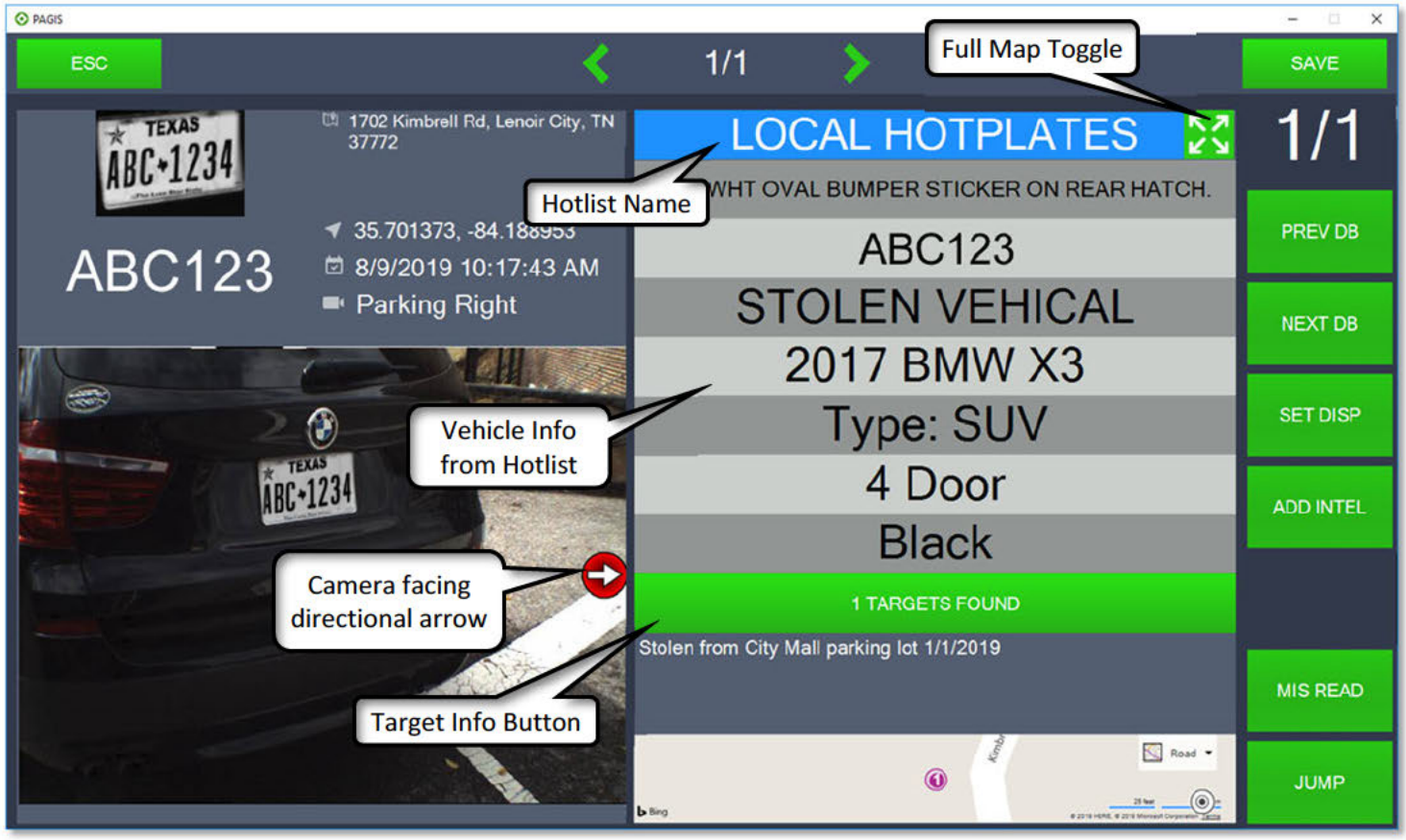
From the Reads Review, the user can interact with the following:

- IR Patch: The user can click on the IR "Patch" plate image to open a full-screen view.
- OCR Patch: The user can click on the OCR "Patch" image to edit the license plate number if necessary/Misread.
- Color OV Image: The user can click on the color image to open a full-screen view.
- Map: The user can manipulate the interactive map of the read location (Map Type, Scroll, and Zoom).

2.9.4 Hits

Users can manually access the Hits Section by first selecting the Review icon from the Live View Screen and then clicking the Hits Button. The Hits Screen is also divided into two main sections. The left side displays the information gathered from the ALPR equipment during the read. And the right side displays the information provided by the associated alert list.

NOTE: Each time a VLP matches a Database value (a license plate read by the system matches a Hotlist entry), PAGIS plays an audible tone and automatically displays the Hit Screen to alert the user.



2.9.4.1 Hit Screen Attributes

Hit Count and Navigation Buttons: Displays the total Hit count as well as the Next/Previous navigation buttons.
IR Patch Image: A thumbnail image of the license plate from the IR camera.
OCR Text: The character string the OCR engine generated from the current plate.
GPS Location: The GPS coordinates at the time of the hit. (If a GPS device is not attached, the Lat/Long is displayed as 0,0).
Date and Timestamp: The date and time when the read/hit was captured.
Overview Image: The overview image of the vehicle from the Color Camera. (**NOTE**: Color images require visible light)
Camera Name: The name of the camera that captured the read ("Right Parking" in the screenshot).
Hotlist Name: This is the name of the Hotlist or "Database" where the plate was matched.
Target Button: When available, this indicates a person of interest is associated with the Hit and opens the Targets Screen.
Vehicle Information: The area of grey bars will display the related vehicle information from the Hotlist. Any information added manually by the user will appear in the Text Box near the bottom of the screen.
Interactive Map: Shows the location the Hit took place. Users can access full-screen view by clicking the map or the toggle .

2.9.4.2 Hit Screen Function Buttons



The Hit Count Indicator: shows how many Hotlists the current Hit has registered against.



Previous DB button: This button moves the user to the previous Database/Hotlist that produced a Hit.



Next DB button: Pressing this button moves the user to the next Database/Hotlist that produced a Hit.



The Set Disposition button: prompts the user to report the disposition of the hit by selecting one of the approved codes assigned in BOSS by the Administrator.



The Add Intel button: allows the user to add additional information regarding the current Hit.



The Misread button: allows the user to flag the Hit as a misread.



The Jump button: Allows the user to "jump" to a specific Hit instead of navigating one at a time.

2.9.4.3 Interactive Buttons – Hits Screen

- IR Patch: The user can click on the IR "Patch" image to open a full-screen view.
- OCR Patch: The user can click on the OCR "Patch" image to edit the license plate number if necessary/Misread.
- Target Button: Shows associated person(s) of interest and opens the Targets Screen.
- Color OV Image: The user can click on the color image to open a full-screen view.
- Map: The user can manipulate the interactive map of the read location (Map Type, Scroll, and Zoom).

2.9.4.4 Set Disposition – Additional Detail



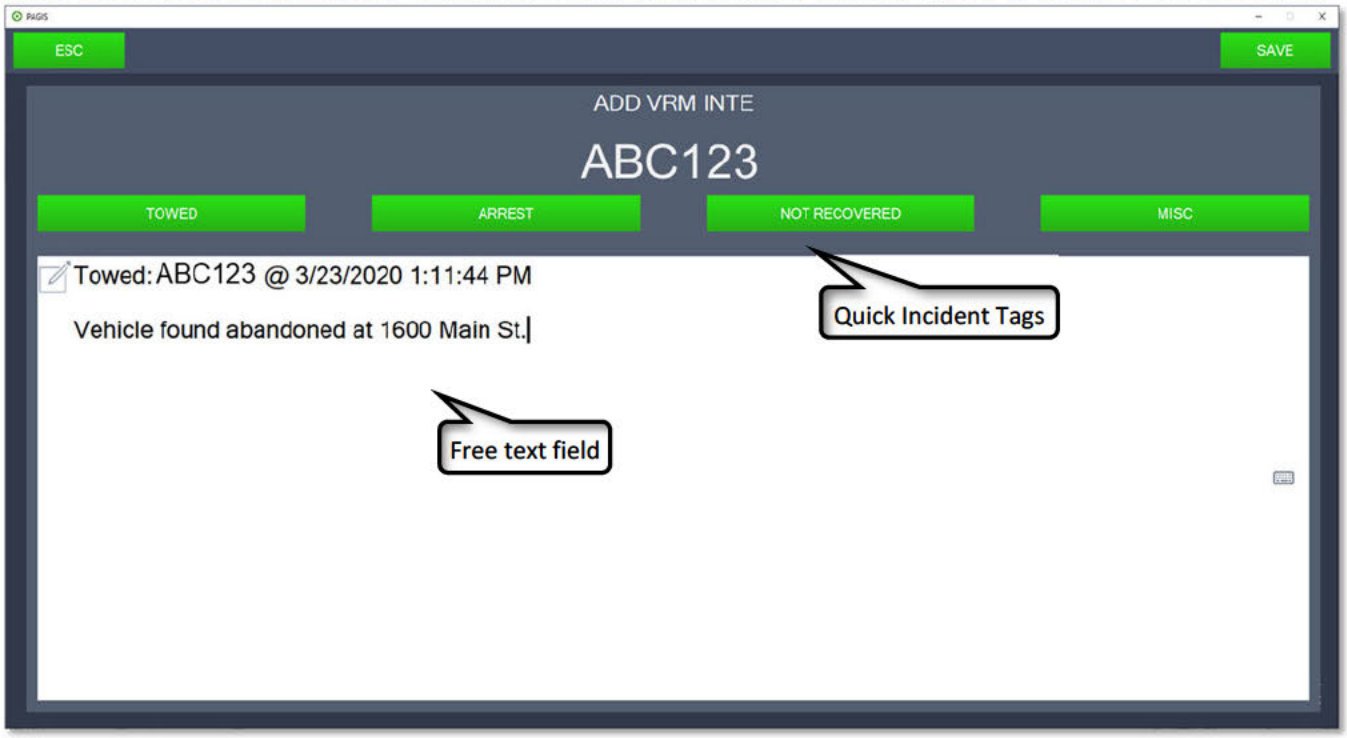
PAGIS allows for additional information to be added to a record in the form of a Disposition. Once Hits are flagged with a disposition code, the Agency is capable of running a "Reads Statistics by Disposition Report" in BOSS. Thus, providing valuable metrics and understanding to leadership in regard to their ALPR Enterprise.

When the "Set Disp" button is selected, the user is prompted to choose from a list of predefined values set by the Agency/BOSS Administrator. Once a disposition is selected and Saved, the disposition is reported to BOSS and will also show up in the Hits Review Screen text box in PAGIS on the next alert notification.

2.9.4.5 Add Intel – Additional Detail

5472

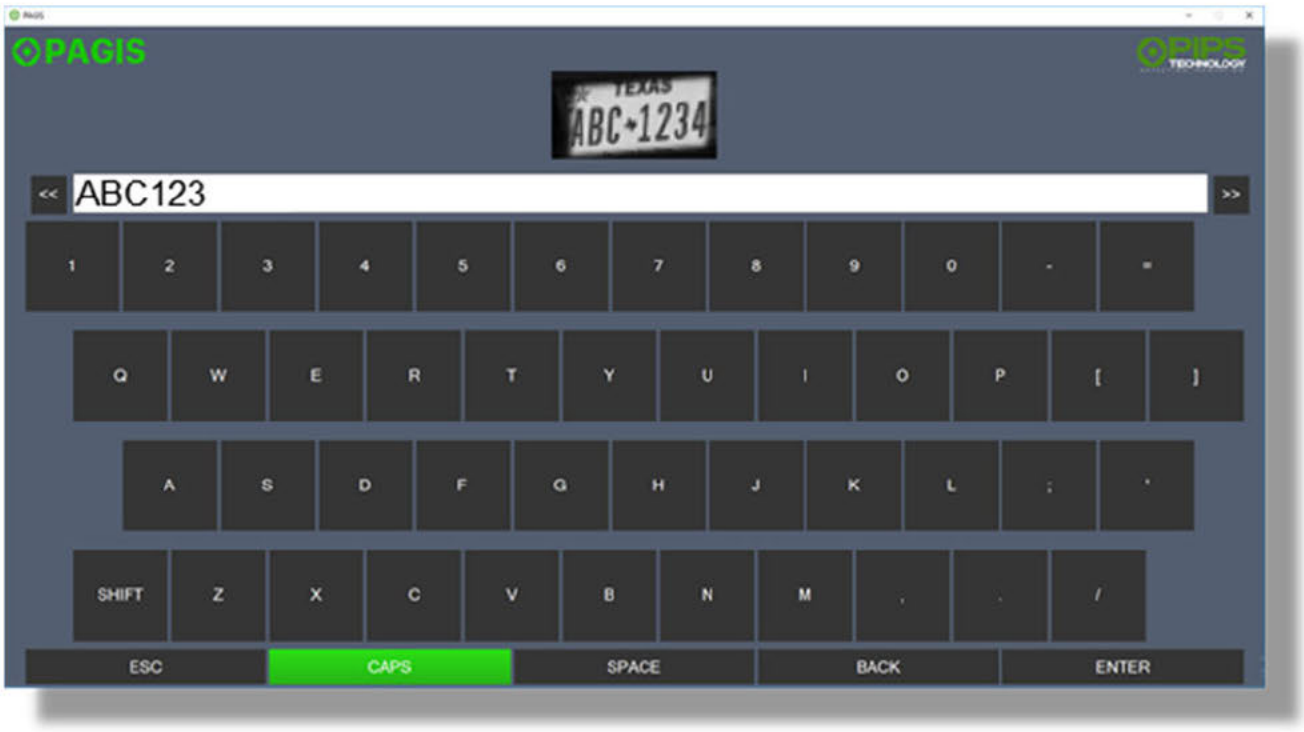
The Add Intel button launches the Intel screen. The user is prompted to assign one of four values: Towed, Arrest, Not Recovered, and Misc. by clicking the associated button at the top of the screen. The user may also enter additional detail regarding the license plate/vehicle. After clicking the Save button, the intel will now appear in the Hits Screen text box.



2.9.5 Misreads

PAGIS allows the user to mark Reads and Hits with incorrect OCR translations as a Misread. This is most commonly done by Agencies for Hits only as users typically don't have time to review every single Read from their shift. Once an errant Hit is corrected, the system updates the record to show it as a Misread and thus improves Agency Hit Reporting.

Correcting a plate read can be accomplished by clicking on the "OCR Patch" in either the Hits or Reads review screen. When the user clicks on the OCR Patch, the OCR Edit Screen opens and allows the user to update the Vehicle License Plate (VLP) data.



2.9.5.1 Marking a Record as a Misread:

The user can mark a record as a Misread from both Reads or Hits Review Screen. Each user can either simply flag the record as a Misread or update the OCR Patch information. **NOTE**: This ability is only available until the user has performed an End Shift function.

Manually Flagging a Read or Hit as a Misread:

1. Navigate to either the Reads or Hits Review Screen
2. Click on the Misread button on the Right
3. Click Save
4. Take note that the record title has now changed from “Read” to “Misread”

Updating the Read/Hit OCR Patch:

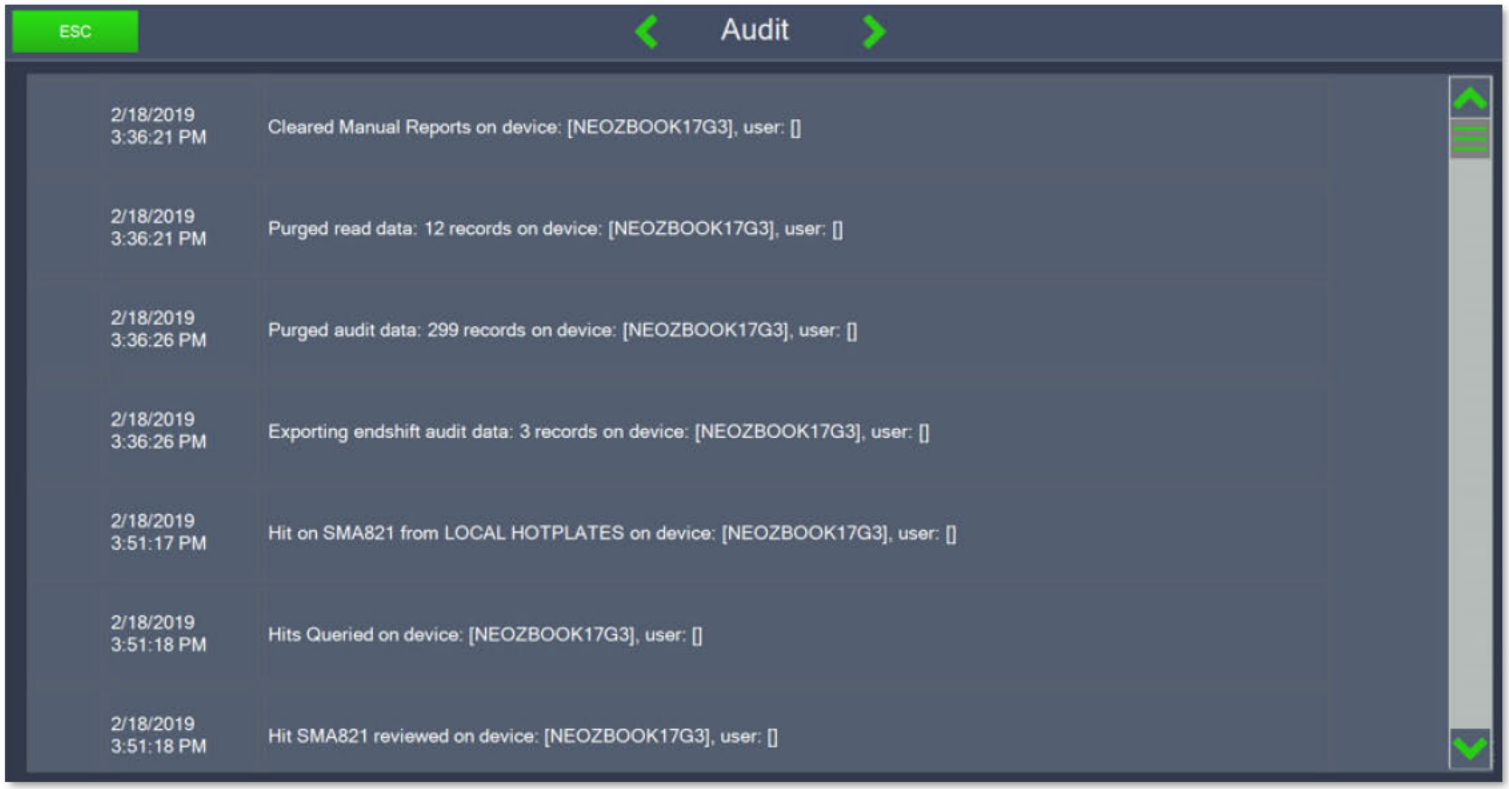
1. Navigate to either the Reads or Hits Review Screen
2. Click on the OCR Patch (Text just under the IR Plate Image)
3. Use the keyboard or on-screen keypad to update the Vehicle License Plate Number
4. Click the Enter Button to Save the changes (and exit back to the Review Screen)
5. When the user saves the changes to the OCR Patch, the record (Read/Hit) is automatically flagged as a Misread

2.9.6 Audits

5474

PAGIS logs both user and key system activity during each use of the software. The audit log captures various information like Read searches, synchronizations, hits, and user login attempts. The Audit Report is viewed in PAGIS by navigating to the Review section and selecting “AUDITS”.

NOTE: Performing an End Shift or syncing the database clears the current log.



2.9.7 Targets

PAGIS has the ability to display information regarding Persons of Interest in response to a Hit alert. Targets are created by BOSS/Hotlist Administrators, and typically provide detailed information about owners of a registered vehicles. When configured, Target data is always linked to unique VLP data (a specific License Plate). If PAGIS registers a Hit on a Plate with a target ID, the Target Information Button is displayed in the Hit Alert window and allows the user to access the Target Screen.



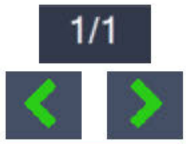
2.9.7.1 The Targets Screen

When a PAGIS user clicks the Target Information Button from a Hit Alert, the Targets Screen opens. This screen displays the information from the BOSS server about the Person(s) of Interest matched to the Hit (license plate).



2.9.7.2 Targets Screen Navigation Buttons

If a Hit alert has more than one Target associated with it, the PAGIS user can navigate all Target information with the buttons described below:



Target Count: The left number is the current record. The right number is the total available for review.

Next/Previous button: Arrows on either side of the target count allow the user to navigate back and forth to review the various targets.



Jump button: Allows the user to "jump" to a specific record without the need to navigate one record at a time using the Next/Previous buttons.

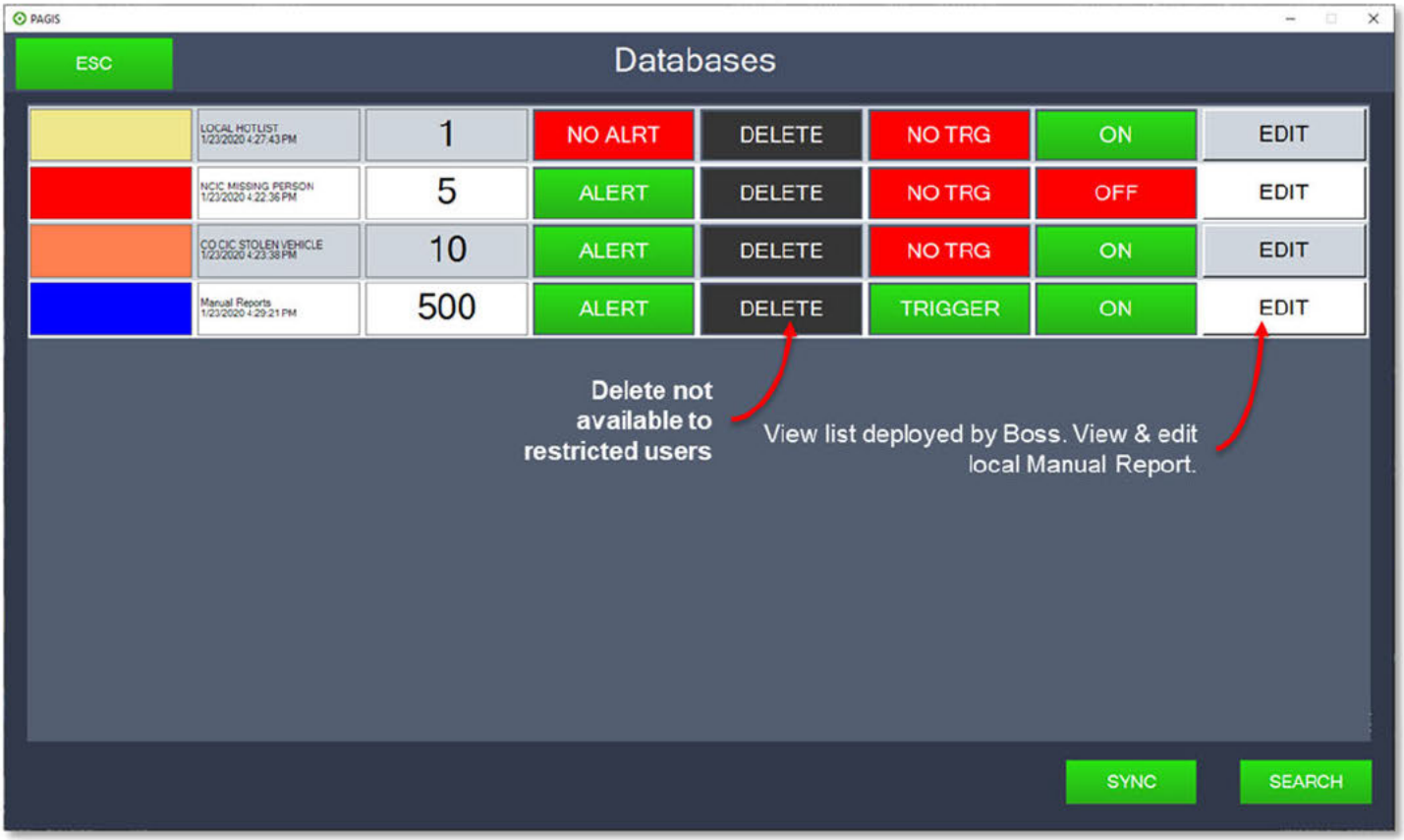


Close button: Returns the user to the previous screen.

2.9.8 Databases

Users can review Hotlists in PAGIS by navigating to the Review section and selecting "DATABASES" on the right. From the Databases Screen, users can toggle Hotlists functions On and Off based on their rights.

NOTE: User rights and Hotlist attributes are configured in BOSS.



2.9.8.1 Databases Screen Functions

Hotlist Color Code: The color attributed to each Hotlist by the BOSS Administrator.

Hotlist Name: The name of the Hotlist given by the BOSS Administrator. Also shows the time/date of the last synchronization.

Hotlist Priority: The priority of the Hotlist assigned by the BOSS Administrator. The lower the number between 1 and 999, the higher the priority. If a plate resides on multiple Hotlists, the list with the higher priority will be displayed first.

Alert Button: Toggles audible alerts On and Off for each Hotlist until the next synchronization.

Delete Button: Based on user rights, allows the user to temporarily delete a Hotlist from PAGIS until the next synchronization. To delete a hotlist, the user must click the button twice (it turns green and then deletes the list).

Trigger Button: Toggles external triggers On and Off. An example of an external trigger is a light bar.

On/Off Button: Disables and enables each Hotlist (each Hotlist is set to On by default).

Edit: View and edit localy created hotplates with a given hotlist, Hotlist/Hotplates deployed via BOSS can only be viewed.

NOTE: Hotlist settings altered in PAGIS will be reset to their default configuration during the next Sync or End Shift. The default configurations are assigned by the BOSS Server/Administrator.

2.9.8.2 Databases Screen Navigation Buttons

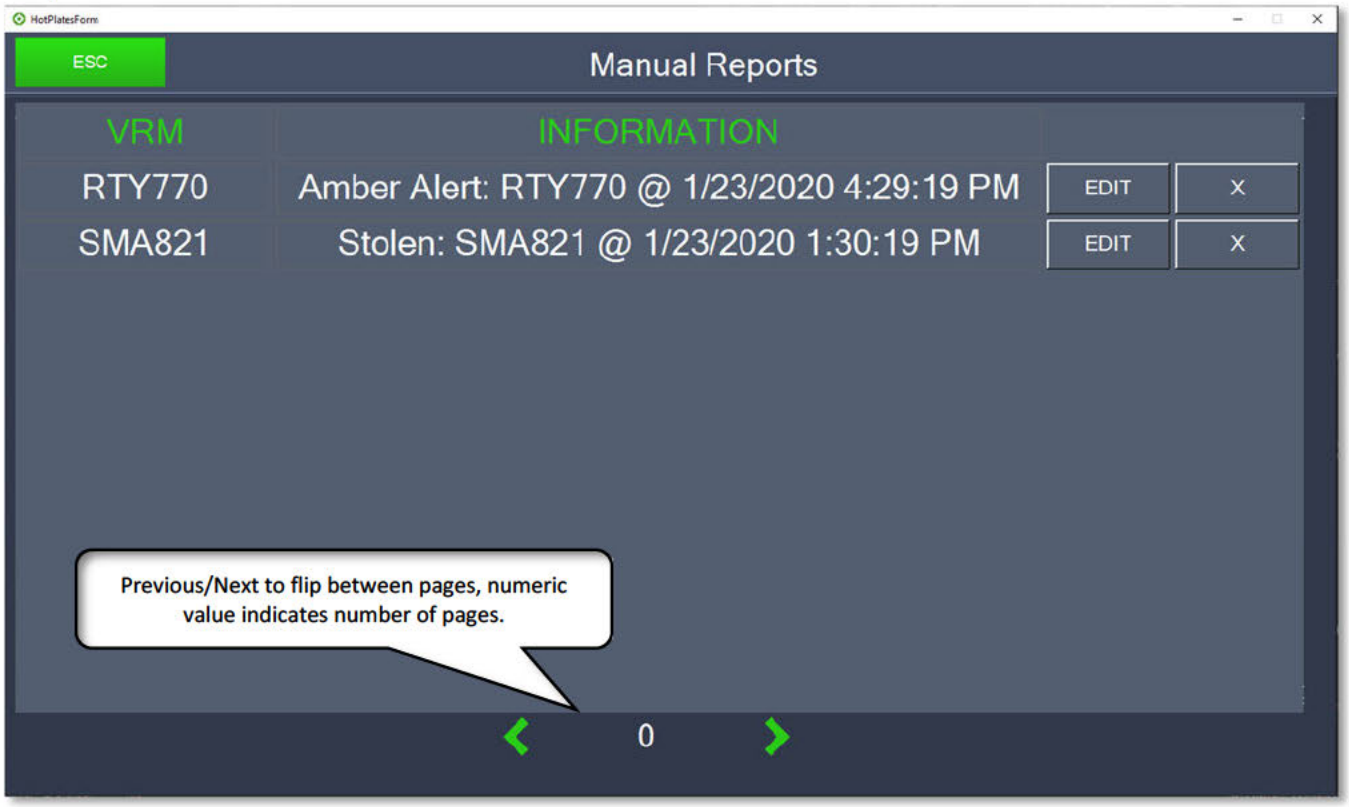
SYNC — **Sync button**: Synchronizes PAGIS with the BOSS server in order to update the Hotlists.

SEARCH — **Search button**: Open the Search Entry Screen (See section 2.8 for more information).

2.9.8.3 Databases Edit- “Manual Reports”

Editing Hotlist has two function based on origin of hotlist.

- Hotlist deployed to PAGIS via BOSS cannot be edited, only the hotplates list can be viewed. Editing/updates are indented to be managed via BOSS.
- Hotlist created in PAGIS, i.e. “Manual Reports” can be managed by PAGIS users, allowing for changes or deletion of the hotplates contained within the hotlist.



EDIT Button: Make changes to the indicustly hotplate information including licanse plate nuamber.
X Button: Remove indivualy hotlist from hotlist.
Previous/Next Button: Scroll thought lising of hotplates contaned within the hotlist. The numeric value indicates the number of pages.

TROUBLESHOOTING TIPS

This section provides some basic troubleshooting tips and information

3.1 Troubleshooting & Tips

- The first login to PAGIS after the new install of an unconfigured version does not require a username or password. Simply click Login to be granted Admin access to the software.
- A good means to test the communication from the MDC to BOSS is ping or telnet (over TCP 8092) through the command prompt.
- A good means to test the communication from the MDC to the SX Processor is ping or telnet (over TCP 9000) via command prompt.
- For many other troubleshooting tips, see Appendix C – Frequently Asked Questions

3.1.1 PAGIS with NetMotion VPN

Agencies utilizing NetMotion VPN software on the MDC will need to apply the following passthrough steps:

1. Login to the NetMotion server as administrator
2. Click Settings > Then select Client > Select Global Client Settings > Then select Passthrough List
3. Click the “Add…” button on the right > Select “Network Address”
4. Enter the following settings (as shown):
    A. IP address:192.168.200.0 (the zero is correct, it's an IP address “range”) Subnet Mask: 255.255.255.0.
    B. Keep all other settings default (as shown) and click OK.
5. The MDC must then disconnect from NetMotion and reconnect again for the settings to be applied locally.

3.1.2 Cisco VPN Client:

Make sure Stateful Firewall is unchecked and "Allow Local LAN".

3.1.3 Microsoft .NET 3.5 Installation

The PAGIS Software requires Microsoft .NET Framework 3.5 specifically. If the MDC doesn’t have .NET, it can be downloaded from the Microsoft website.

3.1.4 Firewall Settings for Client-Server Installations

For client-server installations, the Windows Firewall needs to allow the SX Processor and the MDC to communicate. If the MDC is maintained by a Network Administrator, he or she should be contacted before making changes to the firewall.

Option 1: Allow Microsoft Windows Version 8 or newer to auto-detect the launch of the PAGIS.exe application and use the wizard to add the EXE to the exception list (making note of Public or Private Network settings as necessary).

Option 2: Add PAGIS to the exception list manually by browsing to the install path of PAGIS. The default is below for reference: “C:\Program Files (x86)\PIPS Technology, Inc\PAGIS2\PAGIS.exe”

Option 3: Add the communication ports manually:
TCP 8092
TCP 9000
TCP 9001
TCP 32023
TCP 32029
TCP 10000
TCP 10010
NOTE: XML Datastream uses TCP 10100 and TCP 7000

APPENDIX A: THE GLOSSARY

ALPR/ANPR	“Automatic License Plate Recognition/Automatic Number Plate Recognition”.
BOSS	“Back Office System Software”. This is the ALPR server.
GPS	“Global Positioning System”.
GUI	“Graphical User Interface”.
Hotlist	A database or list that contains vehicle license plates of interest (“alert list”).
IR	Infrared light.
License Plate	Also called a tag or number plate.
MDC	“Mobile Data Computer”. This is the tablet or laptop in the vehicle.
OCR	“Optical Character Recognition” (also referred to as a “cardet”).
OS	“Operating System”.
PAGIS	This is the License Plate Capture Software most commonly used in an ALPR vehicle.
Service	Operation mode of the PAGIS software. Service or “VPRelay” is used to refer to PAGIS instance that is running directly on the PIPS mobile processor without a GUI interface, this mode is intended to run in conjunction with MDC version of PAGIS installed on laptop connected via Ethernet.
Standalone	Operation mode of the PAGIS software. Standalone is used to refer to PAGIS instance that is running directly on the PIPS mobile processor with a GUI interface.
SX	SX is a short notation referencing PIPS’s mobile processor, commonly the SX is followed by the generation number of the processor, i.e. SX3, SX4 & SX4e.
UI	A “User Interface” is the means in which the user can access and navigate the software.
USB Flash Drive	Also called a thumb drive or memory stick.
VLP	“Vehicle License Plate”.
VPN	“Virtually Protected Network”.
VPRelay	Operation mode of the PAGIS software. VPRelay or “Service” is used to refer to PAGIS instance that is running directly on the PIPS mobile processor without a GUI interface, this mode is intended to run in conjunction with MDC versions of PAGIS installed on laptop connected via Ethernet.
Whitelist	Opposite of a standard BOSS Hotlist. This is a list of license plates that should not trigger an alert.

APPENDIX B: PAGIS SOFTWARE DATABASE FILE

This section is used to configure the PAGIS Software when it's not being used with the Back Office System Software (BOSS). Comma-separated value (CSV) format is the only format the PAGIS Software supports for importing data into the vehicles for the purpose of matching against the captured license plate data. PAGIS will support CSV files with any number of columns, called "fields", as long as the first field is the VLP (Vehicle License Plate). **NOTE**: The CSV format is standard ASCII.

Example CSV Files:

1. *ABC123, Red, Ford, Explorer, 1996, WANTED XYZ456, Blue, Audi, A4, 2001, MURDER*
2. *45ABC234, Vehicle wanted in associated with a kidnapping on 12/5/2005 995BD233, Vehicle reported stolen from Liz's Lounge at 6am on 12/1/2005*
3. *UIO223 ABC123*

General Function:

PAGIS calls/utilizes files in pairs. Each database in PAGIS is created using two files; a CSV file, and an INI configuration file. Without both of these files, the database will not load and PAGIS will not "see" it. Each CSV file/hotlist must have the exact same name as the INI configuration file. Example: Stolen.ini and Stolen.csv will work. Stolen.ini and Plates.csv will not.

Reading an INI Configuration File

Lines that appear in brackets [] are called "Headings". The labels that appear inside the headings, are called "values". Values will always contain an equal sign (=). If a line starts with a semicolon, it is considered to be a comment and is not read by the software. There is no limit to the number of comments in the INI file.

The [SETTINGS] Heading

The values in the Settings heading are: NumFiles, DbName, DbColor, Priority, Covert, Alarm, and NumFields.

- NumFiles: Determines how many database files the system should split the specified hotlist into. Generally, this value is set to 1. But for larger hotlists (200,000+ lines), a number of 2-5 may be more desirable.
- DbName: Tells the PAGIS Software what the displayed name of the hotlist should be.
- DbColor: Sets the display color of the hotlist. This is merely an esthetic setting and not a functional setting. The right-hand side of the equal sign is the HEX value representing the ARGB values for the color. If this value is unknown, the Admin should simply leave this line out of the file.
- Priority: Designates the priority of this hotlist in relation to other hotlists in the system. The highest priority database is 1 and the lowest is 999. **NOTE**: if a plate resides on multiple lists the higher priority will be alerted first.
- Covert: Determines whether standard PAGIS Software users are alerted when a hit is made from the database. Covert database can be used for hotlists that are included for information-gathering purposes rather than eliciting user intervention. The system can also be configured to notify via email or SMS message when a hit is made from a covert hotlist.
- Alarm: Sets the audible alert to be played in PAGIS when a hit is made from the hotlist. Values for Alarm are LOW, MED, HIGH
- NumFields: Indicates how many fields (columns) are in the CSV file. If this value is less than the actual number of fields in a file, then the additional fields are placed in the general information area. This value also determines the number of headings of the [Field x] present in the file. For example, if NumFields=2 then there will be two additional headings, [Field 0] and [Field 1]. **NOTE**: Adding "Creation =" will place the timestamp the hotlist was added to the Begin Shift file.

The [FIELD X] Heading

Under the Field heading, there are two configurable values, “Name” and “PAGIS”.

- Name: Tells the system what the name of this field is. If no name is specified, then no name given to the field. The format is Name = <field>
- PAGIS: Specifies how to display the field in the GUI/PAGIS Software.
    - If no value is defined, the field is placed as general information.
    - Values 1-5 represent special fields for the PAGIS Software that translate to the information being displayed in a box of its own when a hit is processed.
    - A value of 6 represents an ID number to cross reference the vehicle from the hotlist with a person from the wanted list.
    - A value of 7 is identical to leaving the value undefined.

Sample INI Configuration File

[Settings] NumFiles=1
DbName=Stolen Vehicles DbColor=ffffff00 Priority=5 Covert=False Alarm=MED NumFields=8
;PAGIS Values
;0 is VRM / VLP (Not User Definable, always Field 0)
;1 is Special Field 1
;2 is Special Field 2
;3 is Special Field 3
;4 is Special Field 4
;5 is Special Field 5
;6 is ID Number (PNC ID, Drivers License, Social Security Number, etc.)
;7 is General Info (Default for all undefined fields) [Field 0]
PAGIS=VRM

Sample INI Configuration File

[Field 0] Name=VRM
[Field 1] Name=Color
PAGIS=3 [Field 2]
Name=Make PAGIS=1
[Field 3] Name=Model
PAGIS=2 [Field 4]
Name=Action PAGIS=4
[Field 5] Name=Warning
PAGIS=5 [Field 6]
Name=PNCID PAGIS=6
[Field 7] Name=Intelligence PAGIS=7

APPENDIX C: FAQ

Q: **HOW DO I ENTER A SUPPORT CASE?**
A: We have a webform you can use here, you can email our Support Team at Support@PIPSTechnology.com, or you can call us on the phone Monday-Friday 8am to 4pm Central Time (9am-5pm Eastern) at (833) 747-7577 Option 2.

Q: **HOW DO WE CREATE USERS IN PAGIS?**
A: The agency BOSS Administrator creates all users, both for BOSS and for PAGIS. Once the user is created in BOSS, the Admin would click the user's name to select/edit the user. Then click the Advanced button and update the PAGIS specific password. Please note that the username and password fields are both case sensitive and the PAGIS users need to be added to a group with the Role that allows them to use PAGIS/LPCS.

If you have any further questions, please feel free to enter a request for support here.

Q: **WHERE DO USERS CHANGE THEIR LOGIN PASSWORD IN PAGIS?**
A: User passwords are created and updated in BOSS via the UI client software. For the majority of our customers using both the PAGIS Software and BOSS, any user accounts or passwords created in the PAGIS Software itself will be overwritten by the user information defined in BOSS during the next sync.

If you have any further questions, please feel free to enter a request for support here.

Q: **HOW DO WE REQUEST AN RMA REPAIR?**
A: To assist with this, please navigate here to review our RMA procedure as well as to download the request form. Please keep in mind that once submitted, all repairs are reviewed for age of equipment and warranty status before final processing takes place. Additionally, incomplete forms and those without much detail often result in processing delays.

If you have any further questions, please feel free to enter a request for support here.

Q: **WE HAVE NEW MDC LAPTOPS IN THE PATROL CARS, HOW DO WE ADD THOSE DEVICES TO BOSS?**
Q: **HOW DO WE EDIT THE DEVICE NAMES IN BOSS?**
A: The initial device template/skeleton is automatically created in BOSS the first time the device attempts to Sync from the field. Devices should NEVER be created manually. For PAGIS laptops, this is done after PAGIS is installed and configured and Begin Shift is launched. However, if the agency would like to organize the device list by updating the "Device Name" field, those steps are below:
1. Login to the BOSS UI with Admin rights
2. Navigate to Admin > Devices
3. Click on a device name to select it > Click Edit
4. Update the name of the device in the "Description" field (Name field cannot be altered)
5. Click Save > This will take you back to the Device Summary List. The "Device Name" field should show the new name

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **WE HAVE A NEW MOBILE COMPUTER/MDC THAT'S NOT SYNCING WITH BOSS.**
Q: **WE KEEP SEEING AN HTTP_STATUS_CODE ERROR WHEN RUNNING BEGIN SHIFT.**
A: This error most commonly means that a new device in the field (laptop/tablet) can "see" the BOSS server, but that it hasn't been enabled yet to "talk" with it. Follow the general steps below to address this issue:
1. The agency BOSS Administrator will need to login to the BOSS UI client and Select Admin
2. Then select Devices and from there, left click on the device/computer name of that MDC to edit it
3. Once in the Edit screen, Enable the device. This will take you back to the Device List.
4. Click the name to edit the device again. Now assign users/Owners and save.
NOTE: The Select button becomes a Save button when selecting which Groups/Users should have access to login to this device
5. Once that is done, navigate to Admin > Hotlists
6. From here, click on each hotlist one at a time to distribute them to the new device being sure to Save the changes next to the

Distribution field. Note again that the Select button becomes a Save button. And there's another Save button at the top left of the edit window.
7. After this is complete, perform Begin Shift from the field unit/MDC and confirm there are no further errors.

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **NEW PAGIS USER CAN'T LOGIN BUT OTHERS CAN.**
Q: **USERS CAN LOGIN TO PAGIS WITH NO CREDENTIALS AT ALL.**
A: Entry or login to the PAGIS software in the field is partially controlled by the Device settings in BOSS. The users themselves must also be properly setup with an LPCS/PAGIS password. To check the current device settings/ access, perform the following steps:
1. Login to BOSS UI (with Administrator rights)
2. Select the Admin Section
3. Select Devices and then Select the Device in question by PC name
4. Once selected click on the Edit button near the bottom
5. Locate and inspect the "Owners" Field (this is a list of users/groups that have access to login to the device)
NOTE: If this field is blank, the device is in an open configuration mode allowing admin level access simply by clicking login (any credentials would also be accepted).
6. To update the device owners, click the "Select" button next to the Owners field (notice it changes to a Save button)
7. Check which Users/Groups of Users should be able to login to PAGIS from this device
8. Click the Save button next to the field
9. And then click Save in the upper left portion of the Edit window
10. Have a previous user or Admin login to PAGIS and perform Begin Shift to sync the new data
11. A PAGIS Admin can confirm by navigating to Admin, Admin, and then Users to review the list
12. Another test would be to have the new user attempt to login

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **WHEN USERS LOGIN TO PAGIS, THEY ONLY SEE A GREY SCREEN.**
Q: **CAMERAS AREN'T SHOWING UP IN PAGIS ANYMORE.**
SEE ALSO: "THE LINK LIGHTS ON OUR ALPR COMPUTER/MDC WON'T TURN ON OR FLASH"
A: Below are some basic troubleshooting steps you'll want to follow before creating a support ticket.
1. Doublecheck the physical power switch on the black box/Processor is On. In many vehicles, there is also an in-line switch in the front of the vehicle that needs to be switched On. When the units are properly powered and on, you should see lights and hear fans running.
2. Confirm that the network adapter settings on the laptop match the proper Static IP scheme for the SX Processor in use. The older scheme is 192.200… and the newer scheme is 192.168…. NOTE: the adapter status in Windows should say "unidentified network". If it says "cable unplugged" the laptop can't "see" the SX.
3. If the power and Static IP settings are good and things still aren't working, test further by disabling the three main software related culprits. Turn off/bypass the local Windows firewall, antivirus, and VPN software one at a time.
4. If you're still not able to see the camera feed after that, you may want to use a different network cable as those can get damaged over time and then confirm that the cord is properly plugged into the ports.
5. If the network cord from the SX Processor is routed through a docking station, then it's possible the dock is preventing the traffic. You should contact the dock's manufacturer for the most recent firmware. To test for this, remove the laptop from the dock, directly connect the network cord to the laptop, and then reconfigure the network adapter settings (remove the static settings from the dock's adapter/ and assign the static IP to the laptop's NIC adapter).

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.
Q: **THE LEFT FRONT CAMERA ON OUR ALPR VEHICLE IS NO LONGER SHOWING IN PAGIS**?
Q: **HOW DO WE TROUBLESHOOT MOBILE CAMERAS**?
A: Below are the main troubleshooting steps to test the camera(s) and cable(s) on a system where only one or two cameras are no longer displaying images.
Step 1: Confirm MDC/SX communication - steps shown in section "Cameras aren't showing up in PAGIS anymore."

Step 2: Access the SX Processor – RDP or directly connect a monitor, keyboard, and mouse to the SX. Contact PIPS Support for help with RDP if the credentials are unknown to the agency.
Step 3: Confirm camera activity – Launch Tools. Then open P6Utility or Mobile Toolkit. Check the camera feeds/function by switching the Input menu to the camera(s) in question
Step 4: Unplug and Reattach the Camera Cables – Note, the cables DO NOT TWIST. The metal locking nut on the cable slides back about a millimeter and the cable comes straight out. Do this at the SX Processor and the Camera. You may need to remove the camera from the mount in order to unplug the cable successfully (most brackets use a #3.5 Hex/Allen Wrench)
Step 5: Swap Port on SX Processor – At the SX Processor, swap the camera cables from the non-working camera to a port with a working port (Take care to note the swap so the cables get back to their original ports). If the camera outage stays at the port site, the issue is most likely the capture card on the SX Processor and will require RMA (Example: working Left cam is swapped to port of non-working Right cam and no longer functions. AND the previous non-working Right cam starts working once it's plugged into the Left cam's port). If the fault/error stays with the camera regardless of SX port, continue to Step 6.
Step 6: Physically Swap Camera Locations – Once all other items are checked, move the camera itself to a working position in order to test the cable. (Example: physically move Left camera to the Right camera position on the top of the vehicle) Connect the cable at the new position and test feed in Tools > P6Utility/Mobile Toolkit. If the camera works at the new location, the issue is most likely a bad cable. If the camera still does not work, the issue is most likely a faulty camera in need of repair/RMA.

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **WE'RE NO LONGER GETTING GPS IN PAGIS.**
Q: **WE'RE NOT SEEING GPS DATA FROM SOME OF OUR FIELD UNITS IN BOSS.**
A: Below are the basic troubleshooting steps for checking the GPS of field units:
1. Login to PAGIS (as Admin)
2. Navigate to Admin section, then click the Admin button
3. Select "System" on the left pane
4. Confirm/Set the button at top to "Default"
5. Remove any value(s) stored in the GPS Connection String field. Leave '5' in the Computer String.
6. Click the Save button to retain changes made.
7. Close PAGIS fully and relaunch and log back in to test (Note: GPS will only show with test reads/hits)
8. For versions of PAGIS 2.9 and up, test with a GPS Connection String of 6 if the blank field doesn't work. Save the changes. Log out. Close the software and then relaunch to test.

Please be advised, that some GPS issues can be caused by local or domain firewall settings, antivirus software, or any other software package monitoring/transmitting network data. To test these, disable or bypass those software options on the MDC and retest.

If these initial troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **HOW DO I INSTALL THE PAGIS SOFTWARE?**
Q: **I JUST LOADED PAGIS ON A MACHINE AND IT CRASHES WITH A .DLL ERROR WHEN I TRY TO LAUNCH IT.**
A: The most common installation of PAGIS is Client/Server or "VPRelay Mode". The .dll error is caused by the installer not being run from the HDD and/or the wrong install option being selected (Example: SupeRex instead of MDC). The best practices for the installation are below. (Note, this does not cover MDC or PAGIS configuration, only the act of installation)
1. Always copy the installer over to the HDD/Desktop of the MDC. Never run it from a thumb-drive or network share
2. Regardless of how you're logged in to Windows, right click the installer and select "run as Admin" or "run with elevated privileges"
3. Continue through the message/error about OS compatibility
4. Click next on the wizard and then be sure to select the MDC option (to use with VPRelay)
5. After that, it's next, next, next, finish the reboot is not necessary

If these steps did not resolve the issue, please feel free to enter a request for support here.

Q: **USERS ARE GETTING HITS/ALERTS ON PREVIOUSLY RECOVERED STOLEN PLATES.**
Q: **USERS AREN'T GETTING HITS FROM KNOWN ACTIVE PLATES.**
Q: **THE HOTLISTS IN PAGIS DON'T SHOW TODAY'S DATE.**
Q: **THE HOTLISTS AREN'T SYNCING WITH BEGIN/END SHIFT.**
A: Whether it's from data latency or just use over time, the local file structure can get some minor corruption and will need to be refreshed. The steps below show the best practices:
1. Login to Windows with Admin rights (ability to uninstall/delete software)
2. Login to PAGIS and perform an End Shift
3. When complete without error, Logout of PAGIS and then Exit/Close the program
NOTE: If the End Shift fails or displays an error, contact Support for additional assistance.
4. If there were no errors, locate the PAGIS icon on the desktop.
5. Right click on the icon and select "Open File Location" (This should open a window where the program was installed)
6. Scroll up and locate the folder labeled "data". Double-click it to open it
7. Select and delete everything in here EXCEPT for "Attributes.db"
8. Once that's complete, Login to the PAGIS software again
9. Perform a Begin Shift. This will pull down fresh data from the server
NOTE: Once complete, the files in the data subfolder as well as the Databases section of PAGIS should be restored.

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **IS PAGIS COMPATIBLE WITH OUR NEW WINDOWS 10 LAPTOPS?**
A: Although there's a warning about compatibility during the install of PAGIS on any Windows OS after XP, it is compatible with all them. However, we have seen errors occur when agencies copy and paste folder structures from previous installations. This of course is not recommended.

Q: **THE LINK LIGHTS ON OUR ALPR COMPUTER/MDC WON'T TURN ON OR FLASH.**
Q: **OUR WINDOWS 10 MDC WAS WORKING BUT HAS STOPPED COMMUNICATING TO THE SX PROCESSOR.**
A: There are many variables with troubleshooting any network connection. And the connection from the ALPR computer to the SX Processor is no different. The following troubleshooting list highlights the most common:
1. The physical network cord is bad/damaged.
A: Test with a different cable and confirm that it is plugged in fully

2. The network adapters are not configured or have incorrect static IPs
A: Confirm the Static IP scheme in use and properly configure the network adapters

3. Local and/or Domain Firewall rules have prevented the flow of communication
A: Disable or bypass these and test again

4. VPN, Anti-Spyware, Antivirus, or other monitoring software has blocked communication
A: Disable or bypass these one at a time and test after each to find the culprit(s)

5. Docking Station Firmware can be incompatible with some newer computers or become corrupt
A: Test by running the network cord straight to the MDC and then configuring the network adapters (NOTE: It would also be a good idea to contact station manufacturer to see what the latest firmware version is and upgrade as necessary)

6. The NIC Drivers have become corrupt
A: Update the specific Networking drivers in use on the MDC through the Device Manager in Windows

7. Turn off all power saving settings of the Ethernet Adapter in the device manager
A: Uncheck "Allow the computer to turn off this device to save power"

8. Check for Windows 10 update 1709 and 1803 as this update will not allow the NIC and Cellular Aircard to run simultaneously
A: Settings > Update and Security > Windows Update > "Update History" link – if there, see the steps in the FAQ

If these troubleshooting steps did not resolve the issue, please feel free to enter a request for support here.

Q: **AS SOON AS WE DOCK OUR MDC, WE LOSE CONNECTION TO THE WIRELESS.**
Q: **OUR WINDOWS 10 LAPTOP LOSES CONNECTION TO THE INTERNET WHEN THE NETWORK CABLE IS PLUGGED IN.**
Q: **OUR MDC HAS MICROSOFT VERSION 1709 OR 1803 AND CAN'T CONNECT TO WIFI WHEN DOCKED.**
A: Microsoft Updates (1709 and 1803) prevent the Wireless connection as soon as a Network cable is plugged into the device. This also occurs for MDCs/laptops that are docked (where the Network cable from the SX Processor is run through the docking station). As of January 2019, the steps to correct this are below.
WIN10 version 1803
1. Open Regedit
2. Expand HKEY_LOCAL_MACHINE
3. Navigate to Software > Policies > Microsoft > WcmSvc > Local
4. Right click on Local > Hover over New > Select "DWORD (32-bit)"
5. Name the new value "fMinimizeConnections"
6. Right click the on the new name > select Modify > Set value data to 1 (leave base Hex) > Click OK
7. Reboot Windows and test

WIN10 version 1709 - Microsoft fixed this with Update KB 4284822. But if you still have issues, the registry steps are below:
1. Open Regedit
2. Navigate to HKEY_LOCAL_MACHINE > Software > Policies > Microsoft > WcmSvc > Local
3. Right click on Local > Hover over New > Select "DWORD (32-bit)"
4. Name the new value "fMinimizeConnections"
5. Right click the on the new name > select Modify > Set value data to 0 (leave base Hex) > Click OK
6. Then Navigate to HKEY_LOCAL_MACHINE\Software\Microsoft\Wcmsvc
7. Right click on Wcmsvc > Hover over New > Select DWORD (32-bit)
8. Name the value "IgnoreNonRoutableEthernet"
9. Right click on the new value > Modify > Set value data to 1 (leave base in Hex) > OK
10. Reboot Win10 and test

If the steps above did not resolve the issue, you may need to address this with Microsoft. Their support site is here.

6 January 2020

PIPS Product Bulletin

With the start of the new year, we have a few announcements and reminders regarding PIPS Technology™ solutions. We are starting 2020 with revamped software and product solutions that have greater capabilities to help you in your daily mission! We dedicate a third of our staff to product and solution improvements and innovations to make your job easier, safer, and more efficient.

BOSS 4 Continued Roll Out

In 2019, we released an early version of our new BOSS 4 software. This new software is a leap forward in design and usability compared to our BOSS 3 product and provides additional features not currently in existing software. The new web-based design also offers the ability to rapidly add features and deploy the software to any number of users in your network. As before, the BOSS software gives you complete control over your data and allows you to dictate who you share data with and how much access to give them.



BOSS 4 provides the ability for you to host inside your own servers/data center as with previous generations of BOSS. However, in response to feedback from the customers, we are also now offering a Hosted Managed Service. Providing industry leading infrastructure and service management, including 99.999% infrastructure availability with the latest in security, this option provides the ability for your teams to focus on front-line duties rather than worrying about Databases, Servers and Infrastructure.

Give us a call at 833-PIPS-LPR (833-747-7577) and speak with our sales team to get a free online demonstration and test run.

New Mobile System Hardware and Software Continued Roll Out

Also, in 2019, we released a new version of our popular mobile system with the SX4e processor and P720 camera. The P720 uses the same form factor as the robust P634 camera, but provides better lenses, better sensors which provides higher quality images, and more lane coverage. The optical performance improvements this technology provides improves detection and recognition rates compared to previous generations of PIPS' products and those of our competitors.

The SX4e is the power-over-ethernet (PoE) version of the processor allowing more versatility in configuration and deployment of the mobile system. System configuration still allows between one to four cameras per processor, but the PoE cable can have 100 feet between processor and camera.

Questions / Concerns? Contact Technical Services (833) PIPS-LPR or (833) 747-7577

Along with the new hardware, we are making continuous improvements to our PAGIS in-car mobile software. This includes security enhancements, more firmware updating, and additional mapping tools. Our development team continues to roll out new changes and features which are available free of charge, during their warranty phase, to those customers who have already upgraded.



If you are interested in any of our new mobile products, please reach out to our sales team for a demonstration. You can also contact our support team to see if your existing system is on the latest software or firmware version. Contact us at 833-PIPS-LPR or at support@pipstechnology.com.

BOSS 3 End of Life Notice – December 31, 2020

At the end of 2020, we will no longer support our BOSS 3 software. This includes software updates and service/support inquires related to this product.

The migration from BOSS 3 to BOSS 4 is designed to be made as simple as possible for the customer, with specific migration tools developed by PIPS to aid the process. Please get in touch so we can discuss how you could migrate to BOSS 4 from BOSS 3. For any customers committing to upgrade before the end of March 2020 we will be crediting any pro-rata BOSS3 support fees against the BOSS 4 license as well as waiving the migration cost.

We will naturally continue to support those customers who have recently purchased software support for the BOSS 3 product until the end of the current obligation.

Questions / Concerns? Contact Technical Services (833) PIPS-LPR or (833) 747-7577

IRIS P500 Latest Software Build with feature enhancements and bug fixes
The IRIS P500 series camera was newly released in 2019 and received superb feedback from those customers who used it, including beating competitor products in numerous “head to head” performance evaluations by customers.

As with all new products we were providing software releases throughout the year in direct feedback from customers for enhancements as well as reported bug fixing highlighted to our Service / Support teams.



We formally released 4 updates during the year and one hot-fix in response to feedback, including the latest hot fix in December 2019. These releases resolved the reported issues, including one that can appear in some of the earlier IRIS cameras under certain circumstances which were not running on the latest released software standard. This manifest itself when the camera first booted, it may erroneously use GMT time instead of the configured time zone. This will cause the camera to record images with the time stamp of GMT instead of local, but not give an indication that the image is using an incorrect time zone. Once the camera is finished booting and synchronizing with its time source (typically within 1 minute), it will use the local time zone, but the images captured during the booting process will have an incorrect timestamp.

We have issued a firmware update to correct this issue. This ensures that the correct time zone is applied to all reads, even during boot up. Please call our support line, 833-PIPS-LPR, to receive the latest firmware and have it setup on your camera system.

NOTE – this only applies to the IRIS P500 series cameras and does not manifest itself in previous generations of our products.

Questions / Concerns? Contact Technical Services (833) PIPS-LPR or (833) 747-7577

New Termination Box (T-Box) Design
In 2020, we begin rolling out a new T-Box design. This design reduces the weight and size of the previous T-Box, while continuing to provide the same functionality. The new design also helps control costs, which in turn helps prevent price increases on the product.

Please call our support line at 833-PIPS-LPR or email us at support@pipstechnology.com to let us know how we can continue to improve this and our other products.

Update to Latest Versions of Software and Camera Firmware
Throughout the year, we have released updates to the firmware of our camera products (both mobile and fixed) along with software updates to PAGIS. We recommend that either your IT staff check to see if your cameras are on the latest patch or contact us to determine your camera status.

Our service staff would be happy to evaluate any of your PIPS products to determine if they are on the latest version. Give our support team a call at 833-PIPS-LPR.

Update Product Passwords
As a means of providing sound security, we recommend changing that the passwords on each camera system and software. In following CJIS policy (code 5.6.2.1.1), we recommend passwords should contain the following:

1. Be a minimum length of eight (8) characters on all systems.
2. Not be a dictionary word or proper name.
3. Not be the same as the User ID.
4. Changed regularly (ideally every 90 days)
5. Not be identical to the previous ten (10) passwords.
6. Not be transmitted in the clear outside the secure location.

Remember, every law enforcement agency that uses CJIS is audited at least once every three years. We are aware of customer being asked about their password policy in relation to their ALPR infrastructure and would urge the ALPR cameras to be considered as part your organizations' password policy.

Regards,



Peter Crary
Global R&D Director, ALPR/ANPR

Questions / Concerns? Contact Technical Services (833) PIPS-LPR or (833) 747-7577

Requirements and Specifications
Back Office Server Software (BOSS4)

On-Premise Applications Server

Below, there are the minimal recommended configurations for different capacity configurations for BOSS4 On-Premise infrastructure.

Application Servers Specifications				
Configuration	**Demo**	**Medium**	**Large**	**High Capacity**
ALPR Devices	1 to 3	3 to 50	50 to 150	Beyond 150
Average Daily Intake	Around 30,000 events	Around 500,000 events	Around 1,500,000 events	Beyond 1,500,000 events
Average of users querying data	3 users	15 users	25 users	Beyond 25 users
Alert list averaging	Around 1M records	Around 2M records	Around 2M records	Around 2M records
Operating System	Amazon Linux / Amazon Linux 2 x64 Linux x64 (RHEL/CentOS, Ubuntu, Debian, SUSE) macOS x64 Windows 10 Professional x64 Windows Server 2016 x64			
Memory	16GB	32GB	64GB	192GB
Processor	x64 2.0 GHz 8 cores o better	Server Processor x64 (Intel Xeon Gold) 2 GHz 4 cores, 8 threads, 4MB cache	Server Processor x64 (Intel Xeon Platinum) 2.4 GHz 16 cores, 32 threads, 8MB cache	Server Processor x64 (Intel Xeon Platinum) 2.4 GHz 24 cores, 48 threads, 24MB cache
Hard Drive	7200 RPM SATA3	SSD SATA3	SSD SATA3 or NVMe PCI Express	SSD SATA3 or NVMe PCI Express
Application Space	128 GB of available space	256GB of available space	320GB of available space	512GB of available space

On-Premise Database Server

BOSS4 uses the MongoDB Database Engine.

Specifications of the Database Server				
Configuration	**Demo**	**Medium**	**Large**	**High Capacity**
ALPR Devices	1 to 3	3 to 50	50 to 150	Beyond 150
Average Daily Intake	Around 30,000 events	Around 500,000 events	Around 1,500,000 events	Beyond 1,500,000 events
Average of users querying data	3 users	15 users	25 users	Beyond 25 users
Alert list averaging	Around 1M records	Around 2M records	Around 2M records	Around 2M records
Database Engine	Mongo DB Community	MongoDB Enterprise		
Operating System	Amazon Linux / Amazon Linux 2 x64 Linux x64 (RHEL/CentOS, Ubuntu, Debian, SUSE) macOS x64 Windows 10 Professional x64 Windows Server 2016 x64			
Processor	x64 2.0 GHz 8 cores o better	Server Processor x64 (Intel Xeon Gold) 2.5 GHz 4 cores, 8 threads, 4MB cache	Server Processor x64 (Intel Xeon Platinum) 2.4 GHz 16 cores, 32 threads, 16MB cache	Server Processor x64 (Intel Xeon Platinum) 2.4 GHz 24 cores, 48 threads, 24MB cache
Memory	N/A	32 GB	128GB	256GB
Hard Drive	7200 RPM SATA3 Not suitable for camera implantation with any kind of data retention expected	SSD SATA3 RAID level redundancy and scheduled DB backups recommended *See sizing chart for storage.*	SSD SATA3 or NVMe PCI Express RAID level redundancy and scheduled DB backups recommended *See sizing chart for storage.*	SSD SATA3 or NVMe PCI Express RAID level redundancy and scheduled DB backups recommended *See sizing chart for storage.*

This document and its contents are intended for the recipient only. Copying, redistributing, or discussing with any other party outside of the intended recipient and PIPS-Neology is prohibited.

Data Storage Requirements

The calculation of storage applies to Cloud and On-Premise configurations.

Approximant Sizing based on Hybrid data, Mobile & Fixed Camera data			
# of records	Database size Metadata and indexes	Repository Size Imagery	Total
1 Million	32GB	153GB	**185GB**
5 Million	64GB	763GB	**827GB**
10 Million	320GB	1.5TB	**1.82TB**
50 Million	1.6TB	7.5TB	**6.1TB**
100 Million	3.2TB	15TB	**18.2TB**

The calculations for storage are approximated based on an average sampling of around 192KB per event.

System Communication Ports

Ports	TCP / UDP	Description
80	TCP	HTTP Web access port for mapping.
443**	TCP	HTTPS Web access for client access, SW Updates, AWS Services.
8090	TCP	Legacy Pagis 268 data port, not required unless using older Pagis SW.
8092	TCP	REST API data port for PAGIS, supports TLS v1.0.
8093	TCP	REST API data port for PAGIS, supports TLS v1.3.
10000	TCP	VES Image port for fixed cameras.
10005	TCP	VES Heartbeat for fixed cameras.
10010	UDP	VES Ping port for fixed cameras.
27017	TCP	MongoDB data connection port.
**	Specific BOSS4 Micro Services require Internet access to AWS Services managed by Neology.	

Additional System Requirements

Application Server:

- Linux x64 (RHEL/CentOS, Ubuntu, Debian, SUSE).
- MacOS x64.
- Windows 10 Professional x64 or newer.
- Windows Server 2016 x64 or newer.

Database Server:

- MongoDB.

Client-Side:

- Chrome v72 and newer, we are currently working to validate more browsers.
- Standalone Alert application- Windows version 7 and up, x32/x64.

Remote Access:

- Scheduled or 24x7 remote access is required during installation and testing.

This document and its contents are intended for the recipient only. Copying, redistributing, or discussing with any other party outside of the intended recipient and PIPS-Neology is prohibited.

Frequently Asked Questions, FAQ's.

Q. Support for other Operating Systems?
A. Currently supported are Windows based x64 OS's, MacOS x64, Linux x64 (RHEL/CentOS, Ubuntu, Debian, SUSE). The preferred OS is Linux for BOSS application server.

Q. Can Boss work in virtual OS's?
A. Yes, supported are Windows based x64 OS's, MacOS x64, Linux x64 (RHEL/CentOS, Ubuntu, Debian, SUSE). The preferred OS is Linux for BOSS application server.

Q. How long does a typical BOSS4 installation take?
A. Boss4 installation and setup can vary depending on requirements, typical installations can take anywhere for 1-3 days to complete and possible longer depending on data migration.

Q. What Database programs are supported?
A. Currently MongoDB is supported, other databases will be supported in future releases.

Q. Can you migrate data from non-PIPS ALPR servers into BOSS4?
A. No. We can only migrate data from existing BOSS3 systems.

Q. Can existing BOSS3 database files be utilized when upgrading to BOSS4?
A. No. BOSS4 is a completely new database structure, however data can be migrated.

Q. How long can data migration take.
A. Data migration can vary depending on volume, anywhere from hours to days.

Q. What data is miraged from BOSS3?
A. Customizable among the following. Reads, Hits, Users, Groups, Roles, Devices, Sites, and Hotlist.

Q. Can BOSS4 reside on same OS as database application?
A. Yes. Only small demo or trial configurations can support same OS for both.
A. No. Production deployments it is not recommended.

Q. Can BOSS4 ports be customized?
A. No. Current BOSS4 version does not support customer port configurations.

Q. Can BOSS4 versions share data with older BOSS3 versions?
A. Yes. Data sharing is built into our latest versions to connect with other older versions of BOSS3.

Q. How are the database tables created?
A. BOSS4 application installation and start configures the required database structure needed.

This document and its contents are intended for the recipient only. Copying, redistributing, or discussing with any other party outside of the intended recipient and PIPS-Neology is prohibited.

PIPS Fixed ANPR Camera User Manual

PIPS Fixed ANPR Camera User Manual

Version 4.9.11308 created on 2020-12-04 13:14:46 ; with commands from versions: P492:version 4.9.11308 .
Copyright © 2007-2017 Neology

Table of Contents

1. Introduction 1
P382 1
P392+/P492 2
Assumptions 2
Conventions 2
2. Getting started 4
Connectivity 4
Discovery 4
Serial RS-232 5
Ethernet 5
Networking setup 5
Basic Configuration 6
Connecting 6
SSH 6
Restarting and Shutting Down 7
Restarting after changing settings 7
Switching off for planned maintenance 7
Power-cycling 7
3. PIPS ANPR Toolkit 8
Viewfinder 8
Vehicle Events 9
Review 9
Camera Software 9
Software Management 10
Software Installation 10
4. Camera technical overview 11
Interfaces: Output mechanisms 11
5. Configuration using Webmin 13
Camera control 13
Network 13
Mounting network disks 13
NFS 14
Windows shares 14
6. PIPS ANPR Shell 15
PIPS Shell Commands 15
ACS - Access Control System (acs) 15
ANPR Vehicle Analyser (anpr) 24
Asynchronous Payload Matching (asyncp) 27
BOF2 protocol (bof2) 28
IR Camera (cam1) 30
Overview Camera (cam2) 34
Client vehicle event reporter (client) 36
Contexts (contexts) 37
Plate Database Matcher (dbmatcher) 40
Diagnostics and Exceptions Manager (diagnostics) 42
File Logger (filelog) 43
Vehicle Fusion (fusion) 43
GPS Time Manager (gps) 46
Heartbeat (heartbeat) 46
Image File Outputter (ifo) 47
JPEG Service (jpegService) 48
JTMS - Journey Time Measurement System (jtms) 49
External Led Control (ledControl) 50
Metadata store (metadata) 50
OEM Modules (modules) 53

Network user interface manager (netuis) 54
NTP Monitor (ntpMonitor) 54
Licence options (options) 55
Patch Overlay Control (patchoverlay) 55
PCI Camera Source (pciSource) 56
PIXI Contexts (pixicontexts) 56
Power Manager (power) 56
Relay Out (relayOut) 56
SAP - Serial Application Port (sap) 57
Vehicle Image Selector (selector) 57
Hardware Monitoring sensors (sensors) 58
Console Logger (stdout) 58
System Details (system) 58
Trigger Control (trig) 60
Trigger Script (trigScript) 64
UTMC Delivery Module (utmc) 65
UTMC V1.2 Delivery Module (utmcv12) 67
VES - Violation Enforcement System (ves) 68
Vehicle Event Database (vfeDB) 78
Logging bits 79
Notifications 82
7. Format strings 84
Control Characters 84
Replacement specifier 85
Format 85
Format Detail 85
List of replacement values 86
Examples 96
8. PIXI Protocol 98
Protocol 98
Example documents 101
Root objects 102
Subobjects 103
Properties 104
Logging 105
Notifications 107
Issue Command 108
Event data 109
Event data with pull 110
PIXI Documents 111
commands.xsd 111
output.xsd 113
common.xsd 117
List of PIXI values 119
PIXI values image_* 119
PIXI values cam_* 119
PIXI values hazcam_* 120
PIXI values event_* 120
PIXI values file_* 120
PIXI values hazard_* 121
PIXI values heartbeat_* 121
PIXI values imglocaltime_* 122
PIXI values imgutctime_* 122
PIXI values jpeg_* 123
PIXI values location_* 123
PIXI values globalmeta_* 124
PIXI values timeoffset_* 125
PIXI values plate_* 126

PIXI values triglocaltime_* 127
PIXI values trigutctime_* 128
PIXI values site_* 128
PIXI values supplementary_* 129
PIXI values localtime_* 129
PIXI values utctime_* 130
A. Technical Details 131
Communication 131
Console Serial RS-232 131
Ethernet 131
Network details 132
Filesystem layout 133
Backup 135
B. Software installation and upgrades 136
C. Factory Defaults 137
D. File transfers 138
SFTP 138
SCP 138
FTP 138
NFS 140
CIFS/Samba (Windows shares) 140
Transfer troubleshooting 140
Network problems 140
Permissions 141
E. Software tools 142
PIPS ANPR Toolkit 142
Windows 7 142
PuTTY 142
Filezilla 142
WinSCP 142
NFS Server on Windows 142
F. Nano - text editor 143
Opening and creating files 143
Saving and exiting 143
Cutting and pasting 143
Searching for text 143
G. rc-update 144
Introduction 144
rc-update commands 144
runlevels 144
Examples 144
Other information 144
H. Viewfinder Protocol 145
Viewfinder commands 145
Viewfinder messages 146
Version 1 146
Version 2 146
Version 3 147
Version 4 148
I. Vehicle Event Viewer Protocol 149
Vehicle Event Viewer commands 149
Vehicle Event Viewer data 149
Header Format 149
J. Legal Notices 152
English 152
Copyright Notice 152
Warranty 152
Service 152

Technical Support 152
Design Changes 153
Trademarks 153
FCC Declaration 153
Français 153
Notification de Copyright 153
Garantie 153
Service 153
Support Technique 153
Changements de Conception 154
Marques Déposées 154
K. Contact information 155

List of Figures

4.1. Objects in the system and how they fit together. 11
8.1. Link with no heartbeat, camera will close when no command has been received for 5 minutes. 100
8.2. Link with heartbeat, client chooses when to end by closing the link. 101
8.3. Get Root Objects - a list of all configureable objects is collected, some may have subobjects 102
8.4. Get subobjects of an object - a list of all subobjects is collected, some may have subobjects. The list may be empty, as in the example 103
8.5. Get properties of an object - a list of all the properties of an object. The list may be empty. 104
8.6. Start some logging. Asynchronous messages will be sent back by the Camera containing the log messages 105
8.7. Start notification messages. Asynchronous messages will be sent back by the Camera containing the notification messages of the requested events 107
8.8. Issue a command and receive the responses. 108
8.9. Connect to the camera and get events as it reads vehicles. 109
8.10. Here we are collecting (pulling) certain vehicle details when a particular vehicle is found. 110

List of Tables

7.1. Format characters 85
8.1. PIXI Packet Format 99
A.1. TCP/IP and UDP/IP Port numbers 133
C.1. Default IP configuration 137
K.1. Contact Information 155

Chapter 1. Introduction

This manual is for the Neology ANPR cameras listed inside the front cover. These cameras are very similar so most of this manual covers them all. Where differences occur the manual will note them.

The P382, P392+ and P492 share many common features, the highlights of which are

- ANPR Camera, illuminator and processor in one package
- Provides savings in system cost, complexity and timescales
- Neology proven camera and processor technology

This manual is only as up to date as the software it ships with. The corresponding version number is listed in the Revision note. Trying to use this manual with the wrong version of the software will be frustrating where differences occur.

P382

P382 is a fully integrated number plate reading camera incorporating both the camera and the recogniser within a single sealed enclosure. It is designed for use in the highest performance applications where it is necessary to provide the ANPR function across a full 4metre carriageway (3.5m with 0.5m overlap). The unit comprises a high resolution monochrome CCD camera with high sensitivity in the infra-red, surrounded by two banks of IR LEDs. Patented filter / flash technique gives suppression of headlights and bright sunlight. Field-by-field control of camera parameters allows the use of the ‘triple flash’ technique to reduce problems of plate-to-plate variability.

An optional independent, integrated, synchronous, colour camera may be configured to the same focal length as the monochrome camera, or to a wider field of view, as required. Therefore an ANPR read will have a colour overview image associated with it.

The integrated number-plate recogniser incorporates the Neology ‘Autoplate’ ANPR engine, which has been proven in many countries worldwide. Patented real-time video triggering upon plate presence provides excellent plate detection. A vehicle presence trigger input is also provided for the most demanding applications, e.g. taking an overview picture of a vehicle with a missing plate.

P382 can be integrated into a wide variety of systems via relay output, RS232, TCP/IP Ethernet with socket and FTP protocols (100baseT). Wireless IP connectivity over GPRS, EDGE or 3G is provided by fitting an optional modem. Additionally IEE802.11b/g ‘WiFi’ may be fitted to give local wireless operation. IP connectivity, (wired or wireless), provides time-lock of distributed cameras to a central server via NTP. A GPS unit may be fitted giving very high accuracy time and position information.

Real-time JPEG hardware compression is provided for both IR and colour images and can be used to provide a real-time IP video stream of the traffic. This can be used to record the image stream for ground-truthing.

P382 is fully web-enabled and can be configured and monitored from a standard web-browser on a PC.

External devices such as DSRC, Radar, Weigh-in-Motion or ticketing systems can be integrated into the system via RS232 or TCP/IP. A flexible interface allows this data to trigger the camera or be added asynchronously to the data set which the camera provides for each vehicle.

The Vehicle Enforcement System (VES) application software offers socket based transfer of Summary and Evidential Records via either push or pull protocols with full key handling, authentication, encryption and local storage of up to 60,000 events. Pre and post event contextual images showing the direction of travel may also optionally be captured. The direction of travel may also be captured.

- 4 metre road width coverage, using 1392 x 512 pixel sensor
- Powerful processor
- Reading multiple number plates in a single field of view

- Embedded Linux operating system, offering standard Linux connectivity including encrypted links
- Multiple concurrent access to viewfinder and event viewer
- Hardware MJPEG streaming of the video streams (50fps, 1392 x 512) eliminating the need for a high performance frame-grabber on a PC for data acquisition

P392+/P492

P392+/P492 is a fully-integrated number plate recognition unit incorporating camera (s), illuminator and data and image processing within a single sealed enclosure. The unit comprises a monochrome camera surrounded by two sets of IR LEDs. Neology patented filter/flash technique provides suppression of headlights and bright sunlight. Field-by-field control of camera parameters allows the use of ‘triple flash’ technique to reduce any problems of plate to plate variability.

P392+/P492 can also include an optional independent, integrated, synchronous, colour camera. The colour camera can be configured to the same focal length as the monochrome camera, or to a wider field of view as required enabling ANPR (Automatic Number Plate Recognition) reads to have associated colour overview images.

The integrated number-plate recogniser incorporates the Neology ‘AutoPlate’ ANPR engine, proven in many countries worldwide. Patented real-time video triggering upon plate presence provides excellent plate detection. A vehicle presence trigger is also provided for the most demanding applications, for example taking an overview picture of a vehicle with a missing plate.

P392+/P492 can be integrated into a wide variety of systems. Wireless IP connectivity over GPRS, EDGE or 3G can be provided by fitting an optional internal modem.

IP connectivity (wired or wireless), provides a time-lock of distributed cameras to a central server via NTP.

Real-time JPEG hardware compression is provided for both IR and colour images and can be used to provide a real-time IP video stream of the traffic. This can be used to record the image stream for ANPR data verification.

P392+/P492 is fully web-enabled and can be configured and monitored from a standard web-browser. External devices such as DSRC, radar, weigh-in-motion or ticketing systems can be integrated into the system. A flexible interface allows this data to trigger the camera or be added, without synchronisation, to the data set which the camera generates for each vehicle.

- Reading multiple number plates in a single field of view.
- Embedded Linux operating system, offering standard Linux connectivity including encrypted links.
- Multiple concurrent access to viewfinder and Neology client monitor application.
- Hardware MJPEG streaming of the video streams (50fps, 752x480 - P392/P392+ or 2048x720 P492) eliminating the need for a high performance frame-grabber on a PC for data acquisition.

Assumptions

The P382, P392+ and P492 are networked cameras, and a course in networking is beyond the scope of this manual. You are expected to have a working understanding of TCP/IP networking, or be able to consult with someone who can help you with this.

Conventions

We use several typographic conventions in this manual to describe things including interaction with a computer terminal.

Commands to be typed in are described as follows:

- `command`

The name of the command.

- {required_argument}
  A required argument to the command.
- [optional_arument]
  An optional argument to the command.
- [*replace_me*]
  Text which should be replaced by you to indicate, for example, the file to be worked on

these can be combined, for example

`ls` [-l] [*directory*]
describes part of how to use the ls command in Linux.

Some text needs to be typed in exactly as given

```
type this in exactly
```

and sometimes we give some representative response from the system

```
and it will print this out,
or at least something similar
```

We will also provide links to other sections of the book, for example this section is the section called “Conventions”[2] or sometimes external references, like this one to our web homepage: http://solutions.Pips.co.uk/wps/portal/Neology/en_GB/TrafficSafety/Systems/-/AutomaticNumberPlateRecognition/. If the medium you are reading this on supports it, you may be able to click to go to the appropriate place. Obviously, this doesn't work on printed copies!

Chapter 2. Getting started

It is highly recommended that you get familiar with your P382, P392+ or P492 camera indoors prior to taking the camera to the roadside.

Connectivity

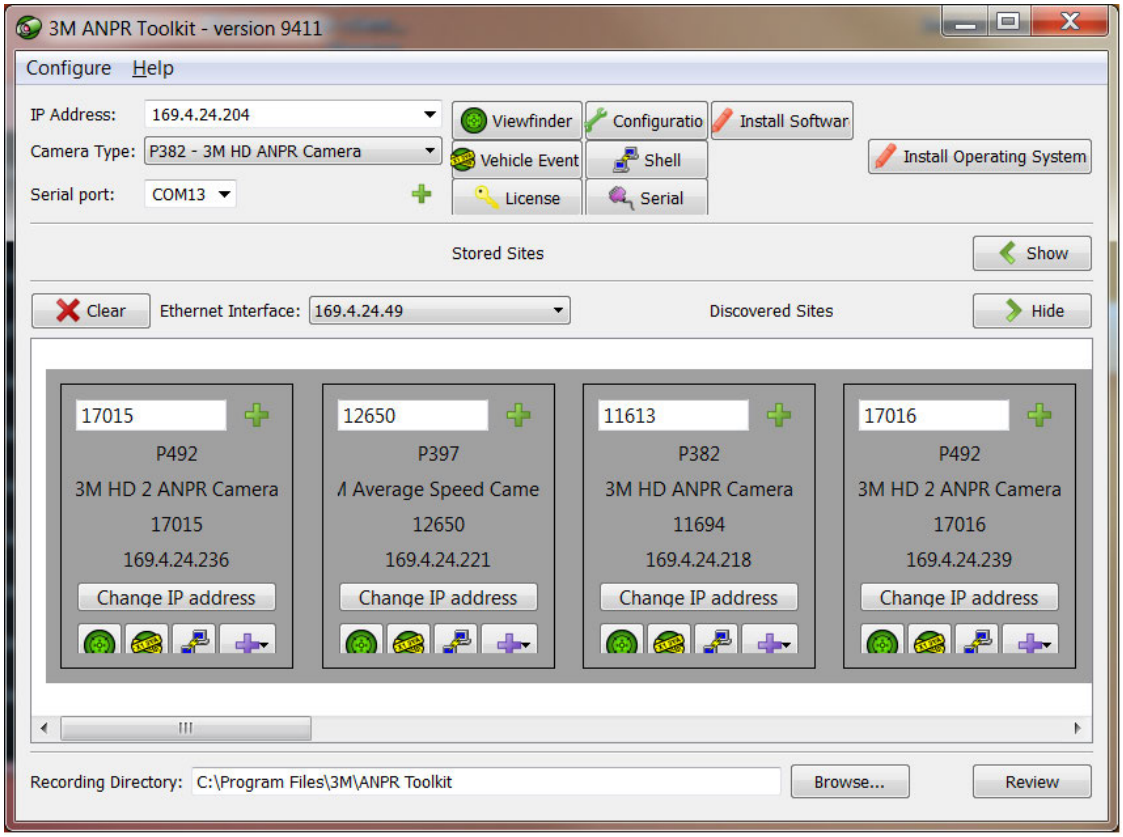
The PIPS ANPR Toolkit application should be installed on your PC, the camera connected to is often the easiest way to connect to the camera. If for some reason you cannot use this you will either need to connect via serial or via SSH and configure the network by hand the section called “Networking setup” [5].

Discovery

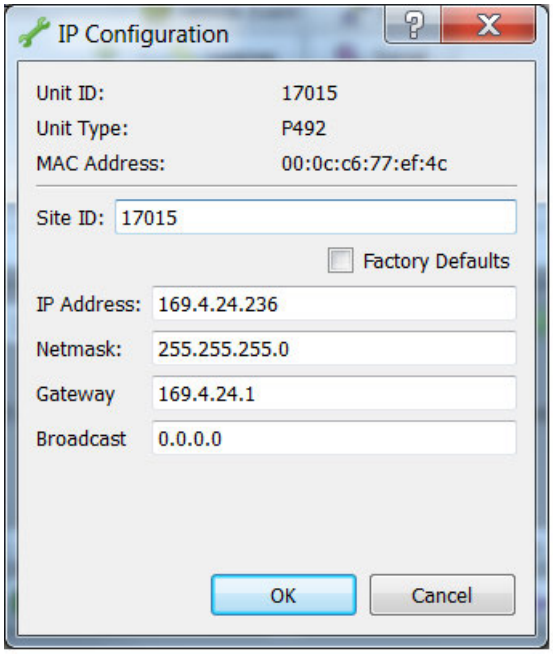
To use Discovery you will need to install the PIPS ANPR Toolkit (refer to Chapter 3, *PIPS ANPR Toolkit*[8]). If you connect the camera to the same ethernet as the PC on which you are running the toolkit and run the Toolkit you should be able to see the P382, P392+ or P492 in the list of discovered cameras.

Note

You can connect the camera to the same switch or hub, through multiple switches and hubs, or just use a cross over ethernet lead. However, the discovery protocol cannot traverse routers or gateways in your network.



If you start the application and select the network interface on your PC which matches the one to which the P382, P392+ or P492 is connected you should be able to see the camera. To identify the correct camera if you have multiple cameras on the network you should cross reference the serial number with that printed on the back of the camera. To configure the IP address of the camera click on `Change IP Address` edit the values displayed. Once you press OK, the camera will store the options and the address will change.



After around one minute you should be able to ping the camera and go on to configure the rest of the camera (see the section called “Connecting” [6]).

Serial RS-232

Full details on the console serial port are available in the hardware manual.

You will need a serial terminal, such as Kea! Term for Windows, PuTTY for Windows (see the section called “PuTTY” [142]), Minicom for Linux, or Hyperterminal for Windows (not recommended due to quirky behaviour). This should be connected at a line speed of 38,400 bits per second with 8 bits of data, no parity and 1 stop bit. This is often abbreviated to 38,400 8N1. No flow control is necessary. This should be connected to an appropriate serial port on the PC.

The system will boot into linux, eventually presenting you with the login prompt:

```
 * Starting portmap ...                                    [ ok ]
 * Mounting network filesystems ...                        [ ok ]
 * Starting sshd ...                                       [ ok ]
 * Starting vixie-cron ...                                 [ ok ]
 * Starting Webmin ...                                     [ ok ]
 * Starting local ...                                      [ ok ]


This is localhost.(none) (Linux i586 2.6.19.2) 01:42:51

localhost login:
```

If this is successful you can log in as root using by typing in **root** and then entering the root password (given in Appendix C, *Factory Defaults* [137].

Ethernet

As an alternative you can connect via ethernet. Knowledge of TCP/IP networking is assumed when reading this manual. The camera will be shipped from the factory with the settings specified in Appendix C, *Factory Defaults* [137]. If you can set up an SSH session to the camera then you do not need to use the serial port to configure the camera.

Networking setup

To use this section you are already logged into the camera via serial or SSH. You do not need to do this if you can use the IP discovery program (see the section called “Discovery”[4]). If you are not logged in, return to an earlier section to get a login prompt working. To set up networking we edit `/opt/config/current/netmon.xml`.

```
nano /opt/config/current/netmon.xml
```

Note

A guide to how to use nano is available in Appendix F, *Nano - text editor* [143]

Basic Configuration

In its basic form you can just edit the existing contents to change the IP address, netmask and gateway. The file should look like:

```
<?xml version="1.0"?>
<netmon>
  <main>
    <services>ethernet</services>
    <hostname>Camera</hostname>
  </main>
  <ethernet>
    <ip>aa.aa.aa.aa</ip>
    <netmask>bb.bb.bb.bb</netmask>
  </ethernet>
  <routes>
    <default>ethernet cc.cc.cc.cc</default>
  </routes>
</netmon>
```

Where `aa.aa.aa.aa` is the IP address you'd like to assign to the camera, `bb.bb.bb.bb` is the netmask, and `cc.cc.cc.cc` is the default gateway (remove this section if you don't want one). Under many circumstances this is acceptable.

Connecting

Although configuration is possible over the console serial port, the natural way to connect to the P382, P392+ or P492 is via the network, so we will get that working next. You may wish to skip this and move straight onto Chapter 5, *Configuration using Webmin* [13] to use the built in webserver to configure the camera.

SSH

Secure Shell or SSH is a secure networking protocol which can be used for many things, but here we will use it to provide a shell on the camera. It is running on the standard port, 22.

Many operating systems have an ssh client built in which can be invoked by typing ssh from the command line. Briefly:

`ssh` [*`user`*`@`] {*`hostname`*}
However Windows does not have one, we recommend PuTTY (see the section called “PuTTY” [142]). Any ssh client capable of SSH2 should work, feedback is welcomed on other implimentations. There is an SSH client available in Webmin under Others → SSH/Telnet Login which requires Java, but if you can see webmin I'd recommend you use that instead where possible as documented in Chapter 5, *Configuration using Webmin* [13]

Launch your ssh client to log into the camera, referring to Appendix C, *Factory Defaults* [137] for the root password. Once you have logged in you have the network working correctly and you can configure and use the camera.

You are logged into a Linux shell, and can use many normal Linux commands to navigate. A brief set of useful commands and arguments are given here.

- `ls` [-l] [*`directory`*]
  get a directory listing, similar to **dir** under DOS
- `pwd`
  display the current working directory
- `cd` {*`directory`*}

change directory to given directory. Use `..` to go up one directory

- `nano` {*`filename`*}
  edit a file. See Appendix F, *Nano - text editor* [143] for more details.
- `cat` {*`filename`*}
  quickly show a file.
- `less` {*`filename`*}
  display a file, so you can scroll up and down.
- `ftp` [*`ip_address`*]
  launch the FTP client to transfer files to or from a remote machine. TODO - xref

This is only a very brief list. A good list can be found online at http://www.ss64.com/bash/, and a comprehensive introduction which is worth reading at http://en.flossmanuals.net/command-line/. These links are not under our control and may expire with time.

Note

Manual pages are *not* installed on the camera so you cannot refer to them there. Sorry.

Restarting and Shutting Down

Due to the possibility of corrupting the filesystem, the following should as far as possible be adhered to for P382, P392+ and P492 cameras.

Restarting after changing settings

Some settings require that the camera is restarted before the change is applied. To do this, users must issue the reboot command via ssh or use the reboot button in webmin. Users must not switch off the power supply to the camera.

Switching off for planned maintenance

When wanting to switch off the camera, it is recommended that users do not simply remove the power from the camera or unplug the connector. Instead, best practice is to connect to the camera using ssh (eg. Putty) and issue the shutdown now command. After this, you should wait approximately 30 seconds for the camera to shut down, and then remove the power within a further 30 seconds.

Power-cycling

If you wish to power cycle the camera to attempt to recover from some error you should use the shutdown now command via ssh to cleanly shutdown the camera and remove power from the camera 30 seconds after issuing this command. Keep power off the camera for over 30 seconds before re-applying it.

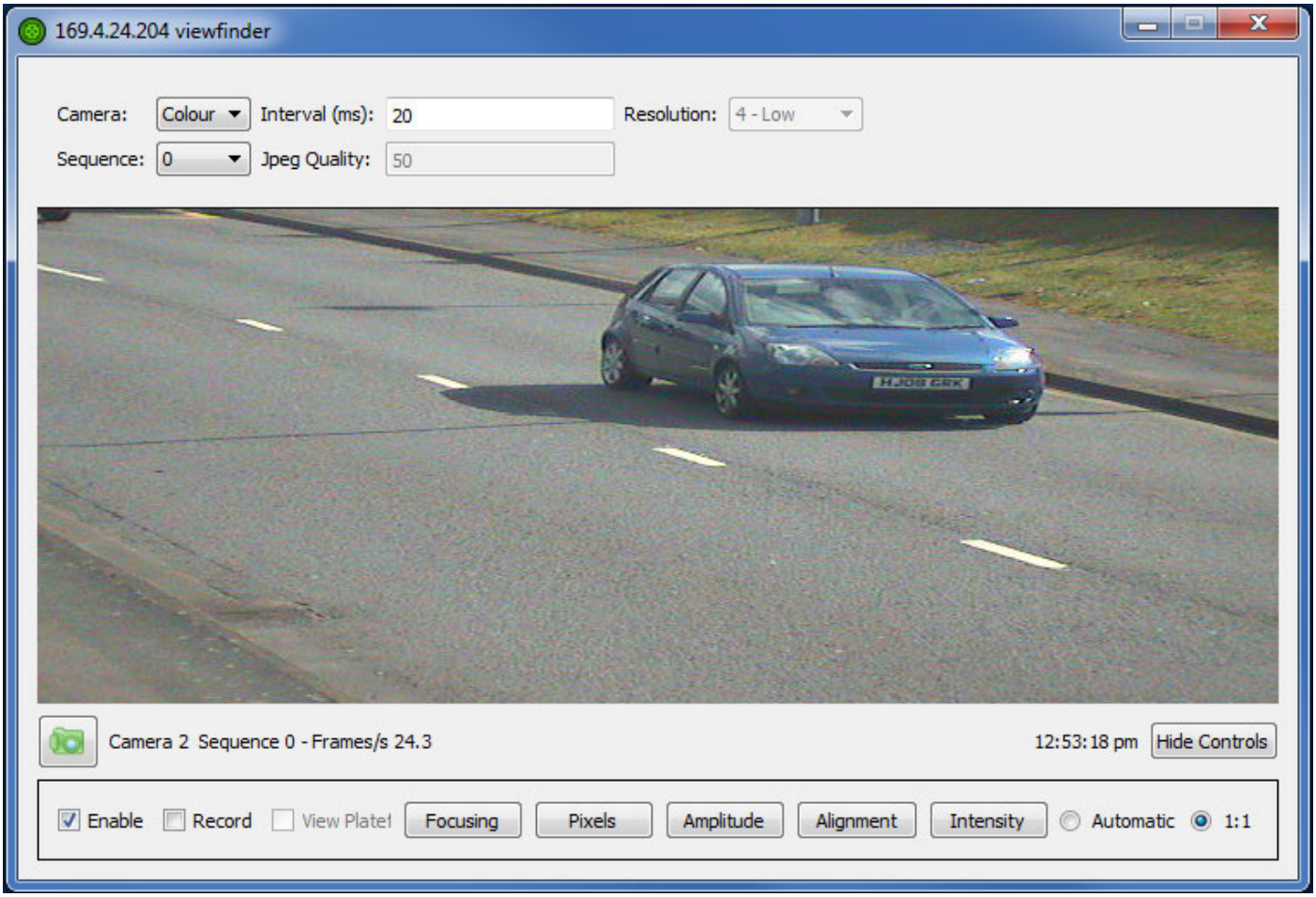
If you are unable to issue the shutdown command due to the problem you are trying to resolve, you must still observe the long delay between removing power and re-applying it – re-applying power to the camera too quickly can cause problems.

Chapter 3. PIPS ANPR Toolkit

PIPS ANPR Toolkit (see the section called “PIPS ANPR Toolkit”[142]) is a valuable tool in diagnosing, setting up and maintaining your camera. To use it, launch the viewer from the Start → PIPS → Toolkit on Windows. You can then enter the IP address of the camera you wish to view, or select it from the drop down list if you have viewed it before.

Viewfinder

By pressing the **`Viewfinder`** button, you can launch a "through the camera" viewer.



From this you can select to view either camera, and whichever sequence number of the camera you wish (which are valid is dependent on the `numentries` parameter of the camera you are viewing, by changing the drop down list. Camera 1 is the infra-red camera, 2 is the colour one.

You can speed up or slow down the image rate dependent on your PC loading and network bandwidth - if you select a low interval it will cause more loading. Quality and Resolution have no effect on a P382, P392+ or P492.

The Enable checkbox connects or disconnects the viewfinder from the camera. If the Record box is checked then the Toolkit will record the received images. The radio buttons can be used to select the size of the images as displayed by the viewfinder.

The buttons along the bottom of the window provide access to other tools. The Enable checkbox connects or disconnects the viewfinder from the camera.

Vehicle Events

By pressing the **`Vehicle Events`** button, you can launch an event viewer, which shows each vehicle that the camera detects separately.



The Enable checkbox connects or disconnects the event viewer from the camera. If the Record box is checked then the Toolkit will record the received data and images.

The radio buttons are used to select the protocol used to connect to the camera. If the PIXI protocol is selected then the Configure PIXI button can be used to select the event data and image to display. The Expand All Show More option can be used to show additional data received via PIXI.

The trigger button can be used to send a TCP trigger to the camera. The trigger message can be configured using the Trigger Config tab.

The Clear button clears the display.

Review

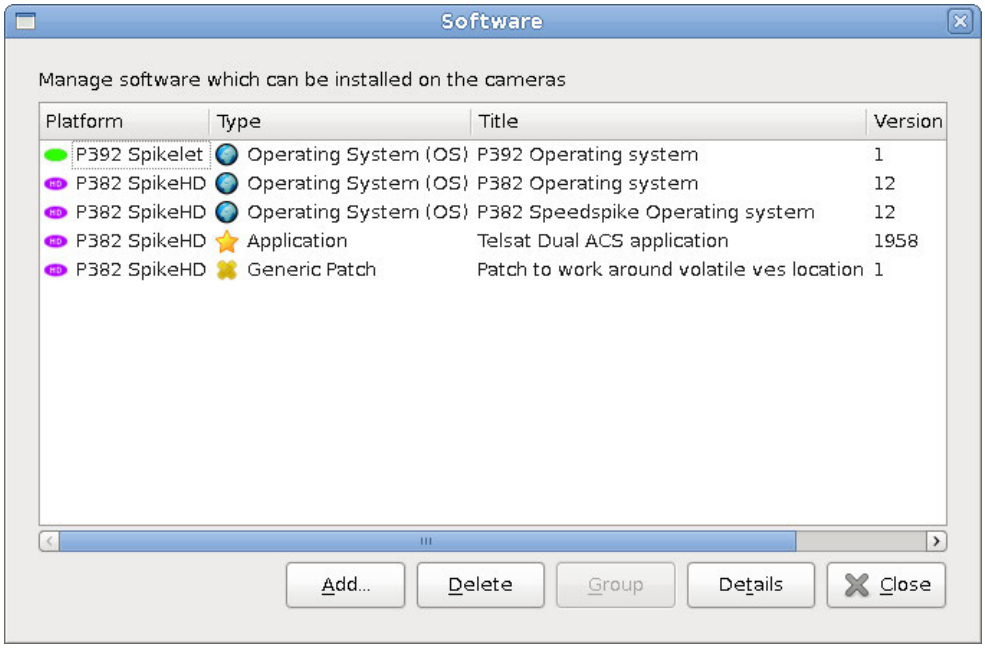
In the viewfinder and vehicle events view you can select to disable or enable updates, and also record the data using the tick boxes in the lower left hand corner. If you have recorded events you can view them by pressing the **`Review`** button. This is currently functional but not complete.

Camera Software

The toolkit allows you to maintain the software on your cameras. There are two parts to this.

Software Management

By selecting Configure → Software from the menus of the toolkit you can *locally* manage software which you can install on the camera.



- Add: You can add software distributed from PIPS to your pool of available software to install. Mostly these will be .tar.lzma files, but also the libcardet files which are number plate reading engines can be placed here. The files will be copied and stored by the application in it's own private repository..
- Delete: Delete items from your local pool of files. Any groups which depend on these files also get deleted.
- Group: Group a set of items together for ease of installation. Once grouped together a set of files will behave like a single unit and can all be installed together to ease installation. Example uses are grouping an ANPR library with an application to install the two together, or adding a patch to an os to install as one.
- Close: Close the dialogue box.

Software Installation

Software can be installed on the camera by clicking on the small orange pencil. Some basic options as to what type of installation to do, and it will ask you to enter details for the camera so that it can connect. To perform an operating system installation you must be connected via a serial port and via ethernet.

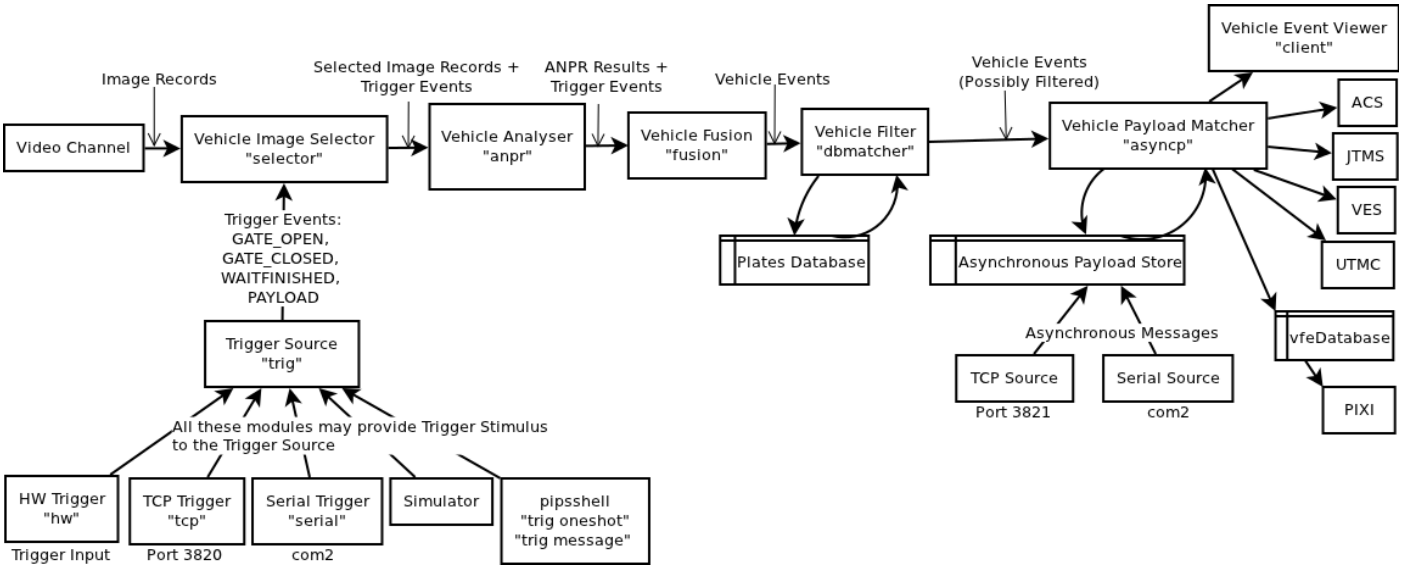
A critical concept is that some software contains a 'complete operating system' (OS) and some does not. To install a complete operating system there is quite a lot more work required, so these software packages are separated from the non-OS components

Chapter 4. Camera technical overview

The P382, P392+ and P492 are very configurable, and complex to understand. This chapter will hopefully help you to understand the internals and what they do so that you can make wise choices in setting up.

This diagram shows the objects in the system and how they fit together. Each of the individual objects is documented more completely in the section called “PIPS Shell Commands”[15], but this overview will help you put those pieces together.

Figure 4.1. Objects in the system and how they fit together.



Interfaces: Output mechanisms

The P382, P392+ and P492 have various mechanisms for outputting the resulting data from their operation and delivering it to another system for processing. This chapter describes them each in brief to allow you to understand and choose what to use. Most of these systems can be used at the same time as one another.

- *ACS* stands for Access Control System. It is a simple network delivery of image and text files via FTP or SFTP. It is designed for production use, and is recommended as a simple way to get started. This simplicity does not mean it is unsuitable for large scale deployments, but it does require a reasonable amount of bandwidth. It is very flexible in which images are available and what metadata is contained in the text file and the filenames. More detail on configuring the system is available in the section called “ACS - Access Control System (acs)”[15] and the available metadata list is Chapter 7, *Format strings* [84]. I would recommend developing with ACS unless you have a reason why you cannot use it. You can use this delivery mechanism alongside others, such as PIXI. There is a separate ACS interface document available which is for legacy systems, and not particularly relevant to the P382, P392+ and P492.

- *PIXI* is an XML based interface for collecting information and controlling all aspects of the camera. It can flexibly push and pull data from the camera, and requires no configuration on the camera. All configuration can be done via this protocol. For more complex requirements that cannot be met with ACS we would encourage the use of this protocol, which is fully documented in Chapter 8, *PIXI Protocol* [98].

- *JTMS* stands for Journey Time Measurement System. This is a relatively simple TCP/IP mechanism for delivering data suitable for measuring journey times. It uses very little bandwidth, and is not flexible for other uses. It does not provide any images. More detail on configuring this system is available in the section called “JTMS - Journey Time Measurement System (jtms)” [49]

- *VES* stands for Violation Enforcement System. This is a complex TCP/IP mechanism for delivering data suitable for many uses. It can provide images, encryption and push and pull of data. There is a separate interface document

available under an NDA (Non-Disclosure Agreement) from Neology describing this interface in detail. For new developments, unless you need encryption we'd encourage the use of PIXI instead of VES.

- *UTMC* stands for Urban Traffic Management and Control. This is a web-base mechanism for delivering data. A camera can be configured to deliver data to one or more UTMC servers. Protocol versions 1.0 and 1.2 are supported.
- *SAP* is the serial application port. This provides delivery of the plate or other metadata via the second serial port on the camera (COM2). It is flexible, but obviously cannot deliver images. More detail on configuring the system is available in the section called “SAP - Serial Application Port (sap)”[57] and the available metadata list is Chapter 7, *Format strings* [84]. You may (as with all the other output systems) use this in conjunction with other output mechanisms listed here. The serial port may only be used for one function at once.
- *Image File Output* is a debugging system, and should not be used for any production system. It places fixed filename images on the local /storage device. It may have a performance impact on the system if it is used.
- *Viewfinder* is a legacy TCP/IP protocol for viewing live images from the camera. It does not guarantee the delivery of any images. The protocol is defined in Appendix H, *Viewfinder Protocol* [145]. This is used by the Toolkit.
- *Vehicle Event Viewer* is a legacy TCP/IP protocol for viewing read images from the camera. It does not guarantee the delivery of any images and is therefore not suitable for production use. The protocol is defined in Appendix I, *Vehicle Event Viewer Protocol* [149]. This is used by the Toolkit.

Chapter 5. Configuration using Webmin

The camera provides a web administration utility called webmin. You can access this from your web browser on

`https://camera.ip.address/`

You will need to log in, referring to Appendix C, *Factory Defaults* [137] for the root password.

From here you can configure many aspects of the camera. This manual will take you through some of the more important ones. You can break the camera using some of these options, don't play unless you understand what you are doing.

Note

The web interface is only available over the https protocol, not the http protocol. Ensure you put the s in the URL

On the P392+ and P492 cameras (and only these models) should have the /backup.pl script run from the command line after any change - once that change is determined to be satisfactory. Changes include:

- New OS and application installations
- Application upgrades, Cardet upgrades
- Configuration changes

Running backup ensures that should a file system corruption be recoverable via this mechanism, the recovery will be to the last backed up state.

Camera control

Initially you will be presented with the camera application interface to configure the camera aspects of the system. This is accessible under Others → Camera Application if you need to get back to it. This manual is available from this page (indeed, you may be reading it there right now!). As well as this all the configuration options and commands are available with online help. This help is also printed for reference in Chapter 6, *PIPS ANPR Shell* [15] should you need it.

Webmin allows all of the shell parameters and commands to be accessed, as listed in Chapter 6, *PIPS ANPR Shell* [15].

You can also manage the anpr libraries from here and upload new ones by selecting Spike II (382) Application → ANPR Vehicle Analyser → Library Manager → Manage number plate libraries

Network

The network configuration is available under Networking → Networking Configuration and allows control of the IP address parameters and the hostname of the camera. It is important to set up the hostname of the camera to something useful and unique as several subsystems use it to identify the camera. The factory default is the serial number of the camera.

You can also set up an on camera firewall Networking → Linux Firewall.

Caution

Incorrectly configuring the firewall can make the camera *completely unresponsive* to network control, including webmin and SSH, requiring you to access it via the RS232 port or return it to Pips.

Mounting network disks

The P382, P392+ and P492 have the ability to save files to disk, which can be remotely mounted over NFS. Most operating systems come with an NFS server, so you can just use those. Windows users may wish to see the section

called “NFS Server on Windows”[142]. You can also mount CIFS and SMB "Windows shares" from windows servers or workstations.

NFS

Once you have a directory exported so that the camera can see it you can mount it via the System → Disk and Network Filesystems menu option. Use the drop down list to select **`Network Filesystem (nfs)`** and make sure you fill in the Mounted As, NFS Hostname and NFS Directory to be **`/storage/`*`pre-created-directory`***, the IP address of the server and the directory you have entered in `/etc/exports` respectively.

Windows shares

There are so many versions of Windows, and depending upon what you have installed it is hard to tell if you will need to use CIFS. In theory it is downwards compatible, but you definitly need it for Windows 2003 server shares. If it fails try **`Windows Networking Filesystem`** instead of **`Common Internet Filesystem`** in the instructions below.

You can mount a windows share via the System → Disk and Network Filesystems menu option. Use the drop down list to select **`Common Internet Filesystem (cifs)`** and make sure you fill in the Mounted As, Server Name and ShareName to be **`/storage/`*`pre-created-directory`***, the IP address of the server and the share name you have shared respectively. I would not attempt to use server names rather than IP addresses, although it may work for you, it may be unreliable. You will almost definitly have to fill in Login Name and Login Password details.

Chapter 6. PIPS ANPR Shell

The shell is an alternative way to access and control the camera's parameters. You can start it whilst at the linux command prompt (either via SSH or on the console serial port) by typing

```
/opt/PIPS/PIPSshell

 Welcome to the PIPS ANPR Camera shell - 127.0.0.1
 Shell Version Version 4.7.9540 built at 13:06:54 on Mar 17 2015
 (Using library version Version 9540 built at 15:02:53 on Mar 20 2015)

 Log: Mon Mar 23 11:39:24 2015 - NetUI.cpp:1179:Copyright (C) Neology UK Ltd., 2006-2013. All Rights Reserved. on 17015
 Log: Mon Mar 23 11:39:24 2015 - NetUI.cpp:1180:Serial number: 17015
 Log: Mon Mar 23 11:39:24 2015 - NetUI.cpp:1181:Version 4.7.9540 built at 15:03:29 on Mar 20 2015
 Log: Mon Mar 23 11:39:24 2015 - NetUI.cpp:1182:libPIPSLinux:Version 9540 built at 15:02:53 on Mar 20 2015
 Log: Mon Mar 23 11:39:24 2015 - NetUI.cpp:1183:Hardware: Version 647 (Cap 406), Internal JPEG Compressor, Square Platefinder, Dual JPEG, Mono flash table,
 Log: Mon Mar 23 11:39:24 2015 - NetUI.cpp:1211:Sensor 0CMV2000 (CMOS): Width: 2048, Height: 720 @ 50FPS as a Monochrome Processing sensor
 Log: Mon Mar 23 11:39:24 2015 - NetUI.cpp:1211:Sensor 1CMV2000 (CMOS): Width: 2048, Height: 720 @ 50FPS as a Colour Overview sensor
 Log: Mon Mar 23 11:39:24 2015 - NetUI.cpp:1226:uname: Linux 17015 2.6.36.2 #4 Mon Jan 27 09:49:07 Local time zone must be set--see zic manu armv5tel
 >>
```

The double chevrons are the prompt and you can type in commands here.

The model of commands is one of objects, which have properties and commands. Objects can be nested, and the sub-object's name is separated by a space from the parent. This may sound confusing, re-read it after you have read the list of commands.

- `help` [*`object`*]
  You can see a list of objects by typing **help** with no arguments, and see properties and commands of each object by giving the object name as an argument.
- `history`
  Display a list of old commands you have typed in. The command line supports full “GNU readline” command line editing and history. Basically the arrow keys work like you might hope.
- `quit`
  Leave the shell.

The complete list of objects with their properties and commands follows, but this may be out of date as with any printed material, and I suggest referring to the command line help.

The objects, properties and commands are not guaranteed to stay the same between software releases - although all functionality formally available will remain. Please consult with Neology of details on how to upgrade.

On the P392+ and P492 cameras (and only these models) should have the /backup.pl script run from the command line after any change - once that change is determined to be satisfactory.

PIPS Shell Commands

ACS - Access Control System (acs)

Available on platforms: All

The Access Control System is an output module which sends vehicle details to an external computer for processing. It will output a (configurable) number of jpeg images of the vehicle along with a text record describing the license plate event (LPR). This data may be sent as separate files, named according to the lpr_filename (with .lpr extension) and img_filename (with .jpg extension) properties. Alternatively, the data may be sent within a single packed file consisting of an XML header followed by the binary image data. In this case the filename will be the lpr_filename with a .axi extension and the LPR text record is contained withing the XML header. The XML header also contains data allowing the extraction of the image data.

Platforms	Name	Command	Default Value	Description
All	Append lpr text data	`acs set append_lpr {`*`value`*`}`	false	When using FTP/SFTP the LPR file can be appended onto an existing file if this option

Platforms	Name	Command	Default Value	Description
				is set to true. This can be used for example to create a single .csv file for all events delivered.
All	Buffer the transfer	`acs set buffer_transfers {value}`	true	Stores images in internal non-volatile storage to allow them to be transferred later should the file server be inaccssable for any reason.
All	Output Character Encoding for filenames	`acs set char_set {value}`	0	If in doubt, set this to 0. The character encoding used for strings for filepaths. 0 - ASCII-7bit 1 - ISO8859-1 2 - UTF-8 If using ASCII-7bit any special characters will be converted to nearest ASCII equivalents. If using anything other than ASCII-7, please ensure your server and other software is capable of handling the specific encoding
All	The Delivery Order	`acs set delivery_order {value}`	FIFO	The delivery order is a choise between First In First Out (FIFO) or Last In First Out (LIFO). (If switching between modes the data stored before switching will be lost). (If order is not FIFO or LIFO it will be treated as FIFO).
All	Enabled	`acs set enabled {value}`	false	Allows the ACS system to be enabled and disabled. Disable it unless you are using it.
All	Fast Ftp	`acs set fast_ftp {value}`	false	Accelerate FTP by ignoring what RFC1738 says and just transferring files directly into directories with STOR, rather than CWD first. Most off the shelf FTP servers will accept this happily, and it reduces latency.
All	Output Character Encoding For file Contents	`acs set file_char_set {value}`	0	If in doubt, set this to 0. The character encoding used for strings for LPR file contents. 0 - ASCII-7bit 1 - ISO8859-1 2 - UTF-8 If using ASCII-7bit any special characters will be converted to nearest ASCII equivalents. If using anything other than ASCII-7, please ensure your server and other software is capable of handling the specific encoding
All	Host	`acs set host {value}`		The IP address to which the files will be transferred. LPR files will be transferred last, after the jpeg files.

Platforms	Name	Command	Default Value	Description
All	Fallback Host	`acs set host2` {*value*}		Fallback IP address to which the files will be transferred if transfer to Host fails. LPR files will be transferred last, after the jpeg files.
All	Image filename	`acs set img_filename` {*value*}	%Jts%Id02u%Vm02u%Vd02u%Vh02u%Vn02u%Vs02u%Id02u,%Pps	A format string containing how to construct the image filename. You MUST put %Jtc in this string if you are outputting multiple images per event or else they WILL all have the same filename and overwrite each other. Note this property is only meaningful if transfer_packed is false
All	LPR contents	`acs set lpr_contents` {*value*}	%PNs\n%Pas\n%Pat%Jtu%Etx%Fmw	A format string containing how to construct the data you would like in the LPR file
All	LPR filename	`acs set lpr_filename` {*value*}	%Ei08X.lpr	A format string containing how to construct an LPR or AXI filename. If the transfer_packed property is set 1 (true) an AXI file is transferred. Otherwise an LPR file will sent with any required image files sent separately.
All	Maximum Disk Queue Length	`acs set nlog` {*value*}	100	The maximum number of ACS events which will be stored on the local filesystem before they are overwritten if it is not possible to contact the instation. Warning, arbitrarily setting this to a high value may fill up the device on which you are storing the files and then the system will lose the wrong data or may perform badly.
All	Password	`acs set pass` {*value*}		The password used to log in to the server or to unlock your private key, depending upon which method you're using to transfer.
All	Noread patch	`acs set patch_noread` {*value*}	false	When there is a no read there is also no patch. If you set this to true you'll get the full IR image output as a patch instead of no output.
All	Timeout	`acs set timeout` {*value*}	60	The timeout on operations over the file transfer link. NB: May not be what you expect from legacy systems.
All	Transfer overview context images	`acs set transfer_contexts` {*value*}	true	Transfer the overview context images (if any). The number and offsets of context images are configured under Contexts. Depending on the setting of transfer_packed this may be sent as a JPG file or within an AXI file
All	Transfer hazard IR images	`acs set transfer_hazard_ir` {*value*}	true	Transfer the full infra-red monochrome images. Depending on the setting of transfer_packed this may be sent as a JPG file or within an AXI file
All	Transfer hazard overview images	`acs set transfer_hazard_overview` {*value*}	true	Transfer the overview images (e.g. the colour images). Depending on the setting of transfer_packed this may be sent as a JPG file or within an AXI file
All	Transfer hazard patch images	`acs set transfer_hazard_patch` {*value*}	true	Transfer a small image of just the number plate patch. Depending on the setting of transfer_packed this may be sent as a JPG file or within an AXI file

Platforms	Name	Command	Default Value	Description
All	Transfer IR images	`acs set transfer_ir {value}`	true	Transfer the full infra-red monochrome images. Depending on the setting of transfer_packed this may be sent as a JPG file or within an AXI file
All	Transfer lpr text data	`acs set transfer_lpr {value}`	true	Transfer a text block containing metadata, called LPR data. Depending on the setting of transfer_packed this may be sent as an LPR file or within an AXI file
All	Transfer overview images	`acs set transfer_overview {value}`	true	Transfer the overview images (e.g. the colour images). Depending on the setting of transfer_packed this may be sent as a JPG file or within an AXI file
All	Transfer all data in a single AXI file	`acs set transfer_packed {value}`	false	Normally the data is transferred as separate LPR file and up to 3 image (JPG) files. Set this to true to transfer all required data in a single file (with file name lpr_filename.axi) consisting of an XML header followed by image data if required
All	Transfer patch images	`acs set transfer_patch {value}`	true	Transfer a small image of just the number plate patch. Depending on the setting of transfer_packed this may be sent as a JPG file or within an AXI file
All	Transfer path	`acs set transfer_path {value}`	%Shs/	A format string containing the path on theserver you'd like the files transferred to. This should contain / or \ as directory separators. It should end with a directory separator.
All	Transport	`acs set transport {value}`	sftp	The transport mechanism by which the system will transfer files. The options are sftp (recommended), scp, ftp, file. If you use scp the system is unable to create directories, so you must do that for it. File will deliver to the local filesystem under /storage.
All	Username	`acs set user {value}`		The username used to log in to the server

- `acs clearStats`

  Resets all Statistics. Platforms: All.

  Resets all Statistics

- `acs diskq_flush`

  Empty the Disk Queue. Platforms: All.

  All ACS events currently stored in the persistant Disk Queue will be deleted and will not be recoverable. Use this with care.

- `acs diskq_length`

  Length of Disk Queue. Platforms: All.

The number of ACS events stored in the persistant Disk Queue will be reported. Note this value may be non zero even if buffer_transfers is false. If buffer_transfers is false, the system still uses the disk queue, it just wont store items between reboots.

- `acs stats`

  Statistics. Platforms: All.

  Statistics for debugging

Specific Filenames (acs filenames)

Available on platforms: All

If you wish to have more control over the image filenames of the ACS output this section is for you, otherwise you can ignore it. You can specify filenames for each individual image that ACS outputs. If you leave the filenames blank then the standard ACS configuration will apply for that file. If you specify anything for a file, that file will be output with that filename. It will have the transfer_path prepended like with the standard naming scheme. If you want to output to different directories for each file, you can specify the path as part of the filename. If the transfer_path is blank you could output each file to a completely different directory. You cannot specify the lpr filename here as it is already available as a solo format string in the main ACS section.

Platforms	Name	Command	Default Value	Description
All	Hazard Full IR Filename	`acs filenames set haz_ir_filename {`*`value`*`}`		The format string used for the filename for the hazard full IR images.
All	Hazard Overview Filename	`acs filenames set haz_oview_filename {`*`value`*`}`		The format string used for the filename for the hazard overview images.
All	Hazard Patch Filename	`acs filenames set haz_patch_filename {`*`value`*`}`		The format string used for the filename for the hazard patch images.
All	Full IR Filename	`acs filenames set ir_filename {`*`value`*`}`		The format string used for the filename for the full IR images.
All	Overview Filename	`acs filenames set oview_filename {`*`value`*`}`		The format string used for the filename for the overview images.
All	Patch Filename	`acs filenames set patch_filename {`*`value`*`}`		The format string used for the filename for the patch images.

Context 1 (acs filenames context1)

Available on platforms: All

If you wish to have more control over the image filenames of the ACS output this section is for you, otherwise you can ignore it. You can specify filenames for each individual image that ACS outputs. If you leave the filenames blank then the standard ACS configuration will apply for that file. If you specify anything for a file, that file will be output with that filename. It will have the transfer_path prepended like with the standard naming scheme. If you want to output to different directories for each file, you can specify the path as part of the filename. If the transfer_path is blank you could output each file to a completely different directory. You cannot specify the lpr filename here as it is already available as a solo format string in the main ACS section.

Platforms	Name	Command	Default Value	Description
All	Contexts Filename			

Platforms	Name	Command	Default Value	Description
		`acs filenames context1 set filename {`*`value`*`}`		The format string used for the filename for this context images.

Context 2 (acs filenames context2)

Available on platforms: All

If you wish to have more control over the image filenames of the ACS output this section is for you, otherwise you can ignore it. You can specify filenames for each individual image that ACS outputs. If you leave the filenames blank then the standard ACS configuration will apply for that file. If you specify anything for a file, that file will be output with that filename. It will have the transfer_path prepended like with the standard naming scheme. If you want to output to different directories for each file, you can specify the path as part of the filename. If the transfer_path is blank you could output each file to a completely different directory. You cannot specify the lpr filename here as it is already available as a solo format string in the main ACS section.

Platforms	Name	Command	Default Value	Description
All	Contexts Filename	`acs filenames context2 set filename {`*`value`*`}`		The format string used for the filename for this context images.

Context 3 (acs filenames context3)

Available on platforms: All

If you wish to have more control over the image filenames of the ACS output this section is for you, otherwise you can ignore it. You can specify filenames for each individual image that ACS outputs. If you leave the filenames blank then the standard ACS configuration will apply for that file. If you specify anything for a file, that file will be output with that filename. It will have the transfer_path prepended like with the standard naming scheme. If you want to output to different directories for each file, you can specify the path as part of the filename. If the transfer_path is blank you could output each file to a completely different directory. You cannot specify the lpr filename here as it is already available as a solo format string in the main ACS section.

Platforms	Name	Command	Default Value	Description
All	Contexts Filename	`acs filenames context3 set filename {`*`value`*`}`		The format string used for the filename for this context images.

Context 4 (acs filenames context4)

Available on platforms: All

If you wish to have more control over the image filenames of the ACS output this section is for you, otherwise you can ignore it. You can specify filenames for each individual image that ACS outputs. If you leave the filenames blank then the standard ACS configuration will apply for that file. If you specify anything for a file, that file will be output with that filename. It will have the transfer_path prepended like with the standard naming scheme. If you want to output to different directories for each file, you can specify the path as part of the filename. If the transfer_path is blank you could output each file to a completely different directory. You cannot specify the lpr filename here as it is already available as a solo format string in the main ACS section.

Platforms	Name	Command	Default Value	Description
All	Contexts Filename			

Platforms	Name	Command	Default Value	Description
		`acs filenames context4 set filename {`*`value`*`}`		The format string used for the filename for this context images.

Context 5 (acs filenames context5)

Available on platforms: All

If you wish to have more control over the image filenames of the ACS output this section is for you, otherwise you can ignore it. You can specify filenames for each individual image that ACS outputs. If you leave the filenames blank then the standard ACS configuration will apply for that file. If you specify anything for a file, that file will be output with that filename. It will have the transfer_path prepended like with the standard naming scheme. If you want to output to different directories for each file, you can specify the path as part of the filename. If the transfer_path is blank you could output each file to a completely different directory. You cannot specify the lpr filename here as it is already available as a solo format string in the main ACS section.

Platforms	Name	Command	Default Value	Description
All	Contexts Filename	`acs filenames context5 set filename {`*`value`*`}`		The format string used for the filename for this context images.

Context 6 (acs filenames context6)

Available on platforms: All

If you wish to have more control over the image filenames of the ACS output this section is for you, otherwise you can ignore it. You can specify filenames for each individual image that ACS outputs. If you leave the filenames blank then the standard ACS configuration will apply for that file. If you specify anything for a file, that file will be output with that filename. It will have the transfer_path prepended like with the standard naming scheme. If you want to output to different directories for each file, you can specify the path as part of the filename. If the transfer_path is blank you could output each file to a completely different directory. You cannot specify the lpr filename here as it is already available as a solo format string in the main ACS section.

Platforms	Name	Command	Default Value	Description
All	Contexts Filename	`acs filenames context6 set filename {`*`value`*`}`		The format string used for the filename for this context images.

Context 7 (acs filenames context7)

Available on platforms: All

If you wish to have more control over the image filenames of the ACS output this section is for you, otherwise you can ignore it. You can specify filenames for each individual image that ACS outputs. If you leave the filenames blank then the standard ACS configuration will apply for that file. If you specify anything for a file, that file will be output with that filename. It will have the transfer_path prepended like with the standard naming scheme. If you want to output to different directories for each file, you can specify the path as part of the filename. If the transfer_path is blank you could output each file to a completely different directory. You cannot specify the lpr filename here as it is already available as a solo format string in the main ACS section.

Platforms	Name	Command	Default Value	Description
All	Contexts Filename			

Platforms	Name	Command	Default Value	Description
		`acs filenames context7 set filename {`*`value`*`}`		The format string used for the filename for this context images.

Context 8 (acs filenames context8)

Available on platforms: All

If you wish to have more control over the image filenames of the ACS output this section is for you, otherwise you can ignore it. You can specify filenames for each individual image that ACS outputs. If you leave the filenames blank then the standard ACS configuration will apply for that file. If you specify anything for a file, that file will be output with that filename. It will have the transfer_path prepended like with the standard naming scheme. If you want to output to different directories for each file, you can specify the path as part of the filename. If the transfer_path is blank you could output each file to a completely different directory. You cannot specify the lpr filename here as it is already available as a solo format string in the main ACS section.

Platforms	Name	Command	Default Value	Description
All	Contexts Filename	`acs filenames context8 set filename {`*`value`*`}`		The format string used for the filename for this context images.

Event Filter (acs filter)

Available on platforms: All

Platforms	Name	Command	Default Value	Description
All	Tag Regex	`acs filter set tag_regex {`*`value`*`}`	.*	

Using ACS

ACS uses various different file transfer protocols. It is recommended that you use SFTP as it is secure, can create directories, and has less network overhead than the FTP protocol. Historically ACS used the FTP protocol and that is also still possible. A suitable FTP server is required (FileZilla server is recommended for MS Windows platforms). SCP is also supported, but most platforms which work with SCP also work with SFTP which is able to create directories, wheras SCP is not.

Based on a number plate read event, ACS can transfer the following information:

- LPR data which consists of text metadata regarding the plate read event. LPR data will be transferred if **`transfer_lpr`** is set. The exact content of LPR text may be specified with the **`lpr_contents`** format string.
- A plate patch image in jpeg format. A patch image will be transferred if **`transfer_patch`** is set.
- A complete Infrared (IR) image in jpeg format. An IR image will be transferred if **`transfer_ir`** is set.
- A colour overview image in jpeg format. An overview image will be transferred if **`transfer_overview`** is set.

This ACS event data data may be transferred as separate files (up to 3 jpeg image files and an LPR textfile). These files are named according to the **`lpr_filename`** and **`image_filename`** properties.

Alternatively, if the **`transfer_packed`** property is set, all the required data is packed into a single AXI file. An AXI file consists of an XML header section followed by binary image data for whichever of the images are required. The advantage of using a packed AXI file is that there is less transfer overhead (a particular problem with normal FTP, a single transfer vs. up to four separate transfers) and may simplify processing at the receiver (no need to correlate the multiple files that relate to a single plate read event). One disadvantage with the packed format is that the file needs to be unpacked. However, the format is very simple (see the section called “ACS Event XML Schema”[23]) and should be easy to decode.

Older ACS systems only ever transferred separate files. Thus, for compatibility reasons, it may be necessary to disable the **`transfer_packed`** property.

Authentication

If you are using SFTP or SCP you can authenticate with your server in two ways.

- Conventional username and password, in a similar way to keyboard authentication. This is generally accepted as less secure, but is trivial to setup and may be good enough. To do this just set the **`user`** and **`pass`** properties and log in with those. This is the only option with conventional FTP.
- Using an SSH public key. You will need to create a public/private key pairing and install both of these onto your camera as `/opt/config/current/key_acs` and `/opt/config/current/key_acs.pub`. You can do this on the camera using **`ssh-keygen -t rsa`**. You must also give the public key to the server to allow it to authenticate - on a conventional openssh system this would be done by appending the public key into `~/.ssh/authorized_keys2` for the user you're going to transfer as. Once this is done you set up the user in the **`user`** field and if your private key has a passphrase enter that into the **`pass`** property.

ACS Event XML Schema

The packed AXI file format consists of an XML header followed by binary data for whatever images are required. The XML header part is a NULL terminated string. Binary data starts immediately after the NULL character. This XML header data contains the LPR text (if required) and, for each required image, the offset from the start of the binary data to the start of the image and the image length. This information is sufficient to extract the individual jpeg images.

The XML schema for the header is as follows:

axi.xsd

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
  <xs:element name="acs_event_header">
    <xs:complexType>
      <xs:sequence>
        <xs:element minOccurs="0" maxOccurs="1" ref="lpr"/>
        <xs:element minOccurs="0" maxOccurs="1" ref="patch"/>
        <xs:element minOccurs="0" maxOccurs="1" ref="full"/>
        <xs:element minOccurs="0" maxOccurs="1" ref="overview"/>
        <xs:element minOccurs="0" maxOccurs="1" ref="hazardPatch"/>
        <xs:element minOccurs="0" maxOccurs="1" ref="hazardFull"/>
        <xs:element minOccurs="0" maxOccurs="1" ref="hazardOverview"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:element name="lpr" type="xs:string"/>
  <xs:element name="patch">
    <xs:complexType>
      <xs:attribute name="length" use="required" type="xs:integer"/>
      <xs:attribute name="offset" use="required" type="xs:integer"/>
    </xs:complexType>
  </xs:element>
  <xs:element name="full">
    <xs:complexType>
      <xs:attribute name="length" use="required" type="xs:integer"/>
      <xs:attribute name="offset" use="required" type="xs:integer"/>
    </xs:complexType>
  </xs:element>
  <xs:element name="overview">
    <xs:complexType>
      <xs:attribute name="length" use="required" type="xs:integer"/>
      <xs:attribute name="offset" use="required" type="xs:integer"/>
    </xs:complexType>
  </xs:element>
  <xs:element name="hazardPatch">
    <xs:complexType>
      <xs:attribute name="length" use="required" type="xs:integer"/>
      <xs:attribute name="offset" use="required" type="xs:integer"/>
    </xs:complexType>
  </xs:element>
  <xs:element name="hazardFull">
    <xs:complexType>
      <xs:attribute name="length" use="required" type="xs:integer"/>
      <xs:attribute name="offset" use="required" type="xs:integer"/>
    </xs:complexType>
  </xs:element>
  <xs:element name="hazardOverview">
    <xs:complexType>
      <xs:attribute name="length" use="required" type="xs:integer"/>
      <xs:attribute name="offset" use="required" type="xs:integer"/>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

ANPR Vehicle Analyser (anpr)

Available on platforms: All

This module processes images to read the number plates in them.

Platforms	Name	Command	Default Value	Description
All	Cardet Debugging	`anpr set debugging {value}`	false	Make the engine output debugging files to dlldeb
All	Prioritse Hazard	`anpr set hazard_priority {value}`	false	Only relevant if hazard plate reading engine is loaded. If set true, will try harder to read hazard plates and may therefore improve hazard reading performance. However setting true may cause overall performance to deteriorate slightly.
All	Maximum mean character height	`anpr set max_char {value}`	32	Maximum mean character height above which an exception will be generated
All	Maximum mean horizontal plate angle	`anpr set max_mhpa {value}`	5	Maximum mean horizontal plate angle above which an exception will be generated
All	Maximum mean vertical plate angle	`anpr set max_mvpa {value}`	10	Maximum mean vertical plate angle above which an exception will be generated
All	Maximum Syntax Error Ratio	`anpr set max_ser {value}`	40	The maximum syntax error ratio (as percentage) above which an exception will be generated
All	Minimum mean character height	`anpr set min_char {value}`	16	Minimum mean character height below which an exception will be generated
All	Minimum Mean Plate Quality	`anpr set min_mpq {value}`	2000	The minimum mean plate quality below which an exception will be generated
All	Minimum mean tag confidence	`anpr set min_mtc {value}`	90	Minimum mean tag confidence below which an exception will be generated.
All	Square Plates	`anpr set square {value}`	false	Tell the engine that you have a high number of square plates and to try harder to read these. If you have only a small number of these plates this may degrade overall performance. The system will still read long plates.
All	Threshold of Confidence	`anpr set threshold {value}`	60	The minimum read confidence that the system will pass on to further modules. Set this to zero to pass through images from triggers (in an externally triggered system) when the trigger fires even if we didn't manage to read any number plate.
All	Trigger Passthrough	`anpr set trigger_pass {value}`	true	If selected the system will always pass through an image during a trigger, guaranteeing that you see a picture of a vehicle from which we couldn't read anything when you trigger. This overrides the threshold for triggers only.

Platforms	Name	Command	Default Value	Description
All	White On Black	`anpr set whiteonblack {value}`	false	Tell the engine that you have a high number of white on black plates and to try harder to read these. If you have only a small number of these plates this may degrade overall performance. The system will still read black on white plates.

- `anpr clearstats`

  Clears Cumulative statistics. Platforms: All.

  Resets all statistics collection variables to initial values

- `anpr stats`

  Cumulative statistics. Platforms: All.

  Provides cumulative statistics of longterm vehicle processing

Lane Identification Control (anpr laneId)

Available on platforms: All

This control is for determining what lane a number plate is travelling in. There is a maximum of four lanes which is designated by the lanes property. There are a lines which is used to differentiate between different lanes. The user will need to ensure that the lines do not cross, if they do no lane information will be provided within the region, a programatic method to prevent crossing has not been provided to enhance the users ability to setup the lane id system.

Platforms	Name	Command	Default Value	Description
All	Lane 1 name	`anpr laneId set Lane1Name {value}`	1	This is the lane which is the left of line 1
All	Lane 2 name	`anpr laneId set Lane2Name {value}`	2	This is the lane which is the left of line 2 and right of line 1
All	Lane 3 name	`anpr laneId set Lane3Name {value}`	3	This is the lane which is the left of line 3 and right of line 2
All	Lane 4 name	`anpr laneId set Lane4Name {value}`	4	This is the lane which is the right of line 3
All	Bottom X position of line 1	`anpr laneId set Line1bottomX {value}`	2048	This is the position of line 1 at the bottom of the image.
All	Top X position of line 1	`anpr laneId set Line1topX {value}`	2048	This is the position of line 1 at the top of the image
All	Bottom X position of line 2	`anpr laneId set Line2bottomX {value}`	2048	This is the position of line 2 at the bottom of the image.
All	Top X position of line 2	`anpr laneId set Line2topX {value}`	2048	This is the position of line 2 at the top of the image
All	Bottom X position of line 3	`anpr laneId set Line3bottomX {value}`	2048	This is the position of line 3 at the bottom of the image.
All	Top X position of line 3	`anpr laneId set Line3topX {value}`	2048	This is the position of line 3 at the top of the image
All	Enables the lane identification system	`anpr laneId set enabled {value}`	false	Enables the lane identification system.

Platforms	Name	Command	Default Value	Description
All	Sets the number of lanes	`anpr laneId set lanes` {*value*}	1	Set the number of lanes the system will recognise

Library Manager (anpr library)

Available on platforms: All

Management of which library you are using for plate recognition. Different libraries are tuned for different regions of the world to enhance recognition of local plates correctly. Using the correct engine for the location and type of plates you are likely to see is important to ensure good read rates. The libraries live in /opt/pips/

Platforms	Name	Command	Default Value	Description
All	Colour Plate Reading Engine	`anpr library set colour` {*value*}	none	The filename of the libcardet colour plate reading engine in use
All	Plate Reading Engine	`anpr library set engine` {*value*}	none	The filename of the libcardet plate reading engine in use
All	Hazard Plate Reading Engine	`anpr library set hazard` {*value*}	none	The filename of the libcardet Hazard plate reading engine in use

- `anpr library list`

  List. Platforms: All.

  List all available engines on this camera

Overview Crop Control (anpr overviewCrop)

Available on platforms: All

Control the overview crop

Platforms	Name	Command	Default Value	Description
All	Overlay Overlay Crop	`anpr overviewCrop set enabled` {*value*}	false	Enables the overlay crop. This creates smaller, cropped, overview images. Ensure that the FocalLength values for cam1 and cam2 are correct if this feature is enabled.
All	Image Height	`anpr overviewCrop set height` {*value*}	480	The height in pixels of the area cropped from the overview image. A value of 0 will cause the images to be cropped to the height of the plate.
All	Horizontal Offset	`anpr overviewCrop set horizontalOffset` {*value*}	-240	The offset in pixels from left edge of the plate to the left edge of the cropped overview image. A negative value indicates that the left edge of the image is to the left of the plate. A positive value indicates that the left edge of the image is to the right of the plate.
All	Horizontal Scale	`anpr overviewCrop set horizontalScale` {*value*}	0	Reduces the width of the cropped image: 0, No scaling; 1, Half Scale; 2, Quarter Scale.
All	Vertical Offset	`anpr overviewCrop set verticalOffset` {*value*}	-400	The offset in pixels from top edge of the plate to the top edge of the cropped overview

Platforms	Name	Command	Default Value	Description
				image. A negative value indicates that the top edge of the image is above the plate. A positive value indicates that the top edge of the image is below the plate.
All	Vertical Scale	`anpr overviewCrop set verticalScale {`*value*`}`	0	Reduces the height of the cropped image: 0, No scaling; 1, Half Scale; 2, Quarter Scale.
All	Image Width	`anpr overviewCrop set width {`*value*`}`	752	The width in pixels of the area cropped from the overview image. A value of 0 will cause the images to be cropped to the width of the plate.

Asynchronous Payload Matching (asyncp)

Available on platforms: All

The payload matching system allows the system to match up Vehicle Events with asynchronously provided payloads (user supplied data).

This data may then be included with the final event sent to the user.

See also the %PA format specifier.

Platforms	Name	Command	Default Value	Description
All	Acknowledge	`asyncp set ack_enabled {`*value*`}`	false	To enable/disable the generation of acks. If enabled the whole message, exactly as sent, will be echoed back to you.
All	Serial Baud Rate	`asyncp set baud {`*value*`}`	115200	The serial port baud rate. For changes to take effect, disable then re-enable. Valid values 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400
All	Binary	`asyncp set binary {`*value*`}`	false	If set true, will allow binary data. Otherwise data must be XML legal ASCII
All	Drop unmatched	`asyncp set drop_unmatched {`*value*`}`	false	Allows the vehicle events to be surpressed if no matching payload is found.
All	Enabled	`asyncp set enabled {`*value*`}`	false	Allows the Filter system to be enabled and disabled. Disable it unless you are using it.
All	Event Match Regex	`asyncp set eventmatch_regex {`*value*`}`		A regular expression (matching the Perl Regular Expression Syntax). If set to anything other than an empty string, it will be used to select an appropriate matching payload for the read event. If set it will be used instead of time proximity. (Selecting by time proximity within the time window is the default behaviour). Unlike the above regex in that this one can use format specifiers to extract information from the vehicle read event - to match to the async payloads.

Platforms	Name	Command	Default Value	Description
All	Match Window in milliseconds	`asyncp set matchwindow {value}`	1000	The maximum period that the times of the async payload and vehicle event may differ and still be considered for matching
All	Maximum age	`asyncp set max_age {value}`	20000	The maximum time in milliseconds that payloads are kept in memory.
All	Payload Regular Expression	`asyncp set payload_regex {value}`	(.*)\n	A regular expression (matching the Perl Regular Expression Syntax) that the incoming string must match in order for a payload to be recognised and stored. The actual payload will be the concatination of those parts of the incoming string that match any subexpressions in the regex, as specified by ()'s. If no ()'s are present in the payload_regex, then the entire incoming string, that matches the regex, will be used as the actual stored payload. Note: If the binary flag is set to false then a payload may only contain XML legal ASCII. If it contains any illegal characters, the entire string will be discarded.
All	TCP Port	`asyncp set port {value}`	3821	The TCP port to be used to accept incoming connections.
All	Message Source	`asyncp set source {value}`	tcp	The source of the messages. Set to either tcp or serial

- `asyncp statistics`

  Cumulative statistics. Platforms: All.

  Provides cumulative statistics of longterm vehicle filter processing

BOF2 protocol (bof2)

Available on platforms: All

The module implements the BOF 2.2 Protocol

Platforms	Name	Command	Default Value	Description
All	Authenticate using username and password	`bof2 set authenticate {value}`	false	Authenticate using username and password
All	Camera Identifier	`bof2 set cameraId {value}`	1	Specified through the use of the a format string, if the value of the format string does not evaluate between -32768 and 32767 it will be 0.
All	Delivery Order	`bof2 set delivery_order {value}`	FIFO	The order in which events can be delivered, First in First Out (FIFO) or Last In First Out (LIFO). NB: Switching between modes deletes all data queued for delivery.

Platforms	Name	Command	Default Value	Description
All	Enabled	`bof2 set enabled {value}`	false	Allows the BOF2 system to be enabled and disabled. Disable it unless you are using it.
All	Feed Identifier	`bof2 set feedId {value}`	1	Also known as Force ID. Specified through the use of the a format string, if the value of the format string does not evaluate between -32768 and 32767 it will be 0.
All	Host	`bof2 set host {value}`	192.168.1.1:8080	IP address and port of the instation which will receive the BOF2.2 data.
All	Event Queue Size	`bof2 set nlog {value}`	100	The maximum number of events which will be enqueued for delivery. This delivery module uses the VFE Database, so events will get deleted based upon the rules set within the VFE database. If an event has been deleted we will continue on to the next in the queue
All	Camera Pan	`bof2 set pan {value}`	0	For CCTV cameras.
All	Password	`bof2 set password {value}`		Password for BOF transport user
All	Path	`bof2 set path {value}`	/bof2/services/InputCaptureWebService	The path on the http url.
All	Camera Preset Position	`bof2 set position {value}`	0	Used to indicate direction of travel on multi-use CCTV cameras
All	Send overview	`bof2 set send_overview {value}`	true	Allows sending of overview image to the BOF2 system to be enabled and disabled.
All	Send Patch	`bof2 set send_patch {value}`	true	Allows sending of patch image to the BOF2 system to be enabled and disabled.
All	Public Signature Of Sender	`bof2 set signature {value}`		Format not specified in BOF 2.2 spec, left as std::string for users
All	Source Identifier	`bof2 set sourceId {value}`	1	Specified through the use of the a format string, if the value of the format string does not evaluate between -32768 and 32767 it will be 0.
All	Camera Tilt	`bof2 set tilt {value}`	0	For CCTV cameras.
All	BOF2.2 transport	`bof2 set transport {value}`	HTTPS	HTTP or HTTPS
All	username	`bof2 set username {value}`	Unattended	Username for BOF user
All	Verify Peer	`bof2 set verifyPeer {value}`	true	Allows the verification of the BOF2 server certificate to be disabled when set to false.
All	Camera Zoom	`bof2 set zoom {value}`	0	For CCTV cameras.

- `bof2 clearStats`

  Resets all Statistics. Platforms: All.

  Resets all Statistics

- `bof2 diskq_flush`

  Empty the Disk Queue. Platforms: All.

All BOF events currently stored in the persistant Disk Queue will be deleted and will not be recoverable. Use this with care.

- `bof2 diskq_length`

  Length of Disk Queue. Platforms: All.

  The number of BOF events stored in the persistant Disk Queue will be reported.

- `bof2 stats`

  Statistics. Platforms: All.

  Statistics for debugging

IR Camera (cam1)

Available on platforms: All

Controls for managing the camera and images that it takes

Platforms	Name	Command	Default Value	Description
All	Sensor ADC gain	`cam1 set ADCgain {value}`	52	This sets the adc gain for the Overview sensor Warning don't alter this value. When finished commit will need to be run.
All	Lens Focal Length	`cam1 set FocalLength {value}`	35	The focal length of the lens in front of the IR sensor. This value must be set correctly if overview cropping is in use
All	Platefinder Regions of Interest Coordinates	`cam1 set ROICoordinates {value}`	(0,0),(2048,0),(2048,720),(0,720)	Region polygon(s) co-ordinates clockwise from Top Left. Region polygons are separated by a semi-colon.
All	Platefinder Regions of Interest	`cam1 set ROIEnabled {value}`	false	Sets whether Region of Interest polygon(s) is used or not.
All	Sensor Vramp	`cam1 set Vramp {value}`	109	This sets the Vramp value for the Overview sensor Warning don't alter this value. When finished commit will need to be run.
All	Points at front of vehicles	`cam1 set front_facing {value}`	true	Sets whether the camera is reading from the front of the vehicle. If you have bi-directional traffic set this false.
All	Horizontal Scale	`cam1 set horizontalScale {value}`	0	This will control the scale the channel (but not the plate patch), 0 = no scaling, 1 = half scaling, 2 = quarter scaling
All	Number of Exposure entries cycled in a sequence	`cam1 set numentries {value}`	0	Number of exposure entries cycled through. Set to 1 to disable exposure sequencing, just using the first entry. Otherwise each exposure will be taken with a different entry from the table.
All	Platefinder bottom plate width	`cam1 set platewidth_b {value}`	180	Sets the plate width for this channel in pixels at the bottom of the image. Try to get your plates to be between 180 and 220 pixels wide (for UK style plates), or 140-180 pixels (for US style plates). Getting this right will improve plate recognition.

Platforms	Name	Command	Default Value	Description
All	Platefinder top plate width	`cam1 set platewidth_t {value}`	180	Sets the plate width for this channel in pixels at the top of the image. Try to get your plates to be between 180 and 220 pixels wide (for UK style plates), or 140-180 pixels (for US style plates). Getting this right will improve plate recognition.
All	Fields of Retard	`cam1 set retard {value}`	0	Sets the number of fields of retard for this video channel. The video will be delayed by this number of fields .This feature is only useful in triggered systems. It adds flexibility by allowing compensation for a chronically late trigger. It is suggested that this feature only be used as a last resort.
All	Sharpening mode	`cam1 set sharpening {value}`	1	ENGINEERING USE ONLY:Then enables image sharpening - mode 0 off, mode 1 old sharpening mode, mode 2 a new sharpening mode
All	Vertical Scale	`cam1 set verticalScale {value}`	0	This will control the scale the channel (but not the plate patch), 0 = no scaling, 1 = half scaling, 2 = quarter scaling

- `cam1 commit`

  Commit the new ADC gain and V Ramp settings. Platforms: All.

  Commits the ADC gain and V Ramp to nand flash

Exposure Controller (cam1 exposure)

Available on platforms: All

An automated controller for the exposures on the camera. It will run with our triple flash system and adjust the sequence entries for shutter and gain appropriatly to optimise the image for plate reading.

Platforms	Name	Command	Default Value	Description
All	Brightness cutoff	`cam1 exposure set bright_cutoff {value}`	5	This value determines the percentage of pixels in the plate which differentiate between an underexposed and a correctly exposed plate .If brightness control is making your plates too bright lower this value or vice-versa. Also see the Brightness overexposure setting and set the two in parallel.
All	Exposure control enabled	`cam1 exposure set enabled {value}`	true	Allows you to switch the exposure controller on or off. It is recommended to use this system, if you disable it you should manually set up the exposure sequence.
All	Good DB Value	`cam1 exposure set good_db_value {value}`	2000	Not normally set by user except for testing purposes (it is automatically updated). This

Platforms	Name	Command	Default Value	Description
				determines at what brightness the system starts after a reboot. This value will be used to adjust the brightness when there is not enough traffic.
All	Maximum gain	`cam1 exposure set max_gain {value}`	11	Maximum gain value that is used by the exposure controller.
All	Maximum shutter length	`cam1 exposure set max_shutter {value}`	1000	Maximum shutter length in microseconds that the exposure controller will use. For most uses leave this at 1000, but if you are trying to read very high speed (>160kph) traffic all the time you can shorten this at the expense of all other traffic reads. This is not recommended.
All	Single Sequence Outside Trigger	`cam1 exposure set single_seq_outside_trig {value}`	false	

- `cam1 exposure info`

  Information. Platforms: All.

  Get detailed information of the status of the exposure controller. For debugging purposes.

- `cam1 exposure setBrightDBValue {dbValue}`

  Set absolute brightness DB value. Platforms: All.

  Instantly, manually set the brightness to a DB value. Mostly used for testing, if the exposure controller is on it will adapt the image again after you do this.

#	Name	Parameter	Description
1	Brightness to set to	dbValue	Brightness DB value.

- `cam1 exposure setbrightness {brightness}`

  Set Brightness. Platforms: All.

  Instantly, manually set the brightness to a value. Mostly used for testing, if the exposure controller is on it will adapt the image again after you do this.

#	Name	Parameter	Description
1	Brightness to set to	brightness	Brightness value.

Overlay Control (cam1 overlay)

Available on platforms: All

One overlay control per chanel

Platforms	Name	Command	Default Value	Description
All	Image Below	`cam1 overlay set below {value}`	false	Enables overlayed text on the Image. If not set the text will be above the image.

Platforms	Name	Command	Default Value	Description
All	Overlay Text Enable	`cam1 overlay set enabled {value}`	false	Enables additional text on the Image
All	Expand	`cam1 overlay set expand {value}`	true	Makes the image larger when the text is added. If not set the text will eat into the visible image area.
All	Text	`cam1 overlay set text {value}`	%Shs %Iy04u/ %Io02d/ %Id02u %Ih02u:%Im02u:%Is02u.%Ii03u	The format string for the overlayed text. This has limitations

Platewidth Control (cam1 platewidth)

Available on platforms: All

Automatically calculate and setup plate widths

Platforms	Name	Command	Default Value	Description
All	Plate width Control Enable	`cam1 platewidth set enabled {value}`	false	Enables Automatic Platewidth Control

- `cam1 platewidth info`

  Information. Platforms: All.

  Get detailed information of the status of the platewidth controller. For debugging purposes.

Sequence 1 (cam1 seq1)

Available on platforms: All

One exposure in the sequence for camera

Platforms	Name	Command	Default Value	Description
All	Gain	`cam1 seq1 set gain {value}`	48	Gain in the camera, which increases brightness (and noise) in the image. An aribrary but linear value.
All	Shutter length	`cam1 seq1 set shutter {value}`	16	Length of time that the shutter is open for, and the flash is fired for. This is 0 for 10 microseconds and 31 for 1 millisecond, linearly running between those values.

Sequence 2 (cam1 seq2)

Available on platforms: All

One exposure in the sequence for camera

Platforms	Name	Command	Default Value	Description
All	Gain	`cam1 seq2 set gain {value}`	48	Gain in the camera, which increases brightness (and noise) in the image. An aribrary but linear value.

Platforms	Name	Command	Default Value	Description
All	Shutter length	`cam1 seq2 set shutter {value}`	16	Length of time that the shutter is open for, and the flash is fired for. This is 0 for 10 microseconds and 31 for 1 millisecond, linearly running between those values.

Sequence 3 (cam1 seq3)

Available on platforms: All

One exposure in the sequence for camera

Platforms	Name	Command	Default Value	Description
All	Gain	`cam1 seq3 set gain {value}`	48	Gain in the camera, which increases brightness (and noise) in the image. An aribrary but linear value.
All	Shutter length	`cam1 seq3 set shutter {value}`	16	Length of time that the shutter is open for, and the flash is fired for. This is 0 for 10 microseconds and 31 for 1 millisecond, linearly running between those values.

Sequence 4 (cam1 seq4)

Available on platforms: All

One exposure in the sequence for camera

Platforms	Name	Command	Default Value	Description
All	Gain	`cam1 seq4 set gain {value}`	48	Gain in the camera, which increases brightness (and noise) in the image. An aribrary but linear value.
All	Shutter length	`cam1 seq4 set shutter {value}`	16	Length of time that the shutter is open for, and the flash is fired for. This is 0 for 10 microseconds and 31 for 1 millisecond, linearly running between those values.

Overview Camera (cam2)

Available on platforms: All

Controls for managing the camera and images that it takes

Platforms	Name	Command	Default Value	Description
All	Sensor ADC gain	`cam2 set ADCgain {value}`	52	This sets the adc gain for the Overview sensor Warning don't alter this value. When finished commit will need to be run.
All	Lens Focal Length	`cam2 set FocalLength {value}`	25	The focal length of the lens in front of the overview sensor. This value must be set correctly if overview cropping is in use
All	Sensor Vramp	`cam2 set Vramp {value}`	109	This sets the Vramp value for the Overview sensor Warning don't alter this value. When finished commit will need to be run.

Platforms	Name	Command	Default Value	Description
All	Automatic White Balance	`cam2 set autoWhiteBalance {value}`	true	Enables automatic white balance.
All	Exposure mode	`cam2 set auto_mode {value}`	true	The exposure mode settings, true - auto mode, false - manual mode.
All	Bayer Pattern	`cam2 set bayerOrder {value}`	1	0, 1, 2 or 3. For PIPS engineering use only.
All	Bypass the Bayer Filter	`cam2 set bypassBayer {value}`	false	For PIPS engineering use only.
All	Chroma Order	`cam2 set chromaOrder {value}`	1	0 = YCbCr, 1 = YCrCb, For PIPS engineering use only.
All	FPN removal enabled	`cam2 set fpnRemovalEnabled {value}`	false	Enables and disables FPN removal. Requires the camera to have had the removal image calibrated using calibrateFPN
All	Gain	`cam2 set gain {value}`	0	The gain value(0-15). This only can be set when in manual mode. Mainly for debug use.
All	Gamma Value	`cam2 set gammaCurve {value}`	2	Specifies the gamma correction value. 0 = 1.00, 1 = 0.45, 2 = 0.50 (recommended), 3 = 0.55.
All	Horizontal Scale	`cam2 set horizontalScale {value}`	0	This will control the scale of the whole channel (but not the overview crop), 0 = no scaling, 1 = half scaling, 2 = quarter scaling
All	Maximum Gain	`cam2 set max_gain {value}`	15	The maximum gain value. This camera will automatically set gain and shutter. Setting this higher will result in less blurring, but may cause more noise
All	Maximum shutter length	`cam2 set max_shutter {value}`	4	The maximum shutter length. This camera will automatically set gain and shutter. Setting this lower will give less blurring in the picture, but in low light you may not be able to see anything in the picture if you set it too low as it will not get enough light. Your hardware description must mention that you have a Overview Shutter Limiter for this to work. Values 1-8 are interpreted as milli-seconds. Other values are interpreted as micro-seconds
All	Colour Saturation	`cam2 set saturation {value}`	256	Sets the image saturation level. The recommended value is 256.
All	Sharpening Mode	`cam2 set sharpening {value}`	0	Selects the image sharpening algorithm. 0 = off (for PIPS engineering use only), 1 = the algorithm used in earlier releases, 2 = the improved algorithm (recommended).
All	Shutter length	`cam2 set shutter {value}`	5000	The shutter length in microseconds(16-7500). This only can be set when in manual mode. Mainly for debug use.
All	Target Brightness	`cam2 set target {value}`	110	The target brightness is value that the brightness controller will try and adjust the average pixel value to reach

Platforms	Name	Command	Default Value	Description
All	Vertical Scale	`cam2 set verticalScale {value}`	0	This will control the scale of the whole channel (but not the overview crop), 0 = no scaling, 1 = half scaling, 2 = quarter scaling
All	White Balance Blue Coefficient	`cam2 set whiteBalanceCoeffBlue {value}`	0	The blue coefficient for the white balance operation. This is a read-only value showing the output of auto white balance.
All	White Balance Red Coefficient	`cam2 set whiteBalanceCoeffRed {value}`	0	The red coefficient for the white balance operation. This is a read-only value showing the output of auto white balance.

- `cam2 calibrateFPN`

  Calibrate the Fixed Pattern Noise reference image. Platforms: All.

  Automatically builds a reference image of the Fixed Pattern Noise on the sensor, to allow this to be removed from the images.

- `cam2 ccm`

  Dump Colour Correction Matrix. Platforms: All.

  Dump Colour Correction Matrix

- `cam2 commit`

  Commit the new ADC gain and V Ramp settings. Platforms: All.

  Commits the ADC gain and V Ramp to nand flash

Overlay Control (cam2 overlay)

Available on platforms: All

One overlay control per chanel

Platforms	Name	Command	Default Value	Description
All	Image Below	`cam2 overlay set below {value}`	false	Enables overlayed text on the Image. If not set the text will be above the image.
All	Overlay Text Enable	`cam2 overlay set enabled {value}`	false	Enables additional text on the Image
All	Expand	`cam2 overlay set expand {value}`	true	Makes the image larger when the text is added. If not set the text will eat into the visible image area.
All	Text	`cam2 overlay set text {value}`	%Shs %Iy04u/ %Io02d/ %Id02u %Ih02u:%Im02u:%Is02u.%Ii03u	The format string for the overlayed text. This has limitations

Client vehicle event reporter (client)

Available on platforms: All

Reports individual vehicle events over the network to a client for live monitoring and diagnostics. Using the ClientView application you can see these images.

Platforms	Name	Command	Default Value	Description
All	Platefinder position instead	`client set platefinder {value}`	false	Show the plate patches from the hardware platefinder rather than the ANPR engine. This is for debugging purposes.

Contexts (contexts)

Available on platforms: All

Control for managing context images associated with an event

Platforms	Name	Command	Default Value	Description
All	Number of Context Images	`contexts set number {value}`	0	Number of context images associated with a vehicle event

Context 1 (contexts ctx1)

Available on platforms: All

An entry defining the offset of a single context image.

Platforms	Name	Command	Default Value	Description
All	Offset	`contexts ctx1 set offset {value}`	250	The offset in milliseconds from the actual read event time. Negative offset will give images prior to the read. Positive offset will give images after the read. Note, the images returned may not have the exact timestamps as specified by the offsets. They will however be the nearest time matching images available. Image timestamp best resolution is affected by the frame rate (for example 50fps implies images are 20ms apart). Images older than a certain period may also be subject to decimation due to limited RAM storage.

Context 2 (contexts ctx2)

Available on platforms: All

An entry defining the offset of a single context image.

Platforms	Name	Command	Default Value	Description
All	Offset	`contexts ctx2 set offset {value}`	250	The offset in milliseconds from the actual read event time. Negative offset will give

Platforms	Name	Command	Default Value	Description
				images prior to the read. Positive offset will give images after the read. Note, the images returned may not have the exact timestamps as specified by the offsets. They will however be the nearest time matching images available. Image timestamp best resolution is affected by the frame rate (for example 50fps implies images are 20ms apart). Images older than a certain period may also be subject to decimation due to limited RAM storage.

Context 3 (contexts ctx3)

Available on platforms: All

An entry defining the offset of a single context image.

Platforms	Name	Command	Default Value	Description
All	Offset	`contexts ctx3 set offset {`*`value`*`}`	250	The offset in milliseconds from the actual read event time. Negative offset will give images prior to the read. Positive offset will give images after the read. Note, the images returned may not have the exact timestamps as specified by the offsets. They will however be the nearest time matching images available. Image timestamp best resolution is affected by the frame rate (for example 50fps implies images are 20ms apart). Images older than a certain period may also be subject to decimation due to limited RAM storage.

Context 4 (contexts ctx4)

Available on platforms: All

An entry defining the offset of a single context image.

Platforms	Name	Command	Default Value	Description
All	Offset	`contexts ctx4 set offset {`*`value`*`}`	250	The offset in milliseconds from the actual read event time. Negative offset will give images prior to the read. Positive offset will give images after the read. Note, the images returned may not have the exact timestamps as specified by the offsets. They will however be the nearest time matching images available. Image timestamp best resolution is affected by the frame rate

Platforms	Name	Command	Default Value	Description
				(for example 50fps implies images are 20ms apart). Images older than a certain period may also be subject to decimation due to limited RAM storage.

Context 5 (contexts ctx5)

Available on platforms: All

An entry defining the offset of a single context image.

Platforms	Name	Command	Default Value	Description
All	Offset	`contexts ctx5 set offset {`*`value`*`}`	250	The offset in milliseconds from the actual read event time. Negative offset will give images prior to the read. Positive offset will give images after the read. Note, the images returned may not have the exact timestamps as specified by the offsets. They will however be the nearest time matching images available. Image timestamp best resolution is affected by the frame rate (for example 50fps implies images are 20ms apart). Images older than a certain period may also be subject to decimation due to limited RAM storage.

Context 6 (contexts ctx6)

Available on platforms: All

An entry defining the offset of a single context image.

Platforms	Name	Command	Default Value	Description
All	Offset	`contexts ctx6 set offset {`*`value`*`}`	250	The offset in milliseconds from the actual read event time. Negative offset will give images prior to the read. Positive offset will give images after the read. Note, the images returned may not have the exact timestamps as specified by the offsets. They will however be the nearest time matching images available. Image timestamp best resolution is affected by the frame rate (for example 50fps implies images are 20ms apart). Images older than a certain period may also be subject to decimation due to limited RAM storage.

Context 7 (contexts ctx7)

Available on platforms: All

An entry defining the offset of a single context image.

Platforms	Name	Command	Default Value	Description
All	Offset	`contexts ctx7 set offset {value}`	250	The offset in milliseconds from the actual read event time. Negative offset will give images prior to the read. Positive offset will give images after the read. Note, the images returned may not have the exact timestamps as specified by the offsets. They will however be the nearest time matching images available. Image timestamp best resolution is affected by the frame rate (for example 50fps implies images are 20ms apart). Images older than a certain period may also be subject to decimation due to limited RAM storage.

Context 8 (contexts ctx8)

Available on platforms: All

An entry defining the offset of a single context image.

Platforms	Name	Command	Default Value	Description
All	Offset	`contexts ctx8 set offset {value}`	250	The offset in milliseconds from the actual read event time. Negative offset will give images prior to the read. Positive offset will give images after the read. Note, the images returned may not have the exact timestamps as specified by the offsets. They will however be the nearest time matching images available. Image timestamp best resolution is affected by the frame rate (for example 50fps implies images are 20ms apart). Images older than a certain period may also be subject to decimation due to limited RAM storage.

Plate Database Matcher (dbmatcher)

Available on platforms: All

The database matching system allows the system to look up number plates in a database.

It is possible to filter out plates based on whether they are found or not.

It is also possible to collect a tag string for plates which are found which can be output by the delivery system.

No spaces or commas are allowed in the plate or tag string.

INSTALLING NEW DATABASE FILES:

Copy a file named [YourPlatesDatabaseName].install into the camera /storage/db/ directory.

For example, for the default plates.db name, you would copy a file named plates.db.install into the /storage/db/ directory.

The system should automatically detect this and install the new file. To confirm this, do a directory listing of the /storage/db/ directory and confirm:

1)That the plates.db.install you just copied in has disappeared (GUI Tool may need refreshing)

2)That the plates.db file md5sum matches the file you installed.

If for some reason this does not work, then copy your plates.db.install into /storage/

and then, using the linux command prompt, move this file into /storage/db/

mv /storage/plates.db.install /storage/db/.

and then verify as above.

Platforms	Name	Command	Default Value	Description
All	Enabled	`dbmatcher set enabled {value}`	false	Allows the Filter system to be enabled and disabled. Disable it unless you are using it.
All	Forward Event on match	`dbmatcher set forward_on_match {value}`	false	Will forward the plate read event only if a match is found in the database. May be enabled simultaneously with forward_on_nomatch. This will have the effect of all plates being forwarded but matching plates will carry their corresponding tags.
All	Forward Event on no match	`dbmatcher set forward_on_nomatch {value}`	false	Will forward the plate read event if no match is found in the database. May be enabled simultaneously with forward_on_match. This will have the effect of all plates being forwarded but matching plates will carry their corresponding tags.
All	Plate Database File Name	`dbmatcher set plates_filename {value}`	plates.db	Specify the filename of the plates SQLite database. This file may be pre-created and placed in the /storage/db/ directory. The SQL to create a compatible database is: CREATE TABLE plateDB(plate TEXT PRIMARY KEY ASC, tag TEXT);

- `dbmatcher insert {plate} {tag}`

  Insert a plate+tag. Platforms: All.

  Adds a plate+tag combination to the plates database.

#	Name	Parameter	Description
1		plate	The plate you wish to insert

#	Name	Parameter	Description
	Plate Entry to insert		
2	Plate Tag	tag	The tag associated with the plate you wish to insert

- `dbmatcher lookup` {*`plate`*}

  Lookup a plate. Platforms: All.

  Determines if a plate exists in the current database. Will confirm if the plate is found and print its tag value

#	Name	Parameter	Description
1	Plate Entry to lookup	plate	The plate you wish to find in the database

- `dbmatcher reload`

  Load the database file. Platforms: All.

  Load the file named by plates_filename. Use this command to reload the plates database file if it has been changed or replaced, or if you have changed the name.

- `dbmatcher remove` {*`plate`*}

  Remove a plate. Platforms: All.

  If the plate exists in the current database it (and its associated tag) will be removed.

#	Name	Parameter	Description
1	Plate Entry to remove	plate	The plate you wish to remove from the database

- `dbmatcher statistics`

  Cumulative statistics. Platforms: All.

  Provides cumulative statistics of longterm vehicle filter processing

Diagnostics and Exceptions Manager (diagnostics)

Available on platforms: All

Diagnostics and Exceptions

Platforms	Name	Command	Default Value	Description
All	Acknowledgents Enabled	`diagnostics set ack_enabled` {*`value`*}	true	If true, the delivery system will await acknowledgement
All	Diagnostic/ Exception ack wait timeout	`diagnostics set ack_timeout` {*`value`*}	30	Period in seconds to wait for an acknowledgement of a diagnostic or exception message
All	Minimum Samples for Diagnostics	`diagnostics set min_samples` {*`value`*}	10	Certain types of diagnostics (e.g. mean values or ratios) are only considered valid after a certain number of samples.

Platforms	Name	Command	Default Value	Description
All	Diagnostic period	`diagnostics set diagnostic_period {value}`	20	Period in minutes between diagnostic updates
All	Diagnostic Delivery Port	`diagnostics set diagnostic_port {value}`	5001	The TCP port that diagnostic messages will be delivered on. Set to
All	Disk Queue Length	`diagnostics set disk_queue_length {value}`	5	The number of diagnostic and exception events that are maintained in a persistent disk queue while the in station receiver is offline. Diagnostics are kept in a seperate queue to exceptions. This value applies to all queues
All	Diagnostics enabled	`diagnostics set enabled {value}`	false	Allows diagnostic and exception reporting to be enabled/disabled
All	Minimum Samples for Exceptions	`diagnostics set exception_min_samples {value}`	20	Certain types of exceptions (e.g. mean values or ratios) are only considered valid after a certain number of samples.
All	Exception Period	`diagnostics set exception_period {value}`	5	Period in minutes between (non-realtime) exception updates
All	Exception Delivery Port	`diagnostics set exception_port {value}`	5002	The TCP port that exception messages will be delivered on
All	Delivery Host	`diagnostics set host {value}`	10.1.1.1	The IP address to which the diagnsotic and exception messages will be transferred.
All	JTMS Compatible	`diagnostics set jtms {value}`	false	Generate JTMS compatible diagnostics instead of VES compatible diagnostics. The differences are small but significant.

File Logger (filelog)

Available on platforms: All

The logger which reports information to specified file. NB: A log file can grow to fill the disk. Use logrotate to manage log files.

Platforms	Name	Command	Default Value	Description
All	Enable file logging	`filelog set enabled {value}`	false	Enable logging to a file. NB, the camera does not manage the file size or archiving. Please use logrotate
All	Log File Name	`filelog set filename {value}`	/var/log/start382.log	Specify the filename to receive log output. NB: To avoid this file growing too large, please use logrotate
All	Print line/file	`filelog set lineFilePrint {value}`	true	Print Linenumber and Filename for logging messages
All	Print time	`filelog set timePrint {value}`	true	Print time for logging messages

Vehicle Fusion (fusion)

Available on platforms: All

The system may read multiple images of any given vehicle, and this subsystem merges those multiple vehicle reads into a single coherant result for output.

Platforms	Name	Command	Default Value	Description
All	Combine hazard and normal plates	`fusion set combine_hazard {value}`	false	If this is set true, an attempt will be made to match the hazard plate with the normal plate of the same vehicle. If successful, a combined event will be forwarded. If a hazard plate is read, it will normally be forwarded as an independant plate read.
All	Distance from edge	`fusion set distance {value}`	256	Distance from the edge specified in the selector parameter to the centre of the plate which will be used to try to select an appropriate plate for you (measured in pixels). May not be used if no distance selector in use.
All	Duplicate Level	`fusion set duplicate_level {value}`	60	Percentage match level at which the numberplates will be considered as duplicates for matching multiple reads of a vehicle together. 100 means they must be identical, and 0 means anything will match anything else (which makes the camera pretty useless).
All	Early result	`fusion set early {value}`	false	Output the first event from a vehicle even if it may well be wrong. Useful if the time between a vehicle being seen and the camera reporting it is critical, otherwise don't choose this
All	Maximum gap	`fusion set gap {value}`	700	Length of time after seeing a vehicle when we pass on the vehicle when we haven't seen it again for this long. Given in milliseconds.
All	Maximum age of vehicle	`fusion set max_age {value}`	2000	Maximum time the vehicle can be in the field of view before we pass it on anyway. Given in milliseconds.
All	No Event Timeout	`fusion set noevent_timeout {value}`	4294967295	If no vehicle event has been delivered within this timeout period (in seconds) a Vehicle Detect Timeout exception will be generated. This is a boolean exception and will be cleared as soon as a vehicle event is forwarded. This cannot be set below 10 seconds
All	Allow out of trigger images	`fusion set outoftrigger {value}`	false	If a vehicle arrives during a trigger we will only deliver images from within the trigger period unless you tick this box. This allows us to deliver better images from earlier.
All	Persistant event id	`fusion set persistantEventId {value}`	true	Set this value to true to keep the next event id in a separate file. Setting this value to false causes the camera to calculate the next event id using the data stored on the VFE database. It takes some time to update the VFE database and

Platforms	Name	Command	Default Value	Description
				the event id sequence may not be updated correctly if the camera app is restarted. If the VFE database is disabled then the event id sequence is reset to 0 when the camera app is restarted. Set this value to true if the uniqueness of event ids is important. Set the value to false if performance is important.
All	Repeating vehicles	`fusion set repeat {value}`	true	If a vehicle stays in the field of view we will pass it on every max_age milliseconds if this is set true, otherwise just once. In the presence of triggers, all vehicles are flushed when the trigger gate closes. Repeats may then still be experienced. In order to prevent repeats in the presence of triggers, set the repeat_on_trigger to false.
All	Repeating vehicles per trigger	`fusion set repeat_on_trigger {value}`	true	If true, a vehicle staying in the field of view we will be forwarded on every trigger (default). Otherwise the vehicle will only be forwarded the first time it is detected within a trigger period.
All	Plate Selector	`fusion set selector {value}`	0	This parameter will allow the system to select an appropriate plate for you. Sometimes we may not be able to select a plate which matches your criteria very well, but we will do what we can. 0=Best plate read. 1=Distance from top edge. 2=Distance from left edge. 3=Plate exposure quality, for better visibility of the non plate text details
All	Set reads forwarded from a trigger to 1	`fusion set single_read_on_trigger {value}`	false	Only applies to triggered systems. Will limit the maximum number of read events delivered per trigger to 1. The vehicle chosen for delivery will be decided according to read confidence. Beware of setting this as vehicles (such as adjacent vehicles) may be missed. Also, if set, a parked vehicle may prevent any other vehicles being read.
All	Supplementary IR Images	`fusion set supplementary_images {value}`	false	Only works for images within a trigger gate open period.

Platforms	Name	Command	Default Value	Description
				If true, up to two additional full IR image will be available for delivery. These will be alternatively exposed IR images (if alternative exposure sequence images are available). If no other sequence images are available the best exposed of the remaining IR images (if any) will be available. In the case where only one image was analysed for the vehicle, no additional image will be available.

- `fusion clearstats`

  Clears Cumulative statistics. Platforms: All.

  Resets all statistics collection variables to initial values

- `fusion stats`

  Cumulative statistics. Platforms: All.

  Provides cumulative statistics of longterm vehicle processing

- `fusion status`

  Current status. Platforms: All.

  Gets the current status of the vehicles being processed by the module

GPS Time Manager (gps)

Available on platforms: All

Manages GPS Time Sync

Platforms	Name	Command	Default Value	Description
All	Enabled	`gps set enabled` {*`value`*}	false	Enables gps time manager

- `gps status`

  Current status of GPS/PPS. Platforms: All.

  Gets the current status of the GPS and PPS time management

Heartbeat (heartbeat)

Available on platforms: All

Platforms	Name	Command	Default Value	Description
All	Heartbeat Content	`heartbeat set content` {*`value`*}	%Shs,%hsx,%lcm,%hfm	A format string specifying the content of the heartbeat message.

Platforms	Name	Command	Default Value	Description
All	Enabled	`heartbeat set enabled {value}`	false	Allows the Heartbeat system to be enabled and disabled. Disable it unless you are using it.
All	Delivery Host	`heartbeat set host {value}`	10.1.1.1	The IP address to which the heartbeat messages will be transferred.
All	Heartbeat period	`heartbeat set period {value}`	60	Period in seconds between heartbeats
All	Heartbeat Delivery Port	`heartbeat set port {value}`	10005	The TCP port that heartbeat messages will be delivered on.

Image File Outputter (ifo)

Available on platforms: All

Stores the images from the camera onto disk. These are just periodic images from the selected camera, like a video stream, not ones of particular interest, and they may or may not contain plates. If you have network mounted a disk this would be most useful, as otherwise you'll quickly fill up the internal storage of the camera. Look at mounting a disk in /storage to use this. This module is designed purely for testing and debugging, not for production systems. There is no guarantee that images will come out at all if the rest of the system is too busy. Image metadata is stored in the filename. The filename format may change without notice.

Platforms	Name	Command	Default Value	Description
All	Anpr Patches	`ifo set anprpatch {value}`	true	When looking at plates, output an extra file for the anpr patch. This file will have the prefix A
All	Bitmap	`ifo set bitmap {value}`	false	Enable this to output bitmap files, otherwise the output is jpeg format. Only works for monochrome images, colour ones are always jpeg format.
All	Colour	`ifo set colour {value}`	false	Enable this to store video images from the colour camera, otherwise look at the monochrome camera. Has no effect on plate images which are always monochrome.
All	Output Directory	`ifo set directory {value}`	/tmp	Directory to receive the files relative to the /storage directory. It is recommended you mount an external network disk here to collect the images.
All	Enabled	`ifo set enabled {value}`	false	Enable or disable the output of raw image files (e.g. this whole module). Should be turned off on production systems.
All	Minimum interval	`ifo set interval {value}`	1000	Minimum number of milliseconds between files, with a busy camera, filesystem or network this may not be adhered to.
All	Hardware Platefinder Patches	`ifo set pfpatch {value}`	false	When looking at plates, output an extra file for the platefinder patch. This file will have the prefix H
All	Plates	`ifo set plates {value}`	true	Enable or disable the output of plate images. These are images where we have read a plate. May be used simultaneously with video if you want. These files will have the prefix P

Platforms	Name	Command	Default Value	Description
All	PreFusion	`ifo set prefusion {value}`	false	When looking at plates, enable or disable looking at the plates prior to processing by the vehicle fusion, instead of after. These plates may be rubbish. If you have no idea what this means you will want it off, it is mainly for debugging.
All	Video	`ifo set video {value}`	false	Enable or disable the output of the video stream. This does not contain every field, just a periodic selection. Enabling this produces a LOT of data. These files will have the prefix V.

- `ifo burst`

  Burst Video. Platforms: All.

  Output a burst of consecutive video fields from the selected camera in the selected format. Will burst for a short while based upon the data rate we can write at. May upset the rest of the camera during the burst, so never do this on a production system. This will work even if the rest of this subsystem is disabled.

JPEG Service (jpegService)

Available on platforms: All

Controls the generation of JPEG images

Platforms	Name	Command	Default Value	Description
All	NASP compliant jpeg patch of 120x60	`jpegService set fixedPatch {value}`	false	Forces the size of the patch to match the requirement in the UK Govenments NASP specification of 120x60 pixels
All	Enable Histogram Stretching	`jpegService set histogramEnable {value}`	true	Set true to enable histogram stretching to improve contrast (recommended).
All	Lower Ignore	`jpegService set lowIgnoreAmount {value}`	300	100 times the percentage of dark pixels excluded from histogram stretching (e.g. 300 = 3%). Only change this value if you are familiar with image processing algorithms or under instruction from PIPS engineers.
All	Maximum Stretch Percentage	`jpegService set maxStretchPercent {value}`	80	Maximum amount to stretch the histogram (1-100%). Only change this value if you are familiar with image processing algorithms or under instruction from PIPS engineers.
All	Minimum Stretch Percentage	`jpegService set minStretchPercent {value}`	40	Minimum amount to stretch the histogram (1-100%). Only change this value if you are familiar with image processing algorithms or under instruction from PIPS engineers.
All	JPEG Target Size	`jpegService set size {value}`	192	Varies the target size of the jpegs, in KB, Patches will be 1/4 of the size
All		`jpegService set targetQuality {value}`	0	
All	Upper Ignore	`jpegService set upIgnoreAmount {value}`	200	100 times the percentage of bright pixels excluded from histogram stretching (e.g. 200 = 2%). Only change this value if you are

Platforms	Name	Command	Default Value	Description
				familiar with image processing algorithms or under instruction from PIPS engineers.

- `jpegService qualities`

  Display qualities. Platforms: All.

  Display the controller selected quality for each channel (or each exposure sequence of each channel) and for patches.

JTMS - Journey Time Measurement System (jtms)

Available on platforms: All

A system for delivering numberplates using very low bandwidth specifically for journey time measurement. Only minimal information is transmitted by the system. To use JTMS you must give your camera a 4 digit numerical hostname, which will be its site ID. This module only supplies tags, you should look at the diagnostics module to enable diagnostics and exceptions in jtms compatible format.

Platforms	Name	Command	Default Value	Description
All	Tag format	`jtms set binary` {*value*}	1	The format of the tag messages. 0 - human readable text messages. 1 - binary messages (more compact). 2 - Extended binary format with state/country, classification, confidence and 24 bit hashed tags.
All	Enabled	`jtms set enabled` {*value*}	false	Allows the JTMS system to be enabled and disabled. Disable it unless you are using it.
All	Host	`jtms set host` {*value*}	192.168.1.1	The IP address of the instation which will receive the JTMS data.
All	Merge Characters	`jtms set mergechars` {*value*}	true	Enable merging of possible ambiguous characters such as 8 and B prior to transmission
All	Maximum Files	`jtms set nlog` {*value*}	6	The maximum number of files which will be stored on the local filesystem before they are overwritten if it is not possible to contact the instation. Warning, arbitrarily setting this to a high value may fill up the device on which you are storing the files and then the system will lose the wrong data or may perform badly.
All	Tag Period	`jtms set period` {*value*}	5	The number of minutes between sending tag messages
All	Time Slot	`jtms set time_slot` {*value*}	0	Time slot which is used by this system for transmission. Use this to spread the network load of your outstations. This is a percentage value and is used as an offset from the beginning of the time which could be used for transmission verses the end of that transmission slot - e.g. 0 it will transmit at the very beginning of the slot, at 100 at the very end.
All	ACK Timeout	`jtms set timeout` {*value*}	60	Number of seconds to wait for an ACK (if ACKs are enabled). Set to zero to disable

- `jtms reset`

Reset statistics. Platforms: All.

Reset the statistics for this module

- `jtms statistics`

  Statistics. Platforms: All.

  Display statistics from this module

External Led Control (ledControl)

Available on platforms: All

Setting to Control the pips illuminator

Platforms	Name	Command	Default Value	Description
All	Length of flash in microseconds	`ledControl set flashTime` {*value*}	1000	Sets the length of the flash in microseconds
All	Enable internal Led's	`ledControl set internalEnable` {*value*}	true	Set this to false to disable the internal LED's
All	Set mode of external Led's	`ledControl set mode` {*value*}	0	Mode 0 = Off, Mode 1 = Synced to Cam1(triple sequence), Mode 2 = Synced to Cam2, Mode 3 = Fixed Length

Metadata store (metadata)

Available on platforms: All

This is an object for storing site metadata as string values. The information stored in here is NOT used by the system, and is just for you to use when creating format strings. The data will be output in the format strings unchanged, and allows you to put per-site data in here, keeping the format strings the same on all sites. You might wish to store lane IDs, zones, site direction or anything else similar in here. We would recommend setting the hostname as the unique site identifer which may be accessed though %Sh. It also provides a way of mapping from long event metadata into short codes for output with the %E* variables. You enter into map_a the long name of the variable you'd like available as %Ea. This part is probably not useful to you at the moment unless you understand this without further explanation.

Platforms	Name	Command	Default Value	Description
All	Mapping a	`metadata set map_a` {*value*}		Name of an event metadata string you'd like visible in %Ea.
All	Mapping b	`metadata set map_b` {*value*}		Name of an event metadata string you'd like visible in %Eb.
All	Mapping c	`metadata set map_c` {*value*}		Name of an event metadata string you'd like visible in %Ec.
All	Mapping d	`metadata set map_d` {*value*}		Name of an event metadata string you'd like visible in %Ed.
All	Mapping e	`metadata set map_e` {*value*}		Name of an event metadata string you'd like visible in %Ee.
All	Mapping f	`metadata set map_f` {*value*}		Name of an event metadata string you'd like visible in %Ef.
All	Mapping g	`metadata set map_g` {*value*}		Name of an event metadata string you'd like visible in %Eg.

Platforms	Name	Command	Default Value	Description
All	Mapping h	`metadata set map_h {value}`		Name of an event metadata string you'd like visible in %Eh.
All	Mapping i	`metadata set map_i {value}`		Name of an event metadata string you'd like visible in %Ei.
All	Mapping j	`metadata set map_j {value}`		Name of an event metadata string you'd like visible in %Ej.
All	Mapping k	`metadata set map_k {value}`		Name of an event metadata string you'd like visible in %Ek.
All	Mapping l	`metadata set map_l {value}`		Name of an event metadata string you'd like visible in %El.
All	Mapping m	`metadata set map_m {value}`		Name of an event metadata string you'd like visible in %Em.
All	Mapping n	`metadata set map_n {value}`		Name of an event metadata string you'd like visible in %En.
All	Mapping o	`metadata set map_o {value}`		Name of an event metadata string you'd like visible in %Eo.
All	Mapping p	`metadata set map_p {value}`		Name of an event metadata string you'd like visible in %Ep.
All	Mapping q	`metadata set map_q {value}`		Name of an event metadata string you'd like visible in %Eq.
All	Mapping r	`metadata set map_r {value}`		Name of an event metadata string you'd like visible in %Er.
All	Mapping s	`metadata set map_s {value}`		Name of an event metadata string you'd like visible in %Es.
All	Mapping t	`metadata set map_t {value}`		Name of an event metadata string you'd like visible in %Et.
All	Mapping u	`metadata set map_u {value}`		Name of an event metadata string you'd like visible in %Eu.
All	Mapping v	`metadata set map_v {value}`		Name of an event metadata string you'd like visible in %Ev.
All	Mapping w	`metadata set map_w {value}`		Name of an event metadata string you'd like visible in %Ew.
All	Mapping x	`metadata set map_x {value}`		Name of an event metadata string you'd like visible in %Ex.
All	Mapping y	`metadata set map_y {value}`		Name of an event metadata string you'd like visible in %Ey.
All	Mapping z	`metadata set map_z {value}`		Name of an event metadata string you'd like visible in %Ez.
All	String a	`metadata set string_a {value}`		A string, access in format strings as %Ma.
All	String b	`metadata set string_b {value}`		A string, access in format strings as %Mb.
All	String c	`metadata set string_c {value}`		A string, access in format strings as %Mc.
All	String d	`metadata set string_d {value}`		A string, access in format strings as %Md.

Platforms	Name	Command	Default Value	Description
All	String e	`metadata set string_e {value}`		A string, access in format strings as %Me.
All	String f	`metadata set string_f {value}`		A string, access in format strings as %Mf.
All	String g	`metadata set string_g {value}`		A string, access in format strings as %Mg.
All	String h	`metadata set string_h {value}`		A string, access in format strings as %Mh.
All	String i	`metadata set string_i {value}`		A string, access in format strings as %Mi.
All	String j	`metadata set string_j {value}`		A string, access in format strings as %Mj.
All	String k	`metadata set string_k {value}`		A string, access in format strings as %Mk.
All	String l	`metadata set string_l {value}`		A string, access in format strings as %Ml.
All	String m	`metadata set string_m {value}`		A string, access in format strings as %Mm.
All	String n	`metadata set string_n {value}`		A string, access in format strings as %Mn.
All	String o	`metadata set string_o {value}`		A string, access in format strings as %Mo.
All	String p	`metadata set string_p {value}`		A string, access in format strings as %Mp.
All	String q	`metadata set string_q {value}`		A string, access in format strings as %Mq.
All	String r	`metadata set string_r {value}`		A string, access in format strings as %Mr.
All	String s	`metadata set string_s {value}`		A string, access in format strings as %Ms.
All	String t	`metadata set string_t {value}`		A string, access in format strings as %Mt.
All	String u	`metadata set string_u {value}`		A string, access in format strings as %Mu.
All	String v	`metadata set string_v {value}`		A string, access in format strings as %Mv.
All	String w	`metadata set string_w {value}`		A string, access in format strings as %Mw.
All	String x	`metadata set string_x {value}`		A string, access in format strings as %Mx.
All	String y	`metadata set string_y {value}`		A string, access in format strings as %My.

Platforms	Name	Command	Default Value	Description
All	String z	`metadata set string_z {value}`		A string, access in format strings as %Mz.

OEM Modules (modules)

Available on platforms: All

Allows the specification of the supported OEM module types

Platforms	Name	Command	Default Value	Description
All	Number of ACS	`modules set num_acs {value}`	1	Number of ACS modules. Any change will require a restart to take effect. Set to 0 if you dont need ACS. If set to 1, will be called simply acs. If>1 will be called acs1, acs2 etc.
All	Number of BOF 2	`modules set num_bof2 {value}`	0	Number of BOF 2.2 Delivery modules. Any change will require a restart to take effect. Set to 0 if you dont need the Relay Output. Otherwise set to 1. Only a single Relay Output module is allowed.
All	Number of JTMS	`modules set num_jtms {value}`	1	Number of JTMS modules. Any change will require a restart to take effect. Set to 0 if you dont need JTMS. Otherwise set to 1. Only a single JTMS module allowed. .
All	Number of Relay Output	`modules set num_relayOut {value}`	0	Number of Relay Output modules. Any change will require a restart to take effect. Set to 0 if you dont need the Relay Output. Otherwise set to 1. Only a single Relay Output module is allowed.
All	Number of SAP	`modules set num_sap {value}`	0	Number of SAP modules. Any change will require a restart to take effect. Set to 0 if you dont need SAP. Otherwise set to 1. Only a single sap module allowed.
All	Number of UTMC	`modules set num_utmc {value}`	0	Number of UTMC modules. Any change will require a restart to take effect. Set to 0 if you dont need UTMC.

Platforms	Name	Command	Default Value	Description
				Otherwise set to 1. Only a single UTMC module allowed.
All	Number of UTMCV12	`modules set num_utmcv12 {value}`	0	Number of UTMC Version 1.2 modules. Any change will require a restart to take effect. Set to 0 if you dont need UTMC Version 1.2. Otherwise set to 1. Only a single UTMC Version 1.2 module allowed.
All	Number of VES	`modules set num_ves {value}`	1	Number of VES modules. Any change will require a restart to take effect. Set to 0 if you dont need VES. Otherwise set to 1. Only a single ves module allowed.

Network user interface manager (netuis)

Available on platforms: All

The manager for the network user interfaces. These are the interfaces which the web and shell connect to.

Platforms	Name	Command	Default Value	Description
All	To enable/disable the generation of exceptions	`netuis set exceptions {value}`	false	If true, will transmit an exception when a control connection is made. Will only count the first control connection and will only clear the condition when there have been no connections for 5 minutes

- `netuis status`

  Current status. Platforms: All.

  Display the status of the NetUI servers, how many are in use.

Network user interface (netuis netui1)

Available on platforms: All

Network user interface instance which communicates with users

Platforms	Name	Command	Default Value	Description
All	Print line/file	`netuis netui1 set lineFilePrint {value}`	true	Print Linenumber and Filename for logging messages
All	Print time	`netuis netui1 set timePrint {value}`	true	Print time for logging messages
All	Disconnect timeout	`netuis netui1 set timeout {value}`	300	Disconnect timeout in seconds, for when the interface is inactive

NTP Monitor (ntpMonitor)

Available on platforms: All

Monitors NTP status and generates exceptions if any issues detected.

Platforms	Name	Command	Default Value	Description
All	Allowed missed polls	`ntpMonitor set allowed_missed_polls {value}`	8	Number of allowed consecutive missed polls of NTP server before an exception is flagged. The NTP daemon itself flags after 8 missed polls, so that will always generate an exception. However, 8 polls may take quite some time to complete (hours). While system time should be stable and accurate during this period, some might prefer to know sooner if the NTP server has not been reached. This value is also for consecutive missed polls. Set this to between 0 and 8.

Licence options (options)

Available on platforms: All

Management of the licence file

- `options display`

  Display Licence. Platforms: All.

  Display current licence information

- `options load`

  Read Licence file. Platforms: All.

  Load a new licence file from /storage/options.txt, and install's to system licence information

- `options test` {*on_off*}

  Set System in test mode. Platforms: All.

  Enable test mode, allows 100 Reads before marking number plate unreadable

#	Name	Parameter	Description
1	Test Mode	on_off	Test mode enable / disable

Patch Overlay Control (patchoverlay)

Available on platforms: All

Specify whether the plateread patch has an overlay, and what its contents should be.

Platforms	Name	Command	Default Value	Description
All	Overlay Text Enable	`patchoverlay set enabled` {*value*}	false	Enables additional text on the Image
All	Text	`patchoverlay set text` {*value*}		The format string for the overlayed text. This has limitations

Platforms	Name	Command	Default Value	Description
			%Iy04d/%Io02d/%Id02d_%Ih02d:%Im02d:%Is02d\n%Shs_%Pps_%Pc02d	

PCI Camera Source (pciSource)

Available on platforms: All

The internal camera subsystem, connected via PCI to the processor. These controls are mostly for diagnostics.

- `pciSource clear`

  Reset interrupt latency statistics. Platforms: All.

  Reset counts of interrupts from the PCI camera.

- `pciSource irbufs`

  Dump IR Bufs in use. Platforms: All.

  Dump IR Bufs in use

- `pciSource latency`

  Display interrupt latency statistics. Platforms: All.

  Display details and counts of interrupts from the PCI camera.

PIXI Contexts (pixicontexts)

Available on platforms: All

Manages PIXI contexts

- `pixicontexts list`

  List PIXI Contexts. Platforms: All.

  List existing PIXI persistent LIFOS as well as their lengths.

Power Manager (power)

Available on platforms: All

Power Management subsystem, monitoring the power coming into the system and dealing with power down when the power is cut.

Relay Out (relayOut)

Available on platforms: All

Controls the relay according to plate read events

Platforms	Name	Command	Default Value	Description
All	Relay Action	`relayOut set action {value}`	close	

Platforms	Name	Command	Default Value	Description
All	Enabled	`relayOut set enabled` {*value*}	false	
All	Relay Pulse Period	`relayOut set period` {*value*}	250	
All	Tag Match Regular Expression	`relayOut set tag_regex` {*value*}	.*	

SAP - Serial Application Port (sap)

Available on platforms: All

Simple serial port output

Platforms	Name	Command	Default Value	Description
All	Serial Baud Rate	`sap set baud` {*value*}	9600	The serial port baud rate. For changes to take effect, disable then re-enable. Valid values 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400
All	Enabled	`sap set enabled` {*value*}	false	Allows the SAP system to be enabled and disabled. Disable it unless you are using it.
All	Message contents	`sap set msg_contents` {*value*}	%Pps\n	A format string specifying the message content. The default gives you the plate-read text followed by newline.

Vehicle Image Selector (selector)

Available on platforms: All

Selects images from the hardware platefinder for further analysis and ANPR by the rest of the software.

Platforms	Name	Command	Default Value	Description
All	Previous trigger frame	`selector set pre_trigger_frame` {*value*}	true	Allow the camera to select the frame before the trigger was recieved if it has a lower time proximity to the trigger than the event after
All	Selector queue length	`selector set queueLength` {*value*}	5	Do not chnge this without good reason. By Changing the length of the queue it may change the latency to delivery, but is very likely to affect the read rate
All	Trigger Overview	`selector set triggerOview` {*value*}	false	If this is set *when triggered* the overview will be coincident with the trigger start. If this is not set or the vehicle was not triggered then the overview image will be taken at the same time as the IR image.
All	Triggers Only	`selector set triggersOnly` {*value*}	false	If this is set we will only detect vehicles during the trigger period, otherwise we'll auto detect

Platforms	Name	Command	Default Value	Description
				vehicles all the time but explicitly pass them on when triggered

- `selector statistics`

  Cumulative statistics. Platforms: All.

  Provides cumulative statistics of longterm vehicle processing

Hardware Monitoring sensors (sensors)

Available on platforms: All

This module periodically polls the sensor values

- `sensors dump`

  Dump Current readings. Platforms: All.

  Displays the current readings of the sensors

Console Logger (stdout)

Available on platforms: All

The logger which reports information to the standard out (stdout) device (usually the console). This is probably of no use to you as you probably aren't looking at it.

Platforms	Name	Command	Default Value	Description
All	Print line/file	`stdout set lineFilePrint {`*`value`*`}`	true	Print Linenumber and Filename for logging messages
All	Print time	`stdout set timePrint {`*`value`*`}`	true	Print time for logging messages

System Details (system)

Available on platforms: All

An object for collecting lists of system details and objects.

Platforms	Name	Command	Default Value	Description
All	P392 Bracket Location	`system set bracketBottom {`*`value`*`}`	true	P392 mounted with bracket at the bottom is true otherwise the variable should be false
All	COM2 serial use	`system set com2 {`*`value`*`}`	disabled	This settings determines what the com2 second user available serial port is used for. Options are: 'trig_serial' - generic serial triggering with regex matching and variable baud rate. 'sap' - Serial text output of vehicle plateread events. 'vestrigger' - 19.2k STX delimited trigger messages for VES.

Platforms	Name	Command	Default Value	Description
				'gps' - GPS unit talking NMEA at 4.8k. 'disabled' - not in use.
All	Coordinates Valid	`system set coord_valid {value}`	false	A flag indicating whether these coordinates are valid or not
All	East (not West)	`system set east {value}`	true	Flag indicating whether the longitude value is East or West. 1->East, 0->West
All	North Degrees	`system set latitude {value}`	0	This is the latitude coordinate of this camera, and this is the degree portion of the coordinate. If you have a GPS system attached and working this will be automatically updated everytime we have a lock, otherwise it is manually enterable.
All	North Microdegrees	`system set latitude_micro {value}`	0	This is the latitude coordinate of this camera, and this is the microdegree portion of the coordinate. If you have a GPS system attached and working this will be automatically updated everytime we have a lock, otherwise it is manually enterable.
All	East Degrees	`system set longitude {value}`	0	This is the longitude coordinate of this camera, and this is the degree portion of the coordinate. If you have a GPS system attached and working this will be automatically updated everytime we have a lock, otherwise it is manually enterable.
All	East Microdegrees	`system set longitude_micro {value}`	0	This is the longitude coordinate of this camera, and this is the microdegree portion of the coordinate. If you have a GPS system attached and working this will be automatically updated everytime we have a lock, otherwise it is manually enterable.
All	North (not south)	`system set north {value}`	true	Flag indicating whether the latitude value is North or South. 1->North, 0->South
All	Relay output use	`system set relay {value}`	disabled	This setting determines what the relay input is used for. Options are: 'gpspower' - for use in switching on and off a gps unit (only usable with the serial port com2 also connected to the gps). 'disabled' - not in use.
All	Trigger input use	`system set trigger {value}`	disabled	This setting determines what the trigger input is used for. Options are: 'hwtrigger' - for a triggering vehicles detection. 'gpspps' - for the pulse per second signal from a gps unit (only useable with the serial port com2 also connected to the gps). 'exception' - generate exceptions when the line changes state. 'script' - run a user script on line state change. 'anpr_enable' - only perform anpr when trigger input circiut is completed. 'disabled' - not in use.

- `system crc`

  Display CRCs. Platforms: All.

Display CRCs of the system and configuration

- `system info`

  Display information. Platforms: All.

  Display general information about this camera. Always useful as a debugging aid.

- `system queues`

  Queues. Platforms: All.

  List all queues and their state

- `system reboot`

  Reboot camera. Platforms: All.

  Reboot the camera now unconditionally.

- `system relay`

  Toggle Relay. Platforms: All.

  Change the state of the relay

- `system relay_close`

  Close Relay. Platforms: All.

  Set the state of the relay to closed

- `system relay_open`

  Open Relay. Platforms: All.

  Set the state of the relay to open.

- `system relay_pulse` {*`closed`*} {*`period`*}

  Pulse Relay. Platforms: All.

  Set the relay to a specified state for a period

#	Name	Parameter	Description
1	Pulse Closed	closed	true to set relay closed, then, after period, open. Otherwise relay will open and, after period, close
2	Pulse Period	period	The relay pulse period in milliseconds

- `system restart`

  Restart application. Platforms: All.

  Attempt to restart the application without rebooting. May reboot camera under some circumstances.

Trigger Control (trig)

Available on platforms: All

External trigger control, for when you have wired an external vehicle detector into the camera. To use this you must set the Vehicle Image Selector filter to triggered rather than auto.

Platforms	Name	Command	Default Value	Description
All	Forward All Payloads	`trig set forward_all_payloads {value}`	false	For an already open gate, subsequent trigger stimuli will be processed for payload (while the gate is open). This will for example allow the hardware trigger to cause the gate to open and a TCP trigger (while the gate is open) could provide the payload. Please note that timing is important. If the payload-providing-trigger is late (arrives after the gate has closed) it will generate a new trigger rather than a payload to a current open trigger. See also the trigger payload format specifiers.
All	Trigger Latency	`trig set latency {value}`	0	Sets configurable delay from electrical signal edge to when we regard the trigger to have occurred.
All	Gate open period	`trig set open_period {value}`	250	Sets period during which we enable image processing for the triggering vehicle.
All	Appends the trigger id to all trigger acknowledgement messages	`trig set reply_with_trigger_id {value}`	false	
All	Simulated trigger period	`trig set simulated_period {value}`	1000	Sets the period between simulated triggers. Not for use in a production system.
All	Simulation Mode	`trig set simulation_mode {value}`	false	Enabling simulation mode causes software triggers to be generated at the rate determined by the simulated period
All	Variable Gate Open Period	`trig set variable_period {value}`	false	For an already open gate, the open period will be extended if further stimulus received (e.g. motion detection, physical trigger, TCP trigger). Under this mechanism the gate will always stay open for a minimum of the configured Gate Open Period and for no longer than 2 seconds.
All	Wait period	`trig set wait_period {value}`	700	Sets period after latency expires before we will accept another trigger. Can be used to prevent noisy triggers causing problems.

- `trig message {msg}`

  Single Simulated Trigger with content. Platforms: All.

Generates a single simulated trigger. Note, this will be generated regardless of whether simulation mode is enabled. It takes an argument which will populate the OEM trigger data field for the vehicle. How you next see this information is dependant upon your output mechanism.

#	Name	Parameter	Description
1	Message Content	msg	The OEM trigger data field.

- `trig oneshot`

  Single Simulated Trigger. Platforms: All.

  Generates a single simulated trigger. Note, this will be generated regardless of whether simulation mode is enabled.

- `trig statistics`

  Cumulative statistics. Platforms: All.

  Provides cumulative statistics of longterm trigger processing

Hardware Trigger (trig hw)

Available on platforms: All

This module manages the external trigger input on the rear of the camera. You must connect this up to a 12V external trigger input such as a loop or other vehicle detector for this to be of any use. To use this you must assign the trigger to be 'hwtrigger' in the system parameters.

Platforms	Name	Command	Default Value	Description
All	Debounce time	`trig hw set debounce {value}`	1	Number of milliseconds for which a trigger has to be stable before it is accepted by the system. Increasing this will remove false short triggers from the system at the expense of the same amount of latency in the trigger. It could also miss triggers if your trigger system produces very short pulses and you set it too high. This debounce parameter is applied for all uses of the trigger input, including scripts and exceptions.
All	Falling Edge	`trig hw set falling_edge {value}`	false	This chooses which edge of the signal will be used to trigger on, if unselected you will trigger on the rising edge of the signal. You will need to refer to the manual for your trigger source to determine which it produces when a vehicle enters the field of view.

- `trig hw clearcount`

  Clear Hardware trigger count. Platforms: All.

  Resets the count of number of hardware triggers recorded to 0

- `trig hw count`

  Hardware trigger count. Platforms: All.

Provides a count of number of hardware triggers recorded

- `trig hw status`

  Current trigger status. Platforms: All.

  Gets the current status of the trigger input signal

Serial Trigger (trig serial)

Available on platforms: All

This module manages Serial Triggers. These may be sent into com2.

Platforms	Name	Command	Default Value	Description
All	Acknowledge	`trig serial set ack_enabled` {*value*}	true	To enable/disable the generation of acks. If enabled the whole message as sent will be echoed back to you.
All	Serial Baud Rate	`trig serial set baud` {*value*}	115200	The serial port baud rate. For changes to take effect, disable then re-enable. Valid values 2400, 4800, 9600, 19200, 38400, 57600, 115200, 230400
All	Serial triggers enabled	`trig serial set enabled` {*value*}	false	If true, will detect and propogate triggers from com2.
All	Heartbeat Regular Expression	`trig serial set heartbeat_regex` {*value*}	disabled	If the string arriving on the trigger port matches this regex, it will NOT generate a trigger, it will simply echo the pattern back exactly as received. Notes: To disable it, set it to the string disabled. Heartbeat will work regardless of the ack_enabled setting
All	Trigger Regular Expression	`trig serial set trig_regex` {*value*}	(.*)\n	A regular expression (matching the Perl Regular Expression Syntax) that the incoming string must match in order for a trigger to be generated. The trigger payload will be the concatination of those parts of the incoming string that match any subexpressions in the regex, as specified by ()'s. If no ()'s are present in the trig_regex, then the entire incoming string, that matches the regex, will be used as the trigger payload. Note: A trigger payload may only contain XML legal ASCII. If it contains any illegal characters, no trigger will be generated.

TCP Trigger (trig tcp)

Available on platforms: All

This module manages TCP Triggers. These are sent in to a server socket on port 3820.

Platforms	Name	Command	Default Value	Description
All	Acknowledge	`trig tcp set ack_enabled {value}`	true	To enable/disable the generation of acks. If enabled the whole message, exactly as sent, will be echoed back to you.
All	TCP triggers enabled	`trig tcp set enabled {value}`	true	If true, will detect and propogate TCP Socket triggers.
All	Heartbeat Regular Expression	`trig tcp set heartbeat_regex {value}`	disabled	If the string arriving on the trigger port matches this regex, it will NOT generate a trigger, it will simply echo the pattern back exactly as received. Notes: To disable it, set it to the string disabled. Heartbeat will work regardless of the ack_enabled setting
All	Trigger Regular Expression	`trig tcp set trig_regex {value}`	(.*)\n	A regular expression (matching the Perl Regular Expression Syntax) that the incoming string must match in order for a trigger to be generated. The trigger payload will be the concatination of those parts of the incoming string that match any subexpressions in the regex, as specified by ()'s. If no ()'s are present in the trig_regex, then the entire incoming string, that matches the regex, will be used as the trigger payload. Note: A trigger payload may only contain XML legal ASCII. If it contains any illegal characters, no trigger will be generated.

Trigger Script (trigScript)

Available on platforms: All

This module will run a unix binary when the trigger input changes state. You must connect this up to an external trigger input for this to be of any use. To use this modules you must assign the trigger to 'script' in the system parameters. Note, each script must finish running before we will run the next script if the scripts take time to execute and the trigger makes fast transitions. The use of this feature is obviously unsupportable as you can cause anything to run which could cause the system to become unstable. It is suggested you get your script verified by PIPS if you do require support. These scripts will run a maximum of once every 5 seconds.

Platforms	Name	Command	Default Value	Description
All	Falling Edge	`trigScript set falling {value}`		This is the full path to a binary (usually a unix shell script) will be run on the falling edge of the trigger. If this is left blank or an invalid binary nothing will happen. This script will be run at bootup if the trigger input is low at bootup.

Platforms	Name	Command	Default Value	Description
All	Rising Edge	`trigScript set rising {value}`		This is the full path to a binary (usually a unix shell script) will be run on the rising edge of the trigger. If this is left blank or an invalid binary nothing will happen. This script will be run at bootup if the trigger input is high at bootup.

UTMC Delivery Module (utmc)

Available on platforms: All

The UTMC module is a delivery module which sends vehicle event data to an external computer (instation) using the UTMC protocol.

Platforms	Name	Command	Default Value	Description
All	Authenticate using username and password	`utmc set authenticate {value}`	false	authenticate
All	UTMC Camera ID	`utmc set cameraID {value}`	0	The UTMC camera ID
All	Minimum Samples for Diagnostics	`utmc set diagnostic_min_samples {value}`	10	Certain types of diagnostics (e.g. mean values or ratios) are only considered valid after a certain number of samples.
All	Diagnostic period	`utmc set diagnostic_period {value}`	20	Period in minutes between diagnostic updates
All	Diagnostics and Exceptions Enabled	`utmc set diagnostics_exceptions_enabled {value}`	false	Send diagnostics and exceptions.
All	Timeout (in seconds) for DNS caching	`utmc set dnsCacheTimeout {value}`	60	Selectable option to change the timeout used by the DNS cache within libCURL. 60 to maintain backwards compatability, or 0 to completely disable DNS caching.
All	Enabled	`utmc set enabled {value}`	false	Allows the UTMC system to be enabled and disabled. Disable it unless you are using it.
All	Minimum Samples for Exceptions	`utmc set exception_min_samples {value}`	20	Certain types of exceptions (e.g. mean values or ratios) are only considered valid after a certain number of samples.
All	Exception Period	`utmc set exception_period {value}`	5	Period in minutes between (non-realtime) exception updates
All	Host	`utmc set host {value}`	192.168.1.1:8080	IP address and port of the instation which will receive the UTMC data.
All	Maximum number of vehicles in a batch	`utmc set maxBatchSize {value}`	100	The Maximum number of vehicles that can be in a batch, if the number of vehicles becomes larger than this number we will send out a batch
All	Merge Characters	`utmc set mergechars {value}`	true	

Platforms	Name	Command	Default Value	Description
				Enable merging of possible ambiguous characters such as 8 and B prior to transmission (for tags only)
All	Maximum Files	`utmc set nlog {value}`	100	The maximum number of files which will be stored on the local drive if it is not possible to contact the instation. Once this number has been stored, the oldest will be overwritten. Warning, arbitrarily setting this to a high value may fill up the device on which you are storing the files and then the system will lose the wrong data or perform badly (or not at all).
All	Password for transport	`utmc set password {value}`		Password
All	Path	`utmc set path {value}`	utmc	The path on the http url.
All	Tag Period	`utmc set period {value}`	5	The number of minutes between sending tag messages
All	Send Tag	`utmc set sendTag {value}`	true	Send hashed plates
All	Send VRN	`utmc set sendVRN {value}`	false	Send raw plates (VRNs)
All	Time Slot	`utmc set time_slot {value}`	0	Time slot which is used by this system for transmission. Use this to spread the network load of your outstations. This is a percentage value and is used as an offset from the beginning of the time which could be used for transmission verses the end of that transmission slot - e.g. 0 it will transmit at the very beginning of the slot, at 100 at the very end.
All	ACK Timeout	`utmc set timeout {value}`	60	Number of seconds to wait for an ACK (if ACKs are enabled). Set to zero to disable
All	UTMC transport	`utmc set transport {value}`	HTTP	HTTP or HTTPS
All	Use Gzip	`utmc set useGzip {value}`	true	Encode with gzip to save bandwidth
All	Use SOAP	`utmc set useSOAP {value}`	true	Wrap with SOAP envelope
All	Username for transport	`utmc set username {value}`		Username

- `utmc clearstats`

  Clear statistics. Platforms: All.

  Reset the statistics for this module

- `utmc stats`

  Statistics. Platforms: All.

Display statistics from this module

UTMC V1.2 Delivery Module (utmcv12)

Available on platforms: All

The UTMC module is a delivery module which sends vehicle event data to an external computer (instation) using version 1.2 of the UTMC protocol.

Platforms	Name	Command	Default Value	Description
All	Authenticate using username and password	`utmcv12 set authenticate {value}`	false	authenticate
All	UTMCV1_2 Camera ID	`utmcv12 set cameraID {value}`	0	The UTMCV1_2 camera ID
All	Timeout (in seconds) for DNS caching	`utmcv12 set dnsCacheTimeout {value}`	60	Selectable option to change the timeout used by the DNS cache within libCURL. 60 to maintain backwards compatability, or 0 to completely disable DNS caching.
All	Enabled	`utmcv12 set enabled {value}`	false	Allows the UTMCV1_2 system to be enabled and disabled. Disable it unless you are using it.
All	Host	`utmcv12 set host {value}`	192.168.1.1:8080	The IP address and port of the instation which will receive the UTMCV1_2 data.
All	Merge Characters	`utmcv12 set mergechars {value}`	true	Enable merging of possible ambiguous characters such as 8 and B prior to transmission (for tags only)
All	Maximum Files	`utmcv12 set nlog {value}`	100	The maximum number of files which will be stored on the local drive if it is not possible to contact the instation. Once this number has been stored, the oldest will be overwritten. Warning, arbitrarily setting this to a high value may fill up the device on which you are storing the files and then the system will lose the wrong data or perform badly (or not at all).
All	Password for transport	`utmcv12 set password {value}`		Password
All	Path	`utmcv12 set path {value}`	utmc	The path on the http url.
All	Send ANPR Image	`utmcv12 set sendANPRImage {value}`	true	Send the ANPR Image (the image used for the ANPR.)
All	Send Asynchronous Payload	`utmcv12 set sendAsyncPayload {value}`	false	Manufacturer Specific. Will send the asynchrounous payload within the UTMC ManufacturerSpecific area.
All	Send Overview Image	`utmcv12 set sendOverviewImage {value}`	true	Send the overview image
All	Send Plate Patch Image	`utmcv12 set sendPlatePatch {value}`	true	Send patch Image

Platforms	Name	Command	Default Value	Description
All	Send Tag	`utmcv12 set sendTag {value}`	false	Send hashed plates
All	Send VRN	`utmcv12 set sendVRN {value}`	true	Send raw plates (VRNs)
All	ACK Timeout	`utmcv12 set timeout {value}`	60	Number of seconds to wait for an ACK (if ACKs are enabled). Set to zero to disable
All	UTMCV1_2 transport	`utmcv12 set transport {value}`	HTTP	HTTP or HTTPS
All	Use Gzip	`utmcv12 set useGzip {value}`	true	Encode with gzip to save bandwidth
All	Use SOAP	`utmcv12 set useSOAP {value}`	true	Wrap with SOAP envelope
All	Username for transport	`utmcv12 set username {value}`		Username
All	Async. Payload is XML	`utmcv12 set xmlPayload {value}`	false	Manufacturer Specific. The async payload contains further XML tags within the ManufacturerSpecific area.

- `utmcv12 clearstats`

  Clear statistics. Platforms: All.

  Reset the statistics for this module

- `utmcv12 stats`

  Statistics. Platforms: All.

  Display statistics from this module

VES - Violation Enforcement System (ves)

Available on platforms: All

Highly configurable system with many options. Please refer to VES Software Interface Specification

Platforms	Name	Command	Default Value	Description
All	Enable Ack	`ves set ack_enable {value}`	0	When set require ack from instation on summary and/or evidential records. Retry on ack failure. 0x01 - ack required on evidential records (ERs) 0x02 - ack required on individual summary records (SRs) 0x04 - ack required on diagnostics 0x08 - ack required on exceptions 0x10 - ack required when transferring a record from spikestore to instation

Platforms	Name	Command	Default Value	Description
				0x20 - ack required on batched summary records (BSRs)
All	Retry attempts	`ves set ack_retry {value}`	3	Retry transfers this many times before giving up
All	ack timeout	`ves set ack_timeout {value}`	500	Time to wait for an ack (mS). This timeout is used for longg transfer events. Specifically full ERs. On a system connected by hi speed links, system overhead may dominate so this and the short timeout may be identical. Where comms is slow, a separate timeout is beneficial.
All	Alternate Host	`ves set alt_host {value}`	10.1.1.1	Sets the IP address of the alternate instation.
All	Enforcement area	`ves set area {value}`	WEZ	The name of the enforcement zone. This is expected to be a three character field. However up to seven characters are accepted.
All	batched SR interval	`ves set bsr_interval {value}`	300	Interval (seconds) over which SRs are accumulated to build a batch. If no data is collected during the interval, then no batch is generated. The current batch is skipped.
All	batched SR max batches	`ves set bsr_nlog {value}`	12	Maximum number of historic SR batches which may be stored on the camera. When this number is exceeded the oldest batch will be overwritten.
All	batched SR port	`ves set bsr_port {value}`	10007	Port for transfer of batched SRs. This may be the same port as used by standard SRs.
All	Cabinet controller	`ves set cabinet {value}`		Sets the IP address the cabinet controller if present. Used to monitor the cabling and link to detect intrusions or failures.
All	cf age limit	`ves set cf_age_limit {value}`	48	Maximum time (hours) an evidential record may be retained on camera. Records older than this will be deleted.
All	No. of context images	`ves set context_count {value}`	2	Specify the number of supporting context images which must be captured. The permissable range is 0-8. The number must be even. If an odd number is entered, it will be interpreted as the next lower even number.
All	Context image offset	`ves set context_offset {value}`	250	Specify the approximate interval (mS) between context images.
All	Context image order	`ves set context_order {value}`	0	Specify whether context images are split equally before/after the event, all before the event or all after the event.
All	Country Code standard	`ves set country_code {value}`	0	Determines the standard used for country codes. 0 - PIPS ANPR Standard

Platforms	Name	Command	Default Value	Description
				2 - ISO 3166-1 Alpha 2 3 - ISO 3166-1 Alpha 3
All	D&E debug	`ves set de_debug {value}`	0	set debug flags for diagnostic and exceptions module
All	D&E Ping wait time	`ves set de_ping_wait {value}`	15000	Applicable to diagnistics & exceptions only. Amount of time the system should wait for a ping acknowledge message before giving up. The system usually pings the instation before connecting to it. Set to zero to disable these pre-transmission pings.
All	VES Debug	`ves set debug {value}`	0	Bit field specifying which code modules genetate debug information 0x00000001 - main VES process 0x00000002 - summary record transmission 0x00000004 - image (blob) record transmission 0x00000008 - session & initial key exchange 0x00000010 - message port 0x00000020 - heartbeat system 0x00000040 - DSRC trigger system 0x00000080 - NVT control port 0x00000100 - PING events 0x00000200 - show ping replies 0x00000400 - transmission of records from file buffer 0x00000800 - local file index management 0x00001000 - blob generation 0x00002000 - system timing 0x00004000 - match slots 0x00008000 - data cleanup 0x00010000 - encryption 0x00020000 - key exchange 0x00040000 - diagnostics

Platforms	Name	Command	Default Value	Description
				0x00080000 - oem specific 0x00100000 - oem specific 0x00200000 - context capture 0x00400000 - pull archtecture 0x00800000 - image synchronisation 0x01000000 - radar interface 0x02000000 - trajectory computations 0x04000000 - spikestore interface 0x08000000 - batch summary records 0x10000000 - clock drifts 0x20000000 - audit trail 0x40000000 - oem data record
All	Local Directory	`ves set directory {value}`	/ves	Directory where diagnostic and exception files will be created and stored locally on the system before transfer to the host.
All	VES Enabled	`ves set enabled {value}`	false	Enables/Disables VES. If enabled is false on camera startup, VES will not load. To get VES to load, set enabled to true and restart the camera. Once VES is loaded the enable flag has the effect of enabling/disabling the flow of events into VES.
All	Max ER file size	`ves set file_size {value}`	256	Size in kbytes to be preallocated for storage of ERs. Also sets the storage allocation on the Compact Flash device. ERs larger than this size will be discarded.
All	Heartbeat Port	`ves set hb_port {value}`	10005	The TCP/IP port number used for heartbeat messages.
All	Heartbeat period	`ves set heart_beat {value}`	0	The period in seconds between heart beat (hb) messages. If set to 0, no heart beat messages will be sent.
All	Host	`ves set host {value}`	10.1.1.1	Sets the IP address of the instation.
All	Image port	`ves set image_port {value}`	10000	port on host server expecting image data
All	Image port (background)	`ves set image_port_b {value}`	10000	port on host server expecting image data from background process. This may - and usually will - be exactly the same port as the foreground process.
All	Image Timeout	`ves set image_timeout {value}`	5	Timeout in seconds after which a camera as marked as having a possible problem
All	Switch overview to monochrome	`ves set jpeg_mono {value}`	0	Set to force overview image to monochrome

Platforms	Name	Command	Default Value	Description
All	Colour image scale factor	`ves set jpeg_scale {value}`	0	Set Colour image jpeg scale factor. Only applies to systems equiped with hardware jpeg accelerator. 0 - not scaled 1 - 360x288 2 - 180x144
All	Colour image file size	`ves set jpeg_size {value}`	22	Set Colour image jpeg file size (kbytes). Default is 22k. Only applies to systems equiped with hardware jpeg accelerator
All	Key Exchange port	`ves set key_port {value}`	10003	port on camera listening for session start and key exchange requests
All	Lane Name	`ves set lane {value}`	1	short machine name for this ANPR system. Format TBD.
All	Link Timeout	`ves set link_timeout {value}`	20	Timeout in seconds after which image or summary ports will be closed when inactive.
All	VES Site Location	`ves set location {value}`	test site description	A site specific location string. If using pipsshell and the string contains spaces, then quote the whole string with "".
All	Event match window	`ves set match_window {value}`	700	Only applicable to externally triggered systems. This window (mS) specifies the maximum time window between a trigger event and the matching image set. Alternatively, this window may be used when other events must be matched to an image event.
All	Enable trigger match	`ves set matched_trig {value}`	0	Set this parameter to configure the system to use lane controller messages 0-subsystem disabled 1-A message triggers the camera. The message is not retained. 2-A message must be assocciated with a plate event. Any plate event without an assocciated message is disgarded 3-A message triggers the camera and is subsequently associated with the plate event

Platforms	Name	Command	Default Value	Description
				Messages may arrive on either designated tcp/ip connection or on the serial port. However note that trigger events received via tcp/ip are subject to latencies beyond the control of the system and may be unusable in many circumstances
All	batched SR max count	`ves set max_batch_size {value}`	100	Maximum number of records in a SR batch. When this number is reached, the batch will be queued for transmission even if the interval has not expired.
All	Message Port	`ves set msg_port {value}`	10004	The TCP/IP port number used for messages.
All	Message Timeout	`ves set msg_timeout {value}`	60	Timeout in seconds after which the message port will be closed when inactive.
All	Camera Name	`ves set name {value}`	lane	short machine name for this ANPR system. Format TBD.
All	Number of Files	`ves set nlog {value}`	200	Number of image files to store on local disk.
All	Not Alive Counter	`ves set not_alive {value}`	10	If the heart beat process is running (heartbeat period>0) then if the heart beat fails to send its message (i.e. unable to establish a connection for this many attempts), then the system will attempt recovery action.
All	NVT control mode	`ves set nvt_mode {value}`	0	set nvt control channel mode
All	NVT port	`ves set nvt_port {value}`	10002	port on camera listening for NVT control connection
All	NVT channel timeout	`ves set nvt_timeout {value}`	5	Timeout in seconds after which the NVT port will be closed when inactive.
All	OEM contents	`ves set oem_contents {value}`	%PTs	A format string specifying how to construct the data you would like in the OEM field. NB: The OEM field is limited to 64 bytes. Excess data will be truncated.
All	Camera Direction	`ves set orientation {value}`	0	Set camera orientation according to cardinal compass point ie N, NW, W etc.
All	Ping Interval	`ves set ping_interval {value}`	300	Number of seconds interval between ping requests. These ping requests are used to establish whether and which server is online.
All	Ping Port	`ves set ping_port {value}`	10010	Selects the port on which UDP pings will be sent.
All	Ping Wait Time	`ves set ping_wait {value}`	100	Number of milliseconds to wait for a response to a ping request. Ping requests are sent before opening a connection to the host system.

Platforms	Name	Command	Default Value	Description
All	Reference image file	`ves set ref_file {value}`	mem:/ dummy.bin	The name of a file containing a set of reference jpeg images used to prepare dummy records.
All	Remote Network Router	`ves set router {value}`		Sets the IP address of the remote network router. May be used to monitor the cabling and link to detect failures.
All	Session control rules	`ves set rules {value}`	0xffff	Set the rules which specify which items will be checked before a session may be started. This may be hard coded in shipping systems but can be set to facilitate testing. Not all rules may apply to all system builds. 0x001 - check time sync 0x002 - check config crc 0x004 - check tamper switch 0x008 - check equipment 0x010 - only set secret from serial port 0x020 - terminate on network hack 0x040 - terminate on multiple password fail 0x080 - terminate on restart 0x100 - terminate on network tamper.
All	Disk Buffer scan interval	`ves set scan_interval {value}`	30	Interval in seconds between scans of disk buffer system to check for any oustanding files to transfer to host
All	ER transfer throttle	`ves set scan_throttle {value}`	500	throttle background transfer of ERs to approximately one record per this many mS. Set to 0 to disable the throttle
All	security level	`ves set security {value}`	3	This setting defines the security level used by the system 0x00 - no security 0x01 - HMAC - ERs will have an HMAC applied but are sent in clear text 0x02 - ERs are encrypted (AES256 with CBC) 0x04 - ERs are transferred with rolling keys 0x80 - Diagnostics and exceptions are encrypted NB: Batched SRs are always encryypted

Platforms	Name	Command	Default Value	Description
All	SER transfer throttle	`ves set ser_throttle {value}`	500	throttle background transfer of SERs to approximately one record per this many mS. Set to 0 to disable the throttle
All	Enable serial trigger	`ves set serial_trig {value}`	0	Set to enable serial trigger input. This will of course only be meaningfull if the hardware has a serial input available.
All	session options	`ves set session_opts {value}`	0	Set the session security level in use 0x00 - No sessions - no session security 0x01 - Sessions enabled, session control must pass CHAP 0x02 - Sessions enabled, session control is encrypted
All	short ack timeout	`ves set short_ack_timeout {value}`	500	Time to wait for an ack (mS) This timeout is used for short events. Specifically SRs SERs. On systems with slows comms benefit is gained by setting this to a more appropriate value.
All	Slot age limit	`ves set slot_age_limit {value}`	30	Maximum time (seconds) an event (summary and/or evidential record) will spend in ram before being transferred to Compact Flash store (or deleted if no CF store in use)
All	Media Source	`ves set source {value}`	NULL	The name of the media source type. This is expected to be a four character field. However up to seven characters are accepted.
All	SPIKEstore Account	`ves set store_account {value}`	vesstore	Username used for transfer of ERs to SPIKEstore.
All	SPIKEstore enable	`ves set store_enable {value}`	0	When a record is deleted from Compact Flash or ram buffers either through a specific delete request or through age expiry, an option exists to transfer the record to SPIKEstore. This store can provide very long term historical storage of records. Set this option to enable transfer to this store. NB: No facility exists to transfer these records to the host system. It is expected that this and any other housekeeping required will be the direct responsibility of the host system.
All	SPIKEstore Host IP	`ves set store_host {value}`	10.1.1.1	Sets the IP address of the SPIKEstore module.

Platforms	Name	Command	Default Value	Description
All	SPIKEstore Password	`ves set store_password {value}`	vesstore	Password used for transfer of ERs to SPIKEstore.
All	SPIKEstore Path	`ves set store_path {value}`		sub path in which files will be created on SPIKEstore server. NB: This path is NOT created on the host system by the camera software. It is assumed to exist. Transfers will fail if this path does not exist. The path, if set, should terminate in / or \ as appropriate for the SPIKEstore system. This path is used as a prefix to directories and files when they are created on the host.
All	Summary port	`ves set summary_port {value}`	10001	port on host server expecting summary data
All	Summary port (background)	`ves set summary_port_b {value}`	10001	port on host server expecting summary data from background process. This may - and usually will - be exactly the same port as the foreground process.
All	summary rate threshold	`ves set summary_rate {value}`	0	Set a control on transfer of summary records based on the outstanding count of evidential records. Set to zero to disable this control. Minimum active value:10 When set, if there are more outstanding ERs than this count, then transfer of summary records from backing store will be suspended. A hysteresis of 10% is applied.
All	Conf threshold	`ves set threshold {value}`	35	When transfer on threshold set, only ANPR reads with a threshold higher than this will be transferred to the host system.
All	Time slot	`ves set time_slot {value}`	0	Time slot which is used by this system for transmission of diagnostics & exceptions. Use this to spread the network load of your outstations. This is a percentage value and is used as an offset from the beginning of the time which could be used for transmission verses the end of that transmission slot - e.g. 0 it will transmit at the very beginning of the slot, at 100 at the very end.
All	Timeout	`ves set timeout {value}`	300	If no plate image is received on a camera for this many seconds, then a bit will be set in the status register. This may indicate a possible system failure e.g. camera fault or may indicate that a lane is closed.
All	Transfer	`ves set transfer {value}`	0x09f7	Bit field specifying which data must be transferred 0x00001 - transfer patch

Platforms	Name	Command	Default Value	Description
				0x00002 - transfer full IR 0x00004 - transfer scene 0x00008 - transfer context images 0x00010 - explicit delete required on PULL protocol 0x00020 - add text to patch & IR images 0x00040 - discard events below threshold 0x00080 - transfer ERs only on request (PULL protocol) 0x00100 - on tx failure buffer data to local disk 0x00200 - send M001 message 0x00400 - send M002 message 0x00800 - send WARNing messages 0x01000 - send ERRor messages 0x02000 - transfer Hearbeat as H001 messag 0x04000 - transfer session state messages 0x08000 - transfer summary records 0x10000 - create short evidential record 0x20000 - transfer batched summary records 0x40000 - Always transfer ERs via CF and background channel
All	TCPIP trigger port	`ves set trig_port {value}`	10006	TCP/IP Port on camera listening trigger messages. The protocol accepted on this port may be OEM specific.

- `ves aes`

  . Platforms: All.

- `ves clear`

  . Platforms: All.

- `ves delete`

  . Platforms: All.

- `ves init`

. Platforms: All.

- `ves list`

  . Platforms: All.

- `ves ping`

  . Platforms: All.

- `ves rebuild`

  . Platforms: All.

- `ves remove`

  . Platforms: All.

- `ves secret`

  . Platforms: All.

- `ves send`

  . Platforms: All.

- `ves statistics`

  VES Statistics. Platforms: All.

- `ves test`

  . Platforms: All.

- `ves trigger`

  . Platforms: All.

Vehicle Event Database (vfeDB)

Available on platforms: All

Platforms	Name	Command	Default Value	Description
All	Enabled	`vfeDB set enabled` {*value*}	false	Enables the storage capability within the vfeDB
All	Maximum Age	`vfeDB set max_age` {*value*}	0	The Maximum age records are allowed to be specified in minutes. Set to 0 for no time restriction
All	Store Analysis Images	`vfeDB set store_analysis_images` {*value*}	true	This parameter is used to control if analysis images are stored
All	Store Context Images	`vfeDB set store_context_images` {*value*}	true	This parameter is used to control if context images are stored
All	Store Overview Images	`vfeDB set store_overview_images` {*value*}	true	This parameter is used to control if overview images are stored

Platforms	Name	Command	Default Value	Description
All	Store Patch Images	`vfeDB set store_patch_images {value}`	true	This parameter is used to control if patch images are stored
All	Store Supplementary Images	`vfeDB set store_supplementary_images {value}`	true	This parameter is used to control if supplementary images are stored

- `vfeDB statistics`

  Cumulative statistics. Platforms: All.

  Provides cumulative statistics

Logging bits

These commands can be used to turn on and off real time messages from the camera about its status. These are implemented for debugging purposes in the main, and may not be meaningful at all. Turning too many of these on may adversely impact the performance of the camera. It is recommended that you use a pipsshell over SSH to watch logging, rather than serial, as the serial port can become overloaded if you turn too many messages on.

Platforms	Command	Description
All	`log acs bufferdisk_append {on/off}`	Appends to buffer disk queue
All	`log acs bufferdisk_remove {on/off}`	Removals from buffer disk queue
All	`log acs disk {on/off}`	Disk interactions
All	`log acs events {on/off}`	ACS events
All	`log acs filenames {on/off}`	Filename details
All	`log acs images {on/off}`	Image aquisition status
All	`log acs inevents {on/off}`	Incoming events
All	`log acs overviews {on/off}`	Overview aquisition status
All	`log acs transfer {on/off}`	Transfer messages
All	`log anpr allreads {on/off}`	Reports all vehicle read events, may be very noisy
All	`log anpr colour {on/off}`	Reports on colour full screen retries
All	`log anpr laneId {on/off}`	Reports information for debugging and varifiying the lane identification system - Only works on supported platforms
All	`log anpr latency {on/off}`	Reports age of departing ImageRecords associated with events
All	`log anpr noreads {on/off}`	Reports vehicle noread events
All	`log anpr patches {on/off}`	Reports on patches and full screen retries
All	`log anpr performance {on/off}`	Reports time taken by AnprLib_run
All	`log anpr reads {on/off}`	Reports vehicle read events
All	`log asyncp incoming {on/off}`	Incoming vehicle events
All	`log asyncp matches {on/off}`	Reports on Matches made between the async payloads and vehicle events. Also reports failures to match
All	`log asyncpStore payloads {on/off}`	Reports payloads added to store
All	`log bof2 incoming {on/off}`	Incoming Events

Platforms	Command	Description
All	`log bof2 messages` {*on/off*}	BOF2.2 Message Log
All	`log bof2 verbose` {*on/off*}	Display error message from the BOF2.2 instation
All	`log cam2exposure brightness` {*on/off*}	Exposure process debugging
All	`log cam2exposure settings` {*on/off*}	Shutter and gain settings debugging
All	`log client connections` {*on/off*}	Connection events
All	`log client latency` {*on/off*}	Reports age of departing ImageRecords associated with events
All	`log client overviews` {*on/off*}	Overview aquisition status
All	`log client vehicles` {*on/off*}	Vehicle events
All	`log dbmatcher incoming` {*on/off*}	Incoming vehicle events
All	`log dbmatcher matches` {*on/off*}	Matches made by the duplicate matcher
All	`log dbmatcher notification` {*on/off*}	Reasons for passing on this image
All	`log diskDB deletes` {*on/off*}	log when an entity is deleted
All	`log exposure brightness` {*on/off*}	Brightness controller actions
All	`log exposure processing` {*on/off*}	Exposure process debugging
All	`log exposure statistics` {*on/off*}	Collect some data for analysis.
All	`log exposure vehicles` {*on/off*}	Number of vehicles checks
All	`log exposure voting` {*on/off*}	Voting by the exposure subsystem on getting brighter or dimmer
All	`log fusion best` {*on/off*}	Choices made by the best plate chooser
All	`log fusion hazard` {*on/off*}	Hazard Processing
All	`log fusion incoming` {*on/off*}	Incoming vehicle events
All	`log fusion latency` {*on/off*}	Latency of events through the system
All	`log fusion matches` {*on/off*}	Matches made by the duplicate matcher
All	`log fusion noread` {*on/off*}	Noread Processing
All	`log fusion notify` {*on/off*}	Reasons for passing on this image
All	`log fusion resetting` {*on/off*}	Resetting a vehicle
All	`log fusion supplementary` {*on/off*}	Supplementary Image Processing
All	`log fusion timers` {*on/off*}	Event timer details
All	`log fusion traj` {*on/off*}	Trajectory of vehicle
All	`log gps controller` {*on/off*}	GPS Controller status reported at poll interval
All	`log gps sentences` {*on/off*}	Echo GPS sentences
All	`log gps time` {*on/off*}	Time Management status reported at poll interval
All	`log heartbeat incoming` {*on/off*}	Incoming vehicle events
All	`log hwtrigger latency` {*on/off*}	Latency of triggers through the system
All	`log ifo outputName` {*on/off*}	Filenames of output
All	`log jpegService performance` {*on/off*}	Performance measurements on the JPEG system
All	`log jpegService retries` {*on/off*}	Report whether we are having to retry JPEG compressions to fit into the buffers
All	`log jpegService type` {*on/off*}	Reports whether JPEG processing is performed in hardware, or software and what type
All	`log jtms connection` {*on/off*}	Connection issues

Platforms	Command	Description
All	`log jtms incoming` {*on/off*}	Incoming events
All	`log jtms messages` {*on/off*}	See outgoing messages, (Text format only)
All	`log jtms outgoing` {*on/off*}	Outgoing events
All	`log jtms timing` {*on/off*}	Timing information
All	`log ntp peers` {*on/off*}	Logs extracted Peers values as stored internally.
All	`log ntp raw` {*on/off*}	Logs raw unparsed data as received from the ntpq script.
All	`log ntp reach` {*on/off*}	Logs NTP reach processing.
All	`log ntp values` {*on/off*}	Logs extracted NTP values.
All	`log pciSource capIR` {*on/off*}	Outputs periodic updates of IR capture count
All	`log pciSource capOview` {*on/off*}	Outputs periodic updates of overview capture count
All	`log pciSource initialisation` {*on/off*}	Initialisation of the cameras
All	`log platefinder groups` {*on/off*}	Groups process debugging
All	`log platefinder hwoutput` {*on/off*}	FPGA output debugging
All	`log platefinder plates` {*on/off*}	Found plates debugging
All	`log platefinder searchgroups` {*on/off*}	Search group debugging
All	`log platewidth processing` {*on/off*}	PlateWidth process debugging
All	`log platewidth samples` {*on/off*}	PlateWidth collected samples debugging
All	`log platewidth shape` {*on/off*}	PlateWidth plate shape debugging
All	`log power state` {*on/off*}	Power state changes
All	`log relayOut incoming` {*on/off*}	Incoming events
All	`log relayOut outgoing` {*on/off*}	Outgoing events
All	`log sap incoming` {*on/off*}	Incoming events
All	`log sap outgoing` {*on/off*}	Outgoing events
All	`log selector detects` {*on/off*}	Reports generated vehicle detect events
All	`log selector indrops` {*on/off*}	Drops on the input queue
All	`log selector latency` {*on/off*}	Reports generated vehicle detect events associated ImageRecord age
All	`log selector multi` {*on/off*}	Show how many vehicles were detected in each image
All	`log selector notify` {*on/off*}	Notification from selector
All	`log selector performance` {*on/off*}	Reports the time taken to do the software portion of platefinding, the tracking algorithm and disposal algorithm
All	`log selector platefinder` {*on/off*}	Platefinder output
All	`log selector queue` {*on/off*}	Show the internal queue adds and deletes
All	`log selector score` {*on/off*}	Show how vehicles are scored and dropped from the internal queue
All	`log selector score_detail` {*on/off*}	Show details on scoring
All	`log selector tracking` {*on/off*}	Show details of the vehicle tracking
All	`log sensors changes` {*on/off*}	Reports changes in sensor values - currently just voltage, but may be extended to temperature etc. in the future

Platforms	Command	Description
All	`log system crcs` {*on/off*}	Reports changes in CRCs
All	`log transport_2acs failure` {*on/off*}	Brief failure details
All	`log transport_2acs items` {*on/off*}	Items being transferred
All	`log transport_2acs verbose` {*on/off*}	Verbose transfer details
All	`log transport_acs failure` {*on/off*}	Brief failure details
All	`log transport_acs items` {*on/off*}	Items being transferred
All	`log transport_acs verbose` {*on/off*}	Verbose transfer details
All	`log transport_bof2 failure` {*on/off*}	Brief failure details
All	`log transport_bof2 items` {*on/off*}	Items being transferred
All	`log transport_bof2 verbose` {*on/off*}	Verbose transfer details
All	`log transport_utmc failure` {*on/off*}	Brief failure details
All	`log transport_utmc items` {*on/off*}	Items being transferred
All	`log transport_utmc verbose` {*on/off*}	Verbose transfer details
All	`log transport_utmcv12 failure` {*on/off*}	Brief failure details
All	`log transport_utmcv12 items` {*on/off*}	Items being transferred
All	`log transport_utmcv12 verbose` {*on/off*}	Verbose transfer details
All	`log trig events` {*on/off*}	Instruments the triggers events
All	`log trig timers` {*on/off*}	Instruments the trigger timers, probably not of much interest
All	`log trigScript script` {*on/off*}	Show the running of scripts.
All	`log utmc connection` {*on/off*}	Connection issues
All	`log utmc incoming` {*on/off*}	Incoming events
All	`log utmc messages` {*on/off*}	See outgoing messages, (Text format only)
All	`log utmc outgoing` {*on/off*}	Outgoing events
All	`log utmc timing` {*on/off*}	Timing information
All	`log vfeDB deletes` {*on/off*}	Log when database records are deleted
All	`log vfeDB incoming` {*on/off*}	Incoming vehicle events
All	`log vfeDB notification` {*on/off*}	Reasons for passing on this image
All	`log vfeDB overviews` {*on/off*}	Log Overview information
All	`log vfeDB retrievals` {*on/off*}	Log when database objects are retrieved
All	`log videoStore fails` {*on/off*}	Retrieval failures
All	`log videoStore requests` {*on/off*}	Retrieval requests
All	`log viewfinder connections` {*on/off*}	Connection events
All	`log viewfinder sessions` {*on/off*}	Session events

Notifications

These commands can be used to turn on and off real time notifications from the camera. These notifications may be seen via pipsshell or via file logging, but the most useful way to use these notifications is via PIXI. To turn the notifications on/off via pipshell, use the command 'notification <source> <type> [on/off]'.

Platforms	Source	Type	Description
All	acs	datasetComplete	Provides notification of the successful transfer of an entire data-set via ACS. This notification has an

Platforms	Source	Type	Description
			additional property of 'eventId' which identifies the event the data transferred relates to.
All	acs	fileComplete	Provides notification of the successful completion of the transfer of an individual file via ACS. The notification will have an additional 'eventId' property which indicates the event that the file relates to. The property 'destpath' includes the full destination URL of the file which has now been transferred.

Chapter 7. Format strings

Format strings are a powerful tool for configuring the output from the camera. Spend some time studying this chapter to understand how they work if you want to change them. They can be used to configure file names and the format of outputted data in many places. Familiarity with the C (or other languages which have copied it) *printf* command will help in understanding what is going on here.

Only configuration parameters which specify that they are a format string may use this syntax. Please notify us if you think we should make a string into a format string.

Caution

Beware, you can configure the system incorrectly so that you get bad filenames which then cannot transfer. Be especially careful of the characters : / \ and . in your filename strings. Also, most systems won't accept filenames with control characters in them.

A format string consists of any number of parts, but essentially there are three different types of data you can put in it.

- Ordinary characters: which will just be output as is. This is the simplest type of entry. For example: if you want your filename to end in .txt, then just put .txt in the format string at the end. Note, you cannot put a \ or % in the string this way, you need to use a control character to do this.
- Control characters: which are used for unprintable characters which you can't simply enter into your string, such as **\n** for end of line. There is more detail on these in the section called “Control Characters” [84].
- Replacement specifiers: these are completely replaced by other text or numbers which are dependant upon the current item the string is working with. For example **%Pps** would be replaced by the read number plate. This is where the real power of the format strings lies. There is more detail on these in the section called “Replacement specifier” [85].

Control Characters

Each one of these will be replaced by a single control character in the output. These do *not* make sense for filenames, and are likely to cause problems with filesystems and FTP if you try to use them. They are of most use in file contents where you may want to add carriage returns or tabs.

- **\a** Alert (bell) (not often used)
- **\b** Backspace (not often used)
- **\f** Form feed, or new page (not often used)
- **\r** Carriage return. Combined with \n this is the DOS style end of line marker (e.g. **\r\n**.
- **\n** New line. This is the unix style end of line marker.
- **\t** Tab (horizontal)
- **\v** Vertical Tab (not often used)
- **** Gives a single \. Remember to put in two of these when you only want one in the output
- _ Gives a single space. You can use space directly on the P382, P392+ and P492 but this is for compatiblilty with the P357/P372. You cannot currently enter spaces in the shell, only on the web pages, so you'll need to use this from pipsshell.
- **\%** Gives a single %. Otherwise we think the % is the start of a replacement specifier

This paragraph can be skipped if you do not understand it. The escape character is ****, and can be followed by a character to cause various outputs, see above. **\octal-number** as in **\077** and **\hex-number** as in **\x3f** are also supported to output other ascii values - both of those will give a question mark character in ASCII.

Replacement specifier

The real power of format strings is in these. They all start with a % sign and there are a multitude of options for formatting the value. You then specify what the value is you want, and then how you want it presented.

Note

The format differs from printf, in that we must say what we are trying to display in the % as well as how to display it. The minimum length for a replacement specifier is 4 characters, including the % sign

The format goes as follows:

%{*replacement value*}[*format detail*]{*format*}

- *%* indicates the start of a replacement specifier
- *replacement value* is a two character string indicating what it is we wish to display here
- *format detail* is an optional string indicating more detail on how we wish to display it
- *format* is a single character indicating how we wish to display the value, e.g. as a decimal or hexadecimal number. Some values only make sense when displayed with a certain format

Format

The following characters are valid as the format in the replacement specifiers. Not all printf formats are valid.

Table 7.1. Format characters

Character	Desrciption
c	A single character
d	A signed decimal integer
i	A signed decimal integer (the same as d)
o	An octal integer
s	A string
u	An unsigned decimal integer
x	A hexadecimal integer with lower case letters
X	A hexadecimal integer with upper case letters
t	Treat the entry as numeric, and convert it to a string using the asctime() call to give something like 'Wed Jun 30 21:49:08 1993'. Trailing carriage return will be stripped.

Format Detail

An integer value placed here will ensure that the output is at least that many characters long. It will be padded with spaces. If you precede the integer with a 0 then it will pad with zeros instead. This is totally optional.

For example **The plate is %Pp8s\n** Will pad the plate string with spaces so outputting for a plate N7CTR

```
The plate is    N7CTR
```

with 4 spaces between the s and the N.

List of replacement values

Format value C

The camera detail of the plate the vehicle was read on

Platforms	Detail	Data Type	Description
All	Ce	Number	The shutter setting used for this image
All	Cg	Number	The gain setting used for this image
All	Cn	Number	The camera number (starting at zero)
All	CN	Number	The camera number (starting at one)
All	Cs	Number	The sequence setting (starting at zero)
All	CS	Number	The sequence setting (starting at one)

Format value D

The camera detail of the hazard plate the vehicle was read on

Platforms	Detail	Data Type	Description
All	De	Number	The shutter setting used for this image
All	Dg	Number	The gain setting used for this image
All	Dn	Number	The camera number (starting at zero)
All	DN	Number	The camera number (starting at one)
All	Ds	Number	The sequence setting (starting at zero)
All	DS	Number	The sequence setting (starting at one)

Format value E

Unique information about delivery event, Not usable under all circumstances

Platforms	Detail	Data Type	Description
All	Ei	Number	The Event id, which uniquly identifies the event

Format value F

Associated file. Not useable under all circumstances. Primarily for use in ACS's LPR files.

Platforms	Detail	Data Type	Description
All	F1	String	The filename of context image 1
All	F2	String	The filename of context image 2
All	F3	String	The filename of context image 3
All	F4	String	The filename of context image 4
All	F5	String	The filename of context image 5
All	F6	String	The filename of context image 6
All	F7	String	The filename of context image 7
All	F8	String	The filename of context image 8
All	Fl	String	The lpr text filename
All	Fn	String	The IR image filename

Platforms	Detail	Data Type	Description
All	FN	String	The hazard IR image filename
All	Fp	String	The patch image filename
All	FP	String	The hazard patch image filename
All	Ft	String	The transfer path (which is not prepended to the other filenames)
All	Fw	String	The wide angle, overview image filename
All	FW	String	The hazard wide angle, overview image filename

Format value H

The read hazard plate from the vehicle

Platforms	Detail	Data Type	Description
All	Ha	Number	The anpr classification (not useful with many ANPR engines)
All	HA	String	The OEM asynchronous payload. Asynchronous messages injected via serial (or TCP) will be associated with messages based on a closest match within a window. Otherwise an empty string.
All	Hc	Number	The confidence of the hazard plate read
All	HC	Number	The confidence category of the hazard plate read
All	Hf	Number	The confidence of the hardware platefinder
All	HF	Number	The field number
All	Hn	Number	The nationality code (not generally useful, see HN which is)
All	HN	String	The nationality (country and state) of origin of this plate if known
All	Ho	Number	The time offset between the trigger time and the image associated with this read (milliseconds). If not triggered, will be 0
All	Hp	String	The text of the hazard plate
All	Hr	Number	The total number of reads associated with the trigger that caused this plateread (A single trigger can lead to >1 plateread event). For a NOREAD the value will still be 1.
All	Hs	Number	The syntax confidence of the hazard plate read. This is a measure of how confident we are that the hazard plate matched the syntax of the reported country or state.
All	Ht	String	The plate tag, as extracted from the vehicle filter database. Will be blank if no tag entered, the plate is not matched, or the filter is off
All	HT	String	The OEM trigger payload. If you are using serial (or TCP/IP) triggers, this will be the OEM content of those, otherwise it will be boring. Text 'auto' will be returned if not triggered
All	Hx	Number	The x position of the plate's left edge in pixels
All	HX	Number	The width of the plate in pixels
All	Hy	Number	The y position of the plate's top edge in pixels
All	HY	Number	The height of the plate in pixels

Format value h

The camera heartbeat delivery

Platforms	Detail	Data Type	Description
All	hc	Number	The count of heartbeat delivery attempts.

Platforms	Detail	Data Type	Description
All	hf	Number	The count of heartbeat delivery failures.
All	hs	Number	A camera status bitfield (legacy).

Format value I

The image timestamp, the moment the image for the vehicle was captured.

This is a local time and accounts for timezone and daylight saving

Platforms	Detail	Data Type	Description
All	Ia	String	The string am for the morning, pm for the afternoon
All	Ic	Number	Seconds since midnight 1st of January 1970 (commonly known as C time). This is UTC always, included for completeness.
All	Id	Number	The day of the month
All	ID	Number	The day of the year, with January the 1st as zero
All	Ih	Number	The hour, 24 hour clock
All	IH	Number	The hour, 12 hour clock
All	Ii	Number	Milliseconds
All	Il	Number	Indicates if time is locked via NTP
All	IL	String	Indicates if time is locked via NTP as a string
All	Im	Number	Minutes past the hour
All	IM	Number	Tens of minutes past the hour
All	Io	Number	Month of the year (January as one)
All	IO	String	Month of the year as a word, in English
All	IP	String	Month of the year as three letter shortened word, in English
All	Is	Number	Seconds past the minute
All	It	Number	Tenths of seconds
All	Iu	Number	Hundredths of seconds
All	Iv	Number	One if daylight saving is in effect, zero otherwise
All	Iw	Number	The day of the week as a number, with zero being Sunday
All	IW	String	The day of the week as a word, in English
All	IX	String	The day of the week as a three letter shortened word, in English
All	Iy	Number	The year
All	IY	Number	The last two digits of the year

Format value i

The image timestamp, the moment the image for the vehicle was captured.

This is UTC time (like GMT)

Platforms	Detail	Data Type	Description
All	ia	String	The string am for the morning, pm for the afternoon
All	ic	Number	Seconds since midnight 1st of January 1970 (commonly known as C time)
All	id	Number	The day of the month

Platforms	Detail	Data Type	Description
All	iD	Number	The day of the year, with January the 1st as zero
All	ih	Number	The hour, 24 hour clock
All	iH	Number	The hour, 12 hour clock
All	ii	Number	Milliseconds
All	il	Number	Indicates if time is locked via NTP
All	iL	String	Indicates if time is locked via NTP as a string
All	im	Number	Minutes past the hour
All	iM	Number	Tens of minutes past the hour
All	io	Number	Month of the year (January as one)
All	iO	String	Month of the year as a word, in English
All	iP	String	Month of the year as three letter shortened word, in English
All	is	Number	Seconds past the minute
All	it	Number	Tenths of seconds
All	iu	Number	Hundredths of seconds
All	iv	Number	One if daylight saving is in effect, zero otherwise
All	iw	Number	The day of the week as a number, with zero being Sunday
All	iW	String	The day of the week as a word, in English
All	iX	String	The day of the week as a three letter shortened word, in English
All	iy	Number	The year
All	iY	Number	The last two digits of the year

Format value J

JPEG data. Not useable under all circumstances. Primarily for use in output filenames to distinguish between them.

Platforms	Detail	Data Type	Description
All	Jt	Character	The file type. Will be p for a patch, n for an IR image, and w for an overview wide angle image. Context images will be 1 (for context 1), 2 (for context 2). Currently up to 8 context images are supported.

Format value L

The location of the camera

Platforms	Detail	Data Type	Description
All	Ld	Number	The whole number of degrees of latitude (north or south). Will always be positive.
All	LD	Number	The whole number of degrees of longitude (east or west). Will always be positive.
All	Le	Number	The whole number of degrees north we are. Will be negative if we are south.
All	LE	Number	The whole number of degrees east we are. Will be negative if we are west.
All	Lf	Number	The number of millidegrees of latitude we are away from the nearest degree.
All	LF	Number	The number of millidegrees of longitude we are away from the nearest degree.
All	Lg	Number	The number of microdegrees of latitude we are away from the nearest degree.

Platforms	Detail	Data Type	Description
All	LG	Number	The number of microdegrees of longitude we are away from the nearest degree.
All	Ll	Character	A character for latitude, N (north) or S (south) depending upon which hemisphere the location represents.
All	LL	Character	A character for longitude, E (east) or W (west) depending upon which side of the meridian the location represents.
All	Lm	Number	The number of minutes of latitude (north or south) that we are away from the nearest whole degree. Will always be positive.
All	LM	Number	The number of minutes of longitude (east or west) that we are away from the nearest whole degree. Will always be positive.
All	Ln	Number	The number of minutes of latitude (north or south) that we are away from the equator. Will always be positive.
All	LN	Number	The number of minutes of longitude (east or west) that we are away from the equator. Will always be positive.
All	Lo	Number	The number of minutes north that we are away from the equator. Will be negative if we are south.
All	LO	Number	The number of minutes east that we are away from the equator. Will be negative if we are south.
All	Lp	Number	The number of milliminutes of latitude we are away from the nearest minute.
All	LP	Number	The number of milliminutes of longitude we are away from the nearest minute.
All	Lq	Number	The number of microminutes of latitude we are away from the nearest minute.
All	LQ	Number	The number of microminutes of longitude we are away from the nearest minute.
All	LV	String	The string Valid or Invalid depending upon whether the location is deemed good.

Format value M

Metadata strings from the Metadata object. This is purely here so you can have the same format strings on all sites, and just change the metadata in this store

Platforms	Detail	Data Type	Description
All	Ma	String	Metadata string a
All	Mb	String	Metadata string b
All	Mc	String	Metadata string c
All	Md	String	Metadata string d
All	Me	String	Metadata string e
All	Mf	String	Metadata string f
All	Mg	String	Metadata string g
All	Mh	String	Metadata string h
All	Mi	String	Metadata string i
All	Mj	String	Metadata string j
All	Mk	String	Metadata string k
All	Ml	String	Metadata string l
All	Mm	String	Metadata string m
All	Mn	String	Metadata string n
All	Mo	String	Metadata string o

Platforms	Detail	Data Type	Description
All	Mp	String	Metadata string p
All	Mq	String	Metadata string q
All	Mr	String	Metadata string r
All	Ms	String	Metadata string s
All	Mt	String	Metadata string t
All	Mu	String	Metadata string u
All	Mv	String	Metadata string v
All	Mw	String	Metadata string w
All	Mx	String	Metadata string x
All	My	String	Metadata string y
All	Mz	String	Metadata string z

Format value o

The time offsets of overview context images

Platforms	Detail	Data Type	Description
All	o1	Number	The offset (in milliseconds) of context image 1 measured from the vehicle event timestamp
All	o2	Number	The offset (in milliseconds) of context image 2 measured from the vehicle event timestamp
All	o3	Number	The offset (in milliseconds) of context image 3 measured from the vehicle event timestamp
All	o4	Number	The offset (in milliseconds) of context image 4 measured from the vehicle event timestamp
All	o5	Number	The offset (in milliseconds) of context image 5 measured from the vehicle event timestamp
All	o6	Number	The offset (in milliseconds) of context image 6 measured from the vehicle event timestamp
All	o7	Number	The offset (in milliseconds) of context image 7 measured from the vehicle event timestamp
All	o8	Number	The offset (in milliseconds) of context image 8 measured from the vehicle event timestamp

Format value P

The read number plate from the vehicle

Platforms	Detail	Data Type	Description
All	P2	String	The 2-character nationality of origin of this plate if known, as defined by ISO 3166-1
All	P3	String	The 3-character nationality of origin of this plate if known, as defined by ISO 3166-1
All	Pa	Number	The anpr classification (not useful with many ANPR engines)
All	PA	String	The OEM asynchronous payload. Asynchronous messages injected via serial (or TCP) will be associated with messages based on a closest match within a window. Otherwise an empty string.

Platforms	Detail	Data Type	Description
All	Pc	Number	The confidence of the plate read
All	PC	Number	The confidence category of the plate read
All	Pd	String	The direction of travel of the plate read. This will be one of the following strings: AWAY, TOWARD, NOTSET. If NOTSET it indicates the direction could not be determined.
All	PD	String	The subdivision of origin of this plate if known, as defined by ISO 3166-2
All	Pf	Number	The confidence of the hardware platefinder
All	PF	Number	The field number
All	Pg	String	The source of OEM trigger
All	Pi	String	The OEM trigger payload from the first TCP/IP trigger
All	PI	Number	The trigger identifier.
All	PL	String	The lane in which the plate is located.
All	Pn	Number	The nationality code (not generally useful, see PN which is)
All	PN	String	The nationality (country and state) of origin of this plate if known
All	Po	Number	The time offset between the trigger time and the image associated with this read (milliseconds). If not triggered, will be 0
All	Pp	String	The text of the plate
All	Pr	Number	The total number of reads associated with the trigger that caused this plateread (A single trigger can lead to >1 plateread event). For a NOREAD the value will still be 1.
All	Ps	Number	The syntax confidence of the plate read. This is a measure of how confident we are that the plate matched the syntax of the reported country or state.
All	PS	String	The OEM trigger payload from the first Serial trigger
All	Pt	String	The plate tag, as extracted from the vehicle filter database. Will be blank if no tag entered, the plate is not matched, or the filter is off
All	PT	String	The OEM trigger payload. If you are using serial (or TCP/IP) triggers, this will be the OEM content of those, otherwise it will be boring. Text 'auto' will be returned if not triggered
All	Px	Number	The x position of the plate's left edge in pixels
All	PX	Number	The width of the plate in pixels
All	Py	Number	The y position of the plate's top edge in pixels
All	PY	Number	The height of the plate in pixels

Format value R

The trigger timestamp, the moment the trigger started. You should probably be using T instead of this, as if the event was not a triggered one you will not get anything in the string with R.

This is a local time and accounts for timezone and daylight saving

Platforms	Detail	Data Type	Description
All	Ra	String	The string am for the morning, pm for the afternoon
All	Rc	Number	Seconds since midnight 1st of January 1970 (commonly known as C time). This is UTC always, included for completeness.
All	Rd	Number	The day of the month
All	RD	Number	The day of the year, with January the 1st as zero

Platforms	Detail	Data Type	Description
All	Rh	Number	The hour, 24 hour clock
All	RH	Number	The hour, 12 hour clock
All	Ri	Number	Milliseconds
All	Rm	Number	Minutes past the hour
All	RM	Number	Tens of minutes past the hour
All	Ro	Number	Month of the year (January as one)
All	RO	String	Month of the year as a word, in English
All	RP	String	Month of the year as three letter shortened word, in English
All	Rs	Number	Seconds past the minute
All	Rt	Number	Tenths of seconds
All	Ru	Number	Hundredths of seconds
All	Rv	Number	One if daylight saving is in effect, zero otherwise
All	Rw	Number	The day of the week as a number, with zero being Sunday
All	RW	String	The day of the week as a word, in English
All	RX	String	The day of the week as a three letter shortened word, in English
All	Ry	Number	The year
All	RY	Number	The last two digits of the year

Format value r

The trigger timestamp, the moment the trigger started. You should probably be using t instead of this, as if the event was not a triggered one you will not get anything in the string with r.

This is UTC time (like GMT)

Platforms	Detail	Data Type	Description
All	ra	String	The string am for the morning, pm for the afternoon
All	rc	Number	Seconds since midnight 1st of January 1970 (commonly known as C time)
All	rd	Number	The day of the month
All	rD	Number	The day of the year, with January the 1st as zero
All	rh	Number	The hour, 24 hour clock
All	rH	Number	The hour, 12 hour clock
All	ri	Number	Milliseconds
All	rm	Number	Minutes past the hour
All	rM	Number	Tens of minutes past the hour
All	ro	Number	Month of the year (January as one)
All	rO	String	Month of the year as a word, in English
All	rP	String	Month of the year as three letter shortened word, in English
All	rs	Number	Seconds past the minute
All	rt	Number	Tenths of seconds
All	ru	Number	Hundredths of seconds
All	rv	Number	One if daylight saving is in effect, zero otherwise
All	rw	Number	The day of the week as a number, with zero being Sunday

Platforms	Detail	Data Type	Description
All	rW	String	The day of the week as a word, in English
All	rX	String	The day of the week as a three letter shortened word, in English
All	ry	Number	The year
All	rY	Number	The last two digits of the year

Format value S

The site details for this unit

Platforms	Detail	Data Type	Description
All	Sh	String	The site's hostname, the recommended way of identifying a site
All	Sl	Number	The system's library version number
All	Sn	Number	The system's serial number
All	Sv	Number	The system's application version number

Format value s

The supplementary images details

Platforms	Detail	Data Type	Description
All	s1	Number	The offset (in milliseconds) of supplementary image 1 measured from the vehicle event timestamp
All	s2	Number	The offset (in milliseconds) of supplementary image 2 measured from the vehicle event timestamp
All	s3	Number	Supplementary image 1 sequence setting (starting at one)
All	s4	Number	Supplementary image 2 sequence setting (starting at one)
All	s5	Number	Supplementary image 1 shutter setting
All	s6	Number	Supplementary image 2 shutter setting
All	s7	Number	Supplementary image 1 gain setting
All	s8	Number	Supplementary image 2 gain setting

Format value T

The timestamp for the vehicle, which is the trigger timestamp if the vehicle was triggered (see R), or the image timestamp if it was not (see I).

This is a local time and accounts for timezone and daylight saving

Platforms	Detail	Data Type	Description
All	Ta	String	The string am for the morning, pm for the afternoon
All	Tc	Number	Seconds since midnight 1st of January 1970 (commonly known as C time). This is UTC always, included for completeness.
All	Td	Number	The day of the month
All	TD	Number	The day of the year, with January the 1st as zero
All	Th	Number	The hour, 24 hour clock
All	TH	Number	The hour, 12 hour clock

Platforms	Detail	Data Type	Description
All	Ti	Number	Milliseconds
All	Tm	Number	Minutes past the hour
All	TM	Number	Tens of minutes past the hour
All	To	Number	Month of the year (January as one)
All	TO	String	Month of the year as a word, in English
All	TP	String	Month of the year as three letter shortened word, in English
All	Ts	Number	Seconds past the minute
All	Tt	Number	Tenths of seconds
All	Tu	Number	Hundredths of seconds
All	Tv	Number	One if daylight saving is in effect, zero otherwise
All	Tw	Number	The day of the week as a number, with zero being Sunday
All	TW	String	The day of the week as a word, in English
All	TX	String	The day of the week as a three letter shortened word, in English
All	Ty	Number	The year
All	TY	Number	The last two digits of the year

Format value t

The timestamp for the vehicle, which is the trigger timestamp if the vehicle was triggered (see r), or the image timestamp if it was not (see i).

This is UTC time (like GMT)

Platforms	Detail	Data Type	Description
All	ta	String	The string am for the morning, pm for the afternoon
All	tc	Number	Seconds since midnight 1st of January 1970 (commonly known as C time)
All	td	Number	The day of the month
All	tD	Number	The day of the year, with January the 1st as zero
All	th	Number	The hour, 24 hour clock
All	tH	Number	The hour, 12 hour clock
All	ti	Number	Milliseconds
All	tm	Number	Minutes past the hour
All	tM	Number	Tens of minutes past the hour
All	to	Number	Month of the year (January as one)
All	tO	String	Month of the year as a word, in English
All	tP	String	Month of the year as three letter shortened word, in English
All	ts	Number	Seconds past the minute
All	tt	Number	Tenths of seconds
All	tu	Number	Hundredths of seconds
All	tv	Number	One if daylight saving is in effect, zero otherwise
All	tw	Number	The day of the week as a number, with zero being Sunday
All	tW	String	The day of the week as a word, in English
All	tX	String	The day of the week as a three letter shortened word, in English
All	ty	Number	The year

Platforms	Detail	Data Type	Description
All	tY	Number	The last two digits of the year

Examples

Here are a few example format specifiers which might help you concoct your own. All the example output assumes a plate of RG51BTV has been read with confidence 96, on shutter 50/gain 9 at 15:34:30.2234 on 2008/03/27 in the eastern european timezone (GMT+2) on hostname "testsite" and that we're looking at the IR image, and the system is not triggered.

%Shs/

Input	%Shs	/
Output	testsite	/

(example result `testsite/`) This is the default ACS transfer path, just putting the hostname into the path.

acs/%Shs/

Input	acs/	%Shs	/
Output	acs/	testsite	/

(example result `acs/testsite/`) Now we have shifted to putting it into an acs subdirectory, followed by a site dependant hostname.

acs\\%Shs

Input	acs\\	%Shs	\\
Output	acs\	testsite	\

(example result `acs\testsite\`) And this version uses windows style directory separators, which is necessary for some broken windows FTP servers. Note we need to escape the \ by putting \\ in the path.

%Shs/%Iy04d%Io02d%Id02d/%Ih02d%IMd0/

Input	%Shs	/	%Iy04d	%Io02d	%Id02d	/	%Ih02d	%Idm	0/
Output	testsite	/	2008	03	27	/	12	3	0/

(example result `acs/20080327/1230/`) And now we are storing the files in time and date subdirectories, with 10 minutes worth of files per directory. Note the use of %IMd0 at the end which gives us the digit for each of the ten minutes, followed by a 0 which is copied through unchanged.

%Jtc%Id02u%Io02u%Iy04u,%Ih02u%Im02u%Is02u%Iu02u,%Pps,%Pc02u.jpg

Input	%Jtc	%Id02u	%Io02u	%Iy04u	,	%Ih02u	%Im02u	%Is02u	%Iu02u
Output	n	27	03	2008	,	12	34	30	22

Input	,	%Pps	,	%Pc02u	.jpg
Output	,	RG51BTV	,	96	.jpg

(example result `n27032008,12343022,RG51BTV,96.jpg`) This is the default image filename for ACS images. It produces a string starting with a character to identify which type of image it is. Followed by the date in DDMMYYYY format, followed by the time with hundredths of seconds, follwed by the plate and then the confidence. All of these are separated by commas.

%Jtc%Iy04u%Io02u%Id02u_%Ih02u%Im02u%Is02u%Iu02u_%Pps_%Pc02u.jpg

Input	%Jtc	%Iy04u	%Io02u	%Id02u	_	%Ih02u	%Im02u	%Is02u	%Iu02u
Output	n	2008	03	27	_	12	34	30	22

Input	_	%Pps	_	%Pc02u	.jpg
Output	_	RG51BTV	_	96	.jpg

(example result `n20080327_12343022_RG51BTV_96.jpg`) Now we have changed the commas to underscores, and swapped the date around to be YYYYMMDD.

%Jtc%ty04u%to02u%td02u%th02u%tm02u%ts02u%tu02u,%Pps,%Pc02u,%Ced,%Cgd.jpg

Input	%Jtc	%td02u	%to02u	%ty04u	%th02u	%tm02u	%ts02u	%tu02u
Output	n	27	03	2008	10	34	30	22

Input	,	%Pps	,	%Pc02u	,	%Ced	,	%Cgd	.jpg
Output	,	RG51BTV	,	96	,	50	,	9	.jpg

(example result `n2703200810343022,RG51BTV,96,50,9.jpg`) This time we are using GMT trigger time if the system is triggered, instead of local time of the image. We're also putting the shutter and gain settings for the read into the plate. We have also gone back to commas, loosing the separator between the date and time.

Chapter 8. PIXI Protocol

Note

PIXI was formerly known as NetUI, but has been renamed as it has been extended and the old name became inappropriate for the functions delivered.

This is a highly technical appendix describing the raw protocol you can use to communicate with and control the camera. This is of no interest unless you want to do that.

Using this protocol you can implement anything that the pipsshell, web interface to the camera application or manual generation tools can do. It is able to query application parameters, set them, issue commands, watch logging parameters and find out other details from the camera application. You can also get the camera to push images and event data to you, and collect image and event data (pull) from the camera.

Protocol

This protocol is run over TCP/IP to the camera, on port 3382. On OS release version 8 or later this port is firewalled off from the outside world, you will have to add a firewall rule to allow your remote application to access the camera. The protocol is a simple encapsulation of XML documents within a couple of boundaries. The XML must be correctly formed, if it is not then nothing in the message will be processed. The messages are not compressed, nor are they encrypted in any way.

Warning

Opening this port up may be a security risk to the camera.

The suggested way of working is to set up an ssh tunnel into the camera which will provide a way around the firewall without compromising it, and requires zero setup. This will also encrypt the data on the wire.

The XML may refer to some extra binary data which will follow the XML data.

The basic packet format is

Table 8.1. PIXI Packet Format

Name	Bytes	Content
Head	2	1. 0x0000 if there are no binary blobs in this data 2. 0x0001 if there are one or more binary blobs in the data
Length	2	XML Document length in bytes, as 2 byte, big endian value. Maximum length that the camera will accept is 16k. This is only the XML document portion.
Data	as required	Fully formed XML document adhering to schema below
Binary Length	0 or 4	Length of the binary blob if marked as present by the header.
Binary Data	0 or as required	Zero or more binary blobs. The position and size of the individual may be determined from the XML content.
End	4	0xffffffff

The link observes the following:

1. Multiple documents can be passed down the same link.

2. The link will stay open for a period of time, the camera will close it after 5 minutes of inactivity. To prevent this happening you can send heartbeat message which will be echoed back to you to show the camera is alive.

3. Either end can send a message unsolicited.

4. The camera responds to messages in the order in which the messages were received. This is on a per-connection basis, each connection can execute in parallel with others.

5. The camera will allow a maximum of 5 links at once.

Figure 8.1. Link with no heartbeat, camera will close when no command has been received for 5 minutes.

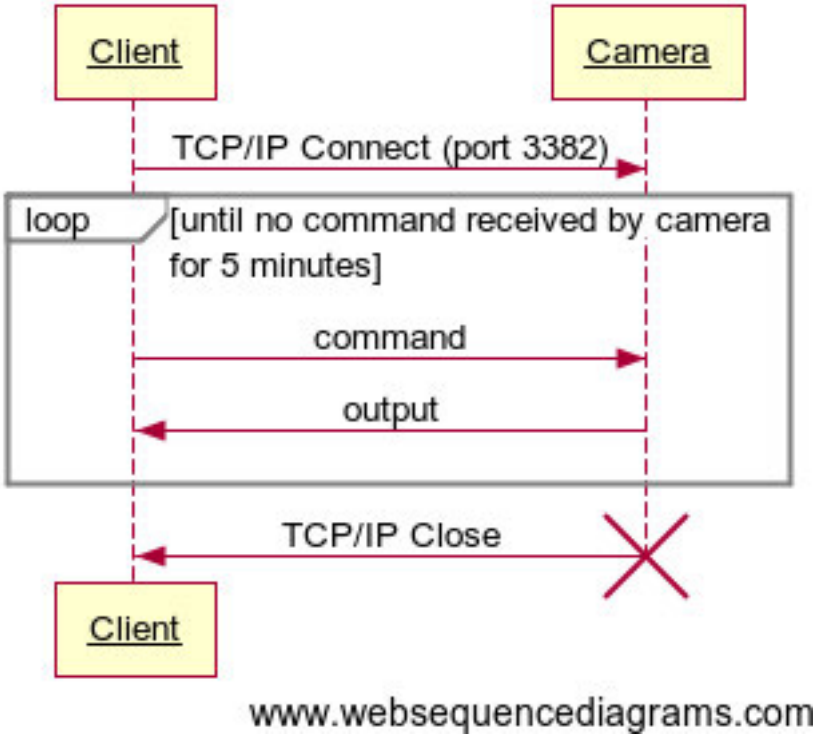
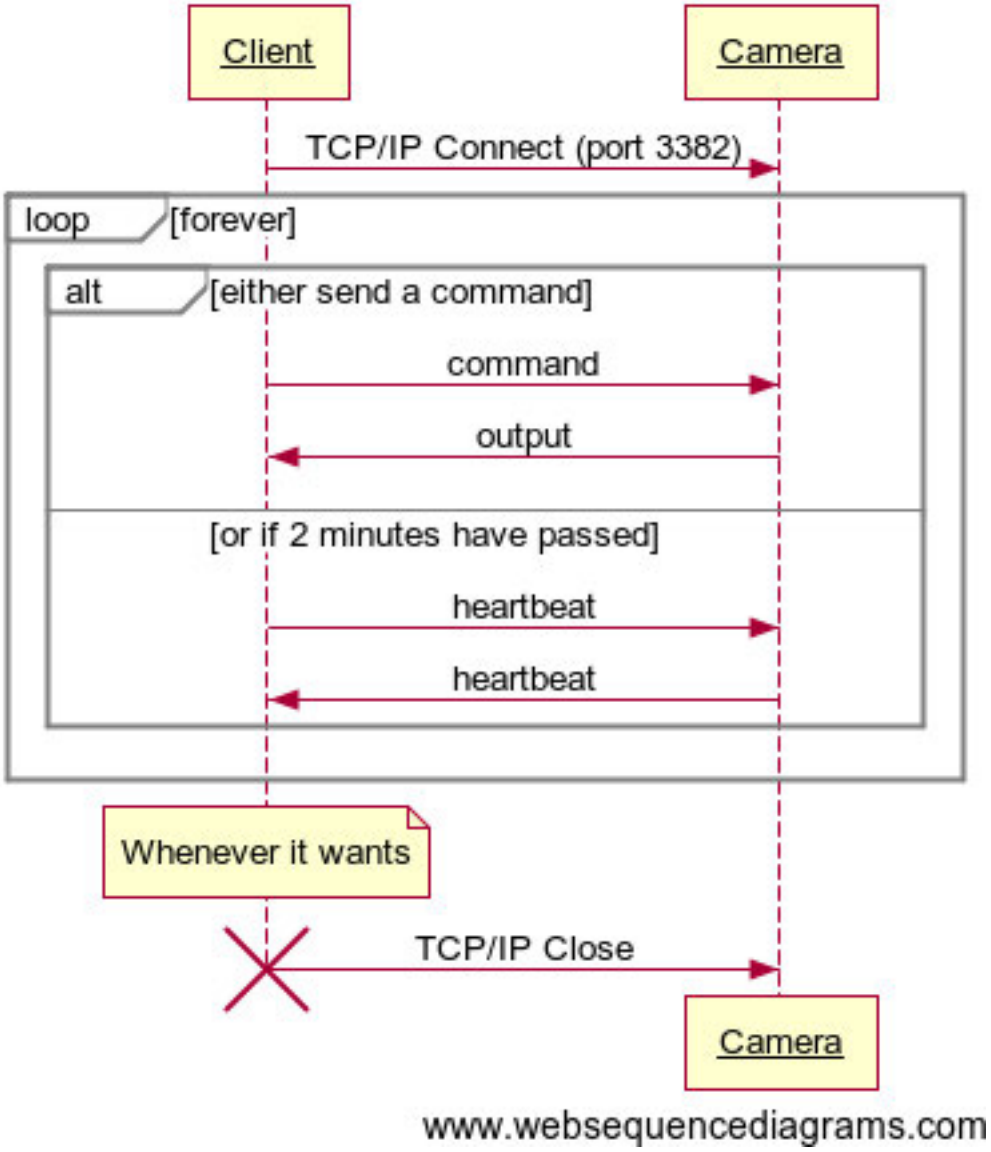


Figure 8.2. Link with heartbeat, client chooses when to end by closing the link.



Example documents

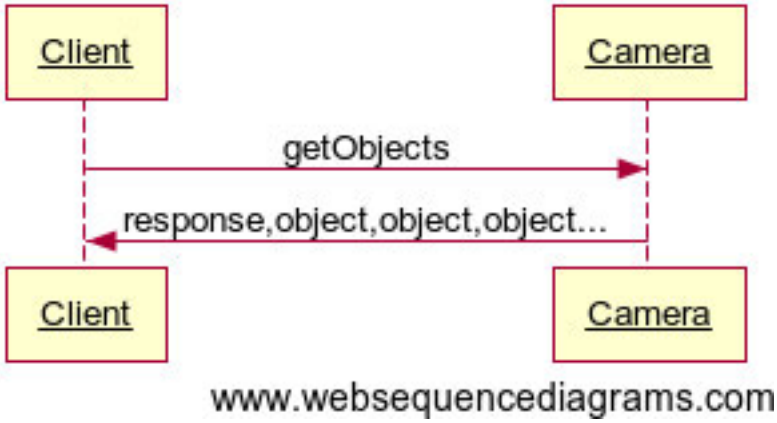
Here are few example documents to help you with composing your own messages and developing an application. In each case the PC/Instation/Handheld/other device is referred to as the Client, and the end that is implemented in the P382, P392+ and P492 is the Camera.

Note

All examples are "pretty printed" with space and formatting to make them easier to read. The camera will actually respond with documents without formatting, and for efficiency reasons I would suggest also sending unformatted documents.

Root objects

Figure 8.3. Get Root Objects - a list of all configureable objects is collected, some may have subobjects



This command to gets the root objects from the camera:

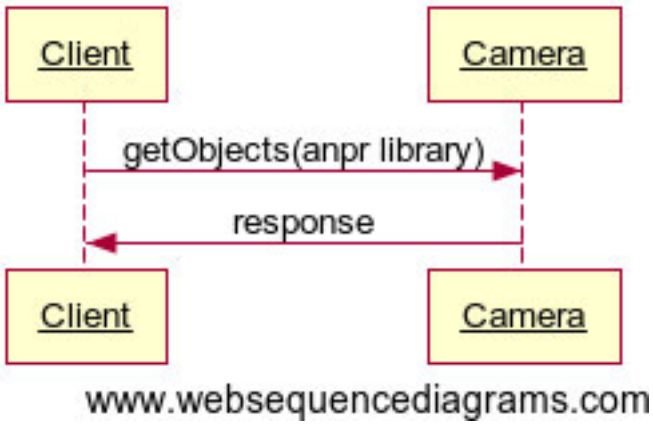
```
<?xml version="1.0"?>
<commands>
  <getObjects name=""/>
</commands>
```

And the reply with the root objects

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

Figure 8.4. Get subobjects of an object - a list of all subobjects is collected, some may have subobjects. The list may be empty, as in the example



A command to get a subobject's objects

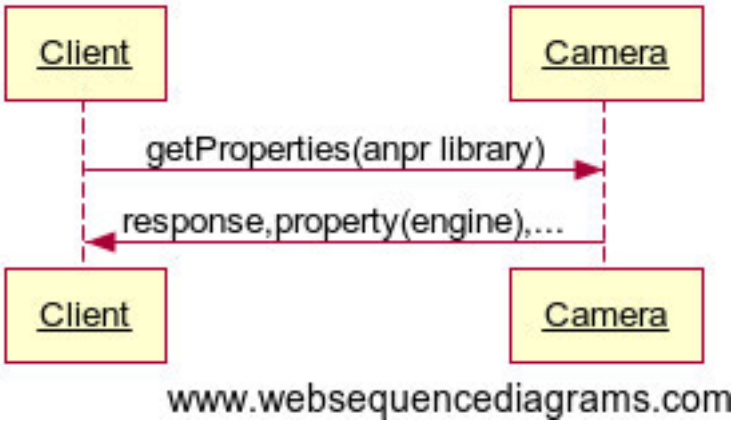
```
<?xml version="1.0"?>
<commands>
  <getObjects name="anpr library"/>
</commands>
```

And the reply, with no subobjects

```
<?xml version="1.0"?>
<output>
  <response name="getObjects">
    <object>anpr library</object>
    <success>false</success>
  </response>
</output>
```

Properties

Figure 8.5. Get properties of an object - a list of all the properties of an object. The list may be empty.



And now getting the properties of an object

[redacted]

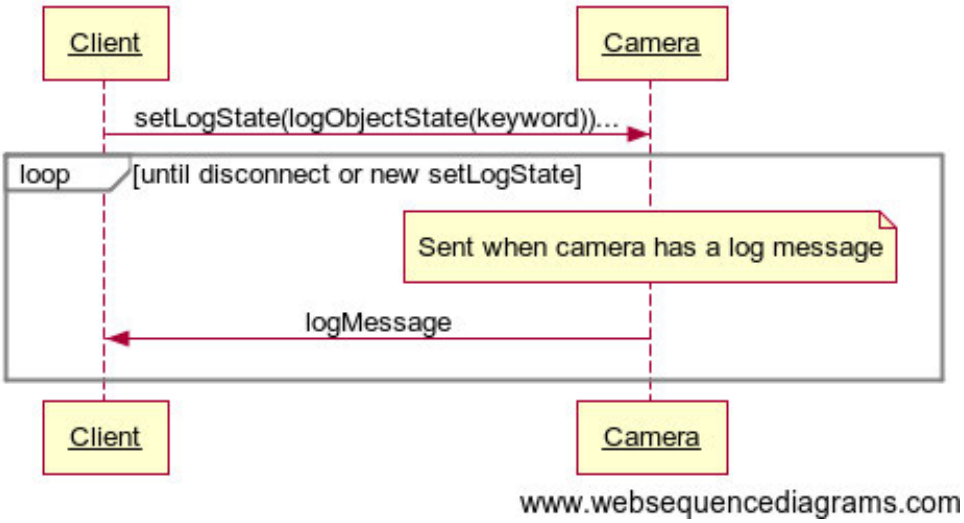
```
</commands>
```

And the reply, with just one property

[redacted]

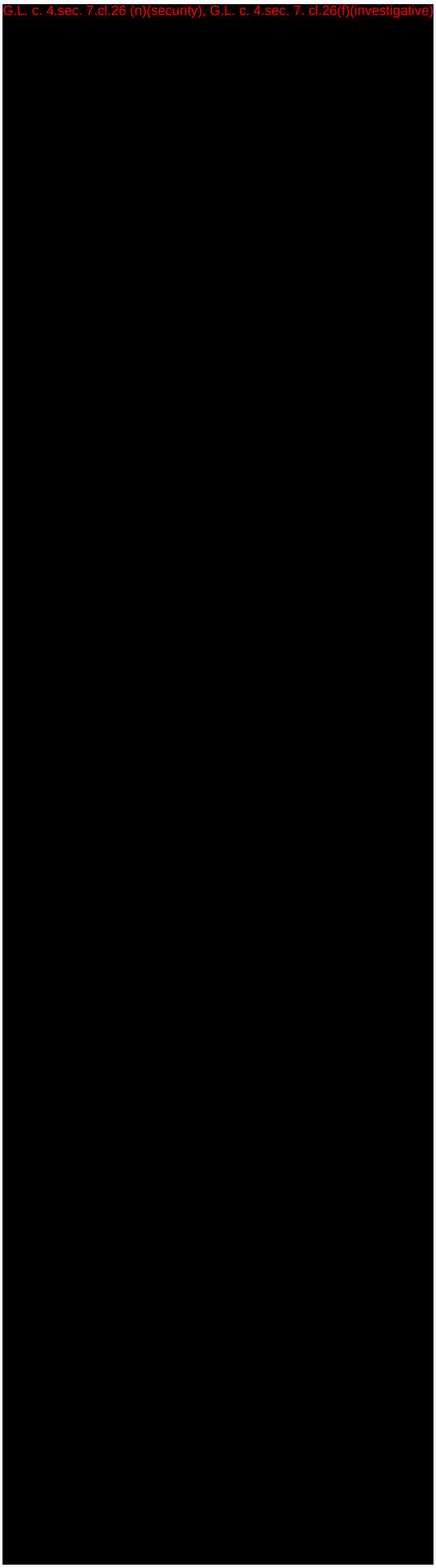
Logging

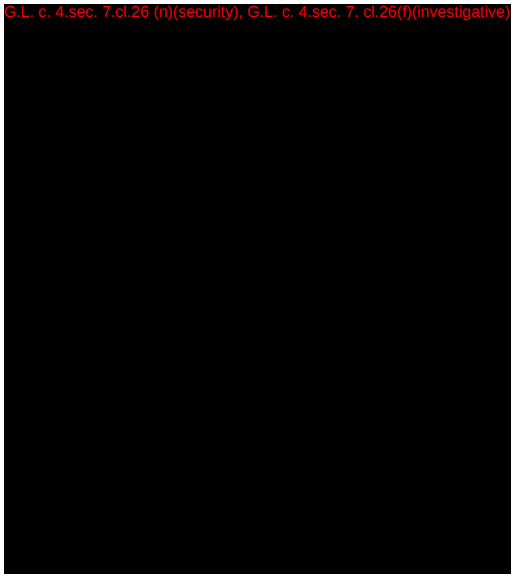
Figure 8.6. Start some logging. Asynchronous messages will be sent back by the Camera containing the log messages



Now setting up logging (note, no immediate reply)

[redacted]
G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

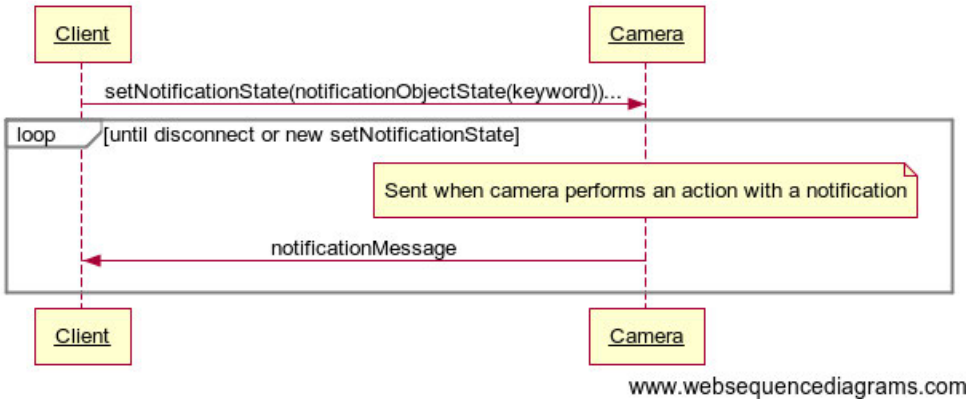

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)



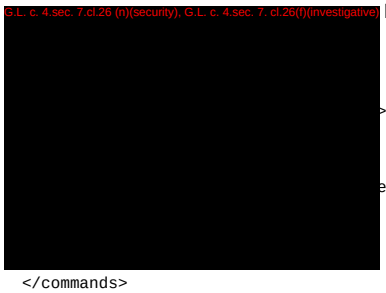

```
</commands>
```

Notifications

Figure 8.7. Start notification messages. Asynchronous messages will be sent back by the Camera containing the notification messages of the requested events

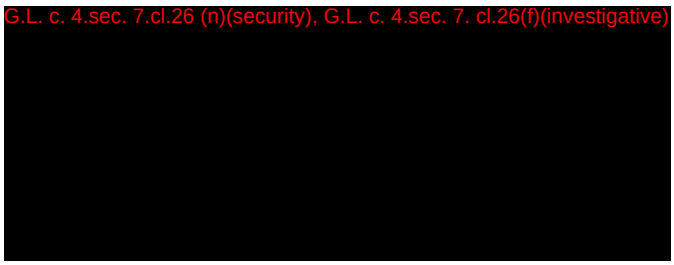


To enable notifications, send a setNotificationState message listing the notifications that you wish to enable. Note that reply from this message.




```
>
e">
</commands>
```

When an event for which you have registered a notification occurs, you will now receive an unsolicited notificationMessage

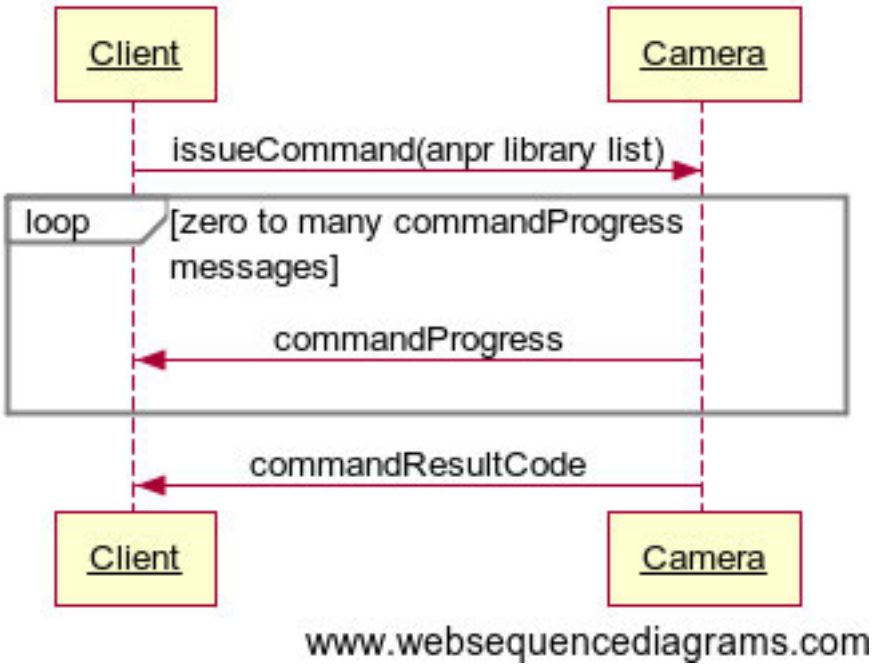


All notifications will have the source, type, and timeDate values, indicating when the notification was triggered, and what triggered it. Each notification type may have additional properties that are specific to that notification type. The available notifications are:

Platforms	Source	Type	Description
All	acs	datasetComplete	Provides notification of the successful transfer of an entire data-set via ACS. This notification has an additional property of 'eventId' which identifies the event the data transferred relates to.
All	acs	fileComplete	Provides notification of the successful completion of the transfer of an individual file via ACS. The notification will have an additional 'eventId' property which indicates the event that the file relates to. The property 'destpath' includes the full destination URL of the file which has now been transferred.

Issue Command

Figure 8.8. Issue a command and receive the responses.



A command, which has 3 replies. Note: issueCommand will probably be deprecated in the future

```
<?xml version="1.0"?>
<commands>
  <issueCommand>anpr library list</issueCommand>
</commands>
```

The output, as the command is processed

```
<?xml version="1.0"?>
<output>
  <commandProgress>Available cardet libraries</commandProgress>
</output>

<?xml version="1.0"?>
<output>
  <commandProgress>UK, Ireland, France (version 2212) - libcardet.p382.so.1.2212.UK_IE</commandProgress>
</output>
```

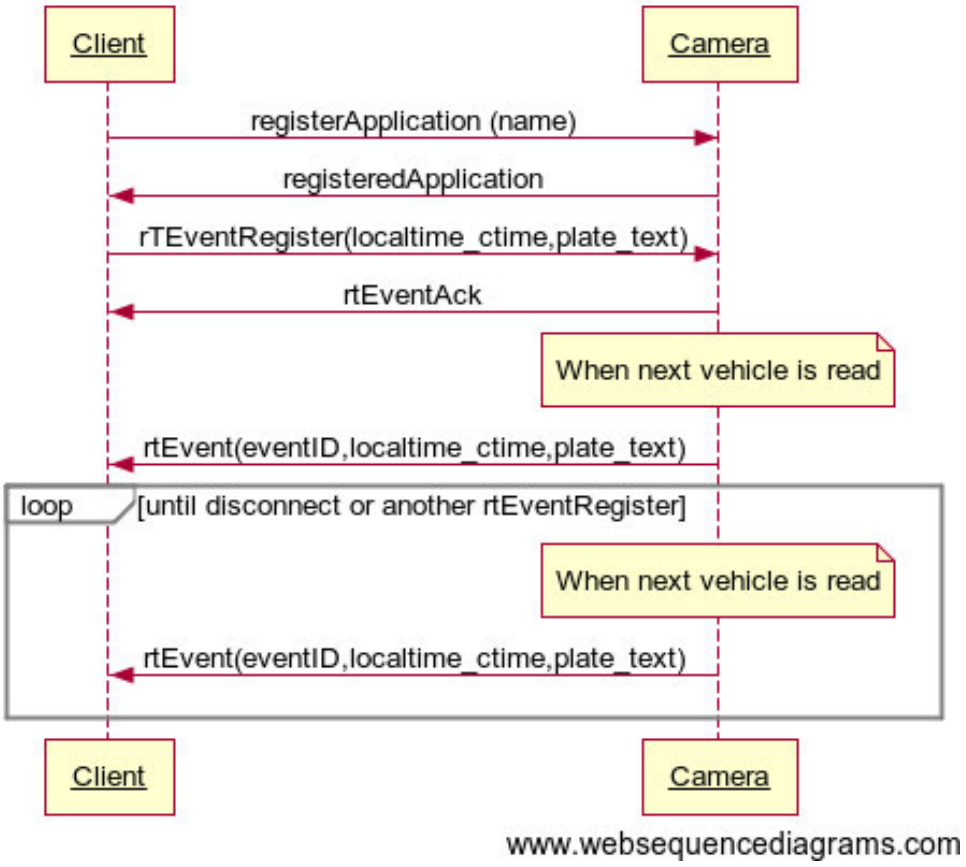
Then the result, one (and only one) of which is guaranteed to arrive

```
<?xml version="1.0"?>
<output>
  <commandResultCode>OK</commandResultCode>
```

```
</output>
```

Event data

Figure 8.9. Connect to the camera and get events as it reads vehicles.



Here we need to register the application, prior to setting up and receiving events as they occur. We are receiving minimal information, just what would be required for say a journey time measurement system. You can request as much data as you like in the rtEventRegister, and it will all be sent on every event.

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

Which come back like follows when they occur. Note the details *are not* in the same order as when they were requested.

```
<?xml version="1.0"?>
```

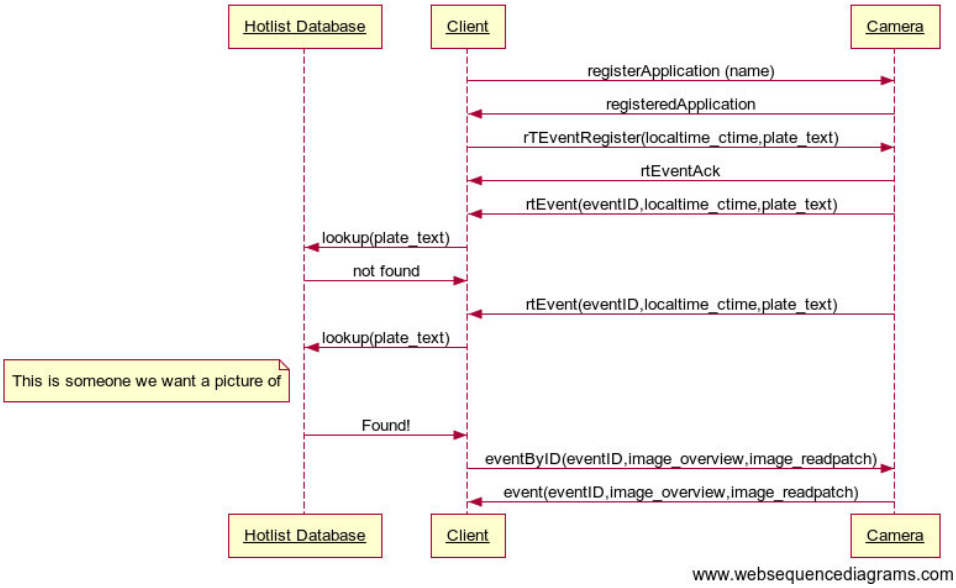
```
<output>
  <rtEvent>
    <eventID>4df5ee07000d6ae9</eventID>
    <eventData name="plate_text">
      <data>FJ05PKV</data>
    </eventData>
    <eventData name="localtime_ctime">
      <data>1308219250</data>
    </eventData>
  </rtEvent>
</output>
```

Alternatively, when registering to receive events you can specify an nlog parameter. This specifies a maximum number of events to buffer on the camera if the client application is not currently connected. This can be used to prevent data-loss should client applications disconnect.

<xi:include></xi:include>

Event data with pull

Figure 8.10. Here we are collecting (pulling) certain vehicle details when a particular vehicle is found.



As an extension to the section called “Event data” [109], here we have a database of vehicles we are particularly interested in and are requesting images for just particular vehicles. This will save bandwidth over pulling data for all vehicles.

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

which gets a response indicating two binary data blobs are following the XML which can be extracted into JPEG files

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

PIXI Documents

The documents you can send across the link are in XML, as defined by the following schemas. You can send documents from the command.xsd schema, and expect to receive documents from the output.xsd schema. The definitive versions of the schemas are found on the camera under the following URLs:

1. `https://camera.ip.address/spikeapp/commands.xsd` - for commands to send to the camera

2. `https://camera.ip.address/spikeapp/output.xsd` - for output from the camera

3. `https://camera.ip.address/spikeapp/common.xsd` - a common file, included by both the other files

These are the definitive versions of these files, and should always be used, not any other versions. They are not generated on the fly, and will only change when software on the camera is changed.

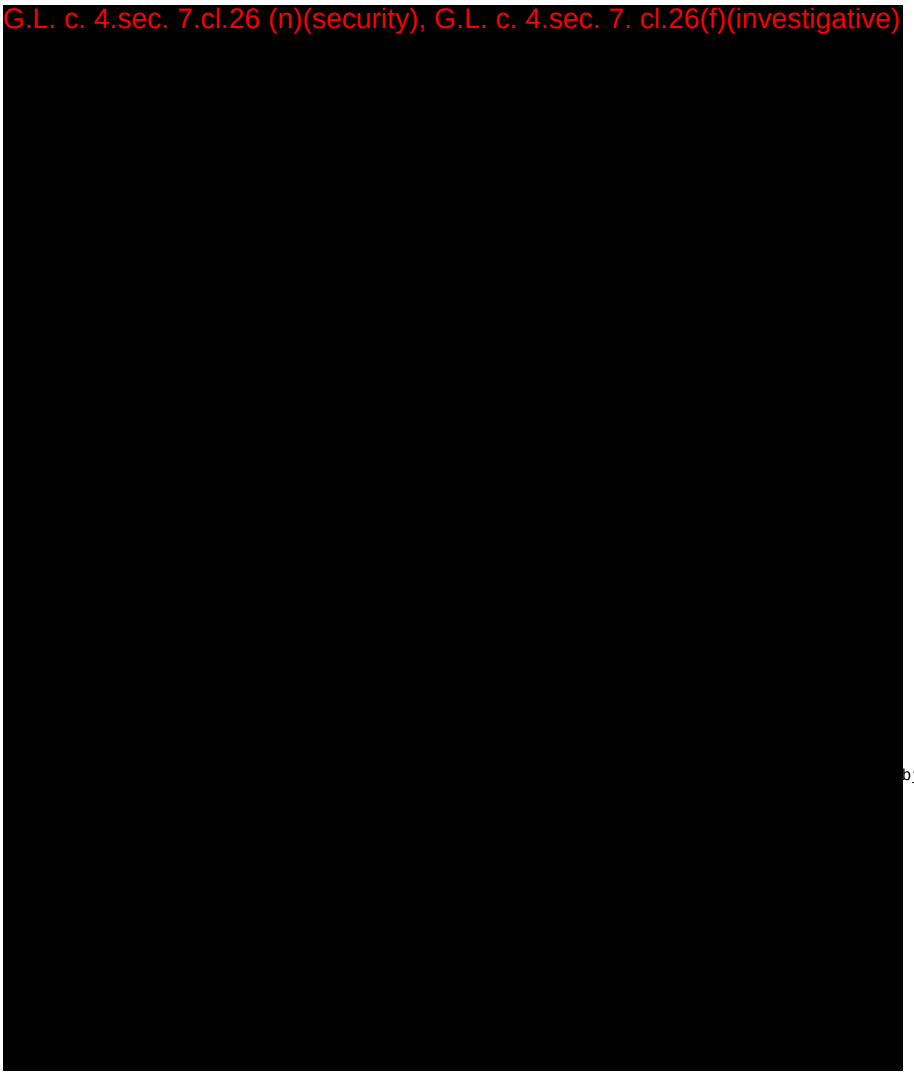
The schemas *will* change between releases of the camera software and are not currently written as extensible. Adding the necessary text into the xsds to make them extensible also makes them confusing, so we have left it out, but consider that they will always be extended in logical ways - for example new parameters, result fields or command. We will maintain backwards compatibility, but rigid checks against historic schemas will fail.

There are a lot of correctly formed documents according to the schemas that are error conditions. For example asking for a non-existant object... for example it is required that you ask the camera for it's objects to verify that the object you want to talk about does exist.

commands.xsd

```
<?xml version="1.0" encoding="UTF-8" ?>
```

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)



```
bjects -->
```

```
    <xsd:attribute name="name" type="objectName" use="required"/>
  </xsd:complexType>
```

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

```
d -->

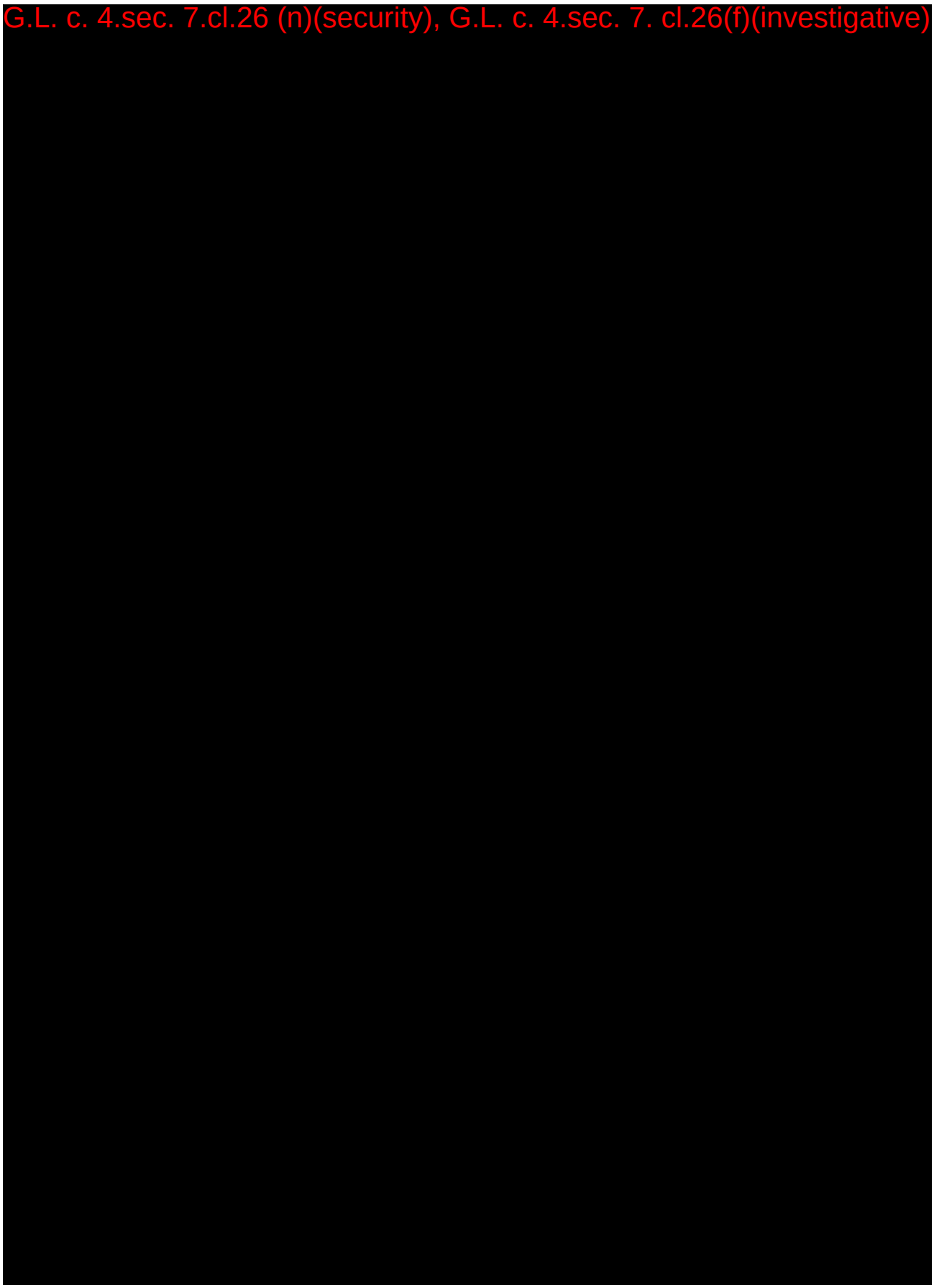
operty"/>

 a replacement is made available -->

 here -->

property/command objects. Also no nesting here -->
```

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)



each must connect with

-->

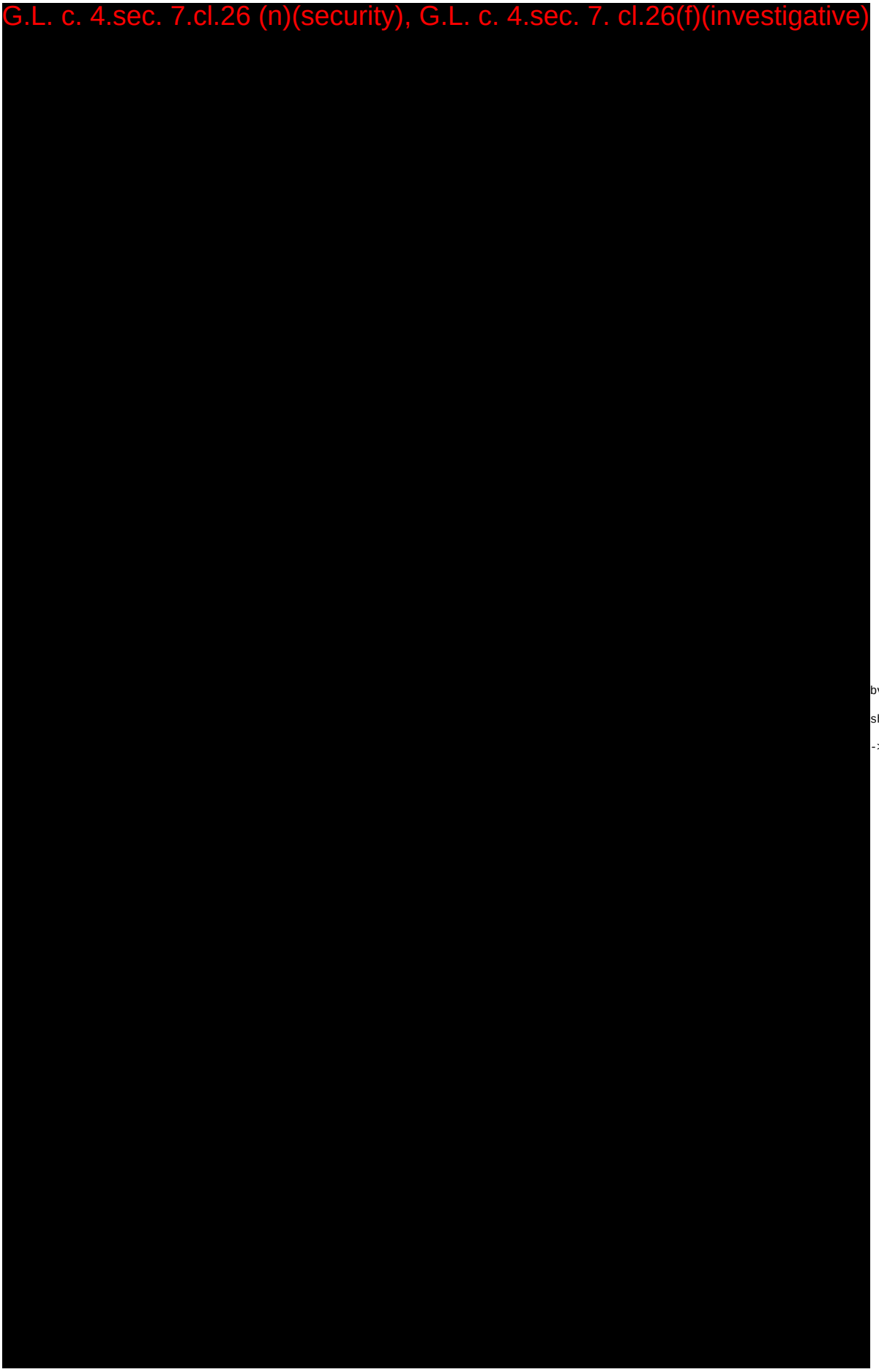
he sequence used is "ev

sing eventID 0 with pre
d as well as the curren

output.xsd

```
<?xml version="1.0" encoding="UTF-8" ?>
<xsd:schema  xmlns:xsd="http://www.w3.org/2001/XMLSchema">
```

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

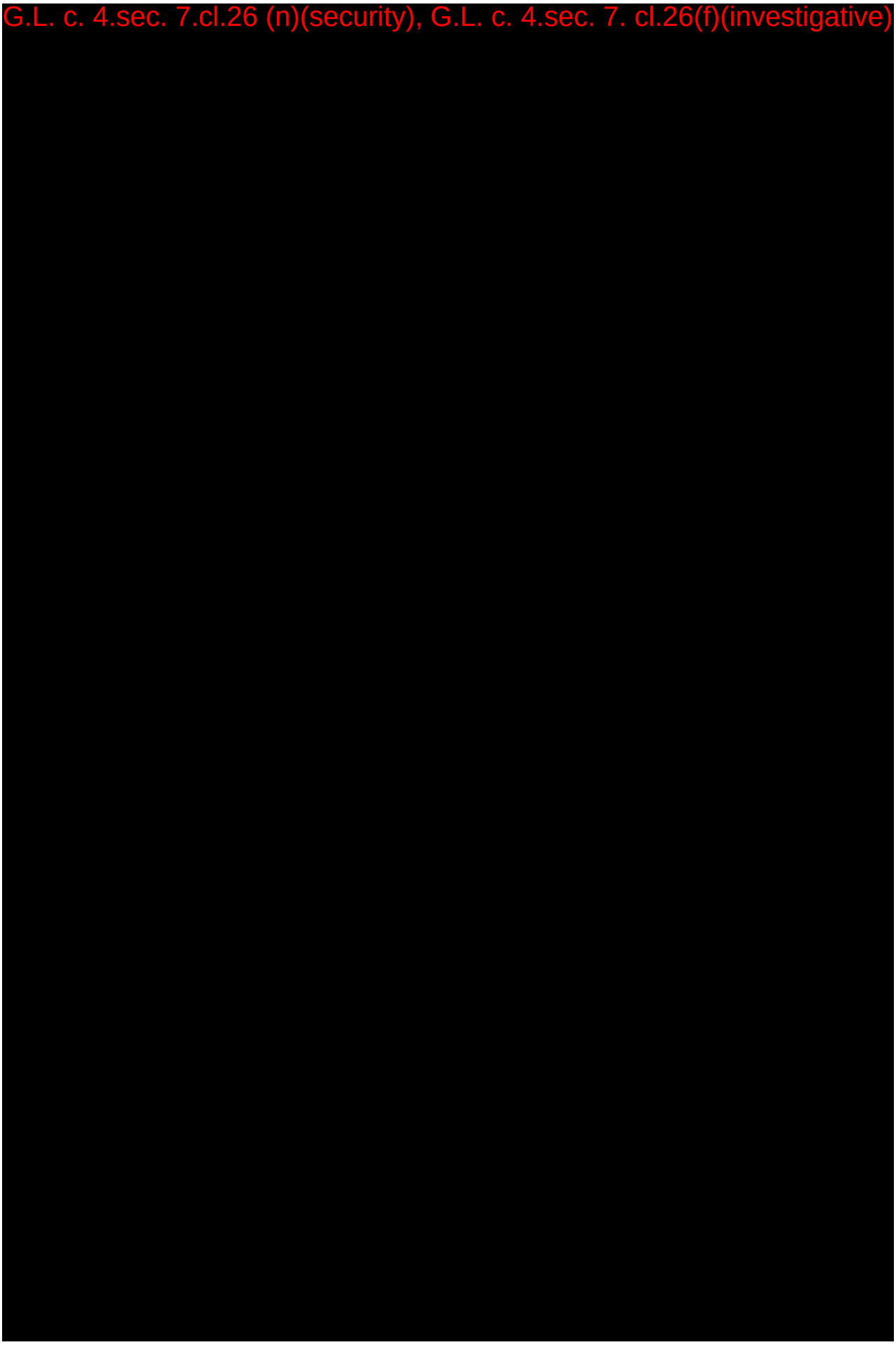


bvious -->

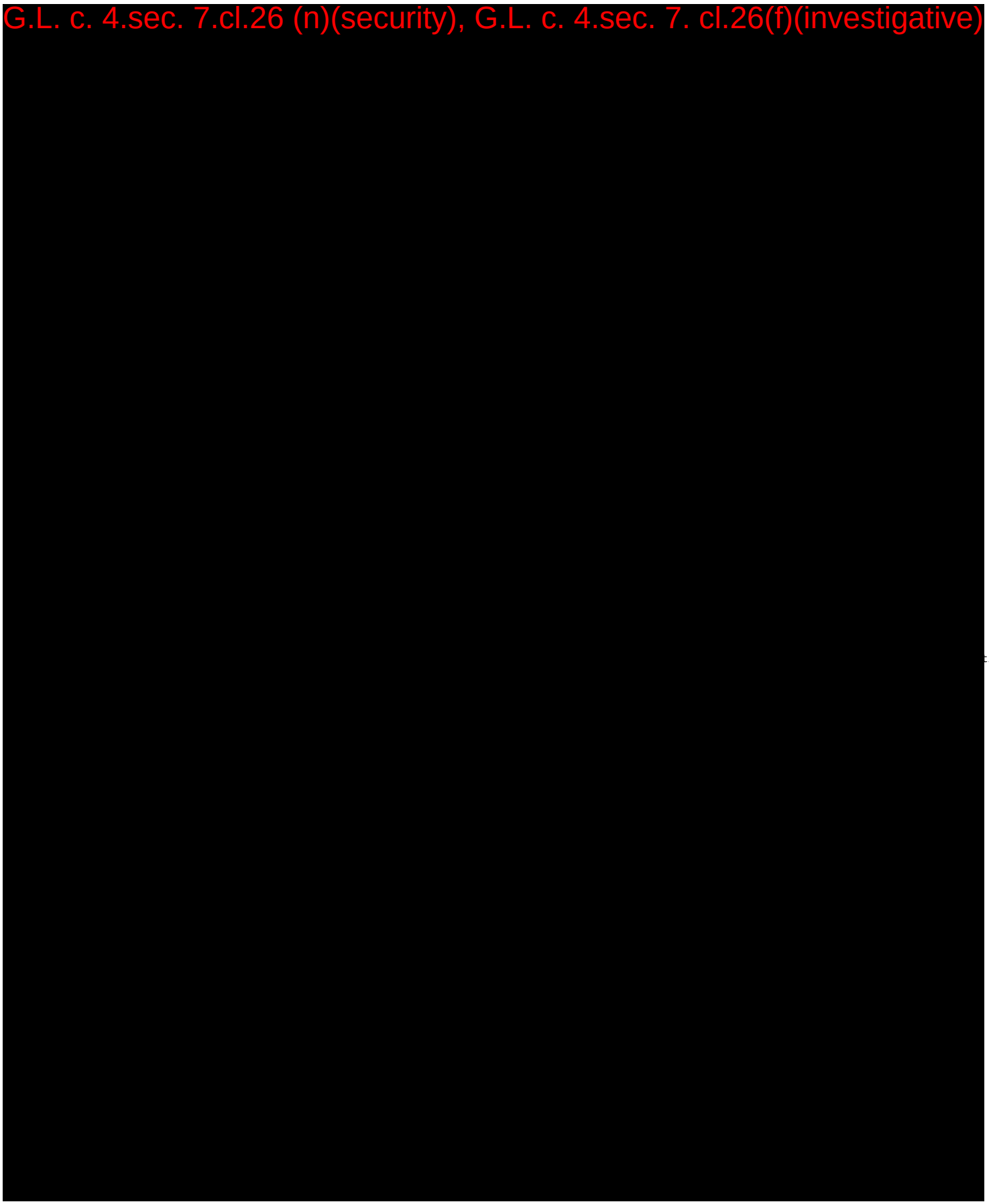
sh text describing failure -->

->

</xsd:group>


G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)



```
<xsd:complexType name="diagnosticEntry">
  <xsd:sequence>
    <xsd:element name="type" type="diagnosticType"/>
    <xsd:element name="resettable" type="xsd:boolean"/>
```

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

tate -->

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

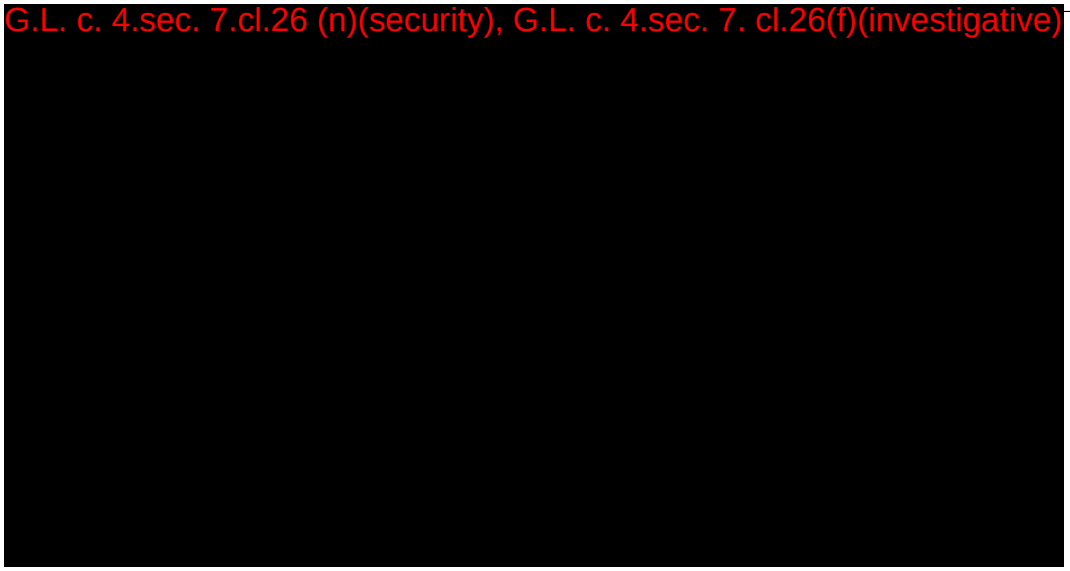
```
  </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="internalNameNoSpace">
  <xsd:restriction base="xsd:string">
```

G.L. c. 4.sec. 7.cl.26 (n)(security), G.L. c. 4.sec. 7. cl.26(f)(investigative)

not initate the save anyway -->

<xsd:sequence>



List of PIXI values

This is a list of all the eventDetails available on the camera and a description of them. The "image" types will return a length and offset, whereas the other types return data.

PIXI values image_*

The images from the cameras. Not all images are always available in all circumstances.

Platforms	Name	Type	Description
All	image_overview	image	The image from the overview taken at the same time as the plate was read, or at the same time as the trigger depending upon settings.
All	image_analysis	image	The full image from the camera from which the number plate was read. Usually this will be an infrared image.
All	image_readpatch	image	The image of the number plate, cropped so that the number plate is all that is visible.
All	image_hazoverview	image	The image from the overview taken at the same time as the hazard plate was read, or at the same time as the trigger depending upon settings.
All	image_hazanalysis	image	The full image from the camera from which the hazard plate was read. Usually this will be an infrared image.
All	image_hazreadpatch	image	The image of the hazard plate, cropped so that the hazard plate is all that is visible.

PIXI values cam_*

The camera detail of the plate the vehicle was read on

Platforms	Name	Type	Description
All	cam_shutter	xsd:integer	The shutter setting used for this image
All	cam_gain	xsd:integer	The gain setting used for this image
All	cam_cam0	xsd:integer	The camera number (starting at zero)

Platforms	Name	Type	Description
All	cam_cam1	xsd:integer	The camera number (starting at one)
All	cam_seq0	xsd:integer	The sequence setting (starting at zero)
All	cam_seq1	xsd:integer	The sequence setting (starting at one)

PIXI values hazcam_*

The camera detail of the hazard plate the vehicle was read on

Platforms	Name	Type	Description
All	hazcam_shutter	xsd:integer	The shutter setting used for this image
All	hazcam_gain	xsd:integer	The gain setting used for this image
All	hazcam_cam0	xsd:integer	The camera number (starting at zero)
All	hazcam_cam1	xsd:integer	The camera number (starting at one)
All	hazcam_seq0	xsd:integer	The sequence setting (starting at zero)
All	hazcam_seq1	xsd:integer	The sequence setting (starting at one)

PIXI values event_*

Unique information about delivery event, Not usable under all circumstances

Platforms	Name	Type	Description
All	event_id	xsd:integer	The Event id, which uniquly identifies the event

PIXI values file_*

Associated file. Not useable under all circumstances. Primarily for use in ACS's LPR files.

Platforms	Name	Type	Description
All	file_context1_file	xsd:string	The filename of context image 1
All	file_context2_file	xsd:string	The filename of context image 2
All	file_context3_file	xsd:string	The filename of context image 3
All	file_context4_file	xsd:string	The filename of context image 4
All	file_context5_file	xsd:string	The filename of context image 5
All	file_context6_file	xsd:string	The filename of context image 6
All	file_context7_file	xsd:string	The filename of context image 7
All	file_context8_file	xsd:string	The filename of context image 8
All	file_lpr	xsd:string	The lpr text filename
All	file_ir	xsd:string	The IR image filename
All	file_hazir	xsd:string	The hazard IR image filename
All	file_patch	xsd:string	The patch image filename
All	file_hazpatch	xsd:string	The hazard patch image filename
All	file_path	xsd:string	The transfer path (which is not prepended to the other filenames)
All	file_overview	xsd:string	The wide angle, overview image filename

Platforms	Name	Type	Description
All	file_hazoverview	xsd:string	The hazard wide angle, overview image filename

PIXI values hazard_*

The read hazard plate from the vehicle

Platforms	Name	Type	Description
All	hazard_classification	xsd:integer	The anpr classification (not useful with many ANPR engines)
All	hazard_asyncpayload	xsd:string	The OEM asynchronous payload. Asynchronous messages injected via serial (or TCP) will be associated with messages based on a closest match within a window. Otherwise an empty string.
All	hazard_readconfidence	xsd:integer	The confidence of the hazard plate read
All	hazard_readconfidencecat	xsd:integer	The confidence category of the hazard plate read
All	hazard_platefinderconfidence	xsd:integer	The confidence of the hardware platefinder
All	hazard_fieldnum	xsd:integer	The field number
All	hazard_natcode	xsd:integer	The nationality code (not generally useful, see HN which is)
All	hazard_nationality	xsd:string	The nationality (country and state) of origin of this plate if known
All	hazard_tiggeroffset	xsd:integer	The time offset between the trigger time and the image associated with this read (milliseconds). If not triggered, will be 0
All	hazard_text	xsd:string	The text of the hazard plate
All	hazard_numreads	xsd:integer	The total number of reads associated with the trigger that caused this plateread (A single trigger can lead to >1 plateread event). For a NOREAD the value will still be 1.
All	hazard_syntaxconfidence	xsd:integer	The syntax confidence of the hazard plate read. This is a measure of how confident we are that the hazard plate matched the syntax of the reported country or state.
All	hazard_tag	xsd:string	The plate tag, as extracted from the vehicle filter database. Will be blank if no tag entered, the plate is not matched, or the filter is off
All	hazard_triggerpayload	xsd:string	The OEM trigger payload. If you are using serial (or TCP/IP) triggers, this will be the OEM content of those, otherwise it will be boring. Text 'auto' will be returned if not triggered
All	hazard_xpos	xsd:integer	The x position of the plate's left edge in pixels
All	hazard_width	xsd:integer	The width of the plate in pixels
All	hazard_ypos	xsd:integer	The y position of the plate's top edge in pixels
All	hazard_height	xsd:integer	The height of the plate in pixels

PIXI values heartbeat_*

The camera heartbeat delivery

Platforms	Name	Type	Description
All	heartbeat_attemptcount	xsd:integer	The count of heartbeat delivery attempts.
All	heartbeat_failurecount	xsd:integer	The count of heartbeat delivery failures.
All	heartbeat_statusbits	xsd:integer	A camera status bitfield (legacy).

PIXI values imglocaltime_*

The image timestamp, the moment the image for the vehicle was captured.

This is a local time and accounts for timezone and daylight saving

Platforms	Name	Type	Description
All	imglocaltime_ampm	xsd:string	The string am for the morning, pm for the afternoon
All	imglocaltime_ctime	xsd:integer	Seconds since midnight 1st of January 1970 (commonly known as C time). This is UTC always, included for completeness.
All	imglocaltime_day	xsd:integer	The day of the month
All	imglocaltime_dayyear	xsd:integer	The day of the year, with January the 1st as zero
All	imglocaltime_hour	xsd:integer	The hour, 24 hour clock
All	imglocaltime_hour12	xsd:integer	The hour, 12 hour clock
All	imglocaltime_millisecond	xsd:integer	Milliseconds
All	imglocaltime_locked	xsd:integer	Indicates if time is locked via NTP
All	imglocaltime_locked_text	xsd:string	Indicates if time is locked via NTP as a string
All	imglocaltime_minute	xsd:integer	Minutes past the hour
All	imglocaltime_tenmin	xsd:integer	Tens of minutes past the hour
All	imglocaltime_month	xsd:integer	Month of the year (January as one)
All	imglocaltime_monthname	xsd:string	Month of the year as a word, in English
All	imglocaltime_monthnamesh	xsd:string	Month of the year as three letter shortened word, in English
All	imglocaltime_second	xsd:integer	Seconds past the minute
All	imglocaltime_tenthsecond	xsd:integer	Tenths of seconds
All	imglocaltime_hundredthsecond	xsd:integer	Hundredths of seconds
All	imglocaltime_daylight	xsd:integer	One if daylight saving is in effect, zero otherwise
All	imglocaltime_dayweek	xsd:integer	The day of the week as a number, with zero being Sunday
All	imglocaltime_dayweekname	xsd:string	The day of the week as a word, in English
All	imglocaltime_dayweeknamesh	xsd:string	The day of the week as a three letter shortened word, in English
All	imglocaltime_year	xsd:integer	The year
All	imglocaltime_year2	xsd:integer	The last two digits of the year

PIXI values imgutctime_*

The image timestamp, the moment the image for the vehicle was captured.

This is UTC time (like GMT)

Platforms	Name	Type	Description
All	imgutctime_ampm	xsd:string	The string am for the morning, pm for the afternoon
All	imgutctime_ctime	xsd:integer	Seconds since midnight 1st of January 1970 (commonly known as C time)
All	imgutctime_day	xsd:integer	The day of the month
All	imgutctime_dayyear	xsd:integer	The day of the year, with January the 1st as zero
All	imgutctime_hour	xsd:integer	The hour, 24 hour clock
All	imgutctime_hour12	xsd:integer	The hour, 12 hour clock
All	imgutctime_millisecond	xsd:integer	Milliseconds
All	imgutctime_locked	xsd:integer	Indicates if time is locked via NTP
All	imgutctime_locked_text	xsd:string	Indicates if time is locked via NTP as a string
All	imgutctime_minute	xsd:integer	Minutes past the hour
All	imgutctime_tenmin	xsd:integer	Tens of minutes past the hour
All	imgutctime_month	xsd:integer	Month of the year (January as one)
All	imgutctime_monthname	xsd:string	Month of the year as a word, in English
All	imgutctime_monthnamesh	xsd:string	Month of the year as three letter shortened word, in English
All	imgutctime_second	xsd:integer	Seconds past the minute
All	imgutctime_tenthsecond	xsd:integer	Tenths of seconds
All	imgutctime_hundredthsecond	xsd:integer	Hundredths of seconds
All	imgutctime_daylight	xsd:integer	One if daylight saving is in effect, zero otherwise
All	imgutctime_dayweek	xsd:integer	The day of the week as a number, with zero being Sunday
All	imgutctime_dayweekname	xsd:string	The day of the week as a word, in English
All	imgutctime_dayweeknamesh	xsd:string	The day of the week as a three letter shortened word, in English
All	imgutctime_year	xsd:integer	The year
All	imgutctime_year2	xsd:integer	The last two digits of the year

PIXI values jpeg_*

JPEG data. Not useable under all circumstances. Primarily for use in output filenames to distinguish between them.

Platforms	Name	Type	Description
All	jpeg_type	xsd:string length='1'	The file type. Will be p for a patch, n for an IR image, and w for an overview wide angle image. Context images will be 1 (for context 1), 2 (for context 2). Currently up to 8 context images are supported.

PIXI values location_*

The location of the camera

Platforms	Name	Type	Description
All	location_latitude	xsd:integer	The whole number of degrees of latitude (north or south). Will always be positive.

Platforms	Name	Type	Description
All	location_longitude	xsd:integer	The whole number of degrees of longitude (east or west). Will always be positive.
All	location_north	xsd:integer	The whole number of degrees north we are. Will be negative if we are south.
All	location_east	xsd:integer	The whole number of degrees east we are. Will be negative if we are west.
All	location_millideglat	xsd:integer	The number of millidegrees of latitude we are away from the nearest degree.
All	location_millideglong	xsd:integer	The number of millidegrees of longitude we are away from the nearest degree.
All	location_microdeglat	xsd:integer	The number of microdegrees of latitude we are away from the nearest degree.
All	location_microdeglong	xsd:integer	The number of microdegrees of longitude we are away from the nearest degree.
All	location_ns	xsd:string length='1'	A character for latitude, N (north) or S (south) depending upon which hemisphere the location represents.
All	location_ew	xsd:string length='1'	A character for longitude, E (east) or W (west) depending upon which side of the meridian the location represents.
All	location_minlatitude	xsd:integer	The number of minutes of latitude (north or south) that we are away from the nearest whole degree. Will always be positive.
All	location_minlongitude	xsd:integer	The number of minutes of longitude (east or west) that we are away from the nearest whole degree. Will always be positive.
All	location_minlatitudetotal	xsd:integer	The number of minutes of latitude (north or south) that we are away from the equator. Will always be positive.
All	location_minlongitudetotal	xsd:integer	The number of minutes of longitude (east or west) that we are away from the equator. Will always be positive.
All	location_minnorthtotal	xsd:integer	The number of minutes north that we are away from the equator. Will be negative if we are south.
All	location_mineasttotal	xsd:integer	The number of minutes east that we are away from the equator. Will be negative if we are south.
All	location_milliminuteslat	xsd:integer	The number of milliminutes of latitude we are away from the nearest minute.
All	location_milliminuteslong	xsd:integer	The number of milliminutes of longitude we are away from the nearest minute.
All	location_microminuteslat	xsd:integer	The number of microminutes of latitude we are away from the nearest minute.
All	location_microminuteslong	xsd:integer	The number of microminutes of longitude we are away from the nearest minute.
All	location_validity	xsd:string	The string Valid or Invalid depending upon whether the location is deemed good.

PIXI values globalmeta_*

Metadata strings from the Metadata object. This is purely here so you can have the same format strings on all sites, and just change the metadata in this store

Platforms	Name	Type	Description
All	globalmeta_a	xsd:string	Metadata string a
All	globalmeta_b	xsd:string	Metadata string b
All	globalmeta_c	xsd:string	Metadata string c
All	globalmeta_d	xsd:string	Metadata string d
All	globalmeta_e	xsd:string	Metadata string e
All	globalmeta_f	xsd:string	Metadata string f
All	globalmeta_g	xsd:string	Metadata string g
All	globalmeta_h	xsd:string	Metadata string h
All	globalmeta_i	xsd:string	Metadata string i
All	globalmeta_j	xsd:string	Metadata string j
All	globalmeta_k	xsd:string	Metadata string k
All	globalmeta_l	xsd:string	Metadata string l
All	globalmeta_m	xsd:string	Metadata string m
All	globalmeta_n	xsd:string	Metadata string n
All	globalmeta_o	xsd:string	Metadata string o
All	globalmeta_p	xsd:string	Metadata string p
All	globalmeta_q	xsd:string	Metadata string q
All	globalmeta_r	xsd:string	Metadata string r
All	globalmeta_s	xsd:string	Metadata string s
All	globalmeta_t	xsd:string	Metadata string t
All	globalmeta_u	xsd:string	Metadata string u
All	globalmeta_v	xsd:string	Metadata string v
All	globalmeta_w	xsd:string	Metadata string w
All	globalmeta_x	xsd:string	Metadata string x
All	globalmeta_y	xsd:string	Metadata string y
All	globalmeta_z	xsd:string	Metadata string z

PIXI values timeoffset_*

The time offsets of overview context images

Platforms	Name	Type	Description
All	timeoffset_context1	xsd:integer	The offset (in milliseconds) of context image 1 measured from the vehicle event timestamp
All	timeoffset_context2	xsd:integer	The offset (in milliseconds) of context image 2 measured from the vehicle event timestamp
All	timeoffset_context3	xsd:integer	The offset (in milliseconds) of context image 3 measured from the vehicle event timestamp
All	timeoffset_context4	xsd:integer	The offset (in milliseconds) of context image 4 measured from the vehicle event timestamp
All	timeoffset_context5	xsd:integer	The offset (in milliseconds) of context image 5 measured from the vehicle event timestamp
All	timeoffset_context6	xsd:integer	The offset (in milliseconds) of context image 6 measured from the vehicle event timestamp

Platforms	Name	Type	Description
All	timeoffset_context7	xsd:integer	The offset (in milliseconds) of context image 7 measured from the vehicle event timestamp
All	timeoffset_context8	xsd:integer	The offset (in milliseconds) of context image 8 measured from the vehicle event timestamp

PIXI values plate_*

The read number plate from the vehicle

Platforms	Name	Type	Description
All	plate_isoalpha2	xsd:string	The 2-character nationality of origin of this plate if known, as defined by ISO 3166-1
All	plate_isoalpha3	xsd:string	The 3-character nationality of origin of this plate if known, as defined by ISO 3166-1
All	plate_classification	xsd:integer	The anpr classification (not useful with many ANPR engines)
All	plate_asyncpayload	xsd:string	The OEM asynchronous payload. Asynchronous messages injected via serial (or TCP) will be associated with messages based on a closest match within a window. Otherwise an empty string.
All	plate_readconfidence	xsd:integer	The confidence of the plate read
All	plate_readconfidencecat	xsd:integer	The confidence category of the plate read
All	plate_direction	xsd:string	The direction of travel of the plate read. This will be one of the following strings: AWAY, TOWARD, NOTSET. If NOTSET it indicates the direction could not be determined.
All	plate_isosubdivision	xsd:string	The subdivision of origin of this plate if known, as defined by ISO 3166-2
All	plate_platefinderconfidence	xsd:integer	The confidence of the hardware platefinder
All	plate_fieldnum	xsd:integer	The field number
All	plate_trigsource	xsd:string	The source of OEM trigger
All	plate_tcppayload	xsd:string	The OEM trigger payload from the first TCP/IP trigger
All	plate_triggerId	xsd:integer	The trigger identifier.
All	plate_laneId	xsd:string	The lane in which the plate is located.
All	plate_natcode	xsd:integer	The nationality code (not generally useful, see PN which is)
All	plate_nationality	xsd:string	The nationality (country and state) of origin of this plate if known
All	plate_triggeroffset	xsd:integer	The time offset between the trigger time and the image associated with this read (milliseconds). If not triggered, will be 0
All	plate_text	xsd:string	The text of the plate
All	plate_numreads	xsd:integer	The total number of reads associated with the trigger that caused this plateread (A single trigger can lead to >1 plateread event). For a NOREAD the value will still be 1.
All	plate_syntaxconfidence	xsd:integer	

Platforms	Name	Type	Description
			The syntax confidence of the plate read. This is a measure of how confident we are that the plate matched the syntax of the reported country or state.
All	plate_serialpayload	xsd:string	The OEM trigger payload from the first Serial trigger
All	plate_tag	xsd:string	The plate tag, as extracted from the vehicle filter database. Will be blank if no tag entered, the plate is not matched, or the filter is off
All	plate_triggerpayload	xsd:string	The OEM trigger payload. If you are using serial (or TCP/IP) triggers, this will be the OEM content of those, otherwise it will be boring. Text 'auto' will be returned if not triggered
All	plate_xpos	xsd:integer	The x position of the plate's left edge in pixels
All	plate_width	xsd:integer	The width of the plate in pixels
All	plate_ypos	xsd:integer	The y position of the plate's top edge in pixels
All	plate_height	xsd:integer	The height of the plate in pixels

PIXI values triglocaltime_*

The trigger timestamp, the moment the trigger started. You should probably be using T instead of this, as if the event was not a triggered one you will not get anything in the string with R.

This is a local time and accounts for timezone and daylight saving

Platforms	Name	Type	Description
All	triglocaltime_ampm	xsd:string	The string am for the morning, pm for the afternoon
All	triglocaltime_ctime	xsd:integer	Seconds since midnight 1st of January 1970 (commonly known as C time). This is UTC always, included for completeness.
All	triglocaltime_day	xsd:integer	The day of the month
All	triglocaltime_dayyear	xsd:integer	The day of the year, with January the 1st as zero
All	triglocaltime_hour	xsd:integer	The hour, 24 hour clock
All	triglocaltime_hour12	xsd:integer	The hour, 12 hour clock
All	triglocaltime_millisecond	xsd:integer	Milliseconds
All	triglocaltime_minute	xsd:integer	Minutes past the hour
All	triglocaltime_tenmin	xsd:integer	Tens of minutes past the hour
All	triglocaltime_month	xsd:integer	Month of the year (January as one)
All	triglocaltime_monthname	xsd:string	Month of the year as a word, in English
All	triglocaltime_monthnamesh	xsd:string	Month of the year as three letter shortened word, in English
All	triglocaltime_second	xsd:integer	Seconds past the minute
All	triglocaltime_tenthsecond	xsd:integer	Tenths of seconds
All	triglocaltime_hundredthsecond	xsd:integer	Hundredths of seconds
All	triglocaltime_daylight	xsd:integer	One if daylight saving is in effect, zero otherwise
All	triglocaltime_dayweek	xsd:integer	The day of the week as a number, with zero being Sunday
All	triglocaltime_dayweekname	xsd:string	The day of the week as a word, in English

Platforms	Name	Type	Description
All	triglocaltime_dayweeknamesh	xsd:string	The day of the week as a three letter shortened word, in English
All	triglocaltime_year	xsd:integer	The year
All	triglocaltime_year2	xsd:integer	The last two digits of the year

PIXI values trigutctime_*

The trigger timestamp, the moment the trigger started. You should probably be using t instead of this, as if the event was not a triggered one you will not get anything in the string with r.

This is UTC time (like GMT)

Platforms	Name	Type	Description
All	trigutctime_ampm	xsd:string	The string am for the morning, pm for the afternoon
All	trigutctime_ctime	xsd:integer	Seconds since midnight 1st of January 1970 (commonly known as C time)
All	trigutctime_day	xsd:integer	The day of the month
All	trigutctime_dayyear	xsd:integer	The day of the year, with January the 1st as zero
All	trigutctime_hour	xsd:integer	The hour, 24 hour clock
All	trigutctime_hour12	xsd:integer	The hour, 12 hour clock
All	trigutctime_millisecond	xsd:integer	Milliseconds
All	trigutctime_minute	xsd:integer	Minutes past the hour
All	trigutctime_tenmin	xsd:integer	Tens of minutes past the hour
All	trigutctime_month	xsd:integer	Month of the year (January as one)
All	trigutctime_monthname	xsd:string	Month of the year as a word, in English
All	trigutctime_monthnamesh	xsd:string	Month of the year as three letter shortened word, in English
All	trigutctime_second	xsd:integer	Seconds past the minute
All	trigutctime_tenthsecond	xsd:integer	Tenths of seconds
All	trigutctime_hundredthsecond	xsd:integer	Hundredths of seconds
All	trigutctime_daylight	xsd:integer	One if daylight saving is in effect, zero otherwise
All	trigutctime_dayweek	xsd:integer	The day of the week as a number, with zero being Sunday
All	trigutctime_dayweekname	xsd:string	The day of the week as a word, in English
All	trigutctime_dayweeknamesh	xsd:string	The day of the week as a three letter shortened word, in English
All	trigutctime_year	xsd:integer	The year
All	trigutctime_year2	xsd:integer	The last two digits of the year

PIXI values site_*

The site details for this unit

Platforms	Name	Type	Description
All	site_hostname	xsd:string	The site's hostname, the recommended way of identifying a site

Platforms	Name	Type	Description
All	site_libver	xsd:integer	The system's library version number
All	site_serialnumber	xsd:integer	The system's serial number
All	site_appver	xsd:integer	The system's application version number

PIXI values supplementary_*

The supplementary images details

Platforms	Name	Type	Description
All	supplementary_1_offset	xsd:integer	The offset (in milliseconds) of supplementary image 1 measured from the vehicle event timestamp
All	supplementary_2_offset	xsd:integer	The offset (in milliseconds) of supplementary image 2 measured from the vehicle event timestamp
All	supplementary_1_seq1	xsd:integer	Supplementary image 1 sequence setting (starting at one)
All	supplementary_2_seq1	xsd:integer	Supplementary image 2 sequence setting (starting at one)
All	supplementary_1_shutter	xsd:integer	Supplementary image 1 shutter setting
All	supplementary_2_shutter	xsd:integer	Supplementary image 2 shutter setting
All	supplementary_1_gain	xsd:integer	Supplementary image 1 gain setting
All	supplementary_2_gain	xsd:integer	Supplementary image 2 gain setting

PIXI values localtime_*

The timestamp for the vehicle, which is the trigger timestamp if the vehicle was triggered (see R), or the image timestamp if it was not (see I).

This is a local time and accounts for timezone and daylight saving

Platforms	Name	Type	Description
All	localtime_ampm	xsd:string	The string am for the morning, pm for the afternoon
All	localtime_ctime	xsd:integer	Seconds since midnight 1st of January 1970 (commonly known as C time). This is UTC always, included for completeness.
All	localtime_day	xsd:integer	The day of the month
All	localtime_dayyear	xsd:integer	The day of the year, with January the 1st as zero
All	localtime_hour	xsd:integer	The hour, 24 hour clock
All	localtime_hour12	xsd:integer	The hour, 12 hour clock
All	localtime_millisecond	xsd:integer	Milliseconds
All	localtime_minute	xsd:integer	Minutes past the hour
All	localtime_tenmin	xsd:integer	Tens of minutes past the hour
All	localtime_month	xsd:integer	Month of the year (January as one)
All	localtime_monthname	xsd:string	Month of the year as a word, in English
All	localtime_monthnamesh	xsd:string	Month of the year as three letter shortened word, in English
All	localtime_second	xsd:integer	Seconds past the minute

Platforms	Name	Type	Description
All	localtime_tenthsecond	xsd:integer	Tenths of seconds
All	localtime_hundredthsecond	xsd:integer	Hundredths of seconds
All	localtime_daylight	xsd:integer	One if daylight saving is in effect, zero otherwise
All	localtime_dayweek	xsd:integer	The day of the week as a number, with zero being Sunday
All	localtime_dayweekname	xsd:string	The day of the week as a word, in English
All	localtime_dayweeknamesh	xsd:string	The day of the week as a three letter shortened word, in English
All	localtime_year	xsd:integer	The year
All	localtime_year2	xsd:integer	The last two digits of the year

PIXI values utctime_*

The timestamp for the vehicle, which is the trigger timestamp if the vehicle was triggered (see r), or the image timestamp if it was not (see i).

This is UTC time (like GMT)

Platforms	Name	Type	Description
All	utctime_ampm	xsd:string	The string am for the morning, pm for the afternoon
All	utctime_ctime	xsd:integer	Seconds since midnight 1st of January 1970 (commonly known as C time)
All	utctime_day	xsd:integer	The day of the month
All	utctime_dayyear	xsd:integer	The day of the year, with January the 1st as zero
All	utctime_hour	xsd:integer	The hour, 24 hour clock
All	utctime_hour12	xsd:integer	The hour, 12 hour clock
All	utctime_millisecond	xsd:integer	Milliseconds
All	utctime_minute	xsd:integer	Minutes past the hour
All	utctime_tenmin	xsd:integer	Tens of minutes past the hour
All	utctime_month	xsd:integer	Month of the year (January as one)
All	utctime_monthname	xsd:string	Month of the year as a word, in English
All	utctime_monthnamesh	xsd:string	Month of the year as three letter shortened word, in English
All	utctime_second	xsd:integer	Seconds past the minute
All	utctime_tenthsecond	xsd:integer	Tenths of seconds
All	utctime_hundredthsecond	xsd:integer	Hundredths of seconds
All	utctime_daylight	xsd:integer	One if daylight saving is in effect, zero otherwise
All	utctime_dayweek	xsd:integer	The day of the week as a number, with zero being Sunday
All	utctime_dayweekname	xsd:string	The day of the week as a word, in English
All	utctime_dayweeknamesh	xsd:string	The day of the week as a three letter shortened word, in English
All	utctime_year	xsd:integer	The year
All	utctime_year2	xsd:integer	The last two digits of the year

Appendix A. Technical Details

Communication

Console Serial RS-232

The console runs at a fixed line speed of 38,400 bits per second with 8 bits of data, no parity and 1 stop bit. This is often abbreviated to 38,400 8N1. Hardware flow control is not supported, Xon/Xoff can be used, but no flow control also works.

Ethernet

The ethernet port is wired to the four Ethernet wires.

The ethernet port is 100BASE-TX autosensing 10/100 Mbit/s and full/half duplex over twisted pair. You must use Category 5e cable to make full use of the bandwidth of the connection, and are limited to 100metres total cable length from the camera to the receiver. If you are having problems with the ethernet link being intermittent or unreliable do ensure your cable meets full Cat 5e specification. The camera will work with a hub or switch with a "straight through" cable (pin 1 to 1, pin 2 to 2) or with a "cross-over" cable directly into the back of a PC. The camera will *not* autosense the RX and TX pairs so you must use the correct cable type for the far end unless that will autosense.

Although the camera is capable of 100Base-TX Full Duplex and will often negotiate to that given an appropriate other end point, sometimes the cable in between is not up to Cat 5e standards and running over long distances will drop packets. It is possible to force the camera to slow down or change to half duplex using a linux command called mii-tool.

`mii-tool` {-F} {*`10baseT-HD`*}
will force set it to 10 Mbit/s and half duplex. mii-tool has many other options, which are detailed below in the manual page for it.

If you need to make a permanent change to the speed of the camera's ethernet link you can put the command into `/etc/conf.d/local.start`, either using nano or by going to the System → Bootup and Shutdown page of webmin where you can edit the same file.

mii-tool

view, manipulate media-independent interface status

`mii-tool` [-v, --verbose] [-V, --version] [-R, --reset] [-r, --restart] [-w, --watch] [-l, --log] [-A, --advertise=*`media,`* ...] [-F, --force=*`media`*] [*`interface`*...]

This utility checks or sets the status of a network interface's Media Independent Interface (MII) unit. Most fast ethernet adapters use an MII to autonegotiate link speed and duplex setting.

Most intelligent network devices use an autonegotiation protocol to communicate what media technologies they support, and then select the fastest mutually supported media technology. The `-A` or `--advertise` options can be used to tell the MII to only advertise a subset of its capabilities. Some passive devices, such as single-speed hubs, are unable to autonegotiate. To handle such devices, the MII protocol also allows for establishing a link by simply detecting either a 10baseT or 100baseT link beat. The `-F` or `--force` options can be used to force the MII to operate in one mode, instead of autonegotiating. The `-A` and `-F` options are mutually exclusive.

The default short output reports the negotiated link speed and link status for each interface. If an interface or interfaces are not specified on the command line, then **mii-tool** will check any available interfaces from *eth0* through *eth7*.

`-v`, `--verbose` — Display more detailed MII status information. If used twice, also display raw MII register contents.

`-V`, `--version`	Display program version information.
`-R`, `--reset`	Reset the MII to its default configuration.
`-r`, `--restart`	Restart autonegotiation.
`-w`, `--watch`	Watch interface(s) and report changes in link status. The MII interfaces are polled at one second intervals.
`-l`, `--log`	Used with `-w`, records link status changes in the system log instead of printing on standard output.
`-F` *media*, `--force=`*media*	Disable autonegotiation, and force the MII to either *100baseTx-FD*, *100baseTx-HD*, *10baseT-FD*, or *10baseT-HD* operation.
`-A` *media,...*, `--advertise=`*media,...*	Enable and restart autonegotiation, and advertise only the specified media technologies. Multiple technologies should be separated by commas. Valid media are *100baseT4*, *100baseTx-FD*, *100baseTx-HD*, *10baseT-FD*, and *10baseT-HD*.

Diagnostics

SIOCGMIIPHY on 'eth?' failed: Invalid argument	If the interface is not running (up), kernel will refuse to report its link state.
SIOCGMIIPHY on 'eth?' failed: Operation not permitted	Most kernels restrict access to root.
SIOCGMIIPHY on 'eth?' failed: No such device	This error is shown, if the kernel does not know about the named device.
SIOCGMIIPHY on 'eth?' failed: Operation not supported	The interface in question does not support MII queries. Most likely, it does not have MII transceivers, at all.

Network details

The P382, P392+ and P492 are network capable cameras which make extensive use of TCP/IP and UDP/IP. They also use raw ethernet packets with type 0xAC01 for local configuration of the IP address details (sometimes known as IP Discovery or Remote IP Configuration). In case you need to pass TCP/IP or UDP/IP through a firewall or network translation device this table lists the appropriate ports.

Table A.1. TCP/IP and UDP/IP Port numbers

Port used for	Port type	Port number
SSH Shell	TCP/IP Server	22
Webmin secure HTTP	TCP/IP Server	443
Viewfinder	TCP/IP Server	9000
Client	TCP/IP Server	3570
PIXI (Unsecured, recommend an SSH tunnel to access). Usually firewalled on camera.	TCP/IP Server	3382
ACS	when FTP Client	21 plus ephemeral data ports
ACS	when SCP/SSH Client	22
NTP (where used)	UDP Client	123
Portmapper (where used for NFS)	UDP and TCP Server	111
NFS (where used)	UDP and TCP	2049
VES	TCP Server	Configurable, defaults [redacted] through [redacted] inclusive)
UDP Ping (may be used by VES)	UDP	10010
Ping	ICMP	No port for ICMP
TCP Trigger	TCP	3820
UTMC	TCP Server	Configurable

Filesystem layout

As you may well discover, the camera's root filesystem is mounted read-only to prevent accidental corruption. This section of the manual documents how the file system is layed out, and what goes where. A base knowledge of linux filesystems, disks, partitions and nomeclature for these is expected to be able to read this section.

There are flash devices within the camera, the internal flash, and the compact flash/SD card (not user removable). The internal flash is no longer used. The other flash card may vary in size, but only any space over 512Mb is available for user storage. It is a build to order option to have storage space in the camera.

On the P382 The flash is `/dev/hda` and on the P392+/P492 is `/dev/mmcblk0` and is partitioned into 5 sections as follows:

- 1 - This is the boot device. On the P382 it contains GRUB, the bootloader and the kernels. On the P392+/P492 it doesn't contain very much - all the boot data is held in NOR flash which is not accessible from linux. It is vital for booting, and there is no alternative. It is not usually mounted, so should be safe from damage. When mounted it exists as `/boot`
- 2 - This is the root filesystem. It is normally mounted as `/` *read only*.
- 5 - It is mounted as `/var` and is used for storing logging information and other run time data.
- 6 - It is mounted as `/opt` and is used for storing the PIPS application, libraries and configuration information. `/opt/pips` contains the ANPR reading engine, the application, the shell and other application files. `/opt/config/current` is a symbolic link to the current configuration of the camera including the usual `/etc`. You should back up `/opt/config/current` to preserve the state of a camera.
- 7 - It is mounted as `/storage` and is used for storing PIPS application data. All output from the camera application goes into this directory. If you have not purchased a larger than 512Mb compact flash this area will be small and should not be used for storage. You can (and should if you want to do this) mount a network filesystem under this directory to store files off camera.

Partition 1 on disk hda is known as `/dev/hda1` and on disk mmcblk0 it is known as `/dev/mmcblk0p1`.

Most of the filesystem is “normal linux” and adheres to the Linux Filesystem Standard (see http://tldp.org/LDP/Linux-Filesystem-Hierarchy/html/). Here are a few highlights and P382, P392+ and P492 specifics:

- `/etc` contains system specific configuration.
  - `fstab` mounted filesystems, included those mounted at boot. You can manipulate this in webmin, see the section called “Mounting network disks” [13]
  - `init.d/` several startup scripts, including those used to start the application and network
- `/opt/pips` contains the PIPS specific code including the applications.
  - `camera_app` the camera application which does ANPR and runs all the output modules
  - `libpipslinux.so.*` the shared library written by PIPS, used by all our applications on the camera
  - `libcardet*` are the ANPR libraries for reading plates. See the section called “Camera control” [13] to manipluate these.
  - `s2driver*` the kernel module (think of it like a windows device driver) for the PCI interface to the cameras and platefinder.
  - `ipconfigd` the IPDiscovery responder, this is what you're using when you use IP Discovery. This is started from `/etc/conf.d/local.start`
  - `modempulse` simple application which assists in turning the modem (where fitted) on and off.
  - `*.msc, *.isc, xcf08p_vo_48_1532.bsd, prog_prom*, jdrive, instfpga.pl` Files for setting up the FPGA. `instfpga.pl` uses the other files appropriately to reprogram the FPGA. Once the FPGA is programmed the camera will need rebooting.
  - `pipsshell` is the camera application's shell, see Chapter 6, *PIPS ANPR Shell* [15].
  - `uid.pl` generates a unique ID for this camera for use in VES.
  - `netmon.pl` manages the network and NTP on the camera.
- `/opt/config` contains all local configuration.
  - `current` is a symbolic link to the current configuration. You can use this to quickly switch configurations if you understand how to maniplate symbolic links.
  - `current/state.xml` is the camera script, containing all the configuration used by the camera application. This is XML, and must be correct or we will discard it. Hand edits are possible, but do take care. You can check it with **`xmllint`**
  - `current/netmon.xml` is the network configuration script. This is XML, and must be correct or we will discard it. Hand edits are possible, but do take care. You can check it with **`xmllint`**
  - `current/etc` is the actual `/etc` which is linked to here
- `/var` writable area used by linux. In particular contains linux's log files, see `log/messages` in particular. Equivalent of the event log on the P372.
- `/storage` writable area used by our application. This is user storage and all paths you enter in the application are relative to this directory, so entering `foo` as a directory will store the files in `/storage/foo`. This will contain the compact flash storage size minus 500Mb.

Backup

On the P392+ and P492 cameras (and only these models) should have the /backup.pl script run from the command line after any change - once that change is determined to be satisfactory. Changes include:

- New OS and application installations
- Application upgrades, Cardet upgrades
- Configuration changes

Appendix B. Software installation and upgrades

This appendix covers software maintenance of the camera which you may need to do, including upgrading or changing the software installed on the camera.

The camera software has a version numbering scheme to help you decide what action to take when new versions become available. The format of a version number is *major.minor.revision*. The "revision" will be an increasing "revision" number, always larger for later releases. For bug fixes, "revision" will increase. For minor enhancements, "minor" will increase. For major new features, or architectural changes, "major" will increase.

Optionally we may append the characters 'a', 'b' or "rc" to indicate alpha, beta or release candidate.

If only the revision number is increased, backward compatibility is guaranteed without any config changes.

If the minor number is increased, backward compatibility *may* be affected if deemed absolutely necessary. This will be clearly highlighted in the release note.

If the major number is increased, backward compatibility *may* be affected if deemed necessary or desirable. This will be clearly highlighted in the release note.

In general we will always try to maintain backward compatibility where it makes sense. Always refer to the release notes for more details on the changes that have occurred.

The old mechanisms of manual installation and web based installation are no longer possible nor supported. All software installation is managed via the PIPS ANPR Toolkit which is documented in Chapter 3, *PIPS ANPR Toolkit* [8].

Appendix C. Factory Defaults

On the P382 the password for the root user is *382*

On the P392+/P492 the password for the root user is *392*

The default network configuration stored in(`/opt/config/current/netmon.xml`) is

Table C.1. Default IP configuration

IP address	`10.20.xxx.yy`
Network mask	`255.255.0.0`
Default gateway	`10.20.100.1`

where `xxx` are the first three digits of the serial number of the camera, and `yy` are the last two. The serial number is printed on a sticker on the rear of the P382, P392+ and P492

Caution

It is important to note any changes which you make to these parameters. Without these details it may be impossible to maintain the camera and it may have to be returned to Neology for servicing

Appendix D. File transfers

This section describes how to transfer files to or from the camera by various means. You can pick which of these you want to try, although not all are suitable for all situations.

SFTP

SFTP stands for Secure File Transfer Protocol. It is an encrypted protocol, and is a partner to SSH. Like you can log onto a system using SSH, you can use SFTP to transfer files in both directions. It is simple to use if you are familiar with the ubiquitous FTP, and plenty of front ends make it's use trivial. It is the recommended way of transferring files, requiring little setup to use.

Multiplatform — The filezilla program (see the section called “Filezilla” [142]) provides a two window commander style interface for accessing the camera via sftp.

Windows — The WinSCP program (see the section called “WinSCP” [142]) provides an explorer or commander style interface for accessing the camera via scp and sftp.

To use SFTP I recommend a graphical browser unless you're happy to train yourself in the use of a command line version.

SCP

SCP stands for Secure CoPy. It is an encrypted protocol, and is also a partner to SSH. Like you can log onto a system using SSH, you can use SCP to transfer files in both directions. It is simple to use, but does not provide directory listings or any other features you might expect - you will need to use SSH for directory listings as a partner to SCP. As SCP is available on most operating systems as a built in, and is also available on the camera for camera-to-camera copies it is useful to understand.

Windows — The WinSCP program (see the section called “WinSCP” [142]) provides an explorer style interface for accessing the camera via scp and sftp.

Windows — The PuTTY project (see the section called “PuTTY” [142]) also provides PSCP for Windows. If you want to use it, put it on your path, or current directory, and use **pscp** instead of **scp** in the command examples.

Mac OS X — scp is a built in command.

Linux — scp is provided if you have ssh installed, which you most likely will do.

SCP is used like the standard DOS or Unix copy commands. You specify a source and target file to transfer, just one of them happens to be on a remote computer.

- `scp {`*`SourceFile`*`} {`*`user@host:directory/TargetFile`*`}`
  to copy a file to the remote computer
- `scp {`*`user@host:directory/SourceFile`*`} {`*`TargetFile`*`}`
  to copy a file from the remote computer

Note

SCP can be used from on the camera too; if you have a computer with an SSH server you can scp out from the camera, or from one camera to another.

FTP

FTP stands for File Transfer Protocol. It is a simple open protocol, and is purely for transferring files. To use it you will need an FTP server installed on a PC accessible via the network from the camera. There are various options available

for each operating system. FTP is not recommended, but included here as people familiar with our older cameras will be familiar with FTP. This is a quick introduction to FTP, not a complete guide. There are books available on the subject, or guides on the internet.

Windows	For Windows we recommend the free FileZilla server, which is a download from http://filezilla-project.org/. This is simple to setup and enable users without requiring rights to add users to the PC.
Windows (alternative)	For Windows you can also use the FTP server which comes with the OS as part of IIS. You can install this from Start → Settings → Control Panel+Add/Remove Programs. It is tricky to set up correctly, and requires that you create a Windows user, and assign them correct permissions to work right. I do not recommend it as FileZilla is easier to use.
Mac OS X	MacOS X comes with an FTP server which can be enabled using the Sharing Pane.
Linux	Different distributions of Linux come with different FTP servers which are probably not installed or enabled by default. I recommend the ProFTPd software, but any FTP server should work correctly.

If you now connect to the camera's shell you should be able to ftp from the camera and transfer files. A typical session is shown below.

Note

The use of the bin command to enable all binary transfers may be necessary otherwise binary files may get corrupted, and does no harm so always do it.

```
pole ~ # ftp 80.177.196.175
Connected to 80.177.196.175 (80.177.196.175).
220 ProFTPD 1.3.1rc3 Server (Alan's ProFTPD) [::ffff:80.177.196.175]
Name (80.177.196.175:root): ftp_boot
500 AUTH not understood
SSL not available
331 Password required for ftp_boot
Password:
230 User ftp_boot logged in
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> bin
200 Type set to I
ftp> lcd /opt/config/current
Local directory now /opt/config/released
ftp> put state.xml
local: state.xml remote: state.xml
200 PORT command successful
150 Opening BINARY mode data connection for state.xml
226 Transfer complete
8089 bytes sent in 0.000208 secs (3.8e+04 Kbytes/sec)
ftp> cd 382
250 CWD command successful
ftp> lcd /storage
Local directory now /storage
ftp> get instapp.pl
local: instapp.pl remote: instapp.pl
200 PORT command successful
150 Opening BINARY mode data connection for instapp.pl (3132 bytes)
226 Transfer complete
3132 bytes received in 0.00201 secs (1.5e+03 Kbytes/sec)
ftp> cd app
250 CWD command successful
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
drwxr-xr-x   2 alan     alan         4096 Jul 23 23:00 254
drwxr-xr-x   2 alan     alan         4096 Sep 10 13:33 384
drwxr-xr-x   2 alan     alan         4096 Sep 25 11:39 435
drwxr-xr-x   2 alan     alan         4096 Oct 24 16:04 540
226 Transfer complete
ftp> cd 540
250 CWD command successful
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
-rw-r--r--   1 alan     alan      4553379 Oct 24 16:04 distrib.tbz2
226 Transfer complete
ftp> get distrib.tbz2
local: distrib.tbz2 remote: distrib.tbz2
200 PORT command successful
150 Opening BINARY mode data connection for distrib.tbz2 (4553379 bytes)
226 Transfer complete
```

```
4553379 bytes received in 0.741 secs (6e+03 Kbytes/sec)
ftp> quit
221 Goodbye.
pole ~ #
```

The **put** and **get** commands actually transfer files. **lcd** changes *local* directory, **cd** changes remote directory. **ls** will list files

Note

You cannot FTP from a remote computer into the P382, P392+ and P492

NFS

NFS stands for Network File System. This is an open protocol for sharing filesystems between computers. Unlike FTP and SCP this allows the camera to see remote files as if they were local files, rather than actually needing room to store them on its local storage. NFS is quite paranoid and must have all permissions correct before it will work. When it fails it doesn't usually give a helpful error message.

Windows see the section called “NFS Server on Windows” [142] to install nfs.

Mac OS X nfs is built in, but needs enabling.

Linux an nfs server is available for linux, see your distribution documentation to find out how to install it.

Setting up NFS involves editing /etc/exports and restarting the nfs server to pick up those changes. Once this is done you should be able to mount the exported filesystem from Webmin, as described in the section called “Mounting network disks” [13]. I'd suggest mounting the file system under /storage. Once this is done you should be able to list and access files on the remote PC as if they were local, using the standard **cd**, **ls** and **cp** commands.

CIFS/Samba (Windows shares)

CIFS is the latest version of Windows networking. It is available as samba for Linux and MacOS X, but it doesn't make as much sense as using NFS for those OSes.

Once you have a windows share set up you can mount the directories using webmin.

Transfer troubleshooting

A complete troubleshooting guide is beyond the scope of this manual, but I hope to give some hints and tips. Most problems boil down to one of two things, networking or permissions.

Network problems

- Can you ping the camera from the PC? If not then check your ethernet is correctly connected, networking settings are correct, and there is no firewall?
- Can you ping the PC from the camera? Both directions should work.
- Can you access the service on the PC from itself (not appropriate for all transfer types)? e.g. Can you FTP to the PC from itself?
- Is there a firewall running on the PC?
- Is there a second or third firewall running?
- Is there a firewall on the network in between?
- Or how about a NAT (network address translation) device?

- What happens if you telnet from either end to the service's port number? You should at least connect...

Permissions

- Do you have permissions to access the file you are trying to access? Can you read it locally on that machine?
- Do you have permissions to write to the file you are trying to write to?
- How about the directory that it is in?
- Do you have write permissions granted by the transport (e.g. FTP write permissions)? Or read permissions? *These permissions are separate from the permissions on the files... this often catches people out*
- Does the particular pairing of camera and PC allowed, lots of these services can restrict by IP address?

Appendix E. Software tools

This appendix lists some useful software tools you may wish to use with your camera

PIPS ANPR Toolkit

The PIPS ANPR Toolkit (P374) is available from PIPS. It consists of various software applications to install, diagnose and maintain PIPS cameras, including the P382, P392+ and P492. It is available as a package for Microsoft Windows 7.

Windows 7

To install the applications just double click on the installer executable and select the options you require.

PuTTY

PuTTY is a free terminal client. It can connect to the P382, P392+ and P492 via both the serial port and via SSH. It also provides the pscp SCP program. It is available from http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html and is highly recommended. A version of PuTTY is installed with the PIPS ANPR Toolkit.

Filezilla

Filezilla is a commander like file transfer program for many platforms suitable for using with the camera. It is available from http://filezilla-project.org/.

WinSCP

WinSCP is an explorer like file transfer program for Windows suitable for using with the camera. It is available from http://winscp.net/.

NFS Server on Windows

Windows does not come with an NFS server, however one is available for free as part of the cygwin project, and it is compatible with the P382, P392+ and P492. To install it

1. Download setup.exe from http://www.cygwin.com.
2. You should run this and select the **`nfs-server`** and **`cygrunsrv`** components.
3. Start the shell that is installed to Start → Cygwin → Cygwin Bash Shell and run **`nfs-server-config`**.
4. Now edit *`CYGWIN_DIR`*`/etc/exports` to add a directory to export. Full documentation of the exports file format is available online, but an example would be

   ```
   /cygdrive/d/workspace      80.177.196.176(rw,async,no_root_squash,insecure,no_subtree_check)
   /cygdrive/c/workdir/fish   80.177.196.0/24(ro,async,no_root_squash,insecure,no_subtree_check)
   ```

   which will export `d:\workspace` and the camera at 80.177.196.176 and `c:\workdir\fish` to all 80.177.196.* read-only.
5. Now start the **`Cygwin nfsd`** and **`Cygwin mountd`** services from Start → Settings → Control Panel+Administrative Tools → Services. You will need to restart them if you change the `exports` file.

Appendix F. Nano - text editor

This is a short guide to using the recommended text editor on the P382, P392+ and P492 *nano*. More detailed documentation is available on the web at http://www.nano-editor.org/docs.php

Opening and creating files

Opening and creating files is simple in nano, simply type:

nano {*filename*}
You can start typing immediately to insert text, and move around with the cursor keys.

Saving and exiting

If you want to save the changes you've made, press **Ctrl**+**O**. To exit nano, type **Ctrl**+**C**. If you ask nano to exit from a modified file, it will ask you if you want to save it. Just press **N** in case you don't, or **Y** in case you do. It will then ask you for a filename. Just type it in and press **Enter**.

If you accidentally confirmed that you want to save the file but you actually don't, you can always cancel by pressing **Ctrl**+**C** when you're prompted for a filename.

Cutting and pasting

To cut a single line, you use **Ctrl**+**K**. The line disappears. To paste it, you simply move the cursor to where you want to paste it and punch **Ctrl**+**U**. The line reappears. To move multiple lines, simply cut them with several **Ctrl**+**K**s in a row, then paste them with a single **Ctrl**+**U**. The whole paragraph appears wherever you want it.

If you need a little more fine-grained control, then you have to mark the text. Move the cursor to the beginning of the text you want to cut. Hit **Ctrl**+**6** (or **Alt**+**A**). Now move your cursor to the end of the text you want to cut: the marked text gets highlighted. If you need to cancel your text marking, simply hit **Ctrl**+**6** again. Press **Ctrl**+**K** to cut the marked text. Use **Ctrl**+**U** to paste it.

Searching for text

Searching for a string is easy as long as you think "WhereIs" instead of "Search". Simply hit **Ctrl**+**W**, type in your search string, and press Enter. To search for the same string again, hit **Alt**+**W**.

Note

Note: In nano's help texts the **Ctrl**-key is represented by a caret (^), so **Ctrl**+**W** is shown as ^W, and so on. The Alt-key is represented by an M (from "Meta"), so **Alt**+**W** is shown as M-W.

Appendix G. rc-update

This is a short guide on how to use *rc-update*

Introduction

rc-update is a script for adding/removing/listing available scripts to the boot, default and nonetwork run levels of your computer. these scripts allow you to run programs at your computers boot time.

rc-update is very useful and can be used to start anything from your network card to your login manager.

rc-update commands

adding a script to a runlevel

rc-update add script runlevel

will add a script to that runlevel of your computer.

removing a script from a runlevel

rc-update del script runlevel

will remove a script from the runlevel.

list available scripts and their current runlevel

rc-update show

will show all available scripts and their currently set runlevel(s) if any.

runlevels

boot

default

nonetwork

more runlevels may be added to /etc/runlevels/

Examples

rc-update add pips_app default

This will start the camera application at the default runlevel

rc-update del pips_app default

This will remove the camera application at the default runlevel

Other information

rc update uses scripts in the /etc/init.d/ directory exclusively

Appendix H. Viewfinder Protocol

The Viewfinder Protocol is a method for accessing the camera's video stream. The Viewfinder can be accessed via TCP port 9000.

There are several protocol versions available on the cameras, versions 1, 2, 3 and 4. By default the Viewfinder will be configured to use version 1

To initiate a Viewfinder session, you need to connect to the viewfinder port, to end the session just disconnect.

The viewfinder protocol constantly sends images, but when a session is first opened the camera needs to be set before any data will be sent, this is done by using the VF run command. Data will only stop being sent once the session is closed. The VF run command can be used to change the data that is sent, there may also be a small amount of lag before the changeover happens.

Viewfinder commands

Command	Description
VF set version *version*\n	Sets the version specified by *version* The viewfinder protocol does not respond
VF get channels\n	Gets information on the channels. See example below for output. (Viewfinder Protocol Version 2 or above must be used) The Viewfinder protocol responds with an xml type response
VF run camera *camera* seq *sequence* interval *interval* quality *quality* scale *scale*	Initiates the video stream. camera: The camera which is used to stream video from, required sequence: The sequence which is to be viewed, must be 0 for colour camera, default = 0, optional interval: The time between each frame, specified in ms, default = 2000, optional quality: Not used, optional scale: Not used, optional Viewfinder protocol responds with an image type response

Note

Camera 0 = cam1 in user interface = IR Camera

Camera 1 = cam2 in user interface = Colour Camera

Note

sequence 0 = seq1 in user interface

sequence 1 = seq2 in user interface

sequence 2 = seq3 in user interface

sequence 3 = seq4 in user interface

sequence 4 = seq5 in user interface

sequence 5 = seq6 in user interface

sequence 6 = seq7 in user interface

sequence 7 = seq8 in user interface

Viewfinder messages

This section contains information about the responses from the Viewfinder server

Version 1

In version 1 VF run is the only command that can be used. The following example I will configure the run command to the the IR camera and sequence 0 with 2 frames per second

`VF run camera 0 sequence 0 interval 500\n`

The response from the camera will be the following:

```
VF 1 0 0 11000\n[binary-jpeg-data]
```

Note

The [binary_jpeg_data] is a standalone JFIF (JPEG file interchange format), the specification can be found here, http://www.w3.org/Graphics/JPEG/jfif3.pdf

Note

This will be repeated every 500ms

VF *`version camera sequence jpeg_length`*

Version 2

In version 2 VF run and VF get can be used.

The response from version 2 is as follows

VF *`version type data`*

`VF set version 2`

`VF run camera 0 sequence 0 interval 500\n`

```
VF 2 image 0 0 5265846397017522284 11008\n[binary_jpeg_data]
```

Note

The [binary_jpeg_data] is a standalone JFIF (JPEG file interchange format), the specification can be found here, http://www.w3.org/Graphics/JPEG/jfif3.pdf

The above example gives a type of image which can be decoded as follows

VF *`version`* image *`camera sequence 64Bit_TimeStamp jpeg_length\n[binary_jpeg_data]`*

The 64bit Time Stamp can be decoded as follows, [Upper 32 bit Time stamp].[Lower 32 bit Time stamp].

The upper 32 bit Time stamp is a normal UTC time stamp indicating the number of seconds since 00:00:00 1st January 1970

The lower 32 bit Time stamp is the number milliseconds since the start of the current second

The second example

VF set version 2

VF get channels

```
VF 2 xml 367
<?xml version="1.0"?>
<channels model="P382" count="2">
 <channel0 num_sequence_entries="1">
  <format raw_type="mono" rate="50" quality="fixed" resolution="fixed" pixel_width="1" pixel_height="1"/>
 </channel0>
 <channel1 num_sequence_entries="1">
  <format raw_type="colour" rate="50" quality="fixed" resolution="fixed" pixel_width="2" pixel_height="1"/>
 </channel1>
</channels>
```

Note

The above example has been formatted for readability

The above example give an xml type which can be decoded as follows

VF *version* xml *xml_length*\n[xml_file]

<channels model="P382" count="2">indicates that the camera we are using is a P382 and that there are two possible image sources.

<channel0 num_sequence_entries="1"> indicates on the first channel has only one sequence available

<format raw_type="colour" rate="50" quality="fixed" resolution="fixed" pixel_width="2" pixel_height="1"/>

raw_type indicates that this channel is in colour, this can also be mono, or unknown

rate is not used, and is fixed at 50

quality is fixed so this cannot be changed, if it could this would be a number between 1 and 99

resolution is fixed which means it cannot be changed otherwise it would be a number such as 1, 2 or 4 which would be a defined resolution

pixel_width and pixel_height if pixel_width and pixel_height are the same then no adjustment of the image needs to take place, if they are different i.e. pixel_width = 2 and pixel_height = 1 means that each pixel needs to be made half the width, to view the image correctly.

Version 3

In version 3 VF run and VF get can be used.

The response from version 3 is as follows

VF *version type data*

VF set version 3

VF run camera 0 sequence 0 interval 500\n

```
VF 3 image 0 2 6129809915063042098 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1107 201 252 72 895 602 252 72 1023 92 252 72 93504\n[binary_jpeg_data]
```

Note

The [binary_jpeg_data] is a standalone JFIF (JPEG file interchange format), the specification can be found here, http://www.w3.org/Graphics/JPEG/jfif3.pdf

The above example gives a type of image which can be decoded as follows

VF *version* image *camera sequence 64Bit_TimeStamp PlateFindData jpeg_length\n[binary_jpeg_data]*

The 64bit Time Stamp can be decoded as follows, [Upper 32 bit Time stamp].[Lower 32 bit Time stamp].

The upper 32 bit Time stamp is a normal UTC time stamp indicating the number of seconds since 00:00:00 1st January 1970

The lower 32 bit Time stamp is the number milliseconds since the start of the current second

16 zeroes for future enhancement.

The plate find data describes up to 4 number plates found in the image. For each plate the x and y co-ordinates, width and height are displayed. This gives 16 data items in total.

Version 4

In version 4 VF run and VF get can be used.

The response from version 2 is as follows

VF *version type data*

VF set version 4

VF run camera 0 sequence 0 interval 500\n

```
VF 4 image 0 2 6129809915063042098 0 0 0 0 0 0 0 1107 201 252 72 5352 0 0 895 602 252 72 6737 0 0 1023 92 252 72 8941 0 0 93504\n[binary_jpeg_data]
```

Note

The [binary_jpeg_data] is a standalone JFIF (JPEG file interchange format), the specification can be found here, http://www.w3.org/Graphics/JPEG/jfif3.pdf

The above example gives a type of image which can be decoded as follows

VF *version* image *camera sequence 64Bit_TimeStamp PlateFindData jpeg_length\n[binary_jpeg_data]*

The 64bit Time Stamp can be decoded as follows, [Upper 32 bit Time stamp].[Lower 32 bit Time stamp].

The upper 32 bit Time stamp is a normal UTC time stamp indicating the number of seconds since 00:00:00 1st January 1970

The lower 32 bit Time stamp is the number milliseconds since the start of the current second

The plate find data describes up to 4 number plates found in the image. For each plate the x and y co-ordinates, width and height, plate find confidence, shape and clipped flag are displayed. This gives 28 data items in total.

The shape parameters indicate whether the plate is a number plate (0), a square number plate (1), a hazard plate (2) or a blank hazard plate (3).

The clipped flag indicates that the number plate may be partly obscured.

Appendix I. Vehicle Event Viewer Protocol

This section describes the PIPS Vehicle Event Viewer (aka "Client") protocol. It describes version 3 of the protocol as implemented by the cameras. The Vehicle Events can be accessed via TCP port 3570.

The Vehicle Event Viewer service runs on the camera and will be referred to as the "service". The service provides a stream of Vehicle Plate Read records (containing image and other data) for each vehicle plate read event created by the camera.

To initiate a Viewfinder session, you need to connect to the viewfinder port, to end the session just disconnect.

Entities may use TCP to connect to the camera and monitor this data stream. Any entity connecting to the "service" will be referred to as a "client".

Vehicle Event Viewer commands

Commands are sent to the service in ASCII text delimited by a Carriage Return character ('\r').

Currently, only a single command is recognised and this would normally only be issued once. The command (to select the version) is a string:

"vers[v]\r"

where v is the version "number", a single character in the ranges '1' to '9' or 'a' to 'z'.

The latest version supported on the cameras is 4 although it defaults to 2. If you connect to the service and issue no command, you will receive version 2 data. To switch to version 4, immediately on connection completion, the client should send the following string to the service: "vers4\r"

Vehicle Event Viewer data

The service starts streaming binary data to the client immediately on connection. It does not wait for anything from the client.

The data streamed from the service is binary. The binary data is streamed as a BLOB as follows:

1. Firstly a header structure which begins with a "start of block" pattern followed by information about the event, such as the plate string. It also contains information (lengths in bytes) allowing the end of the header and the start/endings of the subsequent jpeg images to be computed.

2. The header is immediately followed by the patch jpeg image - the length of which is contained in the header. The jpeg data is in JFIF format.

3. The patch jpeg is immediately followed by the colour overview jpeg image - the length of which is contained in the header. The jpeg data is in JFIF format.

Header Format

The header is a packed structure. Currently the cameras default to version 2, so the client must be able to recognise version 2 headers too. Since there is actually little difference between the versions, it is not difficult to support both.

Even if the client switches to version 3 immediately on connection, it is possible that one or more version 2 headers will be received first. Version 2 data may be used or ignored.

The difference between the version 2 and version 3 headers is that the version 3 header has two extra fields appended on the end - namely: utc_timestamp_s and utc_timestamp_ms.

The difference between the version 3 and version 4 headers is that the version 4 header has one extra field appended on the end - namely: m_plate.

The jpeg fields, if present, follow immediately after the header. Their location may be determined by the respective size fields in the header. The jpeg data is in JFIF format.

The version 3 header is shown below:

Note

Entries commented

```
//Not Used
```

are not currently used on the P382. It is possible that at some time in the future they may be used without causing a version number change. It will always be safe to ignore them).

```
struct PTFMPlateHeaderV3
{
 unsigned start; // start of message block indicator
 unsigned header_size; // size of header
 unsigned patch_size; // patch length
 unsigned overview_size; // overview length
 unsigned sum; //Not Used
 unsigned camera; //Not Used
 unsigned flash; //Not Used
 unsigned gain;
 unsigned shutter;
 unsigned seq; // exposure sequence number 0 - 2
 unsigned threshold; //Not Used
 unsigned platefinder_confidence;
 unsigned plateread_confidence;
 unsigned id; //Not Used
 unsigned ticks; // system tick counter at exposure time (ms)
 unsigned location; //Not Used
 unsigned mseq; //Not Used
 unsigned exp[3]; //Not Used
 unsigned event_count[4]; //Not Used
 char  plate_str[16];
 unsigned  utc_timestamp_s;
 unsigned  utc_timestamp_ms;
 char   m_plate[40];
};
```

Each field will be described below:

Note

All integer fields are transmitted in network byte order and will need to be converted back to host byte order before interpretation.

- *start:* A 4 byte pattern which identifies the start of the header. This will be 0x50544632 for version 2, 0x50544633 for version 3 and 0x50544634 for version 4.
- *header_size:* The size of the header (and only the header) in bytes. This will be different between versions. This value may be used to determine where the jpeg data begins.
- *patch_size:* The size in bytes of the patch jpeg. If this is non-zero, then this data begins immediately after the last header byte. (The patch jpeg is in jfif format).
- *overview_size:* The size in bytes of the overview jpeg. If this is non zero, this data begins immediately after the last byte of patch data. (The overview jpeg is in jfif format)
- *sum:*Currently unused
- *camera:* Currently unused
- *flash:* Currently unused. The flash period is equal to the shutter period.
- *gain:* The gain setting for this plate read event

- *shutter:* The shutter setting for this plate read event. A reported value of 0 indicates a shutter period 10us. The maximum value is 31 and indicates a shutter period of 1ms. In order to deduce in-between shutter period's note that there is a linear relationship between these reported values and actual shutter period.
- *seq:*The exposure sequence number, typically a number from 0 to 2 indicating which in a sequence of exposures was used to give this plate read event.
- *threshold:*Currently unused
- *platefinder_confidence:* The platefinder confidence value. This is not normally of much interest to an end user.
- *plateread_confidence:* The confidence of the plate read expressed as a number less than a 100 (where 100 would indicate absolute confidence).
- *id:*Currently unused
- *ticks:* A system monotonic tick count in milliseconds indicating the time of exposure. Has no meaning as an absolute time, but can be useful in relative terms - for example to measure elapsed time between two consecutive events. The tick value is strictly monotonic and therefore is unaffected by changes to the system time.
- *location:*Currently unused
- *mseq:* Currently unused
- *exp:* Currently unused
- *event_count:* Currently unused
- *plate_str:* Number plate string. Null terminated character string.
- *utc_timestamp_s:* (Version 3 and 4 only) UTC Timestamp of plate read image set (seconds). May be used together with utc_timestamp_ms (see below) to provide accurate UTC time.
- *utc_timestamp_ms:* (Version 3 and 4 only) UTC Timestamp of plate read image set (milliseconds)
- *m_plate:* (Version 4 only) The text read from the plate

Appendix J. Legal Notices

English

Copyright Notice

The information within this handbook is authorised for distribution to customers, authorised service centre personnel, and distributors of Neology. Every effort has been made to supply information within this handbook that is correct. However, Neology assumes neither responsibility for its use, nor any infringements of patents or other rights of third parties which would result. No licence is granted by the manufacturer under any patent or patent rights. The manufacturer reserves the right to modify and update the equipment at any time without prior notice.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means to a third party without the prior consent of the copyright holder.

The manufacturer's warranty will be invalidated if untrained personnel operate the equipment or if any attempt is made to service the equipment by untrained personnel.

Warranty

Neology warrants products and spare parts of its own manufacture against faulty materials and workmanship for a period of 12 months, or as modified by the contract, from the date of purchase or on site acceptance, if installed by Neology authorised personnel.

The warranty excludes consumable materials and parts with an inherently limited life and excludes faults arising from misuse, neglect or vandalism.

Neology will replace or repair at its option and at no cost to the purchaser any faulty items reported to it within the warranty period.

Service

Service of this equipment by replacement of parts, on site repair or routine maintenance inspections is available. Please contact Neology for a quotation. There are no user serviceable parts inside the camera.

Technical Support

Should you require technical support, please contact Neology.

Users finding errors or omissions in this document are requested to advise Neology.

Write or telephone:

Neology United Kingdom plc
17 Bartley Wood Business Park
Hook
Hampshire
RG27 9XA
United Kingdom
Telephone: +44 (0)
Email: <anprsupportous@uk.neology.net>

If you telephone please have the following information available:

product name and version number
operating system and version number

Design Changes

Neology reserves the right to change the design of any product from time to time without notice and with no obligation to make corresponding changes in products previously manufactured.

Trademarks

Windows and Windows XP are registered trademarks of Microsoft Corporation.

FCC Declaration

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Français

Notification de Copyright

L'information dans ce manuel est autorisée pour la distribution aux clients, au personnel des services de maintenance autorisés, et aux distributeurs de Neology (ci-après dénommée "La compagnie") Tout effort a été fait pour que l'information dans ce manuel soit correcte. Cependant, "La compagnie" n'assume ni la responsabilité pour son usage, ni aucune infraction à des brevets ou à d'autres droites des tiers qui résulteraient de son utilisation. "La compagnie" n'accorde aucune licence sous aucun brevet ou propriété industrielle. "La compagnie" se réserve le droit de modifier et mettre à jour le matériel à tout moment sans préavis.

Aucune partie de cette publication ne peut être reprise, reproduite ou enregistrée sous quelque forme que ce soit sans l'accord écrit préalable de "La compagnie".

La garantie de "La compagnie" sera infirmée si le matériel est utilisé ou si n'importe quelle tentative est faite de le réparer par un personnel non formé par "La compagnie".

Garantie

Cette garantie s'étend aux produits et pièces de rechange fabriquées par "La compagnie" contre les matériaux défectueux et l'exécution défectueuses pendant une période de 12 mois ou comme modifiée par le contrat, de la date de l'achat ou sur l'acceptation de site, si le matériel est installé par "La compagnie" ou un personnel autorisé.

La garantie exclut les matériaux consommables et les parties avec une durée de vie limitée et exclut des défauts redevant de l'abus, de la négligence ou du vandalisme.

"La compagnie" substituera ou réparera, à son option, et à aucun coût à l'acheteur tous les éléments défectueux reportés au cours de la période de garantie.

Service

Le service de ce matériel par le remplacement des parties, par des inspections de maintenance ou de réparation sur de site est disponible. Prière de contacter "La compagnie" pour la liste des coûts.

Support Technique

Pour tout support technique, prière de contacter "La compagnie" au Royaume-Uni.

Si vous trouvez des erreurs ou des omissions dans ce document prière d'informer "La compagnie"

Écrivez ou téléphonez:

Neology United Kingdom plc
17 Bartley Wood Business Park
Hook
Hampshire
RG27 9XA
United Kingdom
Telephone: +44 (0)
Email: <anprsupportous@uk.neology.net>

Si vous téléphonez, prière d’avoir l'information suivante disponible:

nom de produit et nombre de version
système d'exploitation et nombre de version

Changements de Conception

"La compagnie" se réserve le droit de changer la conception de n'importe quel produit de temps # autre sans communication préalable et sans l'obligation de faire les changements correspondants des produits construits antérieurement.

Marques Déposées

Windows et Windows XP sont des marques déposées de Microsoft Corporation.

Appendix K. Contact information

Table K.1. Contact Information

United Kingdom	USA
Neology United Kingdom plc 17 Bartley Wood Business Park Hook Hampshire RG27 9XA United Kingdom Telephone: +44 (0) Email: <anprsupportous@uk.neology.net>	Neology 12760 Danielson Ct., Suite A Poway CA USA Telephone: +1 (0) 858-391-0260 Fax:+1 (0) 858-391-0264
Web site:http://www.neology.net/	

COMFORT SYSTEMS USA
BCM Controls Corporation

Sierra Wireless Components

Quote #Q001602-BCM v1



Prepared For:

Massachusetts State Police

Brian Egnitz
470 Worcester Rd.
Framingham, MA 01702

P: (508) 410-1188
E: brian.egnitz@MassMail.State.MA.US

Prepared by:

BCM Controls

Bob Fecteau
30 Commerce Way
Woburn, MA 01801

P: 781-897-5151
E: fecteaur@bcmcontrols.com

Date Issued:

03.10.2020

Expires:

06.30.2020

Introduction

Dear Brian,

In accordance with your recent request, outlined as follows is the pricing that you requested for six (6) Sierra Wireless power adapters and twelve (12) cellular paddle antennas.

Thank you for allowing us this opportunity, and please do not hesitate to contact me with any questions.

Sincerely,

Bob Fecteau

COMFORT SYSTEMS USA
BCM Controls Corporation

Scope of Work



1. Scope Details
2. Scope Details
3. Scope Details

Equipment

Qty	Product Details	MSRP	Discount %	Price	Ext. Price
6	**Sierra 12VDC AC Adapter**	$20.00	5	$19.00	$114.00
12	**Sierra Cellular Paddle Antenna**	$14.00	5	$13.30	$159.60
				Subtotal:	**$273.60**

COMFORT SYSTEMS USA
BCM Controls Corporation

Assumptions & Clarifications

General:

- Pricing proposed is FOB: Delivered
- Pricing and warranty provided in accordance with MA State Contract: ITC71
- Pricing excludes any/all technical services labor

Privileged Information Statement

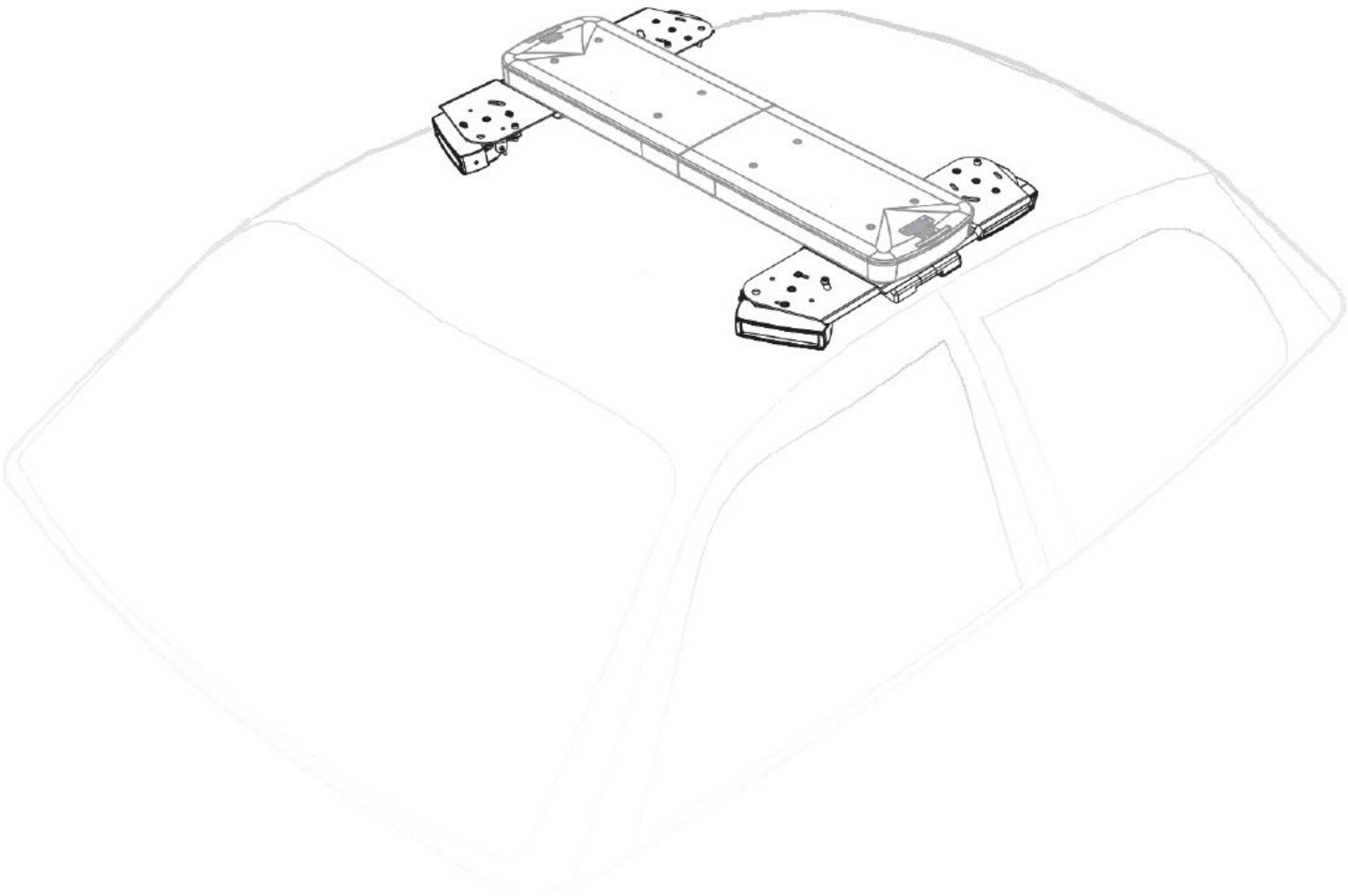
“The information contained in this document and the solution proposed by BCM Controls (BCM) is proprietary and confidential to BCM. These materials can be used solely for the purpose of evaluating a possible transaction between BCM and its existing and prospective customers. No recipient of these materials may use them for their own commercial advantage. The recipient of these materials must hold them in confidence and shall not distribute them, in whole or in part, to any other individual or entity in any form without the prior written consent of BCM.

Quote Summary	Amount
Equipment	$273.60
Total:	**$273.60**

Taxes, shipping, handling and other fees may apply. We reserve the right to cancel orders arising from pricing or other errors.

Acceptance

BCM Controls	**Massachusetts State Police**
Bob Fecteau	Brian Egnitz
Signature / Name	Signature / Name Initials
03/10/2020	
Date	Date



PIPS MOBILE ALPR SOLUTION

Installation Guide

Revised: Nov 2019

SAFETY INFORMATION ____ *4*
Intended System Use ____ 4
RISK REDUCTION ____ *4*
Safety Prerequisites ____ 4
Component Installation ____ 4
Vehicle/Component Safety ____ 5
Maintenance ____ 5
General Safety Precautions ____ 5
PRODUCT OVERVIEW ____ *6*
Applications ____ 6
System Configurations ____ 6
ALPR System Vehicle Power Draw ____ 6
Inventory Lists ____ 7
PHYSICAL INSTALLATION ____ *8*
Unpacking the ALPR System ____ 8
Damaged or Missing Item ____ 8
Planning the ALPR System Installation ____ 8
Assess Existing On-Board Systems ____ 9
Assess Power Source ____ 9
Unpacking the Mobile Cameras ____ 10
Record Each Serial and Model Number ____ 10
Identify Each Camera ____ 10
General Camera Layout ____ 10
Preparing the Zero-Clearance Bracket ____ 11
Changing the Orientation of the Zero-Clearance Bracket ____ 12
Attaching the Zero-Clearance Bracket to the Camera ____ 13
Mobile ALPR Mounting Solutions ____ 14
Mounting the Camera Assembly to the Vehicle ____ 15
Attaching a Camera to Non-Lightbar Mounts ____ 16
Mounting the Mobile Processor ____ 17
WIRING AND CONNECTIONS ____ *18*
The Power Wiring ____ 18
The GPS Antenna ____ 19
The Mobile Camera Cables ____ 19
Connecting Camera Cables to the Processor ____ 19
Connecting the GPS Antenna to the Processor ____ 20

Connecting the Networking Elements to the Processor ____ **20**
Connecting the Power Cable to the Processor ____ **21**
Confirming the Power Status ____ **21**
ALIGNMENT ____ ***22***
ALIGNMENT PROCEDURE ____ ***22***
Alignment Requirements ____ **22**
Tools Required ____ **22**
Distance Marker Diagram ____ **22**
Aligning the Front Left Camera ____ **23**
Aligning the Front Right Camera ____ **23**
Aligning the Right Rear Parking Camera ____ **24**
Aligning the Left Rear Camera ____ **24**
CALIBRATING EXPOSURE TABLES ____ ***25***
Exposure Table Best Practices ____ **25**
Setting the Exposure Table/Plate Illumination ____ **25**
MAINTENANCE AND SERVICE ____ ***26***
Qualifications ____ **26**
Servicing Mobile ALPR Cameras ____ **26**
Cleaning Mobile ALPR Cameras ____ **26**
Servicing the Mobile ALPR Processor ____ **26**
Servicing the 10.4 inch Touchscreen Monitor ____ **26**
Cleaning the Vehicle ____ **26**
APPENDIX A – ALPR COMPONENTS ____ ***27***
APPENDIX B – WIRING DIAGRAM ____ ***28***
APPENDIX C – WIRING DIAGRAM ____ ***29***

SAFETY INFORMATION

Please read, understand, and follow all safety information contained in this guide prior to any attempts to Install or use the Mobile ALPR System. Retain these instructions for future reference.

Intended System Use

The Mobile ALPR System is intended to provide Automatic License Plate Recognition (ALPR) to users by automatically “reading” number plate or license plate characters. It is expected that all users be fully trained in the safe operation of this Mobile ALPR System. Use in any other application is not condoned, may immediately void all warranties, and may lead to an unsafe condition.

RISK REDUCTION

This section lists the recommended best practices to take prior to the installation, during installation, and during operation or maintenance of the Mobile Platform. Failure to adhere to these recommendations may result in hazardous voltages, fire, property damage, and equipment failure due to impact as well as potential injury to installers and users.

Safety Prerequisites

- Refer to the vehicle's service manuals when performing vehicle equipment installation and follow accepted automotive mechanical and electrical installation procedures.
- Review the manufacturer's vehicle wiring diagram prior to the Mobile ALPR System installation to ensure the installation does not affect vehicle operation or mandated safety functions or circuits.
- Installation to be performed only by authorized personnel or certified and/or trained installers.
- Service to be performed only by authorized personnel in compliance with all local, regional, and national applicable motor vehicle codes.

Component Installation

- Do not interact with ALPR system while driving or in hazardous conditions.
- Use only the Mobile ALPR Processor, brackets, and cabling provided.
- Ensure all external electrical connections are protected from the environment.
- Do not kink or pinch cables when routing through the vehicle as this could damage the cable/system.
- Do not get metal shavings inside the Processor. Use an ESD-approved cover if drilling near unit cannot be avoided. After mounting, inspect area and remove any metal shavings.
- Do not co-locate the SX Processor within 18 inches (45.7 cm) of a radio antenna or transmitter.
- Clear both sides of vehicle structure when drilling. Remove burrs from drilled holes and use grommets for wiring. Use care when installing mounting screws.
- Do not mount cameras or components in unapproved locations or mounting brackets. Doing so may immediately void warranty and/or service contract.
- After installation of a component, ensure it is securely attached to the vehicle.
- Avoid placing a magnetic mounting bracket or other magnetic component next to an electronic device.
- Verify all component mounts, power connections and wiring are properly connected prior to powering On the system after installation, maintenance, and/or service.

Vehicle/Component Safety

- After installation, test all vehicle functions, including horn operation, vehicle safety functions, and vehicle lighting systems, to ensure proper operation.
- Ensure the installation has not affected the vehicle operation or changed any vehicle safety function or circuit.
- Locate any ALPR system controls so the vehicle can be operated safely under all driving conditions.
- Do not install equipment or route wiring in the deployment path of an air bag.
- After deployment, inspect ALPR System periodically to ensure proper operation and attachment to vehicle.

Maintenance

- Replace Mobile ALPR System fuses with same size, type, and rating specified in installation guide.
- Always keep the Mobile ALPR Processor vent areas clear.
- Keep the Mobile ALPR Processer in a dry location.
- Do not use cleaning solutions such as strong detergents, solvents, or petroleum-, alcohol-, or ammonia-based products. Use only a soft cloth and a mild soap and water solution.
- The Agency is required to open the Mobile ALPR Processor case in order to remove the battery prior to disposal.

NOTE: Opening the case of the Mobile ALPR Processor will void the warranty. Opening the case may adversely affect any future operation of the processor. Never open the case of the Mobile ALPR Processor unless authorized by PIPS Support or when removing the battery for disposal. All disposal operations must be performed within local guidelines and laws. It is the responsibility of the processer owner to ensure all local and regional regulations are followed for proper disposal.

General Safety Precautions

- Follow safe workplace practices during installation and maintenance.
- The ALPR cameras are Class 1M LED products and emit LED radiation. Do not view directly with the eye or optical instruments.
- Dispose of all system components in accordance with applicable local and government regulations.
- Dispose of lithium-ion batteries and electronic components according to all applicable recycling or waste regulations.
- Ensure to keep all fingers and items clear when mounting magnetic camera brackets.

PRODUCT OVERVIEW

This section discusses the general application, configuration, and ALPR system information.

Applications

- Law Enforcement
- Parking Enforcement
- Community Service Vehicles
- Private Security Vehicles

System Configurations

The PIPS ALPR Mobile SX Processor can be configured in two distinct ways; Client/Server or Stand Alone.

Client/Server (VPRelay) Mode:
The Client/Server configuration consists of a Mobile ALPR Processor, up to four ALPR cameras with mounting brackets, and a network connection to a Mobile Data Computer (MDC)/laptop in the front of the vehicle. The ALPR processor collects images and data for license plate recognition and relays it to the MDC over a static network connection. The primary advantage of the Client/Server configuration is that it allows a user to be notified of "alerts" while operating the vehicle. This is done through mobile ALPR software called "PAGIS" running on the laptop/MDC and displaying the ALPR data inside the vehicle.

Stand-Alone Mode:
The Stand-Alone configuration consists of a Mobile ALPR Processor, up to four mounted ALPR cameras, and a touchscreen monitor. The self-contained system performs all plate recognition and runs its own copy of the PAGIS software. The primary advantage of the Stand-Alone configuration is its deployment flexibility as it does not require the agency to own and maintain MDCs/laptops. Some utilization examples are speed trailers, parked covert vehicles, or in manned patrol units (when equipped with touchscreen monitors and a hotspot/cellular data network).

ALPR System Vehicle Power Draw

When off, the ALPR system should draw around 20miliamps. The chart below shows the power draw when operational.

Component	Current Draw	Total Draw
SX Processor	3.5 A @ 12VDC	3.5 A @12VDC
Camera 1	1.0 A @ 12VDC	4.5 A @12VDC
Camera 2	1.0 A @ 12VDC	5.5 A @12VDC
Camera 3	1.0 A @ 12VDC	6.5 A @12VDC
Camera 4	1.0 A @ 12VDC	7.5 A @12VDC

NOTE: *These calculations do NOT include load from the MDC, Touchscreen monitor, or GPS antenna*

Inventory Lists

Below are the two most common system architectures.

Mobile Law Enforcement Package (Client/Server architecture):

- Mobile ALPR Camera(s) with appropriate infrared illumination
- Mobile ALPR Processor with camera, HDMI, Display Port, and USB 3.0 ports
- Mobile ALPR Processor power cable (three wire)
- Camera cables/connector(s)
- Accessory Kit including Antennas (when applicable)
- Garmin GPS Antenna (16x HVS)
- CAT 5E network cable (25ft.)
- ALPR/OCR Engine specifically for customer region inside the SX4e
- Lightbar Mounting Bracket(s) and Plate(s) for approved lightbar assemblies
- OPTIONAL – Mobile Mounting Bracket
- OPTIONAL – Garmin 16 GPS mount, trunk clip

NOTE: *Approved lightbar assemblies include Federal Signal, Whelen Liberty, Justice and Edge, Code3 Defender, Tomar, and other 13.25-inch and 16.25-inch bars. Non-approved lightbar mounting designs are available but may incur a design charge. Please check with your Sales representative.*

Mobile Law Enforcement Package (Stand-alone architecture):

- Mobile ALPR Camera(s) with appropriate infrared illumination
- Mobile ALPR Processor with camera, HDMI, Display Port, and USB 3.0 ports
- Mobile ALPR Processor Power cable (three wire)
- Camera cable/connector(s)
- Accessory Kit including Antennas (when applicable)
- Garmin GPS Antenna (16x HVS)
- 10.4 Inch Touch Screen Monitor with HDMI and two USB cables (25ft. ea)
- DC-DC power adapter for the touch screen monitor
- License Plate Capture Software (PAGIS) on the SX Processor
- ALPR/OCR Engine specifically for customer region on the SX Processor
- Lightbar Mounting Bracket(s) and Plate(s) for approved lightbar assemblies
- OPTIONAL – Mobile Mounting Bracket
- OPTIONAL – Third party mounting bracket for 10.4 inch monitor (based on vehicle)

NOTE: *Approved lightbar assemblies include Federal Signal, Whelen Liberty, Justice and Edge, Code3 Defender, Tomar, and other 13.25-inch and 16.25-inch bars. Non-approved lightbar mounting designs are available but may incur a design charge. Please check with your Sales representative.*

PHYSICAL INSTALLATION

This section discusses the aspects of the unboxing and physical installation of the ALPR system and its components.

Unpacking the ALPR System

Carefully unbox the ALPR platform, its components, as well as any other products included in the shipment. Inspect each item for any damage caused by shipping prior to installation.

Damaged or Missing Item

If an ordered product is missing, or was damaged during shipping, it cannot be used for installation. Immediately call ALPR Support at (833) 747-7577 Option 2 or email Support@PIPSTechnology.com to generate a support case (Please reference the order number).

Planning the ALPR System Installation

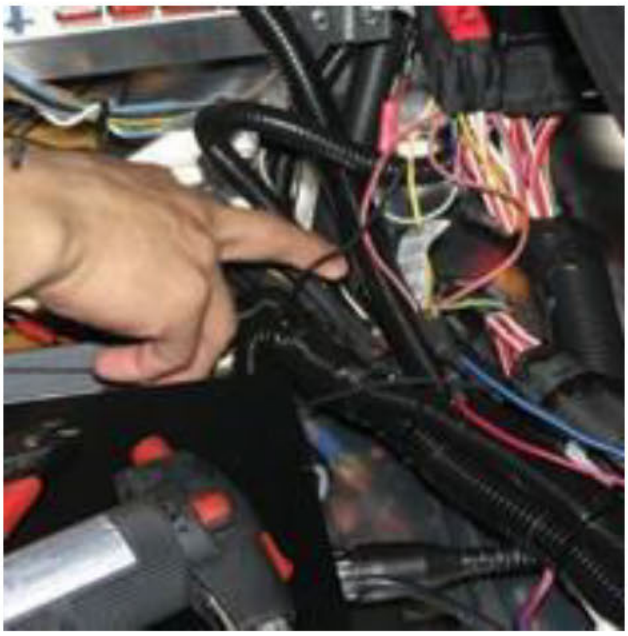
Be sure to assess the vehicle type before moving forward with any installation. Certain vehicle types may require variations of the installation process. For example, the lengths of wiring/cabling needed for an SUV are generally greater than what's needed for a sedan. Understanding these details ahead of time are highly recommended.



Shown - Ford Police Interceptor Utility and Police Interceptor Sedan. Photo courtesy of Ford Motor Company.

Assess Existing On-Board Systems

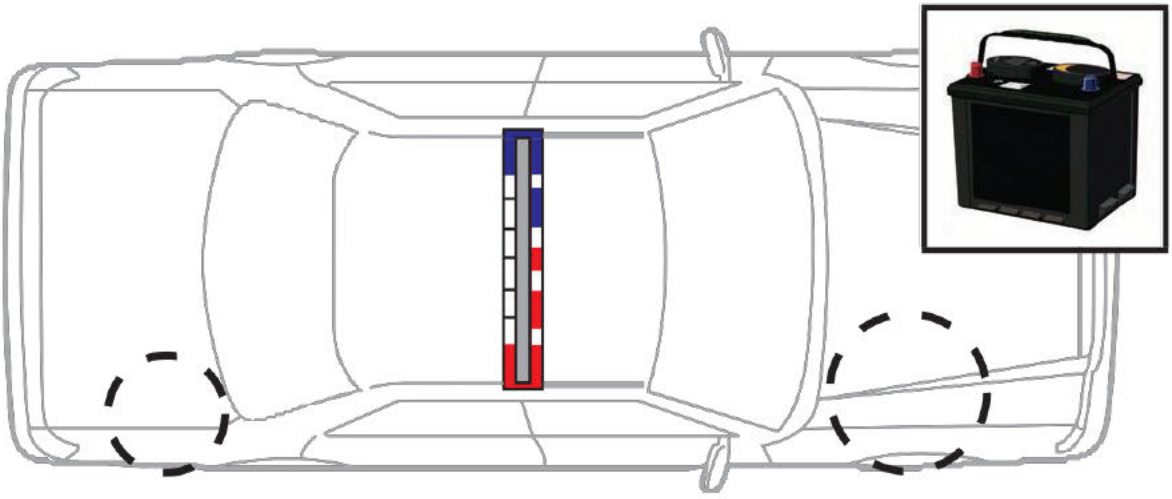
Before any installation steps, the installer should fully understand how each on-board system, radio, laptop, lightbar, etc., has been wired in the vehicle. He/she should then plan the Mobile ALPR Processor installation to take advantage of any existing power taps, wire runs, or other outfitter wiring systems. **NOTE**: To prevent malfunction or potential electrical damage, the installer should also take care to not overload any of the existing vehicle circuits.





Assess Power Source

Most police package vehicles have power distribution in the trunk or in the back of the vehicle. This is the preferred power source for the Mobile Processor. If a power tap is not found, the power must be run to the battery. Be sure to add an in-line fuse at the battery. **NOTE**: For more detail refer to Appendix B and C



Unpacking the Mobile Cameras

Each camera and mounting bracket are packaged individually. Best practice recommends the agency keep the shipping box of each bracket and camera in the unlikely event the unit needs to be returned. If it's not possible to temporarily save the shipping containers, they should be sent to an appropriate recycling center.

Record Each Serial and Model Number

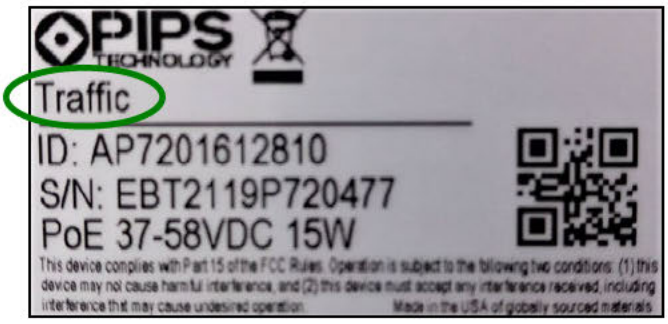
Note the serial and model numbers on the label of the product housing and record it for reference.
IMPORTANT: Please have the model and serial numbers available whenever Customer Support is contacted.

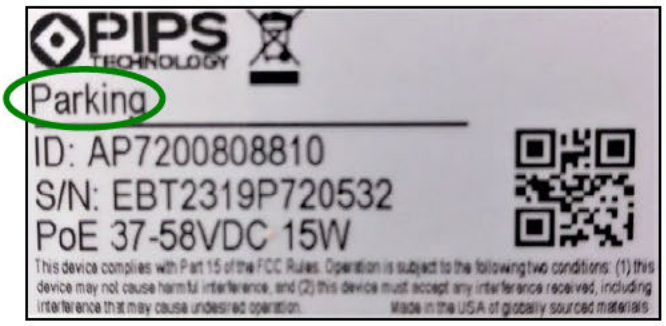
Identify Each Camera

Before mounting cameras to the vehicle, they should be checked for any damage, identified to confirm illumination uniformity, and assigned to the proper mounting locations based on lensing. The steps to identify the cameras and lensing are below:

1. Locate the Identification Label (Contains Serial and Model/ID Number)
2. The Label should say "Traffic" or "Parking"
    a. Traffic cameras are designed to view plates farther down the adjacent lanes
    b. Parking cameras are designed to view plates closer to the ALPR vehicle
3. Make note of the ID Number (This is the "Model Number")
4. Use ID/Model number information to select each camera position

How to Read the ID/Model Number: Example: AP7201612810
[Product: AP720] + [IR Lens: 16] + [OV Lens: 12] + [Illumination Wavelength: 810]





General Camera Layout

The proper mounting location is extremely important to overall function. Placing a camera in the wrong position on the vehicle will reduce the ALPR performance to almost zero. Below is the most common mounting layout:

1. The front left, and front right cameras are nearly always Traffic cameras.
2. The right rear side camera is nearly always a Parking camera and aimed perpendicular to the vehicle.
3. The left rear side camera can either be a second perpendicular parking camera or it can be a rear facing traffic camera.
    a. The advantage of the rear facing camera is its ability to capture rear plates of opposing traffic. This is especially useful in rear license plate only states.

For more detailed mounting information, refer to the alignment section.

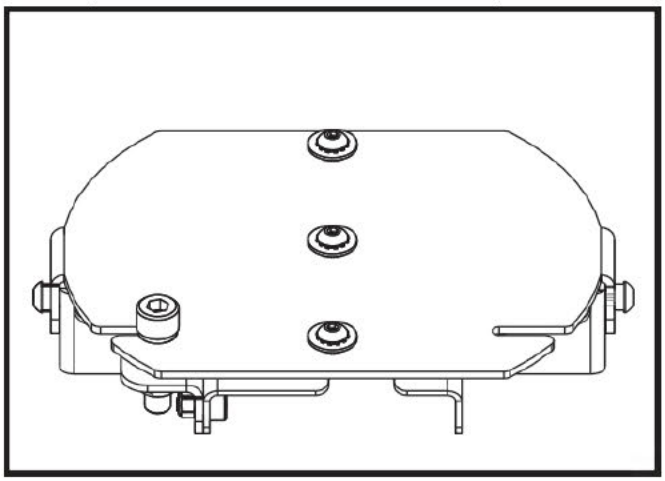
Preparing the Zero-Clearance Bracket

Once the proper camera configuration is determined for the vehicle, it's time to prepare the mounting brackets. There are two bracket configurations, a driver's side or left-handed bracket, and a passenger's side or right-handed bracket. When viewing the bracket from the rear and face up, the right-hand bracket will have the adjustment screw on the right. Since all brackets come this way, the installer will need to manually configure any required left-hand brackets.

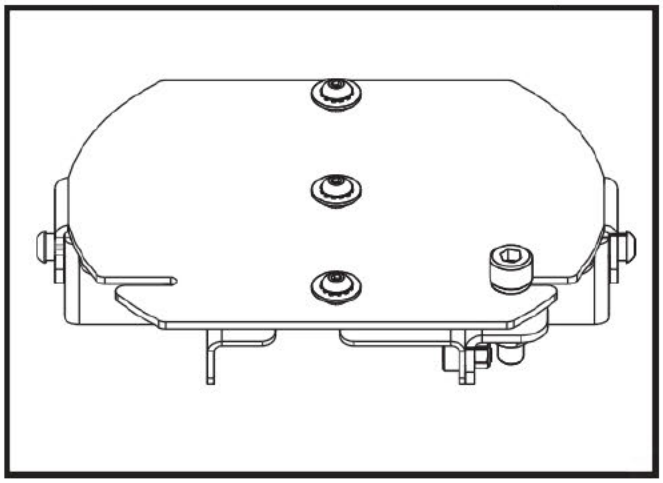
PRO-TIP: To assist with maintenance, PIPS recommends the use of an anti-seizing agent on all screws/bolts for the entire light bar and bracket system.

NOTICE: Zero-clearance brackets only ship with lightbar mounting configurations. Be sure to work with the Sales Department to procure the proper packages for each vehicle.

Left-Hand or Driver's Side Bracket



Right-Hand or Passenger's Side Bracket



Typical Camera and Bracket Configurations

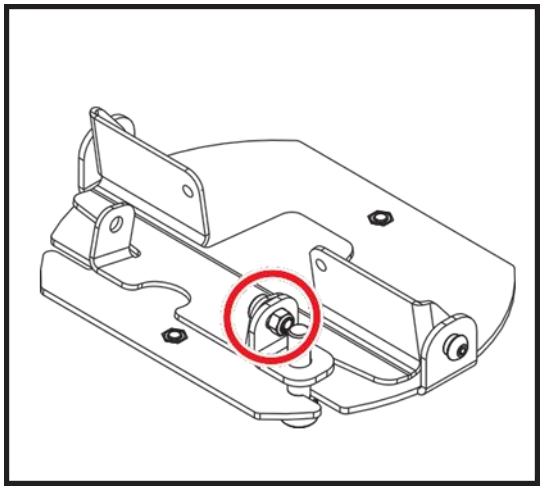
The chart below illustrates the combination of the camera position and the corresponding bracket configuration.

Camera location	Camera type	Bracket type	Camera number
Front/Left	Traffic	Left-hand	1
Front/Right	Traffic	Right-hand	2
Rear/Left	Traffic	Left-hand	3
Rear/Left	Parking	Left-hand	3
Rear/Right	Parking	Right-hand	4

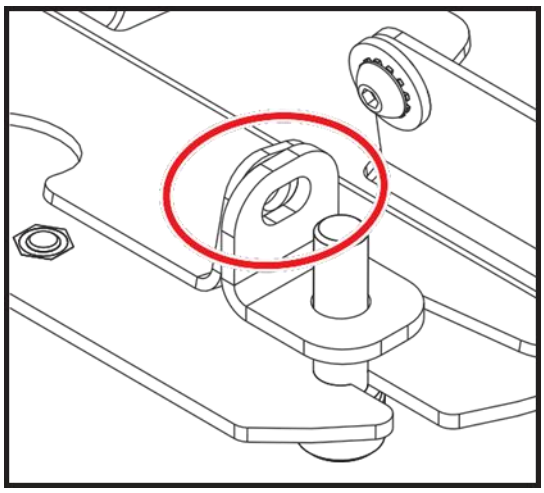
Changing the Orientation of the Zero-Clearance Bracket

In order to convert one or more of the right-hand brackets to left-hand brackets, follow the steps below:

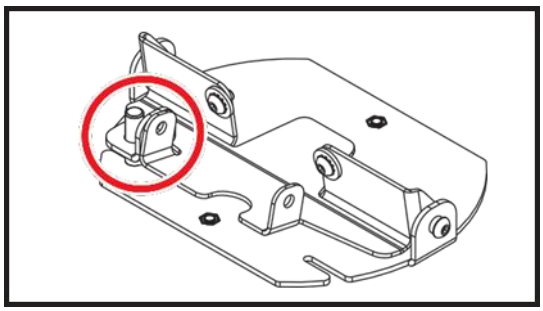
1. Locate the pivot screw on the bracket



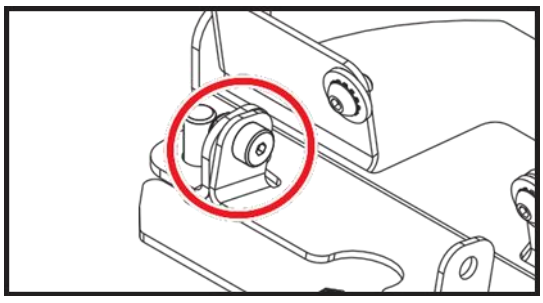
2. Remove the pivot screw from the bracket



3. Slide the pivot screw bracket from the slot and move it to the opposite side of the assembly



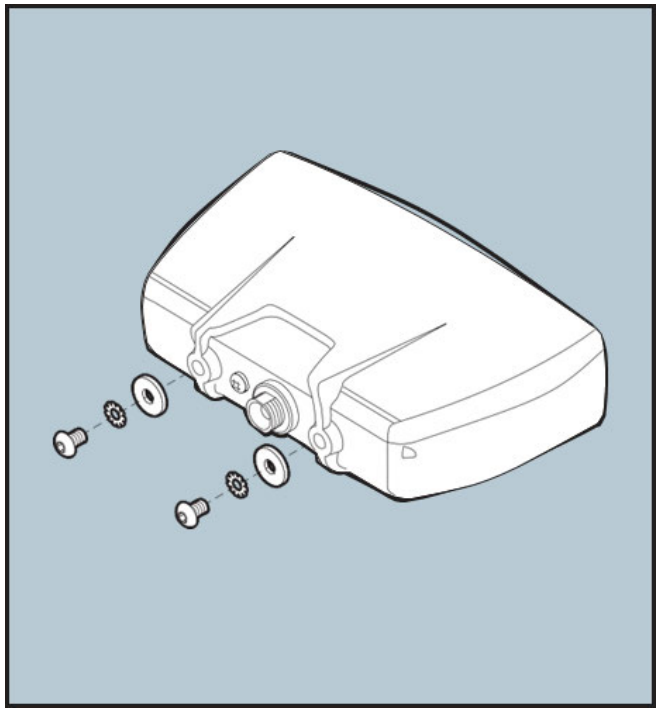
4. Reattach the pivot screw to complete the conversion



Attaching the Zero-Clearance Bracket to the Camera

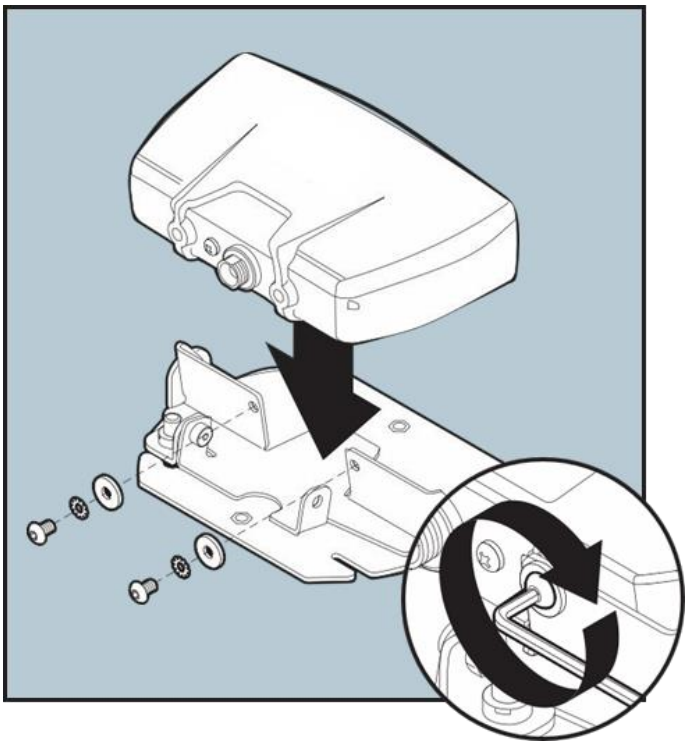
Once all the brackets are assembled, the mobile cameras should be mounted to the brackets.

1. Remove the screws, star washers, and flat washers from the mounting holes at the rear of the camera.



2. With the camera and bracket upside down, install the zero-clearance bracket by sliding the bracket tongue into the camera groove. The camera groove is located on the top rear of the camera.

3. When the tongue is fully seated in the groove, place the star washers and flat washers on the screws. Tighten the screws in the mounting holes.



Mobile ALPR Mounting Solutions

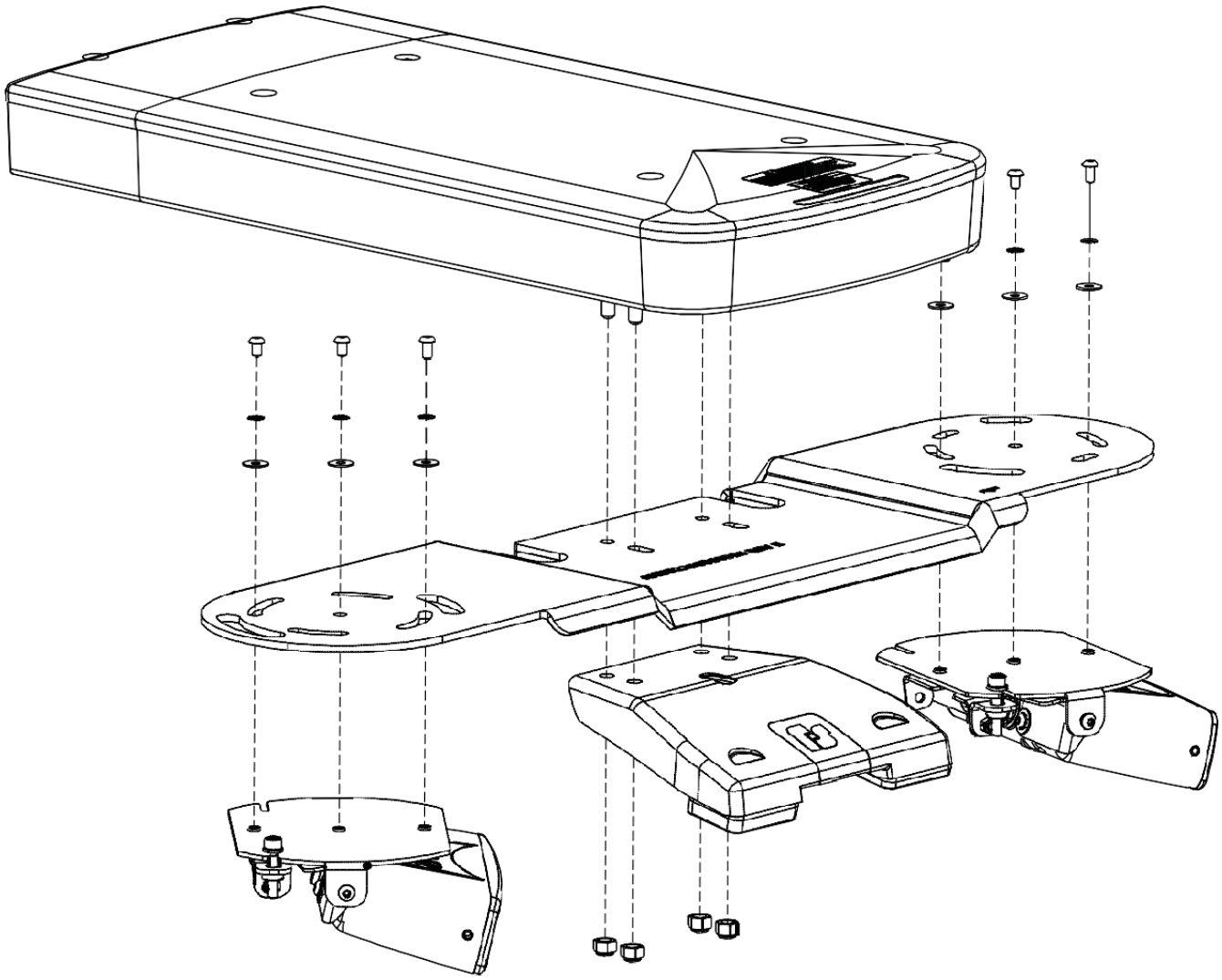
Below are examples of some of the mounting options available.

Supported Lightbar Mounting Options (Manufacturers):

- Federal Signal: Legend, Integrity, Argent, Vista, Raydian, Valor, Vision
- Code3: Defender 13.25 inch & 18 inch wide models
- Whelen: Edge, Justice, Liberty, Legacy, Freedom
- Tomar lightbars
- Unmarked Vehicle lightbar, Federal Signal product

Supported Non-Lightbar Mounting Options:

- Trunk Mount, Single or Dual Options
- Magnet Mounts (supports most vehicles with metallic/ferrous panels)
- Gutter Mounts (support Ford Police Interceptor models and Chevy Tahoe)



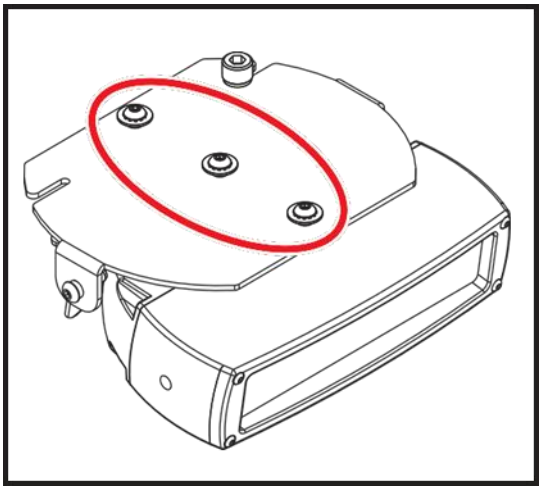
Shown - Classic Lightbar Bracket (Federal Signal "LEGEND")

Mounting the Camera Assembly to the Vehicle

The camera mounting assembly is then installed to the mounting plate attached to the lightbar.

NOTE: Due to the large number of variations between lightbars and mounting plates, this document only illustrates how to attach the camera mounting assembly to an existing mounting plate

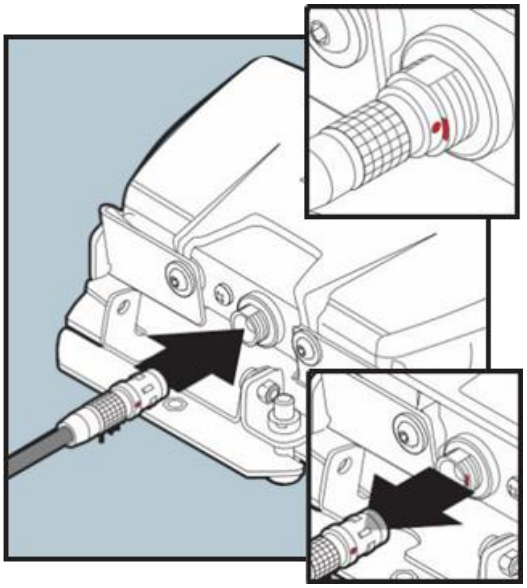
1. With the camera bracket attached to the camera, remove the three screws, star washers, and flat washers.



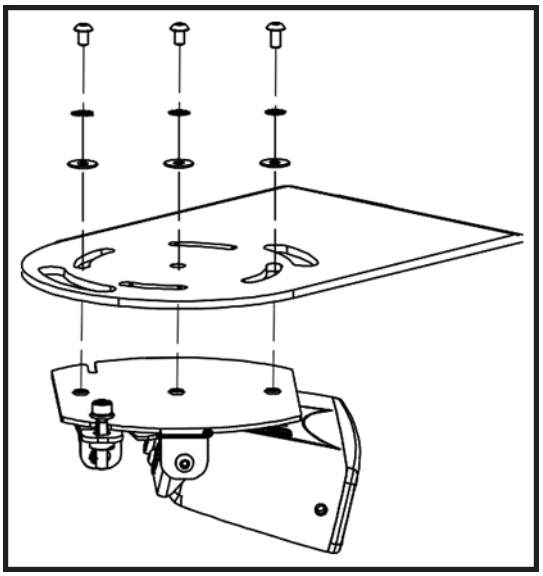
2. Connect the camera cable to the camera:
Align the red dot on connector with red mark on the port and connect using minimal force.

DO NOT FORCE OR TWIST THE CONNECTION. If the connector does not snap in easily, pull the connector out and realign.

PRO-TIP: PIPS recommends use of a bit of di-electric grease in and on the cable connectors.

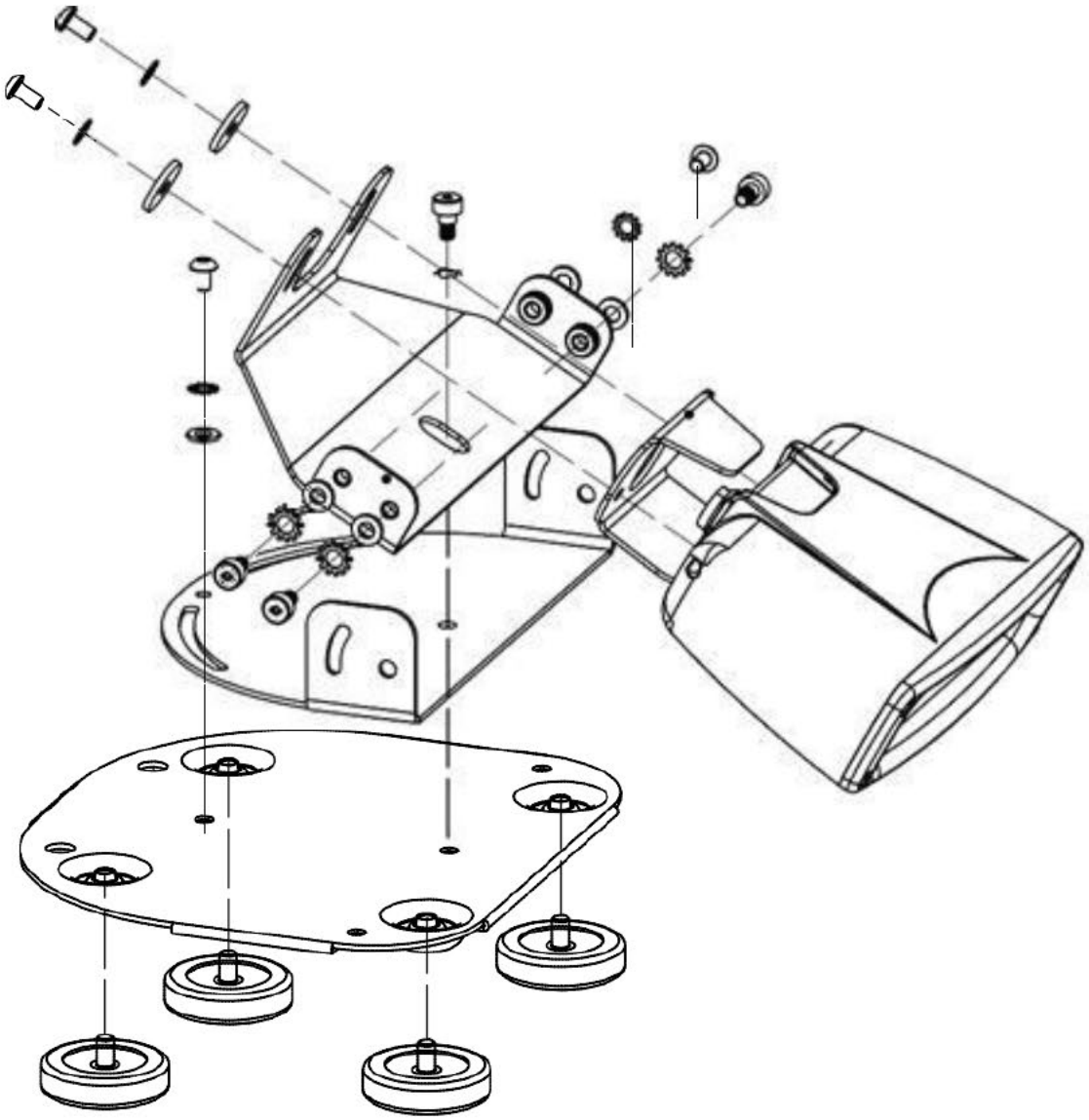


3. Attach the camera mounting assembly/plate to the lightbar bracket. **NOTE**: If the camera isn't perfectly secure, use the stabilizing foot included with the bracket to provide additional stability.



Attaching a Camera to Non-Lightbar Mounts

All Non-Lightbar mounting solutions utilize the Auxiliary 3 axis mounting plate. Once the camera is securely attached to the Aux mounting plate, attach it to the base plate of your bracket.



Shown – Magnet Mount

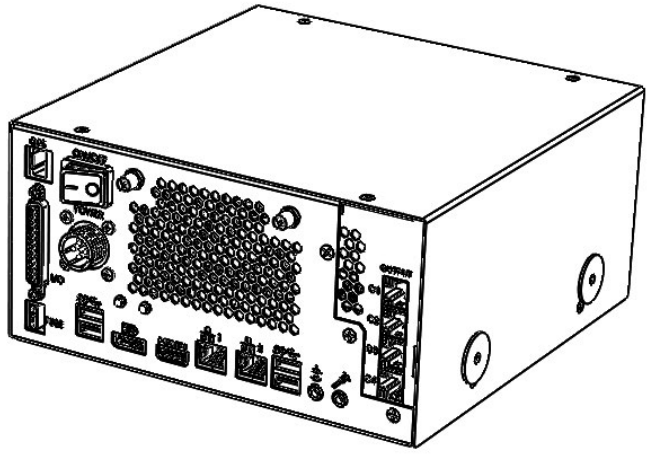
Mounting the Mobile Processor

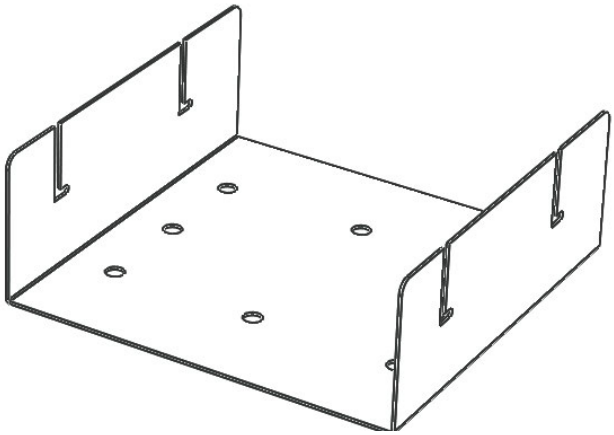
Understanding the vehicle and its current systems is a must when selecting the mounting location of the SupeRex (SX) Processor. Below are the key considerations:

- If the vehicle does not have a utility drawer/tray, be certain of all vehicle systems before drilling or mounting.
- The SX Processor and its bracket can be safely mounted in any orientation.
- Mount the unit with easy access to the rear panel and cables for maintenance/service.
- Be sure to leave adequate room for ventilation, cabling, and any maintenance needs.
- If the vehicle has a utility drawer/tray, mount the SX with enough clearance for ventilation, cabling, and service.
- Before mounting, physically place the SX in the mounting space to properly assess clearance or any dangers.
- Mount the bracket first, then secure the Mobile Processor to the bracket.

Additional Mounting Bracket Considerations:

- The Mobile Processor bracket comes with eight pre-drilled holes (0.375 in dia.). Use at least four of them to mount the bracket to the utility tray or trunk surface.
- For utility tray mounting, secure the unit using at least four 1/4-20UFC-2A bolts with appropriate washers and lock nuts. Hardware not provided.
- For direct trunk surface mounting, secure the unit using at least four #14 (or #16) sheet metal screws with appropriate washers. Hardware not provided.





WIRING AND CONNECTIONS

This section discusses the proper wiring and physical connections to the Mobile Processor. PIPS highly recommends the agency review the owner's manual of the ALPR vehicle to be certain of how to safely run cables and avoid vehicle/equipment damage. The agency is also responsible to fully understand how to safely tie into the on-board electrical systems in the vehicle.

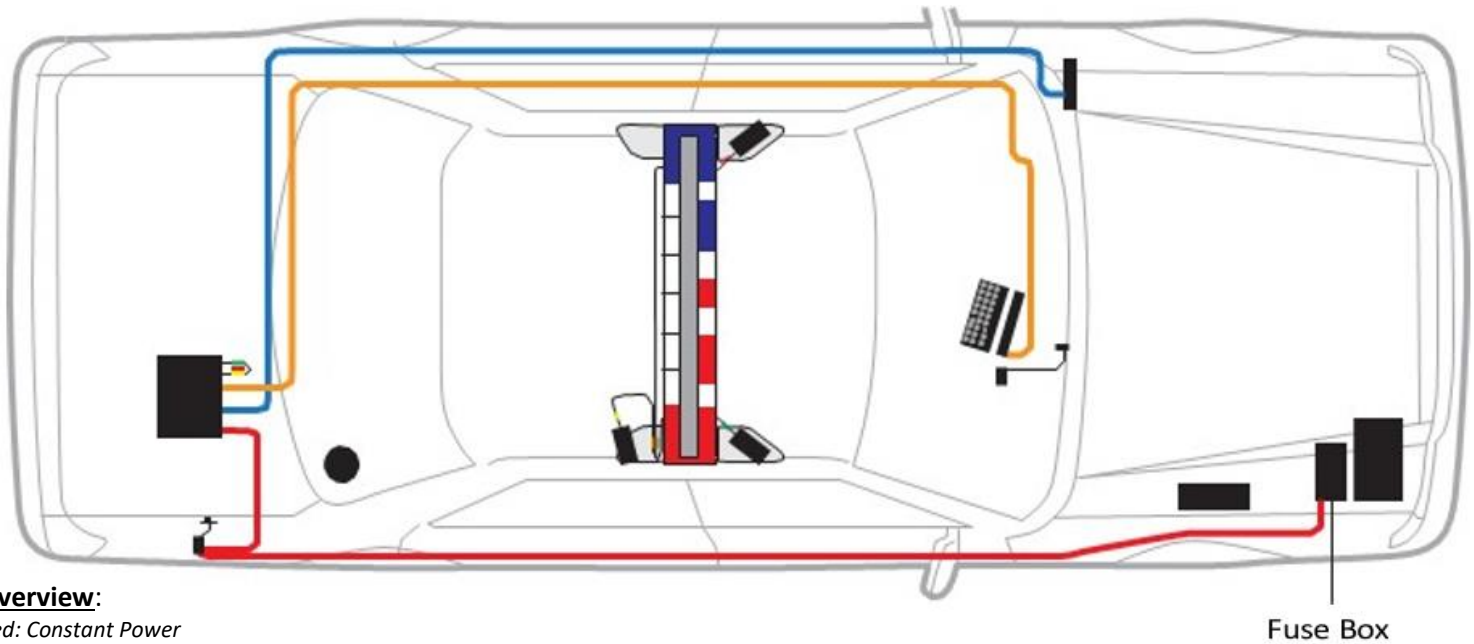
NOTE: Failure to adhere to this recommendation may immediately void all warranties and maintenance agreements.

The Power Wiring

The power cable provided with the Mobile Processor is a 3-wire connector. **NOTE**: The provided length of cable may not fit all vehicles. If wires must be extended, use 14 gauge or heavier. Min draw on 1 Cam system= 4.5AMPS, Max draw on 4 Cam system is 7.5AMPS.

1. Route the red wire (positive) from processor to a constant battery source. For example, a fused connection to the battery or to a vehicle power terminal block. Recommended fuse 20 amps.
2. Route the black wire (ground) from processor to vehicle ground tap.
3. Route the blue wire (remote) from processor to vehicle's ignition (key) source in the fuse panel or police packaging wiring harness. Recommended fuse 5 amps.





Overview:

Red: Constant Power
Blue: Remote/Ignition source
Black: Ground (barely visible off side of Processor)
Gold: Network (CAT5) to laptop or HDMI cable to front touchscreen

The GPS Antenna

The included GARMIN GPS antenna is a powerful omnidirectional receiver that can be mounted in any location with a line of sight to the sky.

1. Locate a position in, or on, the ALPR vehicle with a line of sight to the sky. Common zones are front dash, rear dash, rear window ledge, or on top of the vehicle.

2. Attach the hook side of hook-and-loop take to the underside of the GPS module.

3. Mount the antenna and route the GPS cable to the SX Processor.



GPS 16xHVS: Black PVC-jacketed, 5-meter, foil-shielded, 8-conductor 28 AWG with RJ-45 termination is waterproof up to 1m. Standby Current: < 10 microAmps

The Mobile Camera Cables

As mentioned previously, it's extremely important to review the vehicle manual when running the mobile camera cables.

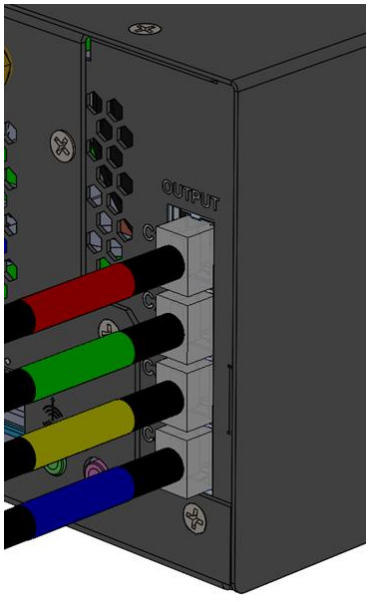
1. Locate the colored indicator rings that came with the Mobile Processor shipment.
2. Band and layout the camera cables to ensure the proper cables are going to the correct camera locations.
3. When run through the vehicle, be certain the cables do not get pinched or impede any of the vehicle airbags.

Color Coded Cable Rings:
Red: Front Left Camera
Green: Front Right Camera
Yellow: Rear Left Camera
Blue: Rear Right Camera

Connecting Camera Cables to the Processor

Connecting the P720 camera cables to the Mobile Processor is straight forward and as easy as plugging in a network cable. After the cables have been safely run through the vehicle, simply plug in the network (RJ45) connector to the appropriate camera port on the Processor (labeled C1-C4).

- Camera 1 Front Left (C1) = Red
- Camera 2 Front Right (C2) = Green
- Camera 3 Rear Left (C3) = Yellow
- Camera 4 Rear Right (C4) = Blue



Connecting the GPS Antenna to the Processor

After the antenna is placed with a line of site to the sky and its cable is securely run back to the Processor, simply plug in the RJ45 connection to the port labeled "GPS" located in the upper left corner of the rear I/O panel.

CAUTION: Plugging the GPS antenna into the wrong port may cause equipment damage and immediately void all warranties. Do **NOT** plug the GPS cable into a NIC or camera port. Do **NOT** plug a camera or network cable into the GPS port.

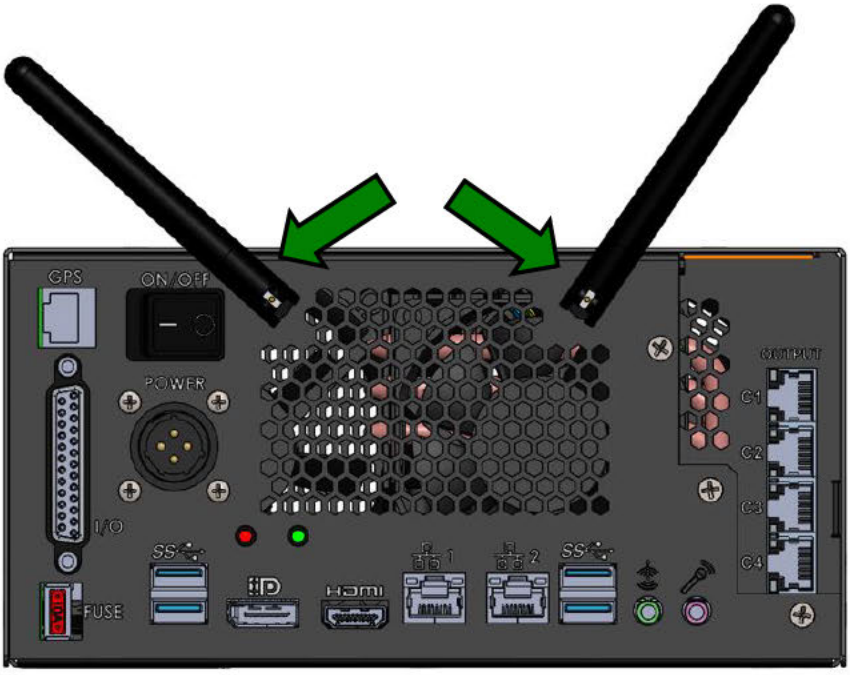


Connecting the Networking Elements to the Processor

The next step is to connect the networking option to the Processor. The most common method is a physical CAT5/6/7 cable from the Processor's NIC port 1 to an MDC/Laptop in the front of the vehicle.

NOTE: The on-board NICs are auto-switching. Meaning the agency can use either a standard network cable or a cross-over cable with no issues.

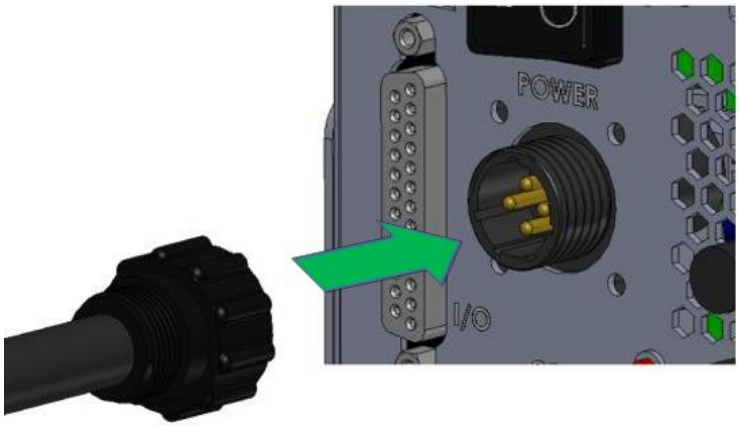
OPTION: In less than 1% of domestic orders, the Mobile Processor is built with Wi-Fi connectivity enabled. If the agency ordered this option, locate the two antennas from the accessories kit shipped with the Processor and install them to the Wi-Fi Networking Posts at the back of the Processor as shown below.

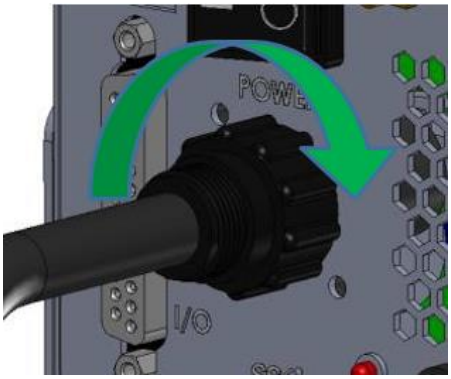


Connecting the Power Cable to the Processor

The last step in connecting all the cables to the Processor is to attach the power cable.

1. Align the notch on the power cable with the connection on the Processor
2. Insert the power cable onto the connection – DO NOT FORCE THE CABLE
3. After seating the cable properly, tighten the screw coupling/locking nut until snug – DON'T OVER TIGHTEN



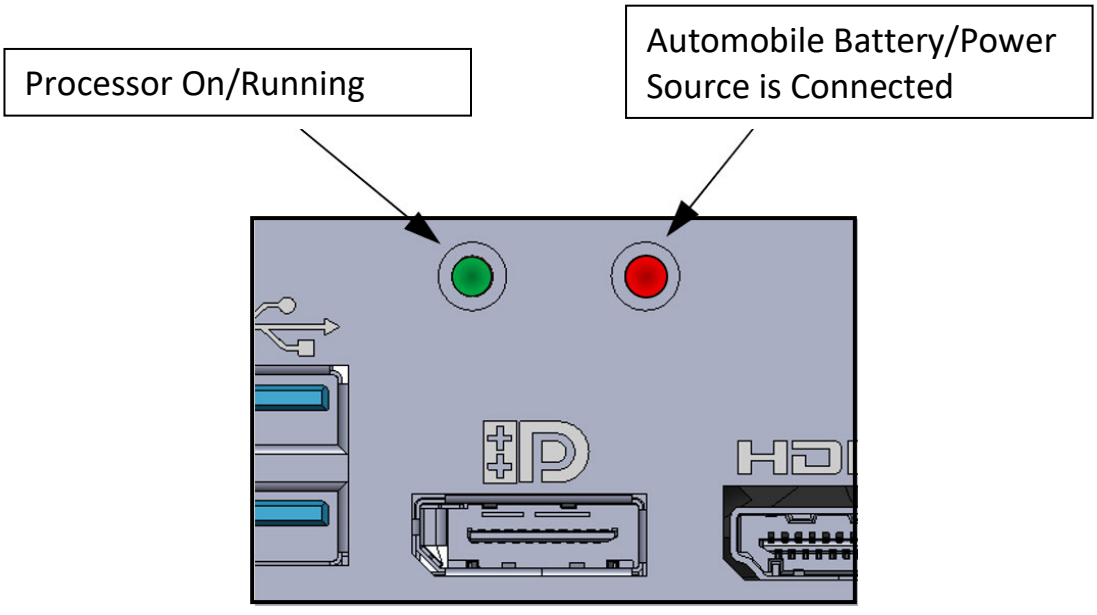


Confirming the Power Status

With all the vehicle wiring complete and the cables connected to the Processor, flip the power switch on the Processor to the On position and start the vehicle. Information on the status lights is below.

- The ignition sensitive fuse (blue wire) will register the start of the vehicle and energize the Processor
- Both the Red and Green LED status lights should illuminate
- The unit will POST and play audible tones (and the fans should spin)
- When ignition power is removed, the Processor will begin its shutdown process, indicated by the green LED flashing
- When the shutdown timer has finished, the unit will completely shut down, indicated by the green LED going out
- Conversely when the ignition is activated, the green light will come on.

NOTE: It is normal for the red LED to stay illuminated. Expected power draw while in standby is roughly 20-40 milliamps.



ALIGNMENT

The purpose of this section is to provide the best practices for the proper alignment of the PIPS Mobile ALPR Dual-Lens Cameras. The more accurate the alignment and illumination, the more effective the ALPR system will be. The values below should be considered as a baseline for general alignment and positioning of the cameras. Based on varying agency vehicles, mounting locations, and use-case scenarios, some fine tuning may be required.

ALIGNMENT PROCEDURE

The steps below assume the ALPR system has been successfully installed, the SX Processor is properly communicating with the cameras, and PAGIS (or Mobile Toolkit) is properly configured and functioning. NOTE: The greater the care taken during this process, the more accurately the ALPR system will perform in the field.

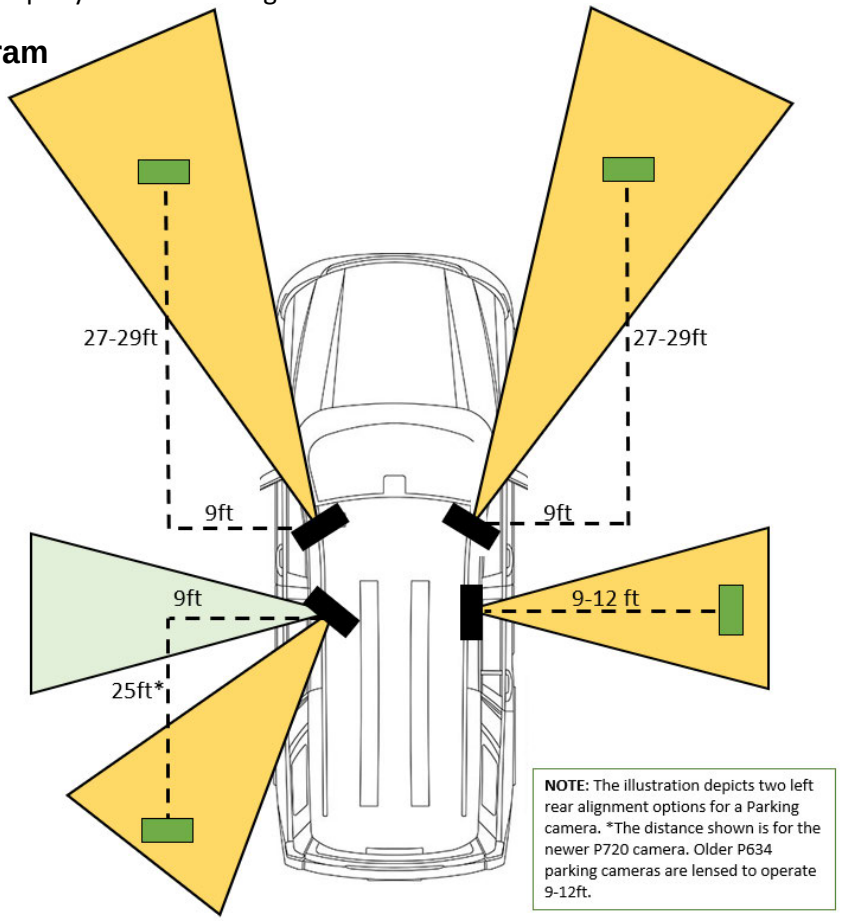
Alignment Requirements

- Large flat area without incline/decline (Ideal dimensions: 30 feet wide by 50 feet deep)
- No atmospheric conditions like fog or rain
- MEASURE ALL DISTANCES FROM THE CAMERA (NOT THE VEHICLE)
- Tripods or stands are stable and place the center of the License Plate at 32 inches above the ground

Tools Required

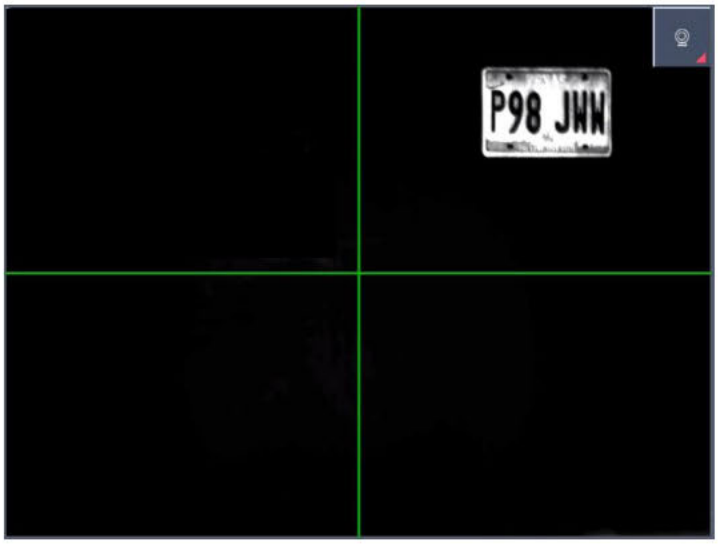
- Step Ladder
- #3, #3.5, and #4 hex/Allen wrench
- Chalk or Tape to mark the ground for template plate distances
- Tripod, tall parking cone, or box to secure test plates at 30-36” above the ground
- Tape measure or distance wheel
- Test license plate
- A configured MDC properly communicating with PAGIS

Distance Marker Diagram



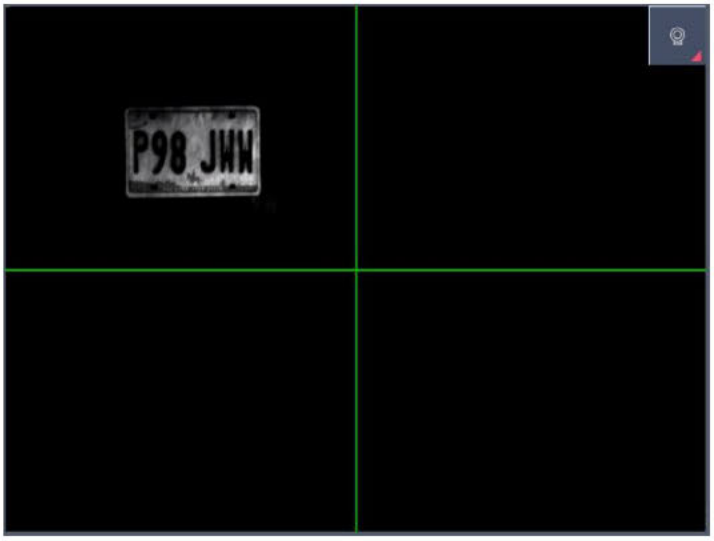
Aligning the Front Left Camera

- Place the completed plate stand on the distance marker
- Launch PAGIS from the MDC
- Login with Admin rights
- Click the Settings button from the top navigation menu (PAGIS 2.12 and above)
- Scroll down on the right-side menu and select “Cam Setup”
- Click the camera name to be aligned
- Use the camera view toggle button to confirm the proper camera is selected then switch the view to Infrared (IR)
- Loosen the mounting screws on the camera bracket just enough to allow for movement
- While monitoring the IR camera feed, position the camera so the plate is viewed as shown below
- Once set, tighten the mounting screws on the bracket to lock the camera in place



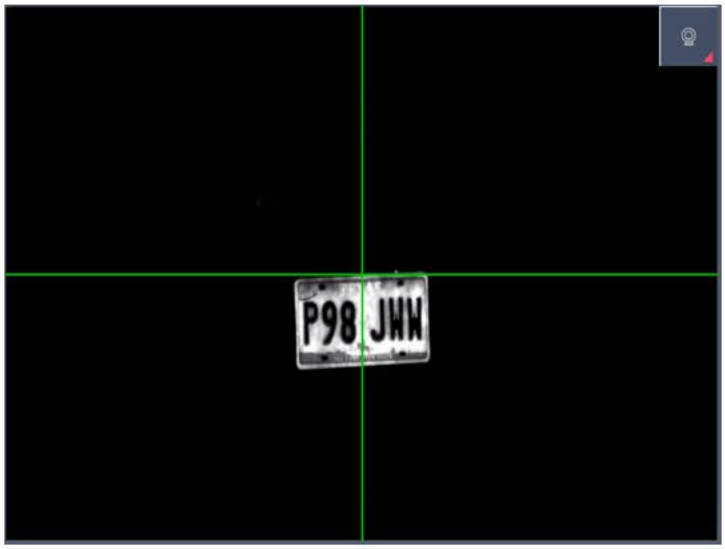
Aligning the Front Right Camera

- Use the preparatory alignment steps from above
- While monitoring the IR camera feed, position the camera so the plate is viewed as shown below
- Once set, tighten the mounting screws to lock the camera in place



Aligning the Right Rear Parking Camera

- Measure 10-12ft to the right side of the vehicle (from the parking camera)
- Place a completed plate stand at the mark
- Launch PAGIS from the MDC
- Login with Admin rights
- Click the Settings button from the top navigation menu (PAGIS 2.12 and above)
- Scroll down on the right-side menu and select "Cam Setup"
- Click the camera name to be aligned
- Use the camera view toggle button to confirm the proper camera is selected then switch the view to Infrared (IR)
- Loosen the mounting screws on the camera bracket just enough to allow for movement
- While monitoring the IR camera feed, position the camera so the plate is viewed as shown below
- Once set, tighten the mounting screws on the bracket to lock the camera in place



Aligning the Left Rear Camera

- Parking Option: Follow the steps for the Right Parking Camera
- Rear Facing Parking Camera Option: Measure 9 feet out and 25 feet down the lane
- Rear Facing (Third) Traffic Camera Option: Follow all steps for front left camera
    - Launch PAGIS from the MDC
    - Login with Admin rights
    - Click the Settings button from the top navigation menu (PAGIS 2.12 and above)
    - Scroll down on the right-side menu and select "Cam Setup"
    - Click the camera name to be aligned
    - Use the camera view toggle button to confirm the proper camera is selected then switch the view IR
    - Loosen the mounting screws on the camera bracket just enough to allow for movement
    - While monitoring the IR camera feed, position the camera so the plate is viewed as shown below
    - Once set, tighten the mounting screws on the bracket to lock the camera in place

CALIBRATING EXPOSURE TABLES

Proper plate illumination is necessary for the mobile ALPR system to function correctly. Administrators should take care not to under or over saturate the plate with Infrared (IR) light. Use the steps below to discover the plate "standard" and then select values just above, and just below that starting point to account for varied environmental conditions over time.

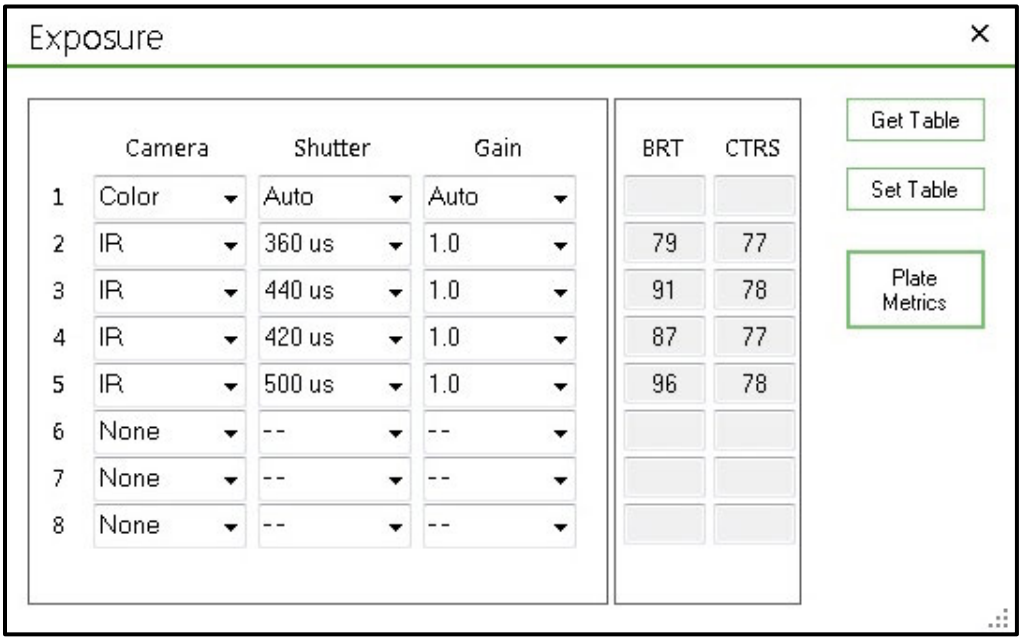
Exposure Table Best Practices

- Only calibrate 1 license plate at a time
- Only use a Gain setting of 1 or 1.5 (values above 1.5 amplify visual "noise" and could lead to misreads)
- Use 1 Color setting and 4 IR settings

Setting the Exposure Table/Plate Illumination

1. Remote Desktop to the SX4e
2. Open Tools from the Desktop
3. Launch Mobile Toolkit
4. The default view is the Infrared (IR) feed of the left front camera (Input 1)
5. Use the Input menu to navigate to the camera to be configured
6. Then from the Settings Menu, select "Exposure"
7. Be sure the plate is clearly viewable for the distance to be calibrated
8. Click the "Get Table" button to import the current exposure settings from the camera
9. Next, use the "Plate Metrics" button to analyze the current illumination
10. Adjust the exposure settings to increase or decrease illumination as necessary
    a. Increasing the Exposure will increase the Brightness (BRT) and Contrast (CTRS)
    b. Ideal BRT is above 60 **NOTE**: BRT over 90 begins to over-saturate the plate and could lead to misreads
    c. Ideal CTRS is roughly 80 (the higher the contrast the better)
11. Be sure to re-run Plate Metrics after each adjustment to the exposure table
12. Once the ideal value is discovered, fill in the other IR fields with values just above, and just below this ideal setting to account for varied atmospheric possibilities
13. Leave the Color setting to "Auto"
14. When all values are selected, click the "Set Table" button to save the changes
15. Then move on to the other cameras

NOTE: In order to read plates two lanes over, the exposure settings will need to be close to the maximum settings. This will over-expose some of the near lane plates and is the tradeoff made by agencies looking to expand ALPR coverage. An example of those settings is below.



MAINTENANCE AND SERVICE

This section discusses the general service and maintenance of the Mobile ALPR System.

Qualifications

To properly install or service the ALPR system, the technician must have a good understanding of automotive electrical systems as well as a proficiency in maintaining computer systems and networks in a mobile environment.

Servicing Mobile ALPR Cameras

Establishing a regular maintenance schedule for the Mobile ALPR cameras extends the life of the system and ensures safety. Periodically check the Mobile ALPR cameras to ensure the camera lenses are clean, all LEDs illuminate when the system is operating, and that all mounted hardware is securely fastened to the vehicle. Also, inspect the camera front cover for cracks, crazing (hairline cracks), discoloration, and other defects.

CAUTION: DO NOT open the camera housing. Each camera is nitrogen purged to remove moisture. If the camera is opened moisture will enter the camera resulting in potential damage to the electronics and accumulation on the lenses. If the camera is opened the warranty is void. For service, support, or replacement please contact Customer Support.

Cleaning Mobile ALPR Cameras

The lens of the camera should be cleaned before each use. Accumulation of insects, road grime, and other debris can obstruct the camera and reduce the plate read capability. To clean the lens, do not use an alcohol or ammonia based cleaner like Windex. Cleaners containing these compounds can damage the polycarbonate cover. PIPS Recommends use of a microfiber cloth and a mild soap and water solution.

Servicing the Mobile ALPR Processor

The housing of each Processor is sealed. If the seals are broken, the warranty of the unit will be void. Software and firmware can be updated at the direction of Customer Support.

Servicing the 10.4 inch Touchscreen Monitor

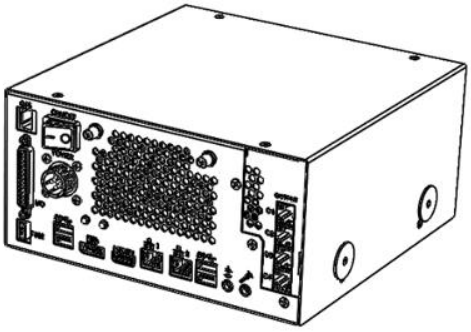
If monitor issues develop, first check the power and video connections. Make sure the cords are connected properly and are not twisted. Then clean the touchscreen. The touchscreen monitor should be cleaned before each use. Oils from fingers accumulate on the screen and can erode performance. To clean the screen DO NOT USE an alcohol or ammonia based cleaner. Cleaners containing these compounds can damage the touch screen. Use of an anti-fog, anti-static cleaner and a microfiber cloth.

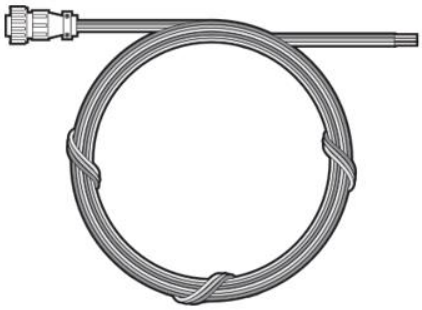
Cleaning the Vehicle

When washing the vehicle, it’s best to avoid automatic car washes that use the older rotating nylon bristles. The fibers can become lodged in the camera brackets and misalign the cameras or damage the acrylic cover plate. Automatic car washes that use Soft Cloth or touchless (high pressure spray) can be used as they do not pose a risk to the cameras. For non-lightbar mounting solutions, it is not recommended to use rotating car wash systems for any brackets that use magnets to secure them to the vehicle.

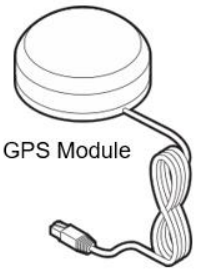
APPENDIX A – ALPR COMPONENTS

Standard Components

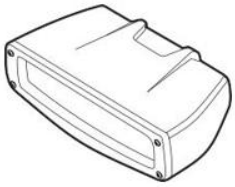




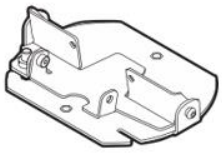
Mobile ALPR Processor
Power Cable



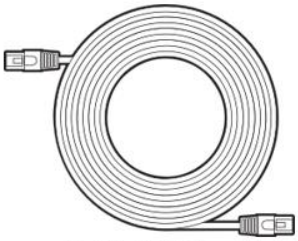
GPS Module



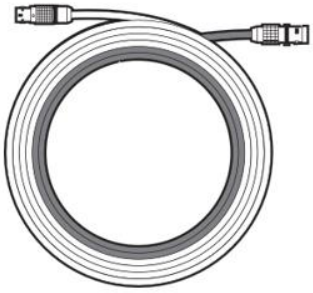
Camera
(1-4 per Processor)



Right-Hand Bracket
(1 per Camera)



Mobile ALPR Processor
Ethernet Crossover Cable



Camera Cable
(1 per Camera)

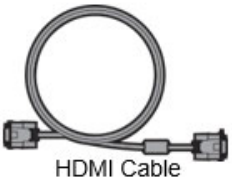
Optional with Stand-Alone Configuration



DC-DC Power Cable

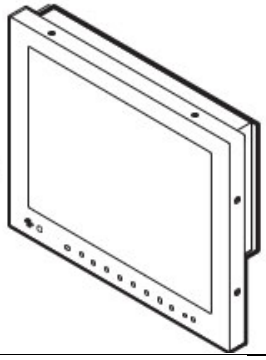


USB Cable
(2 per system)

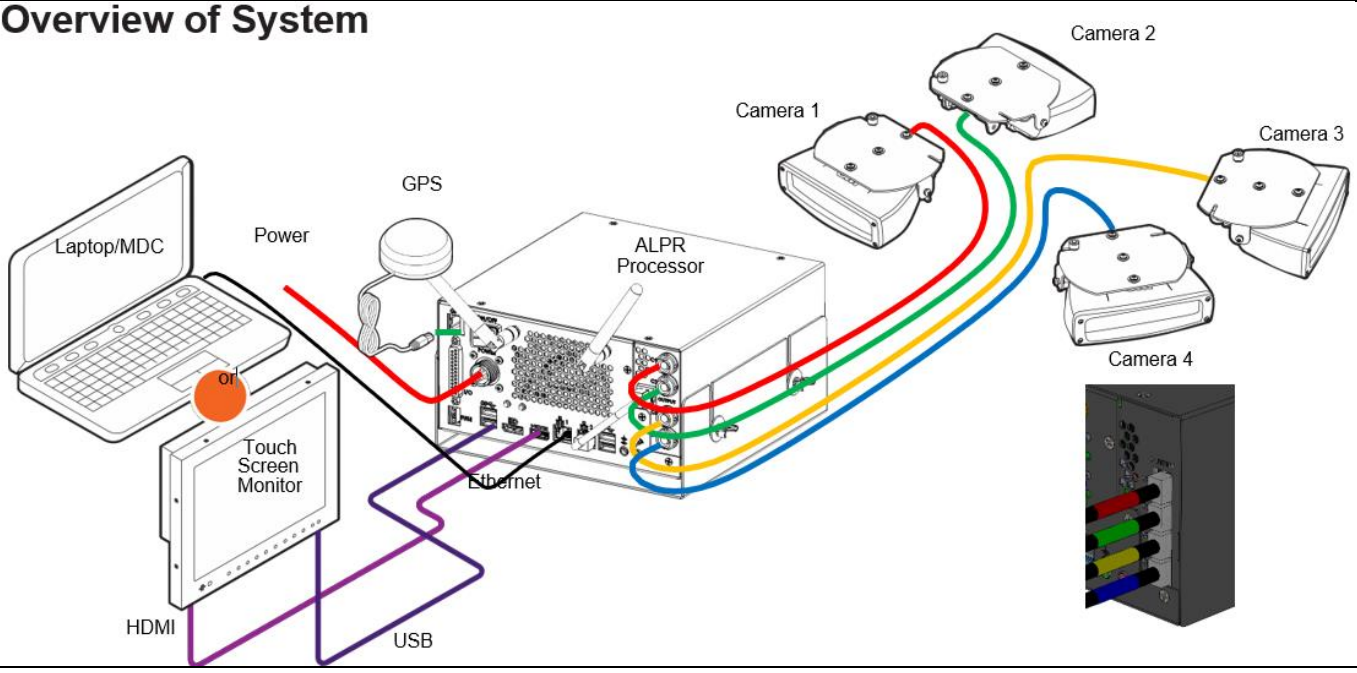


HDMI Cable

Touch Screen Monitor
(Mounting bracket provided by others)

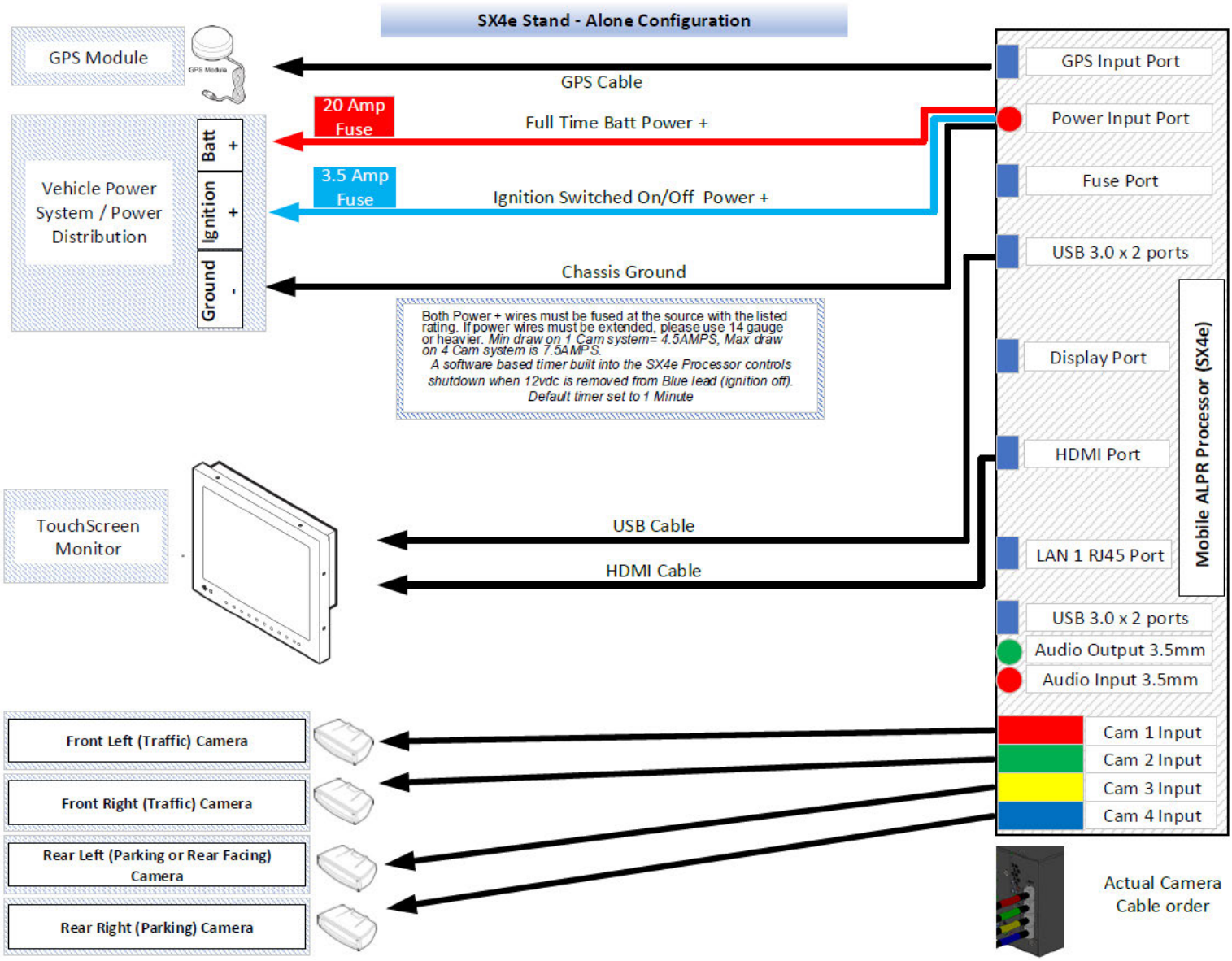


Overview of System



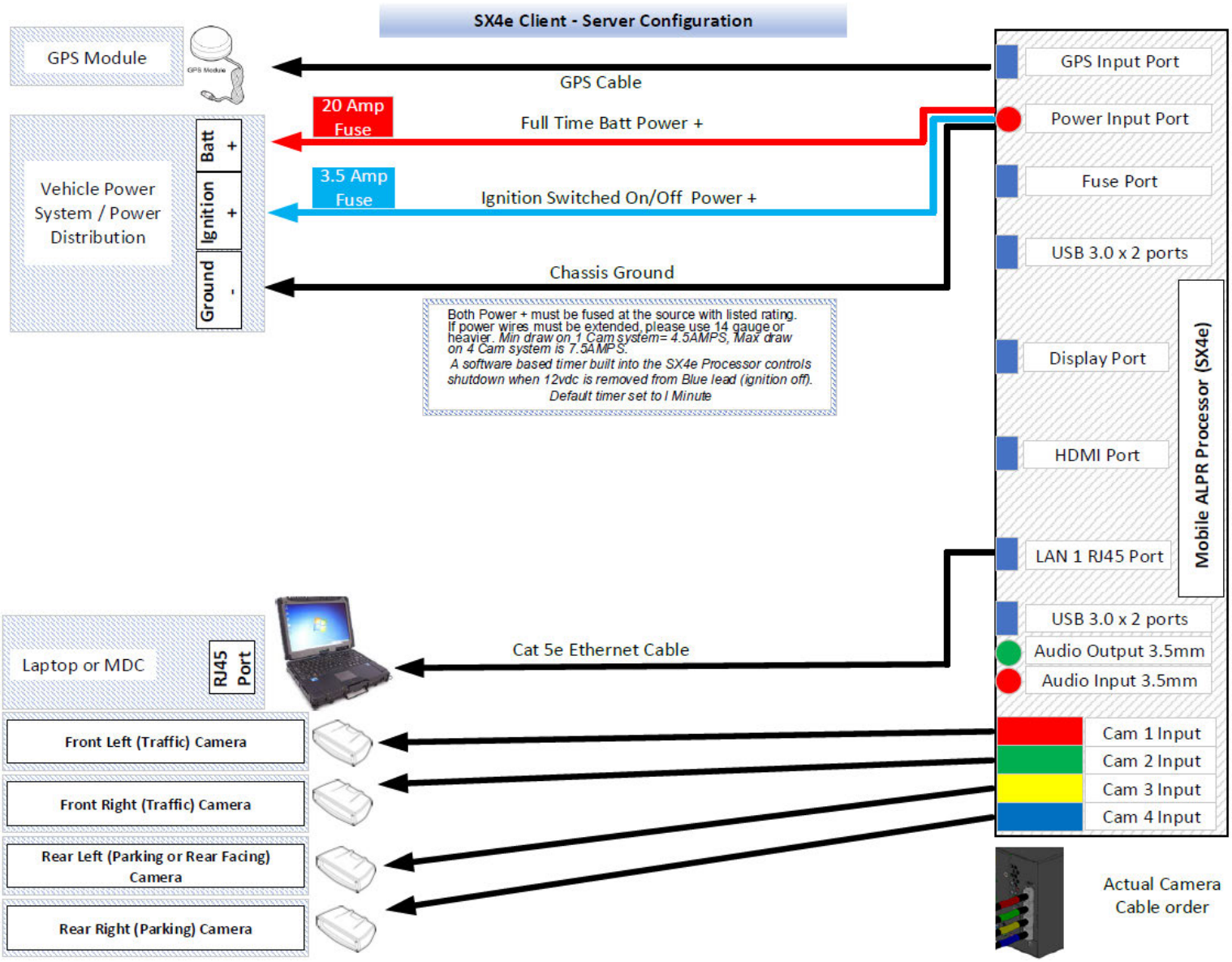
APPENDIX B – WIRING DIAGRAM

Below is the wiring diagram for a Stand-Alone Processor.



APPENDIX C – WIRING DIAGRAM

Below is the wiring diagram for client/server (VPRelay mode) used with a laptop in the front of the vehicle.



UTMC ALPR Protocol

A UTMC Technical Guide
Library reference ***TR007.001c***

Updated July 2020
Cover + 31 pages

Written by UTMC © Copyright UTMC Ltd
Developed in part with PIPS Technology

List of contents

1 Introduction **3**
1.1 About this document 3
1.2 Status of this document 3
1.3 Context 3
1.4 Web service interfaces 4

2 Camera to Instation **5**
2.1 Introduction 5
2.2 PlateRead 5
2.3 ALPR diagnostics 6
2.4 Machine diagnostics 7
2.5 Logs 8
2.6 Images 8
2.7 Camera and Configuration 9
2.8 Configuration request 11
2.9 Heartbeat message 11

3 Instation To Camera **13**
3.1 Introduction 13
3.2 Configuration 13
3.3 Log request 14
3.4 Configuration request 14
3.5 Image request 15
3.6 Acknowledgement 16

4 Tag Hashing algorithm **17**
4.1 About the algorithm 17
4.2 Example 17

Appendix 1 PlateRead Element **19**

Appendix 2 ALPRDiagnostic Element **21**

Appendix 3 MachineDiagnostic Element **23**

Appendix 4 Image Element **25**

Appendix 5 Camera Configuration Elements **26**
A5.1 Camera Element 26
A5.2 Lane Element 27
A5.3 Configuration Element 28

Appendix 6 ImageRequest Elements **31**
A6.1 TimeRangeImageRequest 31
A6.2 PriorVRNImageRequest 31
A6.3 InstanceSetImageRequest 32
A6.4 ContextImageRequest 32

1 Introduction

1.1 About this document

1.1.1 UTMC is a UK-led initiative which provides and maintains a technical framework for traffic management and related systems. It is geared to producing open specifications geared to the needs of real world projects, delivered through an efficient and innovative supply market. UTMC specifications are endorsed by the UK Department for Transport and are published on the UTMC website at: http://www.utmc.uk.com.

1.1.2 To help users get the best out of the UTMC Technical Specification, we provide a set of guidance documents addressing some of the associated issues, ranging from non technical aspects such as procurement policy and operations, to technical aspects such as database design and communications network configuration.

1.1.3 This document is a guidance document primarily for developers, and is concerned with expanding on the technical implementation of UTMC protocols within an ALPR system.

1.2 Status of this document

1.2.1 This document is based on the previous version, TR007 001b, produced by the UTMC ALPR Working Group (2009-2010).

1.2.2 UTMC gratefully acknowledges the work of the members of the Working Group in compiling this guidance and the associated elements of the Technical Specification.

1.3 Context

1.3.1 This protocol is for use by ALPR cameras when connecting to UTMC systems as used by numerous authorities across the UK, with the goal of achieving interoperability between suppliers. Although the primary aim has been to provide standardized ALPR data for journey time systems, the scope of the protocol includes the provision of additional data meeting NAAS requirements (for example images) to satisfy Police requirements in the event that Local Authorities and the Police wish to share cameras.

1.3.2 The UTMC ALPR protocol was developed within the following framework:

- This standard utilises non-proprietary elements and is based on XML. It is recognised that the communications costs associated with the use of XML may be higher at present than those for a less verbose protocol. However, it is hoped that the ease of use and the wide support of XML will lead to the ready exploitation of a forward-looking XML based open standard, particularly in the light of ongoing reductions in communication costs.

- The focus of this protocol is Camera to Instation and Instation to Camera communications. In parallel, a set of attribute extensions have been developed for the Common Database CCTV Data Object, which allow the Instation to add distilled ALPR data to the CDB. This document does not deal with Instation to Instation Journey Time Exchange.

- This protocol should be formed with some consideration of existing protocols and guidance – UTMC, Datex and possibly NTCIP.

- This protocol should be scalable. Elements such as image transfer may not be a requirement of all users. The protocol should be developed in a way to ensure that such additions are optional.

1.4 Web service interfaces

1.4.1 All web interfaces are SOAP (Simple Object Access Protocol) based and are described in WSDL (Web Services Description Language).

1.4.2 To summarise the Instation WSDL, the interface allows the camera to send XML element: <CameraToInstation> and in reply receives an XML element: <InstationToCamera>.

1.4.3 The camera WSDL allows the Instation to send XML element: <InstationToCamera>.

1.4.4 It should be noted that SOAP headers are not included in the UTMC ANPR WSDL files (camera.wsdl and instation.wsdl) or in the xml excerpts shown below. SOAP headers must therefore be generated for any SOAP-compliant implementation.

1.4.5 Both <CameraToInstation> and <InstationToCamera> elements have a mandatory version number attribute:

- SchemaVersion, indicating the version number of the element which contains it (SchemaVersion is a string containing dot-separated numbers (starting with 1.0). The first digit indicates a major revision, the second indicates updates to that revision.)

1.4.6 The xml excerpts shown below relate to V1.2 of the UTMC ALPR Protocol.

2 Camera to Instation

2.1 Introduction

2.1.1 This XML element is intended for transmitting all information from Camera to Instation. It allows for sending: plate data, ALPR and machine diagnostics, proprietary logs, images, current Camera configuration and request for configuration in any combination.

2.1.2 The option must be provided to use Gzip compression of the entire Camera to Instation element. The protocol does not provide for enabling or disabling this feature - it must be enabled or disabled by a commissioning engineer, either on-site or via a remotely connected engineering application.

2.1.3 Mandatory elements are:

- CameraID to identify the Camera
- TimeStamp which is the date and time of message creation

2.1.4 For clarity, each type of information payload is discussed separately; however messages may use any combination of elements.

2.1.5 All array elements include an optional attribute "ManufacturerSpecific" (not shown in the examples) which enables the communication of additional information outside the scope of the pre-defined attributes.

2.2 PlateRead

2.2.1 An optional array of plate read results may be included. For each entry in the array, the following are mandatory:

- InstanceID to identify the plate read event;
- TimeStamp which is the date and time of the sighting;
- LaneID representing the lane in which the plate was travelling;
- VehicleDirection representing the direction the vehicle was travelling in the lane;
- PlateNotRead, a flag to indicate a vehicle has been detected but no plate read.

2.2.2 The following is an example message containing a single plate read.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CameraToInstation xmlns=" http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <CameraID>0</CameraID>
    <TimeStamp>2009-06-29T12:01:59.377+01:00</TimeStamp>
    <PlateReadArray>
        <PlateRead>
            <InstanceID>0</InstanceID>
            <TimeStamp>2009-06-29T12:01:59.379+01:00</TimeStamp>
            <TimeStampError>5</TimeStampError>
            <LaneID>0</LaneID>
            <VehicleDirection>U</VehicleDirection>
            <XYType>OSGB</XYType>
            <XCoord>123456.7</XCoord>
            <YCoord>654321.0</YCoord>
            <PlateNotRead>false</PlateNotRead>
            <VRN>A123BCD</VRN>
            <VRNConfidence>85</VRNConfidence>
```

```
                <Tag>1234</Tag>
                <TagConfidence>90</TagConfidence>
                <Classification>1</Classification>
                <Country>GBR</Country>
                <Make>Ford</Make>
                <Model>Focus</Model>
                <Colour>Red</Colour>
                <Velocity>50</Velocity>
                <VelocityError>5</VelocityError>
            </PlateRead>
        </PlateReadArray>
</CameraToInstation>
```

2.2.3 Where the Camera has been configured to send plate reads immediately, the <PlateReadArray> element will only contain a single <PlateRead> element. Where the Camera is configured to send batches of plate reads, multiple <PlateRead> elements will be present. It is mandatory that each <PlateRead> element contains at least one of <VRN> or <Tag>.

2.2.4 See section 4 for an explanation of the hashing algorithm which is used to convert the <VRN> element to a hashed tag (the <Tag> element) for the purposes of journey time or origin-destination applications.

2.2.5 These elements are described in more detail in Appendix 1.

2.3 ALPR diagnostics

2.3.1 An optional array of ALPR diagnostics may be included (one entry per lane). For each entry in the array, the following are mandatory:

- TimeStamp which is the date and time of end of the diagnostic period;
- DiagnosticType representing whether the entry is a routine diagnostic or an alarm;

2.3.2 The following is an example message containing all defined ALPR Diagnostic objects:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CameraToInstation xmlns=" http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <CameraID>0</CameraID>
    <TimeStamp>2009-06-29T12:01:59.377+01:00</TimeStamp>
    <ANPRDiagnosticArray>
        <ANPRDiagnostic>
            <TimeStamp>2009-06-29T12:01:59.379+01:00</TimeStamp>
            <DiagnosticType>routineDiagnostic</DiagnosticType>
            <LaneID>0</LaneID>
            <MeanVRNConfidence>82</MeanVRNConfidence>
            <MeanTagConfidence>85</MeanTagConfidence>
            <MeanPlateContrast>56</MeanPlateContrast>
            <MeanCharacterHeight>15</MeanCharacterHeight>
            <MeanHorizontalAngle>8</MeanHorizontalAngle>
            <MeanVerticalAngle>2</MeanVerticalAngle>
            <MeanTrajectoryOffset>2</MeanTrajectoryOffset>
            <MeanTrajectoryAngle>11</MeanTrajectoryAngle>
            <MeanVelocity>45</MeanVelocity>
            <MeanVelocityError>4</MeanVelocityError>
```

```
                <PlateToTriggerRatio>90</PlateToTriggerRatio>
                <PlatesNoCountryRatio>3</PlatesNoCountryRatio>
                <PlatesTowardsRatio>43</PlatesTowardsRatio>
                <PlatesAwayRatio>45</PlatesAwayRatio>
                <MeanIRLevel>53</MeanIRLevel>
                <MeanExposure>350</MeanExposure>
                <MeanGain>-10</MeanGain>
            </ANPRDiagnostic>
        </ANPRDiagnosticArray>
</CameraToInstation>
```

2.3.3 These elements are described in more detail in Appendix 2.

2.4 Machine diagnostics

2.4.1 An optional array of machine diagnostics (describing hardware, software and communications performance) may be included. For each entry in the array, the following are mandatory:

- TimeStamp which is the date and time of the end of the diagnostic period;
- DiagnosticType representing whether the entry is a routine diagnostic or an alarm;
- HostName representing the host to which communications diagnostics relate

2.4.2 The following is an example message containing all proposed Machine Diagnostic objects:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CameraToInstation xmlns=" http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <CameraID>0</CameraID>
    <TimeStamp>2009-06-29T12:01:59.377+01:00</TimeStamp>
    <MachineDiagnosticArray>
        <MachineDiagnostic>
            <TimeStamp>2009-06-29T12:01:59.379+01:00</TimeStamp>
            <DiagnosticType>routineDiagnostic</DiagnosticType>
            <MeanCPUTemperature>56</MeanCPUTemperature>
            <MeanTotalCurrent>120</MeanTotalCurrent>
            <MeanIlluminatorTemp>70</MeanIlluminatorTemp>
            <MeanIlluminatorCurrent>90</MeanIlluminatorCurrent>
            <IlluminatorUsage>123</IlluminatorUsage>
            <MeanIlluminatorOutput>90</MeanIlluminatorOutput>
            <LastResetTime>2009-06-29T12:01:59.379+01:00</LastResetTime>
            <NoOfHardwareErrors>0</NoOfHardwareErrors>
            <MeanSignalStrength>-36</MeanSignalStrength>
            <HostName>192.168.1.1</HostName>
            <MeanCommsLag>23</MeanCommsLag>
            <WorstCommsLag>50</WorstCommsLag>
            <NoOfCommsResends>3</NoOfCommsResends>
            <NoOfCommsFailures>1</NoOfCommsFailures>
            <NoOfCommsReconnects>2</NoOfCommsReconnects>
            <MeanSyncDifference>40</MeanSyncDifference>
            <WorstSyncDifference>123</WorstSyncDifference>
            <LastSyncTime>2009-06-29T12:01:59.379+01:00</LastSyncTime>
            <SupplyVoltage>98</SupplyVoltage>
            <TamperAlarm>normal</TamperAlarm>
```

```
            </MachineDiagnostic>
        </MachineDiagnosticArray>
</CameraToInstation>
```

2.4.3 These elements are described in more detail in Appendix 3.

2.5 Logs

2.5.1 An optional array of log messages (representing logged events such as power up, configuration change or communication error) may be included. For each entry in the array, the following is mandatory:

- TimeStamp which is the date and time relating to the log message;

2.5.2 The following is an example message outlining the format of a Log Array:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CameraToInstation xmlns=" http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <CameraID>0</CameraID>
    <TimeStamp>2009-06-29T12:01:59.377+01:00</TimeStamp>
    <LogArray>
        <Log>
            <TimeStamp>2009-06-29T12:01:59.379+01:00</TimeStamp>
            <InstanceID>0</InstanceID>
            <LogMessage>System Restart</LogMessage>
        </Log>
    </LogArray>
</CameraToInstation>
```

2.5.3 The <LogArray> element may contain any number of <Log> elements. LogMessage elements may contain XML or plain text in proprietary format, as long as XML formatting rules are strictly followed.

2.6 Images

2.6.1 An optional array of camera images may be included. For each entry in the array, the following are mandatory:

- TimeStamp which is the date and time at which the image was captured;
- ImageType representing the type of the image e.g. plate patch, ALPR image etc;

2.6.2 The following is an example message containing binary images. Five types of image can be sent: PlatePatch, ALPR Image, Overview Image, Context Image or Context Overview Image:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CameraToInstation xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <CameraID>0</CameraID>
    <TimeStamp>2009-06-29T12:01:59.377+01:00</TimeStamp>
    <ImageArray>
        <Image>
            <InstanceID>0</InstanceID>
            <TimeStamp>2009-06-29T12:01:59.379+01:00</TimeStamp>
```

```
            <VRN>A123BCD</VRN>
            <LaneID>0</LaneID>
            <ImageType>platePatch</ImageType>
            <ImageFormat>jpeg</ImageFormat>
            <BinaryImage>[IMAGE DATA]</BinaryImage>
        </Image>
        <Image>
            <InstanceID>0</InstanceID>
            <TimeStamp>2009-06-29T12:01:59.379+01:00</TimeStamp>
            <VRN>A123BCD</VRN>
            <LaneID>0</LaneID>
            <ImageType>ANPRImage</ImageType>
            <ImageFormat>gif</ImageFormat>
            <BinaryImage>[IMAGE DATA]</BinaryImage>
        </Image>
        <Image>
            <InstanceID>0</InstanceID>
            <TimeStamp>2009-06-29T12:01:59.379+01:00</TimeStamp>
            <VRN>A123BCD</VRN>
            <LaneID>0</LaneID>
            <ImageType>overviewImage</ImageType>
            <ImageFormat>tiff</ImageFormat>
            <BinaryImage>[IMAGE DATA]</BinaryImage>
        </Image>
    </ImageArray>
</CameraToInstation>
```

2.6.3 These elements are described in more detail in Appendix 4.

2.6.4 It should be noted that InstanceID is not required for an ad-hoc context image or any image that may be requested from the Instation where there is no association with a vehicle, and therefore no VRN has been collected with a corresponding Instance ID. However, where an image relates to a plate read, the InstanceID for the plate read is included in the image attributes.

2.7 Camera and Configuration

2.7.1 Optional Camera and Configuration elements may be included in response to a ConfigRequest issued by the Instation via the InstationToCamera element. The following is mandatory in the Camera element:

- HardwareUniqueID which represents a globally unique identifier for the camera

2.7.2 At least one Lane element per camera is mandatory. The following are mandatory in each Lane element:

- LaneID representing the lane relative to the camera to which the lane config applies
- LaneNumber representing the lane position in the carriageway
- LaneDirectionTypeID representing the direction of travel of the carriageway lane
- NormalVehicleDirection - whether vehicles normally travel towards or away from the camera

2.7.3 The following is an example message outlining a Camera and Configuration response to an Instation ConfigRequest, which includes both Camera and Configuration elements:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CameraToInstation xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <CameraID>0</CameraID>
    <TimeStamp>2009-06-29T12:01:59.377+01:00</TimeStamp>
    <Camera>
        < HardwareUniqueID>CA_Traffic:Evo8:7205/0219</ HardwareUniqueID>
        <ShortDescription>My Short description</ShortDescription>
        <LongDescription>My long description</LongDescription>
        <XYType>OSGB</XYType>
        <XCoord>123456.7</XCoord>
        <YCoord>654321.0</YCoord>
        <Height>3.5</Height>
        <TypeID>7</TypeID>
        <MobileCamera>false</MobileCamera>
        <SoftwareVersion>2.1.1</SoftwareVersion>
        <LaneArray>
            <Lane>
                <LaneID>0</LaneID>
                <LaneNumber>1</LaneNumber>
                <LaneDirectionTypeID>5</LaneDirectionTypeID>
                <NormalVehicleDirection>towards</NormalVehicleDirection>
            </Lane>
        </LaneArray>
    </Camera>
    <Configuration>
        <HostName>HOST1</HostName>
        <SendVRNs>true</SendVRNs>
        <SendTags>false</SendTags>
        <SendPlatePatches>false</SendPlatePatches>
        <SendANPRImages>false</SendANPRImages>
        <SendOverviewImages>false</SendOverviewImages>
        <SendPlatesNotRead>false</SendPlatesNotRead>
        <SendANPRDiagnostics>true</SendANPRDiagnostics>
        <SendMachineDiagnostics>true</SendMachineDiagnostics>
        <SendIncrementalLog>true</SendIncrementalLog>
        <SendPeriodicContextImage>true</SendPeriodicContextImage>
        <UseReportingOffset>false</UseReportingOffset>
        <SendHeartbeat>true</SendHeartbeat>
        <StreamPlates>false</StreamPlates>
        <HeartbeatInterval>300</HeartbeatInterval>
        <PlateSendInterval>60</PlateSendInterval>
        <ReportingOffset>15</ReportingOffset>
        <ANPRDiagsSendInterval>1800</ANPRDiagsSendInterval>
        <MachineDiagsSendInterval>3600</MachineDiagsSendInterval>
        <IncrementalLogInterval>600</IncrementalLogInterval>
        <ContextImagePeriod>900</ContextImagePeriod>
        <MaxPlatesToSend>200</MaxPlatesToSend>
        <MinANPRDiagnosticSamples>10</MinANPRDiagnosticSamples>
        <CurrentDateTime>2009-06-29T12:01:59.379+01:00</CurrentDateTime>
    </Configuration>
</CameraToInstation>
```

2.7.4 Elements that are part of the <Camera> element are not configurable by the instation and should be set up on installation of the physical camera by manufacturer specific means (for example pre-configured at the factory or entered by the commissioning engineer).

2.7.5 A number of different lanes may be configured for one camera, however note that the <Configuration> element has no attributes which are lane-specific.

2.7.6 In the <Camera> element, at least one <Lane> element is mandatory. It is anticipated that <Lane> attributes will be entered into the camera by the commissioning engineer – these are not downloadable from the Instation.

2.7.7 Where there are attributes in the <Configuration> element which are not supported by a particular camera, the camera may omit these from the response.

2.7.8 A camera must maintain separate Configuration objects for each host. It will only accept the Configuration for a particular host from that host itself, and will only push a Configuration to the host to which it applies.

2.7.9 The <Camera>, <Lane>, and <Configuration> elements are described in more detail in Appendix 5.

2.8 Configuration request

2.8.1 The following is an example message outlining a request by the Camera for an update of its current Configuration:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CameraToInstation xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <CameraID>0</CameraID>
    <TimeStamp>2009-06-29T12:01:59.377+01:00</TimeStamp>
    <ConfigRequest/>
</CameraToInstation>
```

2.8.2 This is an empty element used by the Camera for requesting the current configuration from the Instation, for example on Camera startup.

2.8.3 The ConfigRequest is directed to a particular host, which will return the Configuration relating only to that host. Where a camera is configured to report to multiple hosts, it is not permitted for one host to have the ability to change the Configuration of another.

2.9 Heartbeat message

2.9.1 The following is an example message outlining a heartbeat, which comprises a CameraToInstation element which is empty apart from the mandatory CameraID and Timestamp attributes:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CameraToInstation xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <CameraID>0</CameraID>
    <TimeStamp>2009-06-29T12:01:59.377+01:00</TimeStamp>
</CameraToInstation>
```

2.9.2 Where a Camera is connected via a network which does provide a fixed IP address (for example some mobile networks), it may not be possible for the Instation to initiate a data transaction with a Camera (it may be impossible to determine the IP address allocated by the network). The Camera should therefore be configured periodically to send a 'Heartbeat' message to allow the Instation to respond with a message to the Camera. This heartbeat message is essentially an empty message which must be sent if no other messages have been sent within a configurable period of time (<HeartbeatInterval>).

3 Instation To Camera

3.1 Introduction

3.1.1 The <InstationToCamera> element is intended primarily for transmitting information from the Instation to the Camera in response to a SOAP call containing the <CameraToInstation> element. It allows for any combination of: a camera configuration, a configuration request, an image request or a log request to be sent. None of these elements is mandatory, hence the <InstationToCamera> element may also be sent empty to provide a receipt acknowledgement.

3.1.2 The option must be provided to use Gzip compression of the entire Instation to Camera element. The protocol does not provide for enabling or disabling this feature - it must be enabled or disabled by a commissioning engineer, either on-site or via a remotely connected engineering application.

3.1.3 Whereas this element is used in response to a <CameraToInstation> element, it mostly contains requests for data from the camera, for the reason that cameras are often connected via mobile networks where the Instation is unable to initiate a TCP/IP connection. Requests for data are therefore 'piggybacked' onto the acknowledgements sent by the Instation to the Camera.

3.1.4 Where the network connection allows the Instation to initiate a TCP/IP connection, the <InstationToCamera> element may also be transmitted on an ad-hoc basis as a SOAP call from the instation to the camera.

3.1.5 All array elements include an optional attribute "ManufacturerSpecific" (not shown in the examples) which enables the communication of additional information outside the scope of the pre-defined attributes.

3.2 Configuration

3.2.1 The Instation may push a new or revised configuration to the camera either at will or in response to a <ConfigRequest> from the camera. It is only possible to push that configuration which is specific to the sending host.

3.2.2 The following is an example message outlining a Configuration response to a camera ConfigRequest (none of the <Configuration> elements is mandatory):

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<InstationToCamera xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <Configuration>
        <HostName>HOST1</HostName>
        <SendVRNs>true</SendVRNs>
        <SendTags>false</SendTags>
        <SendPlatePatches>false</SendPlatePatches>
        <SendANPRImages>false</SendANPRImages>
        <SendOverviewImages>false</SendOverviewImages>
        <SendPlatesNotRead>false</SendPlatesNotRead>
        <SendANPRDiagnostics>true</SendANPRDiagnostics>
        <SendMachineDiagnostics>true</SendMachineDiagnostics>
        <SendIncrementalLog>true</SendIncrementalLog>
        <SendPeriodicContextImage>true</SendPeriodicContextImage>
        <UseReportingOffset>false</UseReportingOffset>
        <SendHeartbeat>true</SendHeartbeat>
        <StreamPlates>false</StreamPlates>
```

```
            <HeartbeatInterval>300</HeartbeatInterval>
            <PlateSendInterval>60</PlateSendInterval>
            <ReportingOffset>15</ReportingOffset>
            <ANPRDiagsSendInterval>1800</ANPRDiagsSendInterval>
            <MachineDiagsSendInterval>3600</MachineDiagsSendInterval>
            <IncrementalLogInterval>600</IncrementalLogInterval>
            <ContextImagePeriod>900</ContextImagePeriod>
            <MaxPlatesToSend>200</MaxPlatesToSend>
            <MinANPRDiagnosticSamples>10</MinANPRDiagnosticSamples>
            <CurrentDateTime>2009-06-29T12:01:59.379+01:00</CurrentDateTime>
        </Configuration>
</InstationToCamera>
```

3.2.3 This is exactly the same <Configuration> element as used for the <CameraToInstation> child element for transmitting the camera's current configuration.

3.2.4 The protocol does not provide for the addition of new hosts to the camera - these must be added or removed by a commissioning engineer, either on-site or via a remotely connected engineering application.

3.2.5 Where there are attributes in the <Configuration> element which are not supported by a particular camera, they will be ignored by the camera.

3.3 Log request

3.3.1 The Instation may request log records from the camera for a specific time period. In the <LogRequest> element, the following (which are the only attributes) are mandatory:

- StartTime which is the date and time at which log records should start;
- EndTime which is the date and time at which log records should end.

3.3.2 The following is an example message containing a response request from the Instation for provision of a Log by the camera:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<InstationToCamera xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <LogRequest>
        <StartTime>2008-11-14T10:50:30.952Z</StartTime>
        <EndTime>2008-11-14T10:50:30.952Z</EndTime>
    </LogRequest>
</InstationToCamera>
```

3.4 Configuration request

3.4.1 The following is an example message outlining a request by the Instation for a camera to upload its current Configuration:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<InstationToCamera xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <ConfigRequest/>
</InstationToCamera>
```

3.4.2 The <ConfigRequest> is an empty element identical to the same child element of the <CameraToInstation> element. (see 2.8).

3.4.3 The <ConfigRequest> is issued by a particular host, and the camera will return only the Configuration relating only to that host.

3.5 Image request

3.5.1 The Instation may request (retrospectively) images related to plate reads which have been stored in a camera. It may also request ad-hoc context images which are not connected with plate reads. There are four different classes of request, depending on the criteria which the Instation wishes to use to identify the required images:

- TimeRangeImageRequest: request images from a specific time period
- PriorVRNImageRequest: request a specific quantity of the most recent images
- InstanceSetImageRequest: request the images for a specific list of plate reads
- ContextImageRequest: request immediate images from one or more camera sensors

3.5.2 Only one of these ImageRequest classes should be used per <InstationToCamera> response, otherwise the instation will not know to which request the images sent by the camera relate.

3.5.3 The following is an example outlining a request from an Instation to a camera requesting the provision of images from a specific time period:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<InstationToCamera xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <TimeRangeImageRequest>
        <StartTime>2008-11-14T10:50:30.952Z</StartTime>
        <EndTime>2008-11-14T10:50:30.952Z</EndTime>
        <ImageTypeArray>
            <ImageType>platePatch</ImageType>
            <ImageType>overviewImage</ImageType>
        </ImageTypeArray>
    </TimeRangeImageRequest>
</InstationToCamera>
```

3.5.4 The following is an example outlining a request from an Instation to a camera requesting a specific quantity of recent images ending at a particular InstanceID:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<InstationToCamera xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <PriorVRNImageRequest>
        <NoOfPriorVRNs>10</NoOfPriorVRNs>
        <EndInstanceID>123456</EndInstanceID>
        <ImageTypeArray>
            <ImageType>platePatch</ImageType>
            <ImageType>overviewImage</ImageType>
        </ImageTypeArray>
    </PriorVRNImageRequest>
</InstationToCamera>
```

3.5.5 The following is an example outlining a request from an Instation to a camera requesting the provision of images for a specific set of plate reads:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<InstationToCamera xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <InstanceSetImageRequest>
        <InstanceIDArray>
            <InstanceID>123456</InstanceID>
            <InstanceID>123454</InstanceID>
            <InstanceID>123452</InstanceID>
        </InstanceIDArray>
        <ImageTypeArray>
            <ImageType>platePatch</ImageType>
            <ImageType>overviewImage</ImageType>
        </ImageTypeArray>
    </InstanceSetImageRequest>
</InstationToCamera>
```

3.5.6 The following is an example outlining a request from an Instation to a camera requesting immediate context images:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<InstationToCamera xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
    <ContextImageRequest>
        <ImageTypeArray>
            <ImageType>contextImage</ImageType>
            <ImageType>contextOverviewImage</ImageType>
        </ImageTypeArray>
    </ContextImageRequest>
</InstationToCamera>
```

3.5.7 These elements are described in more detail in Appendix 6.

3.6 Acknowledgement

3.6.1 The following is an example message outlining an acknowledgement, which comprises an <InstationToCamera> element that is empty:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<InstationToCamera xmlns="http://utmc.uk.com/anpr/schema_1-2" SchemaVersion="1.2">
</InstationToCamera>
```

3.6.2 Where the Instation receives a <CameraToInstation> message and does not require any further information from the camera, the <InstationToCamera> response will be an empty element which provides the camera with an acknowledgment that its transmission has been received.

4 Tag Hashing algorithm

4.1 About the algorithm

4.1.1 Journey time systems based on ALPR require cameras to recognise a plate at two or more locations and to return the recognised plate details to the instation. Although the full plate registration number can be returned to the instation for character by character matching, this may be undesirable in some circumstances. Additionally, to maintain driver and vehicle anonymity, it may be desirable to encrypt or otherwise change the plate string such that the actual registration number cannot be recovered.

4.1.2 ALPR systems are never 100% accurate. Read errors do occur. It is desirable to minimise the effect on the system of these read errors. For example the character D may be read correctly at one location and then the same character may be read as an O at a subsequent location.

4.1.3 The hashing algorithm firstly reduces the possible effect of plate read errors by replacing any characters likely to be confused with one another by a single character. So for example any occurence of O, D, 0 or Q in a plate is replaced with the character O. The following table lists all such substitutions:

ALPR reads character	Reported as
O D 0 Q	O
I 1	I
S 5	S
V Y	V
3 8 B	3
2 Z	2
E F	E
G C	G
H M N W	H

4.1.4 The resultant plate string is then hashed down to a binary number of 24 bits. The hash algorithm chosen is "one_at_a_time_hash". This algorithm has been chosen after reviewing the performance of a large number of algorithms over a database of about 100,000 UK plates and selecting the algorithm which provided the best distribution of hash values.

4.1.5 The "one_at_a_time_hash" hash algorithm was developed by Bob Jenkins. The original reference for the algorithm is: http://www.burtleburtle.net/bob/hash/doobs.html

4.2 Example

4.2.1 Example code (C language) for character substitution and the hash process is shown below.

```
static const char *mixups[] =
{
    "OD0Q", "I1", "S5", "VY", "38B", "2Z", "EF", "GC", "HMNW",
};
#define    NMIXUPS    9

void merge_ambiguous_characters(char *plate)
{
short  i;
char   *cp;

    while(*plate)
    {
        for(i=0; i<NMIXUPS; ++i)
        {
            cp = mixups[i];
            if(ismember(*plate, cp))
            {
                *plate = *cp;
            }
        }
        ++plate;
    }
}


// this function returns the 24 bit hash value directly

unsigned long hash(const char *plate)
{
unsigned   len;
unsigned   hash, i;
const int  hashbits = 24;
char       merge_plate[12];
#define    hashsize(n) ((unsigned)1<<(n))
#define    hashmask(n) (hashsize(n)-1)

    strcpy(merge_plate,plate);
        merge_ambiguous_characters(merge_plate);
    len = strlen(merge_plate);
    for (hash=0, i=0; i<len; ++i)
    {
        hash += merge_plate[i];
        hash += (hash << 10);
        hash ^= (hash >> 6);
    }
    hash += (hash << 3);
    hash ^= (hash >> 11);
    hash += (hash << 15);
    return (hash & hashmask(hashbits));
}
```

Appendix 1 PlateRead Element

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
InstanceID	DYNAMIC	A unique plate reference number for this camera. InstanceID should be incremented for each plate read until the holding variable (typically INT32) wraps, i.e. it is not just unique for a particular timestamp.	uInteger	Y	Combined with CameraID and TimeStamp at Instation to form a unique EventID
TimeStamp	DYNAMIC	ISO 8601 UTC date/timestamp for time of sighting	DateTime	Y	1ms resolution For dateTime format, see section 3.2.7 (dateTime) of W3C document “XML Schema Part 2 - Datatypes Second Edition“
TimeStampError	DYNAMIC	Estimated worst case timestamp error in ms	Integer		
LaneID	DYNAMIC	Camera Lane to which configuration item(s) relate	uInteger	Y	0 is the leftmost lane in the camera field of view. This ID is relative to the camera, not the actual lanes of the carriageway
VehicleDirection	DYNAMIC	Whether vehicle travelling toward or away from camera	Enumerated	Y	e.g. towards, away, unknown. i.e. towards = front plate, away = rear plate
XYType	STATIC	Reference co-ordinate system for XY location	Enumerated		e.g. OSGB or WGS84 (NB OSGB refers to OSGB36 datum)
XCoord	STATIC	X co-ordinate of camera location	Float		e.g. Longitude or Easting (Degrees + decimal degrees for longitude)
YCoord	STATIC	X co-ordinate of camera location	Float		e.g. Latitude or Northing (Degrees + decimal degrees for latitude)
PlateNotRead	DYNAMIC	A vehicle has been detected, but a plate cannot be found or, if found, cannot be recognised	Boolean	Y	Allows an InstanceID to be generated and a PlateRead record to be sent where no plate has been read.
VRN	DYNAMIC	Recognised licence number	Character		No whitespace characters
VRNConfidence	DYNAMIC	Probability that licence number is correct	Percent		0 to 100%
Tag	DYNAMIC	Hashed value formed from VRN	uInteger		In the range 0 to 2^{24} - 1

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
TagConfidence	DYNAMIC	Probability that tag value is correct	Percent		0 to 100%
Classification	DYNAMIC	Class of the recognised vehicle e.g. car, van lorry	uInteger		Numeric values only representing a classification scheme determined by the user.
Country	DYNAMIC	ISO 3166-1 three character country code	Character		e.g. GBR, FRA, DEU
Make	DYNAMIC	Make of Vehicle (Manufacturer)	Character		
Model	DYNAMIC	Model of Vehicle	Character		May be text (e.g. Mondeo) or number (e.g. 520)
Colour	DYNAMIC	Colour of vehicle	Enumerated		See list of standard colours (table below)*
Velocity	DYNAMIC	Estimated vehicle speed in kph	uInteger		
VelocityError	DYNAMIC	Estimated velocity error (magnitude) in kph	uInteger		Mean of the magnitudes of the +ve and -ve error estimates at 95% confidence interval

* A standard set of colours is used as follows:

Red		Green		Dark Purple		Light Brown
Light Red		Light Green		Grey		Dark Brown
Dark Red		Dark Green		Light Grey		Magenta
Orange		Blue		Dark Grey		Turquoise
Light Orange		Light Blue		Gold		
Dark Orange		Dark Blue		Silver		
Yellow		Violet		White		
Light Yellow		Purple		Black		
Dark Yellow		Light Purple		Brown		

Appendix 2 ALPRDiagnostic Element

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
TimeStamp	DYNAMIC	ISO 8601 UTC date/timestamp for end of diagnostic period	DateTime	Y	1ms resolution
DiagnosticType	DYNAMIC	Whether a routine diagnostic or an alarm (warning or fault)	Enumerated	Y	Enumerated type having values "routineDiagnostic", "alarmWarningSet", "alarmWarningClear", "alarmFaultSet","alarmFaultClear"
LaneID	DYNAMIC	Camera Lane to which the Diagnostics relate	uInteger		0 is the leftmost lane in the camera field of view. This ID is relative to the camera, not the actual lanes of the carriageway
MeanVRNConfidence	DYNAMIC	Average Probability that licence number is correct	Percent		0 to 100%
MeanTagConfidence	DYNAMIC	Average Probability that tag value is correct	Percent		0 to 100%
MeanPlateContrast	DYNAMIC	Average plate patch contrast	Percent		0 = all black, 100 = all white
MeanCharacterHeight	DYNAMIC	Average VRN character height in pixels	uInteger		
MeanHorizontalAngle	DYNAMIC	Average character angle to horizontal in degrees	Integer		±90 degrees
MeanVerticalAngle	DYNAMIC	Average character angle to vertical in degrees	Integer		±90 degrees
MeanTrajectoryOffset	DYNAMIC	Average trajectory distance from image centre	Integer		As a percentage of the horizontal image size. -ve for left of centre, +ve for right of centre
MeanTrajectoryAngle	DYNAMIC	Average angle of trajectory to horizontal in degrees	WholeDegrees		Horizontal right to left is zero, increasing anti-clockwise to 360. Values between 180 and 360 for vehicles travelling away from camera.
MeanVelocity	DYNAMIC	Average estimated vehicle speed in kph	uInteger		
MeanVelocityError	DYNAMIC	Average velocity error at 95% confidence interval	uInteger		Value in kph (mean of velocity error magnitude estimates)
PlateToTriggerRatio	DYNAMIC	Ratio of plates recognised to objects detected	Percent		0 to 100%

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
PlatesNoCountryRatio	DYNAMIC	Ratio of plates with unidentified country to all plates	Percent		0 to 100%
PlatesTowardsRatio	DYNAMIC	Ratio of plates towards camera to total plates	Percent		0 to 100%
PlatesAwayRatio	DYNAMIC	Ratio of plates away from camera to total plates	Percent		0 to 100%
MeanIRLevel	DYNAMIC	Average illuminator output level (percentage of max)	Percent		For frames selected for plate recognition
MeanExposure	DYNAMIC	Average exposure time in microseconds	uInteger		For frames selected for plate recognition
MeanGain	DYNAMIC	Average camera gain in dB where max gain is 0dB	Integer		For frames selected for plate recognition

Appendix 3 MachineDiagnostic Element

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
TimeStamp	DYNAMIC	ISO 8601 UTC date/timestamp for end of diagnostic period	DateTime	Y	1ms resolution
DiagnosticType	DYNAMIC	Whether a routine diagnostic or an alarm (warning or fault)	Enumerated	Y	Enumerated type having values "routineDiagnostic", "alarmWarningSet", "alarmWarningClear", "alarmFaultSet","alarmFaultClear"
MeanCPUTemp	DYNAMIC	Average processor board temperature in degrees	Integer		Can be +ve or -ve
MeanTotalCurrent	DYNAMIC	Average current drawn by camera including illuminator in mA	uInteger		Purpose: to identify reduction in illuminator current. Max value is 99,999mA
MeanIlluminatorTemp	DYNAMIC	Average illuminator temperature in degrees	Integer		Can be +ve or -ve
MeanIlluminatorCurrent	DYNAMIC	Average illuminator current in mA (during on-time)	uInteger		Max value is 99,999mA
IlluminatorUsage	DYNAMIC	Total illuminator usage (amps x hours) - cumulative	uInteger		As an indication of illuminator lifetime used
MeanIlluminatorOutput	DYNAMIC	Average illuminator light output as percentage of max when new	Integer		May be > 100%
LastResetTime	DYNAMIC	Date & Time of last CPU reset	DateTime		May be outside this diagnostic interval
NoOfHardwareErrors	DYNAMIC	Number of hardware errors detected	uInteger		
MeanSignalStrength	DYNAMIC	Average signal strength (wireless comms) in dB	Integer		Range is -999dB to 0dB
HostName	DYNAMIC	Name of host to which diagnostics relate	Character	Y	IP address or DNS name
MeanCommsLag	DYNAMIC	Average "round trip" communications delay in ms	uInteger		
WorstCommsLag	DYNAMIC	Worst case "round trip" communications delay in ms	uInteger		
NoOfCommsResends	DYNAMIC	Number of messages re-sent	uInteger		e.g. After failure to open host port
NoOfCommsFailures	DYNAMIC	Number of messages deleted from send buffer after repeated re-send failures	uInteger		
NoOfCommsReconnects	DYNAMIC	Number of reconnections to wireless network	uInteger		

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
MeanSyncDifference	DYNAMIC	Average time correction upon re-synchronisation in ms	Integer		This is a signed value, where a negative difference means the camera clock was fast, and a positive difference means it was slow.
WorstSyncDifference	DYNAMIC	Worst case time correction upon re-synchronisation in ms	Integer		This is a signed value, where a negative difference means the camera clock was fast, and a positive difference means it was slow.
LastSyncTime	DYNAMIC	Date & Time of last successful re-synchronisation	DateTime		May be outside this diagnostic interval
SupplyVoltage	DYNAMIC	Percentage of nominal system SELV supply voltage	Integer		May be >100%
TamperAlarm	DYNAMIC	Indication of unauthorised access to the equipment	Enumerated		Has 3 enumerated values: "normal", "enclosureBreachAlarm", "unauthorisedCommunicationAlarm"

Appendix 4 Image Element

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
InstanceID	DYNAMIC	Unique reference number for this camera to VRN record for a plate in the image	uInteger		
TimeStamp	DYNAMIC	ISO 8601 UTC date/timestamp	DateTime	Y	1ms resolution
VRN	DYNAMIC	Recognised licence plate number	Character		No whitespace characters. Allows images to be transmitted belatedly without the Host needing to refer to a database table referenced by InstanceID in order to associate VRN with images.
LaneID	DYNAMIC	Camera Lane to which image relates	uInteger		0 is the leftmost lane in the camera field of view. This ID is relative to the camera, not the actual lanes of the carriageway
ImageType	DYNAMIC	Whether the image is: a Plate patch (a close-cropped image of the plate as used for recognition) an ALPR image (the full image from which the plate patch has been taken) an Overview image (a visible image of the vehicle to which the plate read relates) a Context image (an uncropped image not related to a plate read) For cameras having separate ALPR and Overview sensors, context images by default relate to the ALPR sensor, but context images from the Overview sensor are also handled.	Enumerated	Y	Format: either "platePatch", "ALPRImage", "overviewImage", “contextImage” (from ALPR sensor) or “contextOverviewImage” (from Overview sensor).
ImageFormat	DYNAMIC	Encoding format of the image e.g. jpeg, tiff	Enumerated		Enumerated type having values "fits", "g3fax", "gif", "ief", "jp2", "jpeg", "jpm", "jpx", "t38", "tiff", "tiff-fx". (These formats are recognised MIME media types maintained in the IANA protocol registry: www.iana.org/assignments/media-types/image/).
BinaryImage	DYNAMIC	Jpeg image base-64 encoded	Binary		

Appendix 5 Camera Configuration Elements

A5.1 Camera Element

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
CameraID	STATIC	Unique identifier for the camera within a system	Character	Y	Local to Instation/Database Cross-reference to definition unique within a system can be compared in use to a "local IP Address"
HardwareUniqueID	STATIC	Globally unique identifier for the camera	Character	Y	Variable length up to 256 characters. Comprises three colon-separated fields i.e. "ManufacturerName:Model:FreeText". Each field any length with no whitespace allowed. ManufacturerName is mandatory, Model is optional - if null is signified by consecutive colons "ManufacturerName::FreeText". Strings must be alphanumeric and may include punctuation marks except colon.
ShortDescription	STATIC	Brief description of camera location	Character		
LongDescription	STATIC	Detailed description of camera location	Character		
XYType	STATIC	Reference co-ordinate system for XY location	Enumerated		e.g. OSGB or WGS84 (NB OSGB refers to OSGB36 datum)
XCoord	STATIC	X co-ordinate of camera location	Float		e.g. Longitude or Easting Degrees + decimal degrees for longitude
YCoord	STATIC	Y co-ordinate of camera location	Float		e.g. Latitude or Northing Degrees + decimal degrees for latitude
Height	STATIC	Height of camera above local ground level	Float		Measured in metres e.g. Height above Lowest road surface in multi-level junction

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
TypeID	STATIC	Type of equipment from generic list	uInteger		Generic ALPR = 5, IR = 6, IR+colour = 7, colour = 8
MobileCamera	STATIC	Whether the camera is mobile or fixed	Boolean		Assume fixed if attribute is absent
SoftwareVersion	STATIC	Software version number of the application generating the machine diagnostics (manufacturer specific)	Character		e.g. 3.5.15.72

A5.2 Lane Element

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
LaneID	STATIC	Camera Lane to which configuration item(s) relate	uInteger	Y	0 is the leftmost lane in the camera field of view This ID is relative to the camera, not the actual lanes of the carriageway
LaneNumber	STATIC	Position of the Lane in relation to the total number of lanes in the carriageway	uInteger	Y	In the range 0 to 99 Lane 0 is the first lane on the left in the direction of travel
LaneDirectionTypeID	STATIC	Direction of the carriageway lane in which vehicles normally travel (Note that this attribute relates to the direction taken by vehicles, not the direction in which the camera is pointing.)	uInteger	Y	e.g. 3 = clockwise, 4 = anticlockwise, 5 = northbound etc Format: see Direction_TypeID in CCTV ALPR Extensions Global Support Object
NormalVehicleDirection	STATIC	Direction relative to the camera in which vehicles normally travel	Enumerated	Y	e.g. towards, away, both "Both" applies for a single track road or tidal lane in a multi-lane road

A5.3 Configuration Element

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
HostName	CONFIG	Name of host to which configuration item(s) relate	Character		The fully qualified host URL or endpoint is set at time of commissioning.
SendVRNs	CONFIG	Whether to send VRN data (true/false)	Boolean		Following config items per host
SendTags	CONFIG	Whether to send Tag data (true/false)	Boolean		
SendPlatePatches	CONFIG	Whether to send plate patch images (true/false)	Boolean		
SendANPRImages	CONFIG	Whether to send full frame ALPR images (true/false)	Boolean		
SendOverviewImages	CONFIG	Whether to send full frame Overview images (true/false)	Boolean		
SendPlatesNotRead	CONFIG	Whether to send PlateRead records where PlateNotRead attribute is true	Boolean		See PlateRead attribute “PlateNotRead”
SendANPRDiagnostics	CONFIG	Whether to send ALPR diagnostics (true/false)	Boolean		
SendMachineDiagnostics	CONFIG	Whether to send machine diagnostics (true/false)	Boolean		
SendIncrementalLog	CONFIG	Whether to send an incremental log file (additions since last send)	Boolean		
SendPeriodicContextImage	CONFIG	Whether to send periodic context images (true/false)	Boolean		Note that in multiple sensor cameras, the sensor from which the context image is to be taken is determined by manufacturer-specific means. For example an image from the overview sensor may be returned during the day and an image from the ALPR sensor at night.

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
UseReportingOffset	CONFIG	Whether the camera should utilise the ReportingOffset (true/false)	Boolean		If false, permits the randomisation of reporting times by another method (for example by starting reporting intervals relative to the last camera power-on or reset) without the need to configure each camera with an individual ReportingOffset. Avoids cameras all reporting at the same time if no ReportingOffset is configured or a default value is assumed.
SendHeartbeat	CONFIG	Whether a generic wrapper should be sent periodically irrespective of whether there is data to send (true/false)	Boolean		Allows the sending of heartbeats to be turned on and off explicitly, rather than relying on whether a HeartbeatInterval has been configured.
StreamPlates	CONFIG	Whether to send a PlateRead record as soon as a plate is recognised (true/false)	Boolean		
HeartbeatInterval	CONFIG	Send at least one generic wrapper during this interval in seconds	uInteger		Maximum value 86400 seconds (=1 day)
PlateSendInterval	CONFIG	Reporting interval for sending VRN and/or tag data in seconds	uInteger		The end of the PlateSendInterval should be aligned with the time of transmission determined by the ReportingOffset, to ensure that the latest plate data is always reported as soon as possible.
ReportingOffset	CONFIG	Reporting time offset as percentage of appropriate send interval	Percent		Relative to a reporting interval commencing at midnight
ANPRDiagsSendInterval	CONFIG	Reporting interval for sending ALPR diagnostics in seconds	uInteger		
MachineDiagsSendInterval	CONFIG	Reporting interval for sending machine diagnostics in seconds	uInteger		
IncrementalLogInterval	CONFIG	Reporting interval for sending incremental log in seconds	uInteger		
ContextImagePeriod	CONFIG	Time interval at which a single context image is returned in seconds	uInteger		Single image only - not a batch

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
MaxPlatesToSend	CONFIG	Maximum number of VRNs/Tags to send per reporting interval	uInteger		Applies when StreamPlates is false - send up to this number of captured plates during a plate reporting interval.
MinANPRDiagnosticSamples	CONFIG	Minimum vehicles to be included in ALPR diagnostic averages	uInteger		Roll samples over from one interval to next
CurrentDateTime	CONFIG	DateTime value to set real time clock. The presence or absence of this attribute in the InstationToCamera response determines whether the Camera clock should be set or not.	DateTime		For dateTime format, see section 3.2.7 (dateTime) of W3C document “XML Schema Part 2 - Datatypes Second Edition“

Appendix 6 ImageRequest Elements

A6.1 TimeRangeImageRequest

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
StartTime	DYNAMIC	ISO 8601 UTC date/timestamp	DateTime	Y	1ms resolution
EndTime	DYNAMIC	ISO 8601 UTC date/timestamp	DateTime	Y	1ms resolution
ImageTypeArray	DYNAMIC	Array element containing 0 to n ImageTypes (list of the types of images required)	Character		See ImageType attribute of Image element (contextImage and contextOverviewImage will be ignored)

A6.2 PriorVRNImageRequest

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
NoOfPriorVRNs	DYNAMIC	Number of most recent VRN instances for which images are required	uInteger	Y	
EndInstanceID	DYNAMIC	The set of images to be sent should end with this InstanceID	uInteger		Used in conjunction with NoOfPriorVRNS to determine the latest InstanceID which should be sent in the set of images defined by these two attributes.
ImageTypeArray	DYNAMIC	Array element containing 0 to n ImageTypes (list of the types of images required)	Character		See ImageType attribute of Image element (contextImage and contextOverviewImage will be ignored)

A6.3 InstanceSetImageRequest

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
InstanceIDArray	DYNAMIC	InstanceArray element containing 0 to n Instance IDs for this camera of VRN records of the plates for which images are required	uInteger	Y	
ImageTypeArray	DYNAMIC	Array element containing 0 to n ImageTypes (list of the types of images required)	Character		See ImageType attribute of Image element (contextImage and contextOverviewImage will be ignored)

A6.4 ContextImageRequest

Attribute Name	Attribute Type	Description	Data Type	Man	Comments
ImageTypeArray	DYNAMIC	Array element containing 0 to n ImageTypes (list of the types of images required)	Character		See ImageType attribute of Image element (anything other than contextImage or contextOverviewImage will be ignored)